Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos sobre Anéis de Inteiros Algébricos de Corpos Ciclotômicos

por

João de Sousa

sob orientação do

Prof. Dr. Orlando Stanley Juriaans

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Fevereiro/2005

João Pessoa - Pb

Códigos sobre Anéis de Inteiros Algébricos de Corpos Ciclotômicos

por

João de Sousa

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Orlando Stanley Juriaans - IME-USP (Orientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB (Co-Orientador)

Prof. Dr. José Robério Rogério - UFC

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Fevereiro/2005

Agradecimentos

- A Deus, por tudo que ele representa pra mim.

- Ao Professor Dr. *Antônio de Andrade e Silva*, que compreende o verdadeiro sentido da palavra *orientação*.

- Ao Pofessor Dr. Orlando Stanley Juriaans, pela compreensão e confiança.

- Ao amigo Andrade e sua esposa, D. Rosângela, pela paciência, dedicação, compreensão, apoio e amizade no momento mais difícil do mestrado.

- Aos professores Nelson Nery, Hélio Pires, Marivaldo e Everaldo que muito contribuiram para a minha formação e que serviram de exemplo para que eu seja uma pessoa melhor.

- Aos amigos Bosco, João Batista e Enéas pelos quais tenho muita gratidão.

- A minha mãe Raimunda e a meus irmãos Cláudia, Marcos e Crisálida.

- Aos colegas do curso de mestrado, em especial aos amigos que sempre tiveram presentes nos momentos de maior dificuldade do curso: Dércio, Joelma, Ében, Ivan Mezzomo, Wilson e Vilmar.

- A Sônia, pela amizade e atenção, competência e presteza no atendimento de secretaria.

- Aos colegas do Departamento de Matemática - UFMT - Campus de Cuiabá.

- Aos Professores do Departamento de Matemática - UFMT- Campus Cuiabá e aos Professores Eistein e Eunice do Deparatmento de Administração-UFMT.

Dedicatória

À minha mãe Raimunda

Aos meus irmãos Cáudia, Marcos e Crisálida.

Resumo

Considerando qualquer corpo finito como um corpo residual do anel de inteiros algébricos de um corpo ciclotômico, selecionamos um sistema de representantes no anel com uma métrica de Manhattan mínima, e introduzimos um peso de Mannheim no corpo finito. Os códigos lineares sobre o corpo finito com o peso de Mannheim são discutidos. Um método geométrico é fornecido para encontrar os representantes no anel dos inteiros Gaussianos.

Abstract

Regarding any finite field as a residue field of the algebraic integer ring of a cyclotomic field, we select a system of representatives in the ring with minimal Manhattan metric, and introduce a Mannheim weight on the finite field. The linear codes over the finite field with the Mannheim weight are discussed. A geometric method to compute the representatives in Gaussian integers is provided.

Notação

R - Anel

$R[x]$ - Anel dos polinômios sobre R

$U(R)$ - Conjunto das unidades de R

$\mathcal{O}_n$ - Anel dos inteiros

$\mathbb{Z}_K$ - Anel dos inteiros de K

$\mathbb{Z}[i]$ - Anel dos inteiros Gaussianos

$\mathbb{Z}_p$ - Anel dos inteiros módulo p

$\mathbb{Z}_p[x]$ - Conjunto dos polinômios na variável x com coeficientes em $\mathbb{Z}_p$

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

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

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

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

$\langle x \rangle$ - Ideal principal gerado por x

$\langle a_1, a_2, \ldots, a_n \rangle$ - ideal gerado por $\{a_1, a_2, \ldots, a_n\}$

$\mathrm{Ann}_R(X)$ - Anulador de X em R

$\mathrm{mdc}(a, b)$ - Máximo divisor comum de a e b

$\varphi(n)$ - Função de Euler

$\frac{R}{I}$ - Anel quociente de R sobre I

$\mathrm{Gal}(F/K)$ - Grupo de Galois de F sobre K

$\mathbb{F}^\bullet$ - Grupo cíclico multiplicativo do corpo $\mathbb{F}$

$\mathbb{F}_p[x]$ - Anel dos polinômios sobre o corpo $\mathbb{F}_p$

F/K - Extensão de um corpo F sobre um corpo K

$\partial(f)$ - Grau do polinômio f

$B_r(x)$ - bola de raio r e centro x

$[F : K]$ - Grau de F sobre K

Φ_n - n-ésimo polinômio ciclotômico

f_α - Polinômio caracteristico de α

ζ_n - Raiz n-ésima da unidade

$\mathrm{irr}(\alpha, K)$ - polinômio irredutível de α sobre K

$\ker \phi$ - Núcleo da função ϕ

$\mathrm{Im}\, \phi$ - Imagem da função ϕ

$|X|$ - Cardinalidade do conjunto X

$\equiv$ - Congruente

$|$ - Divide

$\simeq$ - Isomorfo

$\forall$ - Para todo

$\sum$ - Soma

$\prod$ - Produto

$\mathbb{F}$ - Alfabeto

$\det \mathbf{A}$ - determinante da matriz $\mathbf{A}$

$\lfloor x \rfloor$ - menor inteiro menor do que ou igual a x

$\mathrm{tr}(\alpha)$ - Traço de α

$N(\alpha)$ - Norma de α

$GF(q)$ - Corpo de Galois com q elementos

$K(\alpha_1, \ldots, \alpha_n)$ - menor subcorpo contendo $\alpha_1, \ldots, \alpha_n$ e K

$\Delta[\alpha_1, \ldots, \alpha_n]$ - discriminante de $\{\alpha_1, \ldots, \alpha_n\}$

$\mathcal{C}$ - Código

$\mathbf{c}$ - palavra código

$\mathbf{e}$ - vetor erro

$\mathbf{r}$ - palavra recebida

$\mathbf{s}(\mathbf{x})$ - síndrome de $\mathbf{x}$

$\mathbf{G}$ - Matriz geradora de um código

$\mathbf{H}$ - Matriz de verificação de paridade de um código

$d_H(\mathbf{c}, \mathbf{c}')$ - distância de Hamming entre $\mathbf{c}$ e $\mathbf{c}'$

$d_{\overline{M}}(\mathbf{c}, \mathbf{c}')$ - distância de Mannheim entre $\mathbf{c}$ e $\mathbf{c}'$

$\omega_{\overline{M}}(\mathbf{x})$ - peso de Mannheim de $\mathbf{x}$

$\omega_H(\mathbf{x})$ - peso de Hamming de $\mathbf{x}$

$d_\omega(\mathcal{C})$ - distância consecutiva mínima de $\mathcal{C}$

$\overline{GE}$ - Segmento de reta que passa pelos pontos G e E

Sumário

Introdução

A teoria dos códigos corretores de erros teve início em 1948 com o trabalho de Shannon. Ele mostrou que, usando códigos corretores de erros, é possível projetar sistemas de comunicações digitais com probabilidade de erro tão pequena quanto se deseje. A partir desse trabalho apareceram inúmeras pesquisas em busca de códigos bons, capazes de melhorar o desempenho de sistemas de comunicações digitais.

Os códigos corretores de erros participam do nosso quotidiano de inúmeras maneiras, estando presentes, por exemplo, sempre que fazemos uso de informações digitalizadas, tais como assistir a um programa de televisão, falar ao telefone, ouvir um CD de música, assistir a um filme em DVD, mandar um recado para alguém via Pager ou navegar pela Internet. Atualmente os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade. São exemplos disso todas as comunicações via satélite, as comunicações internas de um computador, o armazenamento de dados em fitas ou disquetes magnéticos, ou o armazenamento óptico de dados.

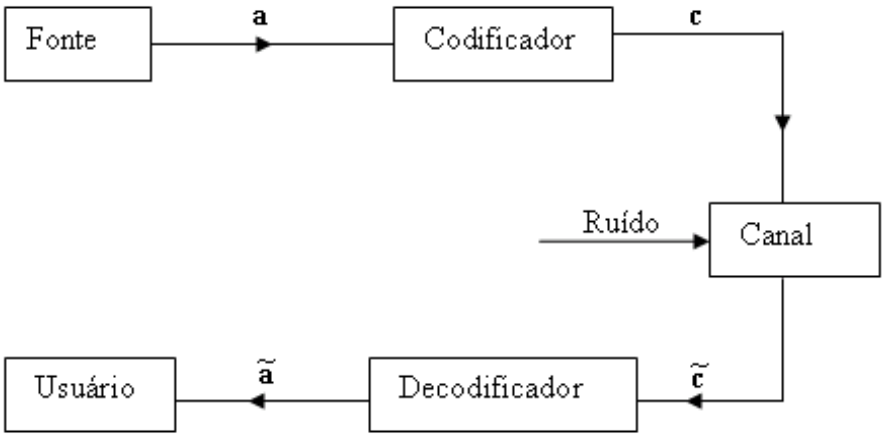

Figura 1: Modelo simplificado de um sistema de codificação.

Na Figura 1, é mostrado um esquema simplificado de um sistema de comunicação

digital.

Neste sistema, o codificador recebe uma sequência de informação $\mathbf{a}$, que depois de codificada resulta na sequência codificada $\mathbf{c}$, chamada de palavra código, que é enviada através do canal, que supomos ser aditivo. Devido a interferências (ruído) no canal , a seqüência que o decodificador recebe é da forma

$$\widetilde{\mathbf{c}} = \mathbf{c} + \mathbf{e},$$

onde $\mathbf{e}$ é o erro adicionado pelo canal, que depois de decodificada resulta na sequência $\widetilde{\mathbf{a}}$, que é enviada para o usuário. O uso de códigos corretores de erros tem como objetivo corrigir os possíveis erros na sequência recebida $\widetilde{\mathbf{c}}$, causados pelo ruído, e recuperar a palavra código enviada e, daí, obter a sequência de informação $\mathbf{a}$, ou seja,

$$\widetilde{\mathbf{a}} = \mathbf{a}.$$

Os primeiros códigos de bloco apareceram em 1950 quando Hamming descreveu uma família de códigos binários capazes de corrigir qualquer padrão de erro simples. Em seguida, Hocquenghem (1959) e Bose e Ray-Chaudheri (1960) descobriram uma família grande de códigos de bloco, definidos sobre corpos finitos $GF(p^n)$. Desde então, surgiram várias técnicas e teorias para construção de códigos e muitos resultados importantes foram obtidos, porém existe uma fonte inesgotável de problemas em aberto. Isso tem atraído, cada vez mais, o interesse de pesquisadores nesta área.

Muitos resultados sobre modulação multidimensional e códigos de treliça multidimensionais têm sido obtidos, contudo, pouco é conhecido sobre códigos de bloco lineares sobre corpos finitos para codificação de sinais multidimensionais. Os trabalhos de Huber, Dong e outros trouxeram alguma luz para o interessante problema da construção de códigos sobre corpos finitos para sinais multidimensionais. Huber descobriu um método para construir códigos sobre corpos finitos para sinais bidimensionais. A idéia pioneira é considerar o corpo residual do anel de inteiros Gaussianos $\mathbb{Z}[i]$ módulo um ideal primo P, que é um corpo finito; e aplicar a norma de Galois para fazer a divisão Euclidiana tal que em cada classe residual, correspondente a cada elemento do corpo finito, exista um único elemento de norma mínima na classe residual, e então cada elemento dos corpos finitos é representado por um inteiro Gaussiano na classe residual. Dessa maneira Huber introduziu o chamado "peso de Mannheim," e construiu códigos lineares para a correção de um erro

de Mannheim. Sua promissora idéia é também usada para os Inteiros de Eisenstein, isto é, os inteiros algébricos do corpo ciclotômico gerado pela raiz sexta da unidade.

Estendendo os resultados de Huber, Dong e Trajano Pires da Nóbrega Neto emitiram novas luzes sobre o problema. Dong considerarou o anel de inteiros algébricos de corpos ciclotômicos que são dominios de ideais principais, e mostrou que, para o corpo residual de tal anel módulo um elemento irredutível, podemos também tomar um elemento na classe residual para representar cada elemento do corpo residual; e construiu códigos lineares sobre o corpo residual, os quais podem corrigir o erro que pertence a um subgrupo do grupo multiplicativo do corpo finito. Dessa maneira, os códigos sobre corpos finitos para sinais com dimensão maior que dois podem ser construídos. No entanto, ele não encontrou uma norma apropriada para estender o peso de Mannheim de Huber.

Trajano Pires da Nóbrega Neto propôs novas classes de códigos lineares sobre anéis de inteiros de extensões quadráticas do corpo racional, e seus códigos são considerados com respeito a uma métrica também de Mannheim, e também para sinais bidimensionais.

Contudo, Dong e Trajano Pires da Nóbrega Neto estabeleceram que novas classes de códigos lineares sobre anéis de inteiros de extensões quadráticas do corpo racional, e seus códigos considerados com respeito a uma métrica de Mannheim e também para sinais bidimensionais, não é necessária sobre os dominios de ideais principais:para todo corpo ciclotômico. Será considerado o anel de inteiros algébricos e o corpo residual módulo um ideal primo é um corpo finito, sobre os quais os códigos para sinais multidimensionais podem ser construídos. Além disso, mudando o ponto de vista da norma de Galois para o peso Manhattan (segundo Huber), um peso de Mannheim de um estilo geométrico pode ser bem definido.

Este trabalho está organizado da seguinte maneira:.

No Capítulo 1, apresentamos algumas definições e resultados da teoria dos grupos e anéis, bem como, alguns resultados da teoria das extensões de corpos e inteiros algébricos. No Capítulo 2 apresentaremos resultados sobre corpos cilclotômicos necessários para o entendimento de nosso trabalho. No Capítulo 3 introduzimos o peso de Mannheim através do peso de Manhattan sobre o anel de inteiros algébricos. As propriedades do peso de Manhattan são discutidadas e é provado que, semelhantemente ao caso do peso de Hamming, a correção do erro de um código sobre os corpos finitos com o peso de Mannheim é determinada pela distância mínima do código. No Capítulo 4, apresentaremos um

método geométrico para determinar um sistema completo de representantes de classes laterais de um ideal primo P em $\mathbb{Z}[\zeta_n]$, quando $n = m = 4$.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados, que serão necessários nos capítulos seguintes. Admitiremos já conhecidos os conceitos e resultados básicos da teoria dos grupos e de anéis. O leitor interessado em mais detalhes pode consultar [1, 8, 12].

1.1 Anéis

Nesta seção apresentaremos alguns resultados clássicos da teoria de anéis que serão necessários para a compreensão desta dissertação.

Um *anel* é um conjunto não vazio R equipado com duas operações binárias adição $(x, y) \to x + y$ e multiplicação $(x, y) \to xy$ tal que as seguintes propriedades valem:

1. R é um grupo comutativo sob a adição.
2. $x(yz) = (xy)z$, para todos $x, y, z \in R$.
3. $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, para todos $x, y, z \in R$.

   Se um anel R satisfaz as propriedades:

4. Existe $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um *anel com identidade.*
5. $xy = yx$, para quaisquer $x, y \in R$, dizemos que R é um *anel comutativo*

   Se um anel R satisfaz a propriedade:

6. Para todos $x, y \in R$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que R é um *anel sem divisores de zero.* Caso contrário, dizemos que R é um *anel com divisores de zero.*

Dizemos que um elemento $x \in R$, $x \neq 0$, é *regular* se x não é um divisor de zero.

Se R é um anel comutativo, com identidade e sem divisores de zero, dizemos que R é um *domínio*. Um elemento $x \in R$ é dito uma *unidade* de R se existir $y \in R$ tal que $xy = yx = 1$. Denotaremos por $U(R)$ o conjunto de todas as unidades de R. Se $U(R) = R^* = R - \{0\}$, dizemos que R é um *corpo*. Salvo menção explícita em contrário, todos os anéis considerados neste trabalho serão comutativos com identidade.

Um subconjunto não vazio S de um anel R é um *subanel* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in S$, tem-se $x - y \in S$;
2. para todos $x, y \in S$, tem-se $xy \in S$;
3. $1 \in S$.

Um subconjunto não vazio I de um anel R é um *ideal* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in I$, tem-se $x - y \in I$;
2. Para todo $x \in I$ e $r \in R$, tem-se $rx \in I$.

Sejam R e S dois anéis. Uma função ϕ de R em S é um *homomorfismo de anéis* se as seguintes condições são satisfeitas:

1. $\phi(x + y) = \phi(x) + \phi(y)$, para todos $x, y \in R$;
2. $\phi(xy) = \phi(x)\phi(y)$, para todos $x, y \in R$;
3. $\phi(1) = 1$.

Um ideal I de R é dito *próprio* se $I \neq R$. Um ideal I de R é dito *finitamente gerado* se existir um subconjunto finito $S = \{x_1, x_2, \ldots, x_n\}$ de R tal que

$$I = \langle S \rangle = Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n = \left\{ \sum_{i=1}^{n} r_i x_i : r_i \in R \right\}.$$

O ideal $I = Rx = \langle x \rangle$ é chamado *ideal principal* gerado por $x \in R$. Um domínio R é um *domínio de ideais principais* se todo ideal de R é principal.

Sejam R um anel e $x, y \in R$, com $x \neq 0$. Dizemos que x *divide* y, em símbolos $x \mid y$, se existir $z \in R$ tal que $y = xz$. Se $y = xz$, com $x, z \in R - U(R)$, dizemos que x é um *divisor próprio* de y. Sejam $x, y \in R^*$, dizemos que x e y são *associados* se existir $u \in U(R)$ tal que $y = ux$.

Lema 1.1 *Sejam R um domínio e $x, y \in R^*$. Então*:

1. *$x \in U(R)$ se, e somente se, $\langle x \rangle = \langle 1 \rangle = R$;*
2. *x divide y se, e somente se, $\langle y \rangle \subseteq \langle x \rangle$;*
3. *x e y são associados se, e somente se, $\langle y \rangle = \langle x \rangle$;*
4. *x é um divisor próprio de y se, e somente se, $\langle y \rangle \subset \langle x \rangle \subset \langle 1 \rangle$.* ■

Sejam I e J dois ideais de R. Então

$$I + J = \{x + y : x \in I \text{ e } y \in J\}$$

e

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J \text{ e } n \in \mathbb{N} \right\}$$

são ideais de R. Note que, a soma e a multiplicação de ideais podem, de forma indutiva, ser generalizada para qualquer número finito de ideais.

Um ideal P de um anel R é um *ideal primo* de R se $P \neq R$ e para todos $x, y \in R$ e $xy \in P$, tem-se $x \in P$ ou $y \in P$.

Teorema 1.1 *Sejam R um anel e P um ideal de R. Então as seguintes condições são equivalentes*:

1. *P é um ideal primo de R;*
2. *Se I e J são ideais de R tais que $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$;*
3. *$\frac{R}{P}$ é um domínio.* ■

Um ideal não nulo M de um anel R é um *ideal maximal* de R se $M \neq R$ e se J é um ideal de R tal que $M \subseteq J \subseteq R$, então $M = J$ ou $J = R$. Dizemos que R é um *anel local* se R tem um único ideal maximal. Neste caso, $U(R) = R - M$.

Proposição 1.1 *Sejam R um anel e M um ideal próprio de R. Então*:

1. *M é maximal se, e somente se, $\frac{R}{M}$ é um corpo.*

2. *M é maximal se, e somente se, $\langle M, r\rangle = R$, para todo $r \in R - M$.* ■

Observação 1.1 *Todo ideal maximal é primo.*

Seja R um anel. Um elemento $p \in R^*$ é *irredutível* sobre R se as seguintes condições são satisfeitas:

1. $p \notin U(R)$;

2. Se $p = bc$, então $b \in U(R)$ ou $c \in U(R)$, isto é, p não tem divisores próprios.

Proposição 1.2 *Seja R um domínio. Então as seguintes condições são equivalentes*:

1. *Para cada $x \in R^*$, com $x \notin U(R)$, o processo de fatoração de x termina após um número finito de passos e resulta na fatoração $x = p_1 \cdots p_k$ de x em fatores irredutíveis de R;*

2. *Se $\langle x_1\rangle \subset \langle x_2\rangle \subset \cdots \subset \langle x_n\rangle \subset \cdots$ é uma seqüência estritamente crescente, então existe $n_0 \in \mathbb{N}$ tal que $\langle x_n\rangle = \langle x_{n_0}\rangle$, para todo $n \geq n_0$.* ■

Seja R um anel. Um elemento $p \in R$ é *primo* sobre R se as seguintes condições são satisfeitas

1. $p \notin U(R)$;

2. Se p divide ab, então p divide a ou p divide b.

Observação 1.2 *Todo elemento primo não nulo é irredutível.*

Um domínio R é chamado um *domínio de fatoração única* se as seguintes condições são satisfeitas:

1. Para todo $a \in R^*$ e $a \notin U(R)$, existem elementos irredutíveis $p_i \in R$, $1 \leq i \leq n$, tais que

$$a = \prod_{i=1}^{n} p_i.$$

2. Dadas duas fatorações em elementos irredutíveis de R,

$$\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j,$$

então $m = n$ e existe uma permutação σ de $\{1, \ldots, n\}$ tal que $p_i = uq_{\sigma(i)}$, onde $u \in U(R)$.

Proposição 1.3 *Seja R um domínio. Suponhamos que a fatoração exista em R. Então R é um domínio de fatoração única se, e somente se, qualquer elemento irredutível é primo.* ■

Proposição 1.4 *Se R é domínio de ideais principais, então R é um domínio de fatoração única.* ■

Uma *função Euclidiana* para um domínio R é uma função $\varphi : R^* \longrightarrow \mathbb{Z}$ tal que

1. Se $a, b \in R^*$ e a divide b, então $\varphi(a) \leq \varphi(b)$;

2. Se $a, b \in R$, com $b \neq 0$, então existem $q, r \in R$ tais que

$$a = bq + r, \text{ onde } r = 0 \text{ ou } \varphi(r) < \varphi(b).$$

Exemplo 1.1 *Seja*

$$R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

o anel dos inteiros de Gauss. Então a função $\varphi : R^* \longrightarrow \mathbb{Z}$ definida por

$$\varphi(\alpha) = a^2 + b^2,$$

onde $\alpha = a + bi$, é Euclidiana. De fato, sejam $\alpha, \beta \in R^*$ e se β divide α, então existe $\gamma \in R^*$ tal que $\alpha = \beta\gamma$. Como $|\gamma|^2 \geq 1$ temos que

$$\varphi(\beta) \leq \varphi(\beta)\varphi(\gamma) = \varphi(\beta\gamma) = \varphi(\alpha).$$

Por outro lado, como podemos identificar $\mathbb{C}$ com o plano, temos que cada $\dfrac{\alpha}{\beta} \in \mathbb{C}$ está no interior ou na fronteira de um quadrado com diagonal de comprimento $\sqrt{2}$. Assim, existe um vértice q com distância menor que ou igual a $\frac{\sqrt{2}}{2}$ de $\dfrac{\alpha}{\beta}$. Logo,

$$\left| \frac{\alpha}{\beta} - q \right| \leq \frac{\sqrt{2}}{2} < 1.$$

Tomando $r = \alpha - q\beta$, *obtemos* $\alpha = q\beta + r$, *onde*

$$|r| = |\alpha - q\beta| = |\beta| \left| \frac{\alpha}{\beta} - q \right| < |\beta| .$$

Assim, $\varphi(r) < \varphi(\beta)$. *Portanto,* φ *é uma função Euclidiana.*

Se um domínio R possui uma função Euclidiana, dizemos que R é um *domínio Euclidiano.*

Teorema 1.2 *Seja* R *é um domínio Euclidiano. Então* R *é um domínio de ideais principais.* ■

1.2 Módulos

Seja R um anel comutativo com unidade. Um *R-módulo* V é um grupo comutativo (aditivo) equipado com uma operação

$$R \times V \longrightarrow V, (r, \mathbf{v}) \longmapsto r\mathbf{v},$$

tal que as seguintes condições são satisfeitas:

1. $r(s\mathbf{v}) = (rs)\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
2. $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$, para quaisquer $r \in R$ e $\mathbf{u}, \mathbf{v} \in V$.
3. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.
4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um R-módulo V é um *R-espaço vetorial* sobre R.

Denotaremos o número de elementos de V (ou cardinalidade de V) por $|V|$.

Exemplo 1.2 *Seja* V *um grupo comutativo. Então é fácil verificar que* V *é um* $\mathbb{Z}$*-módulo com a operação*

$$\mathbb{Z} \times V \to V, (r, \mathbf{v}) \mapsto r\mathbf{v},$$

onde

$$r\mathbf{v} = \begin{cases} (r-1)\mathbf{v} + \mathbf{v} & se\ r > 0 \\ 0 & se\ r = 0 \\ (r+1)\mathbf{v} - \mathbf{v} & se\ r < 0. \end{cases}$$

Em particular, se $|V| = n$, *então* $n\mathbf{v} = 0$, *para todo* $\mathbf{v} \in V$. *Note, então, que* V *é um* $\mathbb{Z}_n$*-módulo, fazendo* $\bar{r}\mathbf{v} = r\mathbf{v}$, *para todo* $r \in \mathbb{Z}$ *e* $\mathbf{v} \in V$.

Um subconjunto não vazio W de um R-módulo V é um *R-submódulo* de V se as seguintes condições são satisfeitas:

1. Para quaisquer $\mathbf{w}_1, \mathbf{w}_2 \in W$, têm-se $\mathbf{w}_1 - \mathbf{w}_2 \in W$,

2. Para quaisquer $r \in R$ e $\mathbf{w} \in W$, têm-se $r\mathbf{w} \in W$.

Sejam S um subconjunto de um R-módulo V e

$$\mathcal{F} = \{W : W \text{ é submódulo de } V \text{ e } S \subset W\}.$$

Então

$$\langle S \rangle = \bigcap_{W \in R} W$$

é o menor R-submódulo de V contendo S e será chamado de *R-submódulo gerado por S*.

Seja V um R-módulo. Se $\mathbf{v} \in V$ pode ser escrito como

$$\mathbf{v} = \sum_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \text{ e } \mathbf{v}_i \in V,$$

dizemos que $\mathbf{v}$ é uma *combinação linear* dos elementos $\mathbf{v}_1, \ldots, \mathbf{v}_n$ sobre R. Neste caso, o conjunto de todas as combinações lineares de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ é o R-submódulo

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle = \left\{ \sum_{i=1}^{n} r_i \mathbf{v}_i : r_i \in R \right\},$$

gerado por $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Quando existe um subconjunto finito S de um R-módulo V tal que $V = \langle S \rangle$, dizemos que V é um *R-módulo finitamente gerado*. Se $S = \{\mathbf{v}\}$, isto é, S consiste de um único elemento, então

$$\langle \mathbf{v} \rangle = \{r\mathbf{v} : r \in R\}$$

e $\langle \mathbf{v} \rangle$ será chamado de *R-submódulo cíclico gerado por $\mathbf{v}$*.

Uma seqüência finita $\mathbf{v}_1, \ldots, \mathbf{v}_n$ de elementos de um R-módulo V será chamada *linearmente independente* se

$$\sum_{i=1}^{n} r_i \mathbf{v}_i = 0 \Rightarrow r_1 = r_2 = \cdots = r_n = 0.$$

Caso contrário, dizemos que a seqüência é *linearmente dependente*. Um subconjunto S de um R-módulo V será chamado *linearmente independente* se qualquer seqüência finita de

elementos distintos de S é linearmente independente. Caso contrário, S é dito *linearmente dependente*.

Um subconjunto S de um R-módulo V será chamado uma *R-base* se as seguintes condições são satisfeitas:

1. $V = \langle S \rangle$.

2. S é linearmente independente.

Um R-módulo V será chamado de *R-módulo livre* se ele possui uma R-base. Quaisquer duas R-bases de um R-módulo livre têm a mesma cardinalidade. A cardinalidade da R-base será chamada de *posto* de V sobre R.

Teorema 1.3 *Sejam R um domínio de ideais principais e V um R-módulo livre de posto n. Então todo R-submódulo W de V é livre com posto $m \leq n$.* ■

Seja V um R-módulo. Para qualquer $X \subseteq V$, definimos o *anulador* de X em R como.

$$\mathrm{Ann}_R(X) = \{r \in R : rx = 0 \ \forall \ x \in X\}.$$

É fácil verificar que $\mathrm{Ann}_R(X)$ é um ideal de R.

Sejam U e V dois R-módulos. Uma função $T : U \to V$ é um *R-homomorfismo* se as seguintes condições são satisfeitas:

1. $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$, para todos $\mathbf{u}, \mathbf{v} \in U$.

2. $T(r\mathbf{u}) = rT(\mathbf{u})$, para todos $\mathbf{u} \in U$ e $r \in R$.

Um R-homomorfismo $T : U \longrightarrow V$ é um *R-isomorfismo* se T for bijetora.. Denotaremos por

$$\mathrm{Hom}_R(U, V) = \{T : U \longrightarrow V : T \text{ é um } R\text{-homomorfismo}\}.$$

Em particular, quando $U = V$ temos que $\mathrm{Hom}_R(U, V) = \mathrm{End}_R(V)$.

Sejam V um R-módulo e W um R-submódulo de V sobre R. Se $\mathbf{v}$ é um elemento arbitrário de V, escrevemos $\mathbf{v} + W$ para representar o conjunto de todas as somas $\mathbf{v} + \mathbf{w}$, com $\mathbf{w} \in W$, isto é,

$$\mathbf{v} + W = \{\mathbf{v} + \mathbf{w} : \mathbf{w} \in W\}.$$

Estes conjuntos são chamados *classes laterais à esquerda* de W em V. De forma análoga, definimos classes laterais à direita. Estas classes particionam V em subconjuntos mutuamente disjuntos de mesma cardinalidade.

No teorema seguinte, utilizaremos as classes laterais de um R-submódulo W e de um R-módulo V em V, para definir um novo R-módulo, chamado *módulo quociente de V por W*, que será denotado por

$$\frac{V}{W}.$$

Teorema 1.4 *Sejam V um R-módulo e W um R-submódulo de V. Então as classes laterais de W em V formam um R-módulo com as seguintes operações de adição e multiplicação escalar:*

1. $(\mathbf{v}_1 + W) + (\mathbf{v}_2 + W) = (\mathbf{v}_1 + \mathbf{v}_2) + W$, *para quaisquer* $\mathbf{v}_1, \mathbf{v}_2 \in V$.

2. $r\,(\mathbf{v}+W) = r\mathbf{v}+W$, *para qualquer* $r \in R$ *e* $\mathbf{v} \in V$. ■

Seja V um F-espaço vetorial. Uma função $B : V \times V \to F$ é uma *forma bilinear* sobre V se as seguintes condições são satisfeitas:

1. $B\,(a\mathbf{u} + \mathbf{v}, \mathbf{w}) = aB\,(\mathbf{u}, \mathbf{w}) + B\,(\mathbf{v}, \mathbf{w})$, para todos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ e $a \in F$.

2. $B\,(\mathbf{u}, b\mathbf{v} + \mathbf{w}) = bB\,(\mathbf{u}, \mathbf{v}) + B\,(\mathbf{u}, \mathbf{w})$, para todos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ e $b \in F$.

Sejam V um F-espaço vetorial e B uma forma bilinear sobre V. Dizemos que B é *degenerada* se existir $\mathbf{v} \in V$, com $\mathbf{v} \neq \mathbf{0}$, tal que

$$B(\mathbf{v}, \mathbf{w}) = 0, \ \ \forall \ \ \mathbf{w} \in V.$$

Caso contrário, dizemos que B é *não degenerada*.

Sejam V um F-espaço vetorial e $\mathbf{v}_1, \ldots, \mathbf{v}_n$ vetores de V. Então $[B(\mathbf{v}_i, \mathbf{v}_j)]$ é uma matriz $n \times n$ sobre F. O *discriminante* de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ com relação a B é definido por

$$\det\left([B(\mathbf{v}_i, \mathbf{v}_j)]\right)$$

e será denotado por

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

Proposição 1.5 *Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma F-base qualquer para V. Sejam $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se*

$$\mathbf{w}_i = \sum_{j=1}^{n} a_{ij}\mathbf{v}_j, i = 1, \ldots, n,$$

com $a_{ij} \in F$, então

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n),$$

onde $\mathbf{A} = [a_{ij}]$. ■

Prova. Seja

$$\mathbf{w}_k = \sum_{l=1}^{n} a_{kl}\mathbf{v}_l, k = 1, \ldots, n.$$

Então é fácil verificar que

$$B(\mathbf{w}_i, \mathbf{w}_k) = \sum_{l=1}^{n} \left(\sum_{j=1}^{n} a_{ij} B(\mathbf{v}_j, \mathbf{v}_l) \right) a_{kl}.$$

Portanto,

$$[B(\mathbf{w}_i, \mathbf{w}_k)] = \mathbf{A}[B(\mathbf{v}_j, \mathbf{v}_l)]\mathbf{A}^t \text{ e } \Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

■

Corolário 1.1 *Sejam V um F-espaço vetorial e $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se $\mathbf{w}_1, \ldots, \mathbf{w}_n$ são linearmente dependentes, então*

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = 0.$$

■

Proposição 1.6 *Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma F-base qualquer para V. Então B é degenerada se, e somente se,*

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n) = 0.$$

Prova. Suponhamos que B seja degenerada. Então existe um vetor $\mathbf{v} \in V$, com $\mathbf{v} \neq \mathbf{0}$, tal que

$$B(\mathbf{v}, \mathbf{w}) = 0, \ \forall \ \mathbf{w} \in V.$$

Em particular,

$$B(\mathbf{v}, \mathbf{v}_j) = 0, \ j = 1, \ldots, n.$$

Como $\mathbf{v} \neq \mathbf{0}$ temos que existem (únicos) escalares $x_1, \ldots, x_n \in F$, não todos nulos, tais que

$$\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n = \sum_{i=1}^{n} x_i\mathbf{v}_i.$$

Logo,

$$0 = B(\mathbf{v}, \mathbf{v}_j) = \sum_{i=1}^{n} x_i B(\mathbf{v}_i, \mathbf{v}_j) \;\; j = 1, \ldots, n,$$

isto é, as colunas da matriz $[B(\mathbf{v}_i, \mathbf{v}_j)]$ são linearmente dependentes. Portanto,

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n) = 0.$$

A recíproca prova-se de modo análogo. ■

Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ F-bases quaisquer para V. Dizemos que elas são *complementares* (*duais*) se

$$B(\mathbf{v}_i, \mathbf{w}_j) = \delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}.$$

Proposição 1.7 *Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ F-bases quaisquer para V. Se elas são complementares, então*

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n) \cdot \Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = 1.$$

■

Proposição 1.8 *Sejam V um F-espaço vetorial e B uma forma bilinear. Então B é não degenerada se, e somente se, qualquer F-base para V possui uma base complementar. Além disso, esta base complementar é única.*

Prova. Seja $V^* = \mathrm{Hom}_F(V, F)$. Então é fácil verificar que V^* é um F-espaço vetorial com $\dim V = \dim V^*$. Seja $\mathbf{v} \in V$ fixado. Então a função $B_{\mathbf{v}} : V \to F$ definida por

$$B_{\mathbf{v}}(\mathbf{w}) = B(\mathbf{w}, \mathbf{v}), \;\; \forall \;\; \mathbf{w} \in V,$$

é uma transformação linear, isto é, $B_{\mathbf{v}} \in V^*$. Assim, a função

$$\phi : V \to V^*$$

definida por $\phi(\mathbf{v}) = B_{\mathbf{v}}$ é um F-isomorfismo, pois B é não degenerada. Em particular, todo $f \in V^*$ é da forma $f = B_{\mathbf{v}}$, para algum $\mathbf{v} \in V$. Agora, seja $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma F-base qualquer para V. Então existe um único $f_j \in V^*$ tal que $f_j(\mathbf{v}_i) = \delta_{ij}$. É fácil verificar que

$$\{\mathbf{w}_1, \ldots, \mathbf{w}_n\},$$

onde $\mathbf{w}_j = f_j = B_{\mathbf{v}_j}$, é uma F-base para V^* com $B(\mathbf{w}_j, \mathbf{v}_i) = \delta_{ij}$. A recíproca é clara. ■

1.3 Extensões de Corpos

Sejam K e F dois corpos. Dizemos F é uma *extensão* de K se $K \subseteq F$ e será denotada por $K \subseteq F$ ou F/K.

Sejam F uma extensão de K e $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$. Então

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

denotará o menor subcorpo de F contendo $\alpha_1, \alpha_2, \ldots, \alpha_n$ e K. Uma extensão F de K é chamada *finitamente gerada sobre* K se existir $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tais que

$$F = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Se existir $\alpha \in F$ tal que $F = K(\alpha)$, dizemos que F é uma *extensão simples* de K e α é chamado um *elemento primitivo* de F sobre K.

Sejam F uma extensão de K e α um elemento de F. Dizemos que α é *algébrico* sobre K se existir $a_0, a_1, \ldots, a_n \in K$, com $a_n \neq 0$, tais que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

isto é, existe um polinômio não nulo $f \in K[x]$ tal que $f(\alpha) = 0$. Caso contrário, α é *transcendente* sobre K. Note que todo $\alpha \in K$ é algébrico sobre K, pois α é raiz do polinômio $p = x - \alpha \in K[x]$. Se todo elemento de uma extensão $K \subseteq F$ for algébrico sobre K, dizemos que F é uma *extensão algébrica*.

Proposição 1.9 *Sejam F uma extensão de K e α um elemento de F. Então a função $\phi : K[x] \to F$ definida por $\phi(f) = f(\alpha)$ é um homomorfismo de anéis tal que*:

1. $\operatorname{Im}\phi = K[\alpha]$ *e* $K \subseteq K[\alpha] \subseteq F$.

2. α *é transcendente sobre* K *se, e somente se,* $\ker\phi = \{0\}$.

3. α *é algébrico sobre* K *se, e somente se,* $\ker\phi \neq \{0\}$.

4. $\frac{K[x]}{\ker\phi} \simeq K[\alpha]$. ■

Sejam F uma extensão de K e $\alpha \in F$ algébrico sobre K. Como $K[x]$ é um domínio de ideais principais temos que $\ker\phi = \langle p\rangle$, onde $p \in K[x]$ é um polinômio mônico de menor grau tal que $p(\alpha) = 0$. Além disso, p é o único polinômio mônico irredutível sobre K tal que $p(\alpha) = 0$, pois $\ker\phi$ é um ideal maximal de $K[x]$. Neste caso, $K[\alpha]$ é um corpo, pois

$$\frac{K[x]}{\langle p\rangle} \simeq K[\alpha],$$

e $K[\alpha] = K(\alpha)$. Vamos denotar $p = \mathrm{irr}(\alpha, K)$.

Seja $K \subseteq F$ uma extensão. Então F com as operações de adição

$$\begin{array}{rccc} + : & F \times F & \to & F \\ & (a,b) & \mapsto & a+b \end{array}$$

e multiplicação por escalar

$$\begin{array}{rccc} \cdot : & K \times F & \to & F \\ & (\lambda, a) & \mapsto & \lambda a \end{array},$$

é um K-espaço vetorial. O *grau* de uma extensão $K \subseteq F$, denotado por $[F : K]$, é a dimensão de F visto como K-espaço vetorial. A extensão será chamada *finita* se $[F : K] = n < \infty$. Caso contrário, a extensão será chamada *infinita*.

Teorema 1.5 *Sejam* F *uma extensão de* K *e* α *um elemento de* F. *Então* α *é algébrico sobre* K *se, e somente se,* $K(\alpha)$ *é uma extensão finita de* K. *Neste caso,*

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

é uma base para $K(\alpha)$ *e* $[K(\alpha) : K] = n = \partial(p)$, *onde* $p = \mathrm{irr}(\alpha, K)$. ■

Proposição 1.10 *Sejam* $K \subseteq F \subseteq E$ *corpos tais que* $[E : F]$ *e* $[F : K]$ *sejam finitos. Então* $[E : K]$ *é finito e*

$$[E : K] = [E : F]\,[F : K]$$

■

Sejam K um corpo e $f \in K[x]$. Um *corpo de decomposição* de f sobre K é uma extensão de F sobre K tal que

1. f fatora-se em F;

2. F é minimal com respeito à condição 1., isto é, se f fatora-se em Z com $K \subseteq Z \subseteq F$, então $Z = F$.

Sejam F e F' extensões de K. Dizemos que um homomorfismo não nulo $\sigma : F \to F'$ *deixa fixado* $\alpha \in F$ se $\sigma(\alpha) = \alpha$. Dizemos que σ é uma K-*imersão* se $\sigma(a) = a$, para todo $a \in K$. O conjunto de todas as K-imersões de F em F' será denotado por $\mathrm{Hom}_K(F, F')$. Um isomorfismo de $\sigma : F \to F'$ tal que $\sigma(a) = a$, para todo $a \in K$, será chamado K-*isomorfismo*. Quando $F = F'$, dizemos que σ é um K-*automorfismo* de F e será dentotado por $\mathrm{Aut}_K(F)$. É fácil verificar que $\mathrm{Aut}_K(F)$ é um grupo com a operação de composição.

Teorema 1.6 *Seja K um corpo. Então qualquer $f \in K[x]$ possui um corpo de decomposição.* ■

Seja K um corpo. Dizemos que K é *algebricamente fechado* se qualquer polinômio não constante sobre K pode ser decomposto em fatores lineares sobre K.

Proposição 1.11 *Seja K um corpo. Então as seguintes condições são equivalentes*:

1. *K é algebricamente fechado.*

2. *Qualquer polinômio não constante $f \in K[x]$ tem uma raiz em K.*

3. *Se F é uma extensão algébrica de K, então $F = K$.* ■

Seja K um corpo. Um *fecho algébrico* de K é uma extensão algébrica F de K tal que as seguintes condições são satisfeitas:

1. F é algebricamente fechado.

2. F é minimal com respeito à condição 1., isto é, se Z é um corpo algebricamente fechado tal que $K \subseteq Z \subseteq F$, então $Z = F$.

Vamos denotar o fecho algébrico de K por $\overline{K}$. Neste caso, $\overline{K}$ é uma extensão algébrica de K.

Seja $K \subseteq F$ uma extensão. Dizemos que F é *normal* sobre K se F é uma extensão algébrica de K e qualquer polinômio irredutível f sobre $K[x]$ fatora-se em $F[x]$ em fatores lineares.

Proposição 1.12 *Sejam $F = K[\alpha]$ com α algébrico, $p = \mathrm{irr}(\alpha, K) \in K[x]$ e N uma extensão normal de K contendo α. Se $\beta \in N$, então as seguintes condições são equivalentes*:

1. *$\beta \in N$ é uma raiz de p.*

2. *$p = \mathrm{irr}(\alpha, K) = \mathrm{irr}(\beta, K)$, para todo $\beta \in N$.*

3. *Existe um único K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$, com $\sigma(\alpha) = \beta$.*

4. *Existe um K-automorfismo $\varphi : N \to N$, com $\varphi(\alpha) = \beta$.* ■

Se pelo menos uma (e portanto todas) das quatro condições da Proposição 1.12 for satisfeita, dizemos que β é um *conjugado de α sobre K*. Conseqüentemente, o número de K-imersões de $K(\alpha)$ em N é igual ao número de raízes de p, isto é,

$$\mathrm{Hom}_K(F, N) \leq \partial(p) = [K[\alpha] : K].$$

Sejam F um corpo e

$$\mathcal{F} = \{K : K \text{ subcorpo de } F\}.$$

Então o corpo

$$P = \bigcap_{K \in \mathcal{F}} K$$

é chamado o *corpo primo* de F.

Teorema 1.7 *Sejam F um corpo e P seu corpo primo. Então $P \simeq \mathbb{Q}$ ou $P \simeq \mathbb{Z}_p$, para algum primo $p \in \mathbb{N}$.* ■

Sejam F um corpo e P seu corpo primo. Dizemos que F tem *característica* 0 se $P \simeq \mathbb{Q}$ e *característica p* se $P \simeq \mathbb{Z}_p$.

Lema 1.2 *Seja K um corpo de característica $p > 0$. Então*:

1. *$pa = 0$, para todo $a \in K$.*

2. $(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}$, *para todos* $a, b \in K$ *e* $k \in \mathbb{N}$.

3. *A função* $\varphi : K \to K$ *definida por* $\varphi(a) = a^p$ *é um homomorfismo de corpos injetor. Neste caso,*

$$\operatorname{Im} \varphi = K^p$$

é um subcorpo de K. ■

Sejam K um corpo e

$$f = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

com $a_n \neq 0$, a *derivada formal* de f é definida como

$$f' = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in K[x].$$

Se a caracteristica de K é zero, então

$$f' = 0 \Leftrightarrow a_i = 0, \;\; i = 1, \ldots, n.$$

Portanto, $f' \neq 0$ se $n > 0$.

Se a caracteristica de K é $p \neq 0$, então

$$f' = 0 \Leftrightarrow i a_i = 0 \Leftrightarrow a_i = 0 \text{ ou } p \mid i, \;\; i = 1, \ldots, n.$$

Em particular, como $a_n \neq 0$ temos que $n a_n = 0$ se $p \mid n$. Portanto, $f' = 0$ se, e somente se, $p \mid n$ e os $a_i = 0$, quando $p \nmid i$, $i = 1, \ldots, n-1$. Neste caso, os termos $a_i x^i$ em f são tais que i é divisível por p. O que significa que f é um polinômio em x^p, isto é, $f \in K[x^p]$.

Um polinômio irredutível f sobre K é *separável* se $f' \neq 0$. Um polinômio qualquer f em $K[x]$ é *separável* se todos os seus fatores irredutíveis são separáveis.

Sejam F uma extensão de K e $\alpha \in F$. Dizemos que α é *separável* sobre K se α é transcendente sobre K ou $\operatorname{irr}(\alpha, K)$ é separável sobre K. Dizemos que F é uma *extensão separável* sobre K se todo elemento de F for separável sobre K.

Seja F uma extensão normal de K. Dizemos que $\operatorname{Aut}_K(F)$ é o *grupo de Galois* de F em K e denotamos por

$$\operatorname{Gal}(F/K) = \operatorname{Aut}_K(F)$$

Teorema 1.8 *Sejam* F *uma extensão normal de* K, $G = \operatorname{Gal}(F/K)$ *e*

$$F^G = \{\alpha \in F : \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

1. *A função* $\gamma : Sub(G) \to Lat(F/K)$ *definida por*:

$$\gamma(H) = F^H$$

é uma bijeção invertendo ordem com inversa

$$\delta(Z) = \mathrm{Gal}(F/Z).$$

2. $F^{\mathrm{Gal}(F/Z)} = Z$ *e* $\mathrm{Gal}(F/F^H) = H$.

3. $F^{H \vee L} = F^H \cap F^L$ *e* $F^{H \cap L} = F^H \vee F^L$,

$$\mathrm{Gal}(F/Z \vee Z') = \mathrm{Gal}(F/Z) \cap \mathrm{Gal}(F/Z') \ \ e \ \ \mathrm{Gal}(F/Z \cap Z') = \mathrm{Gal}(F/Z) \vee \mathrm{Gal}(F/Z').$$

4. $[Z : K] = [G : \mathrm{Gal}(F/Z)]$ *e* $[G : H] = [F^H : K]$.

5. Z *uma extensão normal de* K *se, e somente se,* $\mathrm{Gal}(F/Z)$ *é uma subgrupo normal de* G. ■

Teorema 1.9 *Seja* F *uma extensão separável de* K *com* $[F : K] < \infty$. *Então existe* $\alpha \in F$ *tal que* $F = K[\alpha]$. ■

Teorema 1.10 *Sejam* K *um corpo e* $h, p \in \mathbb{N}$ *com* p *primo. Então*:

1. $|K| = q$, *onde* $q = p^h$ *se, e somente se,* K *é o corpo de decomposição de* $f = x^q - x \in \mathbb{Z}_p[x]$.

2. *Se* $|K| = q$, *onde* $q = p^h$, *então existe um polinômio irredutível* $f \in \mathbb{Z}_p[x]$ *tal que*

$$K \simeq \frac{\mathbb{Z}_p[x]}{\langle f \rangle}.$$

3. *Seja* F *um corpo com* $|F| = p^h$. *Se* K *é um subcorpo de* F, *então* $|K| = p^d$, *para algum* d *dividindo* h.

4. *Seja* F *um corpo com* $|F| = p^h$. *Para cada divisor* d *de* h, *existe um único subcorpo* K *de* F *com* $|K| = p^d$, *a saber,*

$$K = \{\alpha \in F : \alpha^{p^d} = \alpha\}.$$

■

Seja F um corpo. Dizemos que F é um *corpo de Galois* se $|F| = q$, onde $q = p^h$ com $h, p \in \mathbb{N}$, p primo e será denotado por $\mathbb{F}_q$ ou $GF(q)$.

1.4 Traços e Normas

Nesta seção todas as extensões de K, salvo menção explícita em contrário, são separáveis.

Sejam F uma extensão finita de K com $[F : K] = n$ e $\alpha \in F$. Então a função $\phi_\alpha : F \to F$ definida por $\phi_\alpha(\beta) = \alpha\beta$ é claramente uma transformação linear sobre K. Logo, a função $\varphi : F \to \mathrm{End}_K F = \mathrm{Hom}_K(F, F)$ definida por $\varphi(\alpha) = \phi_\alpha$ é um homomorfismo de anéis injetor. Portanto, podemos identificar F com um subcorpo de $\mathrm{End}_K F$. Se

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

é uma K-base para F e

$$\phi_\alpha(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, j = 1, \ldots, n,$$

então

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A})$$

é o *polinômio característico* de α sobre K, onde $\mathbf{A} = [a_{ij}]$ é a matriz $n \times n$ da transformação linear ϕ_α em relação à K-base $\mathcal{B}$.

Teorema 1.11 *Sejam F uma extensão de K com $[F : K] = n$ e $\alpha \in F$. Se $p = \mathrm{irr}(\alpha, K)$, então $f_\alpha = p^k$, onde $k = [F : K[\alpha]]$. Além disso, $f_\alpha = p$ se, e somente se, $F = K[\alpha]$.*

Prova. Seja

$$p(x) = \mathrm{irr}(\alpha, K) = c_0 + c_1 x + \cdots + c_{m-1}x^{m-1} + x^m.$$

Então $\{1, \alpha, \ldots, \alpha^{m-1}\}$ é uma K-base para $K[\alpha]$. Se $\{\beta_0, \ldots, \beta_{k-1}\}$ é uma $K[\alpha]$-base para F, então

$$\{\alpha^i\beta_j : 0 \leq i \leq m-1 \text{ e } 0 \leq j \leq k-1\}$$

é uma K-base para F. Logo, a matriz de ϕ_α nesta base é da forma

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{A}_1 & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{A}_{k-1} \end{pmatrix},$$

onde

$$\mathbf{A}_j = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -c_{m-2} \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}.$$

Portanto,

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = \prod_{j=0}^{k-1} \det(x\mathbf{I} - \mathbf{A}_j) = p(x)^k.$$

Finalmente, se $f_\alpha = p$, então

$$[K[\alpha] : K] = n = [F : K].$$

Logo, $F = K[\alpha]$. Reciprocamente, se $F = K[\alpha]$, então $\partial p = n$ e $f_\alpha = p$. ■

Seja $\mathbf{A}$ a matriz da transformação linear ϕ_α em relação à alguma K-base. O *traço* e a *norma* de α são definidos por

$$\mathrm{tr}(\alpha) = \mathrm{tr}(\mathbf{A}) \text{ e } N(\alpha) = \det(\mathbf{A}).$$

Proposição 1.13 *Seja F uma extensão de K com $[F : K] = n$.*

1. $\mathrm{tr}(a\alpha + b\beta) = a\,\mathrm{tr}(\alpha) + b\,\mathrm{tr}(\beta)$, *para todos $a, b \in K$ e $\alpha, \beta \in F$.*

2. $\mathrm{tr}(a) = na$, *para todo $a \in K$.*

3. $N(\alpha\beta) = N(\alpha)N(\beta)$, *para todos $\alpha, \beta \in F$.*

4. $N(a) = a^n$, *para todo $a \in K$.* ■

Suponhamos que

$$f_\alpha(x) = (x - \alpha_0) \cdots (x - \alpha_{n-1})$$

em $\overline{K}$. Então

$$\mathrm{tr}(\alpha) = \sum_{j=0}^{n-1} \alpha_j \text{ e } N(\alpha) = \prod_{j=0}^{n-1} \alpha_j.$$

De fato, se

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

então

$$a_{n-1} = -\operatorname{tr}(\mathbf{A}) \text{ e } a_0 = (-1)^n \det(\mathbf{A}).$$

Por outro lado, é fácil verificar que

$$\sum_{j=0}^{n-1} \alpha_j = -a_{n-1} \text{ e } \prod_{j=0}^{n-1} \alpha_j = (-1)^n a_0.$$

Portanto, $\operatorname{tr}(\alpha) \in K$ e $N(\alpha) \in K$.

Corolário 1.2 *Seja F uma extensão de K com $[F : K] = n$. Se $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de F, então para todo $\alpha \in F$ temos que*

$$\operatorname{tr}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \text{ e } N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Além disso,

$$\operatorname{tr}(g(\alpha)) = \sum_{i=1}^{n} g(\alpha_i) \text{ e } N(g(\alpha)) = \prod_{i=1}^{n} g(\alpha_i),$$

para todo $\alpha \in F$ e $g \in K[x]$, onde $\alpha_i = \sigma_i(\alpha)$, $i = 1, \ldots, n$. ■

A função $B : F \times F \to K$ definida por $B((\alpha, \beta)) = \operatorname{tr}(\alpha\beta)$ é claramente uma forma bilinear simétrica sobre K. Logo, o discriminante de uma K-base

$$\mathcal{B} = \{1, \theta, \ldots, \theta^{n-1}\}$$

para F é

$$\Delta(\mathcal{B}) = \det(\operatorname{tr}(\theta^{i+j})).$$

Se $\mathcal{B}' = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma outra base para F tal que

$$\alpha_i = \sum_{j=0}^{n-1} a_{ij}\theta^j,$$

onde $\mathbf{B} = [a_{ij}]$ é a matriz mudança de base, então

$$\operatorname{tr}(\alpha_i\alpha_j) = \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a_{il}a_{jk} \operatorname{tr}((\theta^{k+l})).$$

Portanto,

$$\Delta(\mathcal{B}') = (\det \mathbf{B})^2 \Delta(\mathcal{B}).$$

Proposição 1.14 *Seja F uma extensão de K com $[F : K] = n$.*

1. *Se* $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, *são as* K*-imersões de* F, *onde* F *é algebricamente fechado, então*

$$\Delta(\mathcal{B}) = (\det(\sigma_i(\alpha_j)))^2$$

onde

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

é uma K*-base para* F.

2. *Se* $F = K(\alpha)$ *e* $p = \mathrm{irr}(\alpha, K) \in K[x]$, *então*

$$\Delta(\mathcal{B}') = (-1)^{\frac{n(n-1)}{2}} N(p'(\alpha)) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2,$$

onde

$$\mathcal{B}' = \{1, \alpha, \ldots, \alpha^{n-1}\}$$

é uma K*-base para* F.

Prova. Vamos provar apenas o item 1. Sejam

$$\mathbf{A} = [a_{ij}] \text{ e } \mathbf{A}^t = [b_{ij}]$$

onde $a_{ij} = \sigma_i(\alpha_j)$ e $b_{ij} = a_{ji}$. Então

$$\mathbf{A}^t\mathbf{A} = [c_{ij}],$$

onde

$$c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \mathrm{tr}(\alpha_i\alpha_j).$$

Logo,

$$\Delta(\mathcal{B}') = \det(\mathrm{tr}(\alpha_i\alpha_j)) = \det(\mathbf{A}^t\mathbf{A}) = (\det(\mathbf{A}))^2.$$

■

Teorema 1.12 *Seja* F *uma extensão finita de* K. *Então as seguintes condições são equivalentes*:

1. $\mathrm{tr} : F \to K$ *é sobrejetiva.*

2. $\mathrm{tr} \neq 0$.

3. *A forma bilinear* $B : F \times F \to K$ *definida por* $B((\alpha, \beta)) = \mathrm{tr}(\alpha\beta)$ *é não degenerada.*

Prova. É claro. (2 $\Rightarrow$ 1). Para provar que (1. $\Rightarrow$ 2.). Suponhamos que tr $\neq 0$. Então existe $\alpha \in F$ com $\mathrm{tr}(\alpha) = b \neq 0$. Logo,

$$\mathrm{tr}(cb^{-1}\alpha) = cb^{-1}\,\mathrm{tr}(\alpha) = cb^{-1}b = c, \forall c \in K.$$

Portanto, tr é sobrejetiva.

(1. $\Rightarrow$ 3.) suponhamos que tr seja sobrejetiva. Então existe $\alpha \in F^*$ tal que $\mathrm{tr}(\alpha) \neq 0$. Dado $\beta \in F^*$, existe $\alpha\beta^{-1} \in F$ tal que

$$B(\alpha\beta^{-1}, \beta) = \mathrm{tr}(\alpha\beta^{-1}\beta) = \mathrm{tr}(\alpha) \neq 0.$$

Portanto, B é não degenerada.

(3 $\Rightarrow$ 1) Segue da definição. ■

1.5 Inteiros Algébricos.

Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Dizemos que α é um *inteiro* (*algébrico*) sobre R se existir $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Se todo elemento de uma extensão $R \subseteq S$ for inteiro, dizemos que S é uma *extensão inteira* de R.

Teorema 1.13 *Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Então as seguintes condições são equivalentes*:

1. *α é um inteiro sobre R;*

2. *$R[\alpha]$ é um R-módulo finitamente gerado;*

3. *Existe um anel Z com $R[\alpha] \subseteq Z \subseteq S$ tal que Z é um R-módulo finitamente gerado;*

4. *Existe um $R[\alpha]$-módulo V, o qual é um R-módulo finitamente gerado e cujo*

$$\mathrm{Ann}_{R[\alpha]}(V) = \{0\}.$$

Prova. (1. $\Rightarrow$ 2.) Suponhamos que α seja um inteiro sobre R. Então existem $a_0, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Logo,

$$\alpha^n = -(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})$$

e

$$\alpha^{n+k} = -(a_0\alpha^k + a_1\alpha^{k+1} + \cdots + a_{n-1}\alpha^{n+k-1}), \ \forall \ k \in \mathbb{Z}_+.$$

Assim, indutivamente, obtemos

$$\alpha^m = b_0\alpha + b_1\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}, \ \forall \ m \geq n,$$

onde $b_i \in R$, $i = 0, \ldots, n-1$. Portanto, $R[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$ é um R-módulo finitamente gerado.

(2. $\Rightarrow$ 3.) Basta tomar $Z = R[\alpha]$.

(3. $\Rightarrow$ 4.) Tomando $V = Z$, temos, por hipótese, que V é um $R[\alpha]$-módulo, o qual é um R-módulo finitamente gerado. Agora,

$$x \in \mathrm{Ann}_{R[\alpha]}(V) \Rightarrow xv = 0, \ \forall \ v \in V.$$

Em particular, como $1 \in V$ temos que $x = x \cdot 1 = 0$. Portanto, $\mathrm{Ann}_{R[\alpha]}(V) = \{0\}$.

(4. $\Rightarrow$ 1.) Suponhamos que existe um $R[\alpha]$-módulo V tal que

$$V = R\alpha_1 \oplus \cdots \oplus R\alpha_n, \ \ \alpha_i \in V, \ \ i = 1, \ldots, n,$$

e cujo $\mathrm{Ann}_{R[\alpha]}(V) = \{0\}$. Então $\alpha V \subseteq V$. Em particular, $\alpha\alpha_j \in V$, para cada $j = 1, \ldots, n$. Logo, existem $t_{ij} \in R$ tais que

$$\alpha\alpha_i = \sum_{j=1}^{n} t_{ij}\alpha_j, \ \ i = 1, \ldots, n.$$

Ou na forma matricial

$$(\mathbf{T} - \alpha\mathbf{I}_n)\mathbf{X} = \mathbf{O},$$

onde

$$\mathbf{T} - \alpha\mathbf{I}_n = \begin{bmatrix} t_{11} - \alpha & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} - \alpha & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \cdots & t_{nn} - \alpha \end{bmatrix} \ \text{e} \ \mathbf{X} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Como $\det(\mathbf{T}-\alpha\mathbf{I}_n)\mathbf{I}_n = \text{adj}(\mathbf{T}-\alpha\mathbf{I}_n)(\mathbf{T}-\alpha\mathbf{I}_n)$ temos que $\det(\mathbf{T}-\alpha\mathbf{I}_n)\mathbf{X} = \mathbf{0}$. Assim,

$$\det(\mathbf{T}-\alpha\mathbf{I}_n)\alpha_i = 0 \;\; i = 1,\ldots,n,$$

isto é, $\det(\mathbf{T}-\alpha\mathbf{I}_n) \in \text{Ann}_{R[\alpha]}(V) = \{0\}$. Logo, $\det(\mathbf{T}-\alpha\mathbf{I}_n) = 0 \Leftrightarrow \det(\alpha\mathbf{I}_n - \mathbf{T}) = 0$ é uma equação polinomial de grau n em α, a saber,

$$\alpha^n + b_1\alpha^{n-1} + b_2\alpha^{n-2} + \cdots + b_{n-1}\alpha + b_n = 0, \;\; b_i \in R, i = 1,\ldots,n.$$

Portanto, α é um inteiro sobre R. ■

Lema 1.3 *Sejam $R \subseteq S \subseteq T$ anéis.*

1. *Se S é um R-módulo finitamente gerado e T é um S-módulo finitamente gerado, então T é um R-módulo finitamente gerado.*

2. *Se $\text{Ann}_R(S) = \{0\}$ e S é um R-módulo finitamente gerado, então o único ideal I em R com $IS = S$ é $I = R$.*

Prova. 1. Se

$$S = R\alpha_1 \oplus \cdots \oplus R\alpha_m \text{ e } T = S\beta_1 \oplus \cdots \oplus S\beta_n,$$

então

$$T = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} R\alpha_i\right)\beta_j = \sum_{i=1}^{m}\sum_{j=1}^{n} R\alpha_i\beta_j.$$

Portanto, T é um R-módulo finitamente gerado.

2. Suponhamos que

$$S = R\alpha_1 \oplus \cdots \oplus R\alpha_n.$$

Como $\alpha_i \in S$ e

$$S = IS = I\alpha_1 \oplus \cdots \oplus I\alpha_n$$

temos que existem $a_{ij} \in I$ tais que

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \;\; j = 1,\ldots,n.$$

Ou na forma matricial

$$(\mathbf{A}-\mathbf{I}_n)\mathbf{X} = \mathbf{O},$$

onde

$$\mathbf{A}-\mathbf{I}_n=\begin{bmatrix} a_{11}-1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-1 \end{bmatrix} \text{ e } \mathbf{X}=\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Como $\det(\mathbf{A}-\mathbf{I}_n)\mathbf{I}_n = \text{adj}(\mathbf{A}-\mathbf{I}_n)(\mathbf{A}-\mathbf{I}_n)$ temos que $\det(\mathbf{A}-\mathbf{I}_n)\mathbf{X}=\mathbf{0}$. Assim,

$$\det(\mathbf{A}-\mathbf{I}_n)\alpha_i = 0 \;\; i=1,\ldots,n,$$

isto é, $\det(\mathbf{A}-\mathbf{I}_n)\in \text{Ann}(S)=\{0\}$. Por outro lado, a expansão do determinante mostra que $\det(\mathbf{A}-\mathbf{I}_n)=(-1)^n+x$, com $x\in I$, pois $a_{ij}\in I$. Portanto, $1\in I$ e $I=R$. ■

Seja $R\subseteq S$ uma extensão de anéis. O *fecho inteiro* de R em S é definido como

$$R_S=\{\alpha\in S:\alpha \text{ é inteiro sobre } R\}.$$

Dizemos que R é *integralmente fechado* em S se $R_S=R$.

Teorema 1.14 *Sejam $R\subseteq S\subseteq T$ extensões de anéis.*

1. *Se S é um R-módulo finitamente gerado, então S é uma extensão inteira de R.*
2. *Se $\alpha_1,\ldots,\alpha_n\in S$ são inteiros sobre R, então $R[\alpha_1,\ldots,\alpha_n]$ é um R-módulo finitamente gerado.*
3. *Se S é uma extensão inteira sobre R e T é uma extensão inteira sobre S, então T é uma extensão inteira sobre R.*
4. *R_S é um anel com $R\subseteq R_S\subseteq S$.*
5. *Se $S=R_T$, então S é integralmente fechado em T.*

Prova. 1. Seja $\alpha\in S$. Então tomando $S=Z$ no item 3. do Teorema 1.13, temos que α é inteiro sobre R. Portanto, S é uma extensão inteira de R.

2. Vamos usar indução sobre n. Se $n=1$, então pelo item 2. do Teorema 1.13 $R[\alpha_1]$ é um R-módulo finitamente gerado. Suponhamos que $n\geq 2$ e que o resultado seja válido para todo $1\leq k\leq n-1$. Então

$$T=R[\alpha_1,\ldots,\alpha_{n-1}]$$

é um R-módulo finitamente gerado. Além disso, pelo item 2. do Teorema 1.13

$$R[\alpha_1, \ldots, \alpha_n] = T[\alpha_n]$$

é um T-módulo finitamente gerado, pois α_n é inteiro sobre R e, assim, sobre T. Portanto, pelo item 1. do Lema 1.3 , $R[\alpha_1, \ldots, \alpha_n]$ é um R-módulo finitamente gerado.

3. Seja $\beta \in T$ qualquer. Então existem $b_0, \ldots, b_{n-1} \in S$ tais que

$$b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} + \beta^n = 0.$$

Seja

$$S' = R[b_0, \ldots, b_{n-1}].$$

Então β é inteiro sobre S'. Logo, pelo item 3. do Teorema 1.13, temos que $S'[\beta]$ é um S'-módulo finitamente gerado. Como $b_0, \ldots, b_{n-1} \in S$ são inteiros sobre R temos, pelo item 2., que S' é um R-módulo finitamente gerado. Assim, pelo item 1. do Lema 1.3, temos que $S'[\beta]$ é um R-módulo finitamente gerado. Logo, pelo item 2. do Teorema 1.13, temos que β é um inteiro sobre R. Portanto, T é uma extensão inteira sobre R.

4. Basta mostrar que se $\alpha, \beta \in S$ são inteiros sobre R, então $\alpha \pm \beta$ e $\alpha\beta$ são inteiros sobre R. Se $\alpha, \beta \in S$ são inteiros sobre R, então pelo item 2. $R[\alpha, \beta] \subseteq S$ é um R-módulo finitamente gerado. Portanto, pelo item 1. $\alpha \pm \beta, \alpha\beta \in R[\alpha, \beta]$ são inteiros sobre R.

5. Segue do item 3. ■

Corolário 1.3 *Sejam R um domínio de fatoração única e K seu corpo quociente. Então $R_K = R$.* ■

Proposição 1.15 *Seja $R \subseteq S$ uma extensão de domínios tal que S é uma extensão inteira sobre R. Então S é um corpo se, e somente se, R também o é.*

Prova. Suponhamos que S seja um corpo. Então para cada $\alpha \in R^*$, obtemos $\alpha^{-1} \in S$, pois S é um corpo. Logo, por hipótese, existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha^{-1} + \cdots + a_{n-1}(\alpha^{-1})^{n-1} + (\alpha^{-1})^n = 0.$$

Multiplicando esta equação por α^{m-1}, obtemos

$$\alpha^{-1} = -(a_{m-1} + \cdots + a_1\alpha^{m-2} + a_0\alpha^{m-1}) \in R.$$

Portanto, R é um corpo. Reciprocamente, suponhamos que R seja um corpo. Para cada $\alpha \in S^*$, existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0,$$

onde n é mínimo. Então $a_0 \neq 0$ e $a_0^{-1} \in R$. Assim,

$$\alpha(a_1 + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})(-a_0^{-1}) = 1,$$

isto é, α é invertível. Portanto, S é um corpo. ■

Corolário 1.4 *Seja $R \subseteq S$ uma extensão de domínios tal que S é uma extensão inteira sobre R.*

1. *Para qualquer ideal I não nulo de S, $I \cap R$ é um ideal não nulo de R.*
2. *$U(S) \cap R = U(R)$.*
3. *Um ideal M de S é maximal se, e somente se, $N = M \cap R$ é um ideal maximal de R.*

Prova. Vamos provar apenas o item 3. Basta notar que

$$\frac{R}{N} = \frac{R}{M \cap R} \simeq \frac{M + R}{M}$$

e que $\frac{S}{M}$ é uma extensão inteira sobre $\frac{M+R}{M}$, pois se

$$\pi : S \to \frac{S}{M}$$

é o homomorfismo canônico, então $\pi(S) = \frac{S}{M}$ é uma extensão inteira sobre

$$\pi(R) = \frac{M + R}{M}.$$

■

Proposição 1.16 *Sejam R um dominio, K seu corpo quociente com $R_K = R$, F uma extensão finita de K e $S = R_F$.*

1. *Se $\alpha \in S$, então $\sigma_i(\alpha)$ são inteiros sobre R, onde $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de F.*

2. *Se* $\alpha \in S$, *então* $\mathrm{tr}(\alpha), N(\alpha) \in R$.

3. $\alpha \in U(S)$ *se, somente se,* $N(\alpha) \in U(R)$.

4. *Se* $\alpha \in R$ *é tal que* $N(\alpha)$ *é irredutível em* R, *então* α *é irredutível em* S.

5. *Qualquer elemento de* F *pode ser escrito na forma* $\frac{c}{a}$, *onde* $c \in S$ *e* $a \in R$. *Em particular,* F *é o corpo quociente de* S.

Prova. 1. Seja $\alpha \in S$. Então existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Logo

$$0 = \sigma_i(0) = \sigma_i\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sum_{i=0}^{n} a_i\sigma_i(\alpha^i).$$

Portanto, $\sigma_i(\alpha)$ inteiro sobre R.

2. É claro que o $\mathrm{tr}(\alpha) \in K$ e $N(\alpha) \in K$. Por outro lado, como $\sigma_i(\alpha)$ são inteiros sobre R temos, pelo Corolário 1.2, que $\mathrm{tr}(\alpha)$ e $N(\alpha)$ são inteiros sobre R. Logo, $\mathrm{tr}(\alpha), N(\alpha) \in R_K = R$.

3. Suponhamos que $\alpha \in U(S)$. Então existe $\beta \in S$ tal que $\alpha\beta = 1$. Logo,

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Portanto, $N(\alpha) \in U(R)$. Reciprocamente, se $N(\alpha) \in U(R)$, então existe $a \in R$ tal que $aN(\alpha) = 1$. Logo,

$$1 = aN(\alpha) = a\prod_{j=1}^{n} \sigma_j(\alpha).$$

Como $\sigma_j = id$, para algum $j = 1, \ldots, n$, temos que $\alpha \in U(S)$, onde

$$\alpha^{-1} = (a \prod_{i=1, i\neq j}^{n} \sigma_i(\alpha)).$$

4. Segue da definição de elemento irredutível e do item 3.

5. Dado $\alpha \in F$. Como α é algébrico sobre K temos que existem $r_0, r_1, \ldots, r_{n-1} \in K$ tais que

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Fazendo

$$r_i = \frac{a_i}{b_i} \text{ e } \beta = b_0b_1\cdots b_{n-1} \in R,$$

obtemos

$$c_0 + c_1(\alpha\beta) + \cdots + c_{n-1}(\alpha\beta)^{n-1} + (\alpha\beta)^n = 0.$$

Assim, $\beta\alpha \in S = R_F$. Portanto, existe $c \in S$ tal que $\alpha = \frac{c}{\beta}$. ■

Proposição 1.17 *Sejam R um dominio, K seu corpo quociente, F uma extensão de K e $S = R_F$.*

1. *Se $\alpha \in K \cap S$, então existe $c \in R^*$ tal que $c\alpha^n \in R$, para todo $n \in \mathbb{N}$.*

2. *Se $R_K = R$, então $K \cap S = R$.*

3. *Se $R_K = R$ e $\alpha \in S$, então $p = \text{irr}(\alpha, K) \in K[x]$ tem coeficientes em R.*

Prova. 1. Como $\alpha \in K \cap S$ temos que $\alpha = \frac{r}{s}$, com $r, s \in R$ e $\text{mdc}(r, s) = 1$, e existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Logo,

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + r^n = 0 \Rightarrow s \mid 1.$$

Assim, existe $t = s^{-1} \in R^*$ tal que $t\alpha = r \in R$. Portanto, indutivamente, obtemos $c\alpha^n \in R$, para todo $n \in \mathbb{N}$.

2. É claro que $R \subseteq K \cap S$. Mas por 1. $K \cap S \subseteq R$. Portanto, $K \cap S = R$.

3. Suponhamos que $\alpha \in S$ e $p = \text{irr}(\alpha, K)$. Então, pelo item 1.da Proposição 1.16, os conjugados $\sigma_i(\alpha)$ de α são inteiros sobre $R = R_K$. Como os coeficientes de p são polinômios simétricos elementares das raízes temos, pelo item 4. do Teorema 1.14, que eles são inteiros sobre R. Por outro lado, esses coeficientes estão K e $R_K = R$ implica que eles estão em R. ■

Proposição 1.18 *Sejam R um dominio, K seu corpo quociente, F uma extensão de K com $[F : K] = n$ e $S = R_F$. Então existe uma K-base*

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

para F tal que

$$S \subseteq R\alpha_1 \oplus \cdots \oplus R\alpha_n.$$

Prova. Como cada $\gamma \in F$ é algébrico sobre K temos temos que existem $r_0, \ldots, r_{n-1}, r_n \in K$ tais que

$$r_0 + r_1\gamma + \cdots + r_{n-1}\gamma^{n-1} + r_n\gamma^n = 0.$$

Fazendo

$$r_i = \frac{a_i}{b_i} \text{ e } b = b_0 b_1 \cdots b_n \in R,$$

obtemos

$$c_0 + c_1(b\gamma) + \cdots + c_{n-1}(b\gamma)^{n-1} + c_n(b\gamma)^n = 0.$$

Logo,

$$c_n^{n-1}c_0 + c_n^{n-2}c_1(c_n b\gamma) + \cdots + c_{n-1}(c_n b\gamma)^{n-1} + (c_n b\gamma)^n = 0.$$

Tomando $\beta = c_n b\gamma$, obtemos $\beta \in S$. Assim, podemos supor, sem perda de generalidade, que a partir de qualquer K-base

$$\{\gamma_1, \ldots, \gamma_n\}$$

para F, obtemos uma nova K-base

$$\{\beta_1, \ldots, \beta_n\}$$

onde $\beta_i \in S$, $i = 1, \ldots, n$.

Como a forma bilinear $B : F \times F \to K$ dada por $B(\alpha, \beta) = \operatorname{tr}(\alpha\beta)$ é não degenerada temos, pela Proposição 1.8, que existe uma K-base

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

para F dual a K-base

$$\{\beta_1, \ldots, \beta_n\}$$

com $\operatorname{tr}(\alpha_i\beta_j) = \delta_{ij}$.

Afirmação. A K-base $\mathcal{B}$ tem as propriedades desejadas.
De fato, dado $\delta \in S$, existem $x_1, \ldots, x_n \in K$ tal que

$$\delta = \sum_{j=1}^{n} x_j\beta_j.$$

Como $\delta, \alpha_i \in S$ temos que $\delta\alpha_i \in S$, para todo $i = 1, \ldots, n$. Assim, pelo item 3. da Proposição 1.17, $\operatorname{irr}(\delta\alpha_i, K) \in K[x]$ tem coeficientes em R. Logo $\operatorname{tr}(\delta\alpha_i) \in R$. Assim,

$$\operatorname{tr}(\delta\alpha_i) = \operatorname{tr}(\sum_{j=1}^{n} x_j\beta_j\alpha_i) = \sum_{j=1}^{n} x_j \operatorname{tr}(\alpha_i\beta_j) = \sum_{j=1}^{n} x_j\delta_{ij} = x_i,$$

isto é, $x_i \in R$, $i = 1, \ldots, n$. Portanto,

$$\delta \in R\alpha_1 + \cdots + R\alpha_n,$$

ou seja

$$S \subseteq R\alpha_1 + \cdots + R\alpha_n.$$

■

Capítulo 2

Corpos Ciclotômicos

Neste capítulo apresentaremos as principais definições e resultado básicos sobre corpos ciclotômicos, que serão necessários para os capítulos subseqüentes. O leitor interessado em mais detalhes pode consultar [1, 6, 14].

2.1 Corpos de Números

Nesta seção estamos interessados em extensões algébricas de $\mathbb{Q}$ de grau finito, isto é, extensões F sobre $\mathbb{Q}$ tais que $[F:\mathbb{Q}]$ seja finito.

Um subcorpo F de $\mathbb{C}$ é um *corpo de números* (*algébricos*) se ele é uma extensão finita de $\mathbb{Q}$ de grau n, isto é, F é um espaço vetorial sobre $\mathbb{Q}$ de dimensão n. Como a característica de $\mathbb{Q}$ é zero temos, pelo Teorema 1.9, que existe $\alpha \in F$ tal que $F = \mathbb{Q}(\alpha)$ e existem exatamente n F-imersões $\sigma_i : F \to \mathbb{C}$. Além disso, $\alpha_i = \sigma_i(\alpha)$ são as raízes de $p = \mathrm{irr}(\alpha, \mathbb{Q})$. Neste caso,

$$\mathcal{B} = \{1, \alpha, \ldots, \alpha^{n-1}\}$$

é uma $\mathbb{Q}$-base de F como espaço vetorial sobre $\mathbb{Q}$ e, pelo item 2. da Proposição 1.14, o discriminante de p é

$$D_{\mathcal{B}} = \Delta(\mathcal{B}) = (-1)^{\frac{n(n-1)}{2}} N(p'(\alpha)) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

Seja F qualquer corpo de números. Então

$$\mathcal{O}_n = \mathbb{Z}_K = F \cap \overline{\mathbb{Z}}$$

é chamado o *anel dos inteiros* de F, onde

$$\overline{\mathbb{Z}} = \{\theta \in \mathbb{C} : \theta \text{ é um inteiro algébrico}\}.$$

Pela Proposição 1.16, se $\alpha \in F$, então existe $a \in \mathbb{Z}$ tal que $a\alpha \in \mathcal{O}_n$. Além disso, se $\alpha \in \mathcal{O}_n$, então $\mathrm{tr}(\alpha), N(\alpha) \in \mathbb{Z}$ e $F = \mathbb{Q}[\alpha]$, para algum $\alpha \in \overline{\mathbb{Z}}$.

Proposição 2.1 *Sejam $d \in \mathbb{Z} - \{0,1\}$ livre de quadrados, $F = \mathbb{Q}(\sqrt{d})$ e $\mathcal{O}_d$ o seu anel de inteiros. Então*:

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & se\ d \not\equiv 1 (\mathrm{mod}\, 4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & se\ d \equiv 1 (\mathrm{mod}\, 4) \end{cases}.$$

Prova Suponhamos que

$$\alpha = a + b\sqrt{d} \in F, b \neq 0.$$

Então é fácil verificar que

$$p = \mathrm{irr}(\alpha, \mathbb{Q}) = x^2 - 2ax + (a^2 - db^2) \in \mathbb{Q}[x].$$

Logo, pela Proposição 1.16, $\alpha \in \overline{\mathbb{Z}}$ se, e somente se,

$$2a \in \mathbb{Z} \text{ e } a^2 - db^2 \in \mathbb{Z}.$$

Assim, há dois casos a ser considerado:

1º **Caso**. Se $a \in \mathbb{Z}$, então $c = db^2 \in \mathbb{Z}^*$. Seja

$$b = \frac{r}{s} \in \mathbb{Q},$$

com $r, s \in \mathbb{Z}$ e $\mathrm{mdc}(r,s) = 1$. Então

$$cs^2 = dr^2.$$

Assim, se p é um fator primo de s, então $p^2 \mid d$, o que é impossivel, pois d é livre de quadrados. Portanto, $s = \pm 1$ e, assim, $b \in \mathbb{Z}$.

2º **Caso**. Se $a \notin \mathbb{Z}$, então existe um inteiro ímpar $c \in \mathbb{Z}$ tal que

$$a = \frac{c}{2},$$

digamos $c = 2u + 1$. Logo,

$$db^2 \in \mathbb{Z} + a^2 = \mathbb{Z} + \frac{4u^2 + 4u + 1}{4} = \mathbb{Z} + \frac{1}{4},$$

isto é,

$$db^2 = k + \frac{1}{4}, k \in \mathbb{Z}.$$

Seja

$$b = \frac{r}{s} \in \mathbb{Q},$$

com $r, s \in \mathbb{Z}$ e $\text{mdc}(r, s) = 1$. Então

$$4dr^2 = (4k+1)s^2.$$

Como d é livre de quadrado e $\text{mdc}(r, s) = 1$ temos que $s^2 = 4$, ou seja, $s = \pm 2$ e r ímpar. Logo,

$$b = \frac{2e+1}{2}, e \in \mathbb{Z}.$$

Assim,

$$a^2 - db^2 = \frac{4d^2 + 4d + 1}{4} - d\frac{4e^2 + 4e + 1}{4} \in \mathbb{Z} + \frac{1-d}{4}.$$

Logo, $d \equiv 1 (\text{mod}\, 4)$. Portanto, $\overline{\mathbb{Z}} \subseteq \mathcal{O}_d$. Por outro lado, é fácil verificar que

$$\sqrt{d} \text{ e } \frac{1+\sqrt{d}}{2}$$

são inteiros sobre $\mathbb{Z}$. Portanto, $\mathcal{O}_d \subseteq \overline{\mathbb{Z}}$. ■

Uma $\mathbb{Q}$-base de F

$$\{\alpha_1, \ldots, \alpha_n\}$$

é chamada *base integral* para $\mathcal{O}_n$ se $\alpha_i \in \mathcal{O}_n$, $i = 1, \ldots, n$, e todo $\alpha \in \mathcal{O}_n$ pode ser escrito de modo único na forma

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n,$$

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

Teorema 2.1 *Sejam F um corpo de números e $\mathcal{O}_n$ o seu anel de inteiros. Então existe uma $\mathbb{Q}$-base*

$$\{\alpha_1, \ldots, \alpha_n\}$$

para F, a qual é uma $\mathbb{Z}$-base para $\mathcal{O}_n$, de modo que

$$\mathcal{O}_n = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n,$$

isto é, $(\mathcal{O}_n, +)$ é um grupo abeliano livre de posto n.

Prova. Pela proposição 1.18, $\mathcal{O}_n$ está contido em um $\mathbb{Z}$-módulo finitamente gerado. Assim, $\mathcal{O}_n$ é um $\mathbb{Z}$-módulo finitamente gerado. Logo, existem elementos $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_n$ tais que

$$\mathcal{O}_n = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m.$$

Além disso, $\mathcal{O}_n$ é livre de torção e, assim, $\mathcal{O}_n$ é um grupo abeliano livre. É claro que

$$\{\alpha_1, \ldots, \alpha_m\}$$

é um conjunto linearmente independente sobre $\mathbb{Q}$. Logo,

$$\{\alpha_1, \ldots, \alpha_n\}$$

é uma $\mathbb{Q}$-base para F. ■

Exemplo 2.1 *Seja $F = \mathbb{Q}(\sqrt{n})$ e $\mathcal{O}_n$ o seu anel de inteiros. Então*

$$\{1, \sqrt{n}\}$$

é uma $\mathbb{Z}$-base para $\mathcal{O}_n$ se $n \not\equiv 1 (\mathrm{mod}\, 4)$ e

$$\left\{1, \frac{1+\sqrt{n}}{2}\right\}$$

é uma $\mathbb{Z}$-base para $\mathcal{O}_n$ se $n \equiv 1 (\mathrm{mod}\, 4)$.

Lema 2.1 *Sejam F um corpo de números, $\mathcal{O}_n$ o seu anel de inteiros e P um ideal primo não nulo de $\mathcal{O}_n$. Então*:

1. *$P \cap \mathbb{Z} = p\mathbb{Z}$, onde p é número primo em P.*

2. *$\frac{\mathcal{O}_n}{P}$ é uma extensão finita de $\mathbb{Z}_p$. Neste caso,*

$$[\frac{\mathcal{O}_n}{P} : \mathbb{Z}_p] = h$$

é chamado o grau de inércia de P e $\frac{\mathcal{O}_n}{P}$ tem p^h elementos. ■

Teorema 2.2 *Sejam F um corpo de números e*

$$\{\alpha_1, \ldots, \alpha_n\}$$

uma base integral para F. Se I é um ideal de $\mathcal{O}_n$, então existe uma base

$$\{\beta_1, \ldots, \beta_n\}$$

para I da forma

$$\begin{aligned}\beta_1 &= a_{11}\alpha_1\\ \beta_2 &= a_{21}\alpha_1 + a_{22}\alpha_2\\ &\vdots\\ \beta_n &= a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n,\end{aligned}$$

onde $a_{ij} \in \mathbb{Z}$ com $0 \leq a_{ij} < a_{jj}$, $j = 1, \ldots, n$. Neste caso, a norma do ideal I é dada por

$$N(I) = \frac{\Delta(\beta_1, \ldots, \beta_n)}{\Delta(\alpha_1, \ldots, \alpha_n)} = \prod_{i=1}^{n} a_{ii}.$$

Prova. Seja

$$I_n = \{b_n \in \mathbb{Z} : \gamma = b_1\alpha_1 + \cdots + b_n\alpha_n, \ \forall \ \gamma \in I\}.$$

Então I_n é um ideal não nulo $\mathbb{Z}$. Como $\mathbb{Z}$ é um domínio de ideais principais temos que existe um menor inteiro positivo $a_{nn} \in \mathbb{Z}$ tal que $I_n = \langle a_{nn} \rangle$. Escolhendo $\gamma_n \in I$ tal que

$$\gamma_n = a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n.$$

Agora, seja

$$I_{n-1} = \{b_{n-1} \in \mathbb{Z} : \gamma = b_1\alpha_1 + \cdots + b_{n-1}\alpha_{n-1} + b_n\alpha_n, \ b_n = 0, \ \forall \ \gamma \in I\}.$$

Então I_{n-1} é um ideal não nulo $\mathbb{Z}$. Como $\mathbb{Z}$ é um domínio de ideais principais temos que existe um menor inteiro positivo $a_{(n-1)(n-1)} \in \mathbb{Z}$ tal que $I_{n-1} = \langle a_{(n-1)(n-1)} \rangle$. Escolhendo $\gamma_{n-1} \in I$ tal que

$$\gamma_{n-1} = a_{(n-1)1}\alpha_1 + a_{(n-1)2}\alpha_2 + \cdots + a_{(n-1)(n-1)}\alpha_{n-1}.$$

Continuando dessa maneira, obtemos uma base

$$\{\gamma_1, \ldots, \gamma_n\}$$

para I. Finalmente, pelo algoritmo da divisão, obtemos $q_i, r_{ij} \in \mathbb{Z}$ tais que

$$a_{ij} = q_i a_{jj} + r_{ij}, \ \text{ onde } \ 0 \leq r_{ij} < a_{jj}.$$

Assim, multiplicando γ_i por $-q_i$ e somado com γ_{i+1}, obtemos a base desejada

$$\begin{aligned}\beta_1 &= a_{11}\alpha_1\\ \beta_2 &= a_{21}\alpha_1 + a_{22}\alpha_2\\ &\vdots\\ \beta_n &= a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n,\end{aligned}$$

onde $a_{ij} \in \mathbb{Z}$ com $0 \leq a_{ij} < a_{jj}$, $j = 1, \ldots, n$, para I. ■

Corolário 2.1 *Sejam F um corpo de números e $\mathcal{O}_n$ o seu anel de inteiros. Se I é um ideal não nulo em F, então o índice de I em $\mathcal{O}_n$ é o número das classes laterais de $\mathcal{O}_n$ em I.*

Prova. Seja k o índice de I em $\mathcal{O}_n$. Então, pelo Teorema 2.1, obtemos

$$k = \prod_{i=1}^{n} a_{ii}.$$

Afirmação. O conjunto

$$R_0 = \{c_1\alpha_1 + \cdots + c_n\alpha_n, 0 \leq c_i < a_{ii}, 1 \leq i \leq n\}$$

é um sistema completo de representantes de classes laterais de I em $\mathcal{O}_n$.
De fato, seja

$$\alpha = b_1\alpha_1 + \cdots + b_n\alpha_n$$

um elemento qualquer de $\mathcal{O}_n$. Dividindo b_1 por a_{11}, obtemos

$$b_1 = a_{11}q_1 + r_1, 0 \leq r_1 < a_{11}.$$

Então

$$\alpha - q_1\beta_1 - r_1\alpha_1 = b_2\alpha_2 + \cdots + b_n\alpha_n.$$

Dividindo b_2 por a_{22}, obtemos

$$b_2 = a_{22}q_2 + r_2, 0 \leq r_2 < a_{22}.$$

Então

$$\alpha - q_1\beta_1 - r_1\alpha_1 - q_2\beta_2 - r_2\alpha_2 = b_3\alpha_3 + \cdots + b_n\alpha_n.$$

Continuando este processo, obtemos

$$\alpha - \left(\sum_{i=1}^{n} q_i\beta_i\right) - \left(\sum_{i=1}^{n} r_i\alpha_i\right) = 0,$$

isto é,

$$\alpha = \beta + \delta,$$

onde $\beta \in I$ e $\delta \in R_0$. Suponhamos que

$$(\delta + I) \cap (\delta' + I) \neq \emptyset.$$

Então existem

$$\delta = \sum_{i=1}^{n} r_i\alpha_i, \delta' = \sum_{i=1}^{n} r'_i\alpha_i \in R,$$

distintos, tais que $\delta - \delta' \in I$. Seja s o primeiro índice $(1 \leq s \leq n)$ tal que $r_s \neq r'_s$. Então,

$$\sum_{i=s}^{n}(r_i - r'_i)\alpha_i = \sum_{i=1}^{n} b_i\beta_i.$$

Como

$$\beta_i = \sum_{j=1}^{i} a_{ij}\alpha_j,$$

temos que $b_1 = \cdots = b_{s-1} = 0$ e $a_{ss}b_s = r_s - r'_s$, que é uma contradição, pois

$$0 < |r_s - r'_s| < a_{ss} \Rightarrow 0 < b_s < 1.$$

Portanto, $k = [\mathcal{O}_n : I]$. ■

Sejam F um corpo de número e $\sigma_i : F \to \mathbb{C}$, $i = 1, \ldots, n$, as F-imersões. Não é difícil verificar que os conjugados $\sigma_i(\alpha) = \alpha_i$ de α não necessita ser elemento de F. Assim, dizemos que σ_i é *real* se $\sigma_i(F) \subseteq \mathbb{R}$, caso contrário, é *complexo*. É claro que se σ_i é complexo, então $\overline{\sigma}_i : F \to \mathbb{C}$ definida por $\overline{\sigma}_i(\beta) = \overline{\sigma_i(\beta)}$ é um homomorfismo injetivo tal que $\overline{\sigma}_i \neq \sigma_i$ e $\overline{\sigma}_i^2 = \sigma_i$. Assim, denotarermos os homomorfismos reais por $\sigma_1, \ldots, \sigma_k$, os complexos por $\sigma_{k+1}, \overline{\sigma}_{k+1}, \ldots, \sigma_{k+l}, \overline{\sigma}_{k+l}$ e $n = k + 2l$.

Proposição 2.2 *Sejam F um corpo de números e $\psi : F \to \mathbb{R}^n$ definida por*

$$\psi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_k(\alpha), \sigma_{k+1}(\alpha), \overline{\sigma}_{k+1}(\alpha), \ldots, \sigma_{k+l}(\alpha), \overline{\sigma}_{k+l}(\alpha)).$$

Então:

1. *ψ é um homomorfismo injetor.*

2. *$\psi(a\alpha) = a\psi(\alpha)$ para todo $a \in \mathbb{Q}$ e $\alpha \in F$.* ■

Corolário 2.2 *Sejam F um corpo de números e $\{\alpha_1, \ldots, \alpha_n\}$ é uma $\mathbb{Q}$-base para F. Então $\{\psi(\alpha_1), \ldots, \psi(\alpha_n)\}$ é linearmente independente sobre $\mathbb{R}$.* ■

Exemplo 2.2 *Sejam $F = \mathbb{Q}[i]$, $\mathcal{O}_2 = \mathbb{Z}[i]$ e $p = \text{irr}(i, \mathbb{Q}) = x^2 + 1$. Sejam $B = \{1, i\}$ uma base integral para $\mathcal{O}_2$ e $\sigma : F \to \mathbb{C}$ um homomorfismo injetor. Então dado $\alpha \in F$, digamos $\alpha = a + bi$, com $a, b \in \mathbb{Q}$, obtemos*

$$\sigma(\alpha) = a + b\sigma(i).$$

Também

$$-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2.$$

Logo, $\psi(i) = i$ *ou* $\psi(i) = -i$. *Portanto,*

$$\sigma(\alpha) = \alpha \ \ ou \ \ \sigma(\alpha) = \overline{\alpha}.$$

Assim, existem somente dois homomorfismos injetores $\sigma, \overline{\sigma} : K \to \mathbb{C}$. *Logo,* $\varphi : K \to \mathbb{R}^2$ *definida por*

$$\psi(\alpha) = (\mathrm{Re}(\sigma(\alpha)), \mathrm{Im}(\sigma(\alpha)))$$

é um homomorfismo injetor e $\mathbb{Z}^2 = \varphi(\mathcal{O}_2)$ *é um reticulado* ($\mathbb{Z}$*-submódulo*) *de* $\mathbb{R}^2$ *gerado por* $\psi(1)$ *e* $\psi(i)$, *isto é,*

$$\mathcal{B}' = \{(1,0), (0,1)\}$$

é uma $\mathbb{Z}$*-base para* $\mathbb{Z}^2$.

2.2 Raízes da Unidade

Seja F uma extensão de K. Dizemos que $\zeta_n \in F$ é uma *raiz n-ésima da unidade* se ζ_n é raiz do polinômio

$$f = x^n - 1 \in K[x].$$

O conjunto

$$U(n, K) = \{\zeta_n \in K : \zeta_n^n = 1\},$$

é chamado o *conjunto das raízes n-ésimas das unidades* de K e é um subgrupo cíclico de K^* de ordem no máximo n. Neste caso,

$$U(K) = \bigcup_{n \in \mathbb{N}} U(n, K).$$

Se $\zeta_n^n = 1$, mas $\zeta_n^k \neq 1$, para $1 \leq k \leq n-1$, dizemos que ζ_n é uma *raiz n-ésima primitiva da unidade* e denotamos por

$$P(n, K).$$

Proposição 2.3 *Seja* F *uma extensão de* K.

1. *Se* $d \mid n$, *então*

$$U(d, K) \subseteq U(n, K).$$

2. *Se a caracteristica de* K *é* $p > 0$ *e* $n = p^e m$ *com* $p \nmid m$, *então*

$$U(m, K) = U(n, K).$$

Neste caso, $P(n, K) = \emptyset$.

3. $U(n, K) = U(n, F) \cap K$. ■

Proposição 2.4 *Sejam* F *uma extensão de* K *e* $n \in \mathbb{N}$. *Então as seguintes condições são equivalentes*:

1. $P(n, K) \neq \emptyset$.
2. *O número de raízes* n*-ésimas primitivas da unidade em* K *é igual* $\varphi(n)$, *onde* φ *é a função de Euler.*
3. $|U(n, K)| = n$.
4. *Os geradores do grupo cíclico* $U(n, K)$ *são exatamente as raízes* n*-ésimas primitivas da unidade.* ■

Proposição 2.5 *Sejam* F *uma extensão de* K *e* $n \in \mathbb{N}$. *Então as seguintes condições são equivalentes*:

1. $P(n, F) \neq \emptyset$.
2. *O polinômio* $x^n - 1 \in K[x]$ *não tem raízes múltiplas.*
3. *A característica* K *não divide* n.

Neste caso, $P(d, F) \neq \emptyset$, *para todo* $d \mid n$ *e*

$$U(n, F) = \bigcup_{d|n} P(d, F).$$

■

Teorema 2.3 *Sejam* K *é um corpo e* F *um corpo de decomposição de* $x^n - 1 \in K[x]$.

1. *Se característica de* K *é zero, então*

$$\mathrm{Gal}\,(F/K) \simeq H \leq U\,(\mathbb{Z}_n)\,.$$

Neste caso, $|\mathrm{Gal}\,(F/K)| \leq \phi(n)$.

2. Se característica de K é $p > 0$, então

$$\mathrm{Gal}\,(F/K) \simeq H \leq U\,(\mathbb{Z}_m)\,,$$

onde $n = p^e m$ com $\mathrm{mdc}(m, p) = 1$. Neste caso, $|\mathrm{Gal}\,(F/K)| \leq \varphi(m)$.

Prova. Primeiro note que se a característica de K é $p > 0$ e $n = p^e m$ com $\mathrm{mdc}(m, p) = 1$, então pelo item 2. da Proposição 2.3, $x^m - 1$ e $x^n - 1$ têm o mesmo grupo de Galois. Assim, não há perda de generalidade, em supor que $m = n$. Seja $F = K\,(\zeta_n)$ um corpo de decomposição de $x^n - 1$, onde $\zeta_n \in P(n.K)$. Então cada $\sigma \in \mathrm{Gal}\,(F/K)$ é completamente determinado por $\sigma\,(\zeta_n)$. Como $\sigma\,(\zeta_n) \in P(n.K)$ temos que $\sigma\,(\zeta_n) = \zeta_n^k$, com $1 \leq k < n$ e $\mathrm{mdc}\,(k, n) = 1$.

Afirmação. A função $\psi : \mathrm{Gal}\,(F/K) \to U\,(\mathbb{Z}_n)$ definida por

$$\psi\,(\sigma) = \overline{k},$$

onde $\sigma\,(\zeta_n) = \zeta_n^k$ e $\mathrm{mdc}\,(k, n) = 1$, é um homomorfismo de grupos injetor.
De fato, dados $\sigma, \tau \in \mathrm{Gal}\,(F/K)$ com $\sigma\,(\zeta_n) = \zeta_n^k$ e $\tau\,(\zeta_n) = \zeta_n^l$, obtemos

$$\sigma\tau\,(\zeta_n) = \sigma(\tau\,(\zeta_n)) = \sigma\left(\zeta_n^l\right) = \zeta_n^{kl} = \tau\sigma\,(\zeta_n)\,.$$

Logo,

$$\psi\,(\sigma\tau) = \overline{kl} = \overline{kl} = \psi\,(\sigma)\,\psi\,(\tau)\,.$$

Além disso,

$$\sigma \in \ker\psi \Rightarrow \psi\,(\sigma) = \overline{1} \Rightarrow \sigma\,(\zeta_n) = \zeta_n \Rightarrow \sigma = 1.$$

Logo, ψ é injetor. Portanto, pelo primeiro Teorema.de Homomorfismo de grupos, obtemos.

$$\mathrm{Gal}\,(F/K) \simeq H \leq U\,(\mathbb{Z}_n)\,.$$

■

2.3 Corpos Ciclotômicos

Nesta seção apresentaremos a classe de *corpos ciclotômico*, isto é, subcorpos $\mathbb{Q}(\zeta_n)$ de $\mathbb{C}$ gerados por uma raiz da unidade ζ_n.

Seja F um corpo de números com $P(n, F) \neq \emptyset$. O polinômio

$$\Phi_n = \prod_{\zeta_n \in P(n,F)} (x - \zeta_n)$$

é chamado o *n-ésimo polinômio ciclotômico* sobre F. É claro que seu grau é $\varphi(n)$.

Proposição 2.6 *Seja F um corpo de números com $P(n,F) \neq \emptyset$. Então*

1. $$x^n - 1 = \prod_{d|n} \Phi_d.$$

2. *Se $n \geq 2$, então $\Phi_1(0) = -1$ e $\Phi_n(0) = 1$.*

3. $\Phi_n \in \mathbb{Z}[x]$.

4. *Se $n > 1$ é ímpar, então $\Phi_{2n}(x) = \Phi_n(-x)$.*

Prova. Vamos provar apenas o item 1., 3 e 4. Como as raízes do polinômio $x^n - 1$ são os elementos do conjunto $U(n,F)$ temos que

$$x^n - 1 = \prod_{\zeta_n \in U(n,F)} (x - \zeta_n).$$

Assim, agrupamos os fatores $x - \zeta_n$, onde ζ_n é um elemento de ordem d em $U(n,F)$, obtemos

$$x^n - 1 = \prod_{d|n} \prod_{\zeta_n \in P(d,F)} (x - \zeta_n) = \prod_{d|n} \Phi_d.$$

3. Se $n = 1$, então $\Phi_1 = x - 1 \in \mathbb{Z}[x]$. Suponhamos que $n \geq 2$ e que o resultado seja válido para todo k com $1 \leq k < n$. Pelo item 1., obtemos

$$x^n - 1 = \Phi_n g,$$

onde $g \in \mathbb{Z}[x]$, pela hipótese de indução. Portanto,

$$\Phi_n = \frac{x^n - 1}{g} \in \mathbb{Z}[x]$$

4. Primeiro note que $\partial(\Phi_{2n}) = \varphi(2n) = \varphi(n) = \partial(\Phi_n) = \partial(\Phi_n(-x))$. Como o coeficiente líder de Φ_n é igual a 1 temos que o coeficiente líder de $\Phi_n(-x)$ é igual a $(-1)^{\varphi(n)} = 1$ que é o coeficiente líder de Φ_{2n}. Por outro lado, se α é uma raiz de Φ_{2n}, então $-\alpha$ é uma raiz de Φ_n, isto é, Φ_{2n} divide $\Phi_n(-x)$. Portanto, $\Phi_{2n}(x) = \Phi_n(-x)$. ■

Note que a fatoração

$$x^n - 1 = \prod_{d|n} \Phi_d.$$

permite calcular recursivamte Φ_n, para todo $n \in \mathbb{N}$. É claro que $\Phi_1 = x - 1$ e $\Phi_2 = x + 1$. Então

$$x^3 - 1 = \Phi_1 \Phi_3 \Rightarrow \Phi_3 = x^2 + x + 1.$$

Lema 2.2 *Sejam $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$ e $f = \text{irr}(\zeta_n, \mathbb{Q})$. Seja p um número primo tal que $p \nmid n$. Então α^p é uma raiz de f, para toda raiz α de f.*

Prova. Pelo item 3. da Proposição 1.17, temos que $f \in \mathbb{Z}[x]$. Como $\Phi_n(\zeta_n) = 0$ temos que f divide Φ_n em $\mathbb{Z}[x]$, digamos $\Phi_n = fg$, onde $g \in \mathbb{Z}[x]$ é mônico. Se $f(\alpha) = 0$, então $\Phi_n(\alpha) = 0$, de modo que $\alpha \in P(n, \mathbb{C})$.Assim, $\alpha^p \in P(n, \mathbb{C})$, pois $\text{mdc}(p, n) = 1$. Logo, $f(\alpha^p) = 0$ ou $g(\alpha^p) = 0$.

Afirmação. $f(\alpha^p) = 0$ e $g(\alpha^p) \neq 0$

De fato, suponhamos, por absurdo, que $f(\alpha^p) \neq 0$. Então $g(\alpha^p) = 0$. Logo, α é raiz do polinômio $\widehat{g}(x) = g(x^p) \in \mathbb{Z}[x]$, isto é, f divide $\widehat{g}$ em $\mathbb{Z}[x]$, digamos $\widehat{g} = fh$, onde $h \in \mathbb{Z}[x]$ é mônico. Agora, como $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ é um homomorfismo de anéis temos que $\sigma^* : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ definido por

$$\sigma^*\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} \sigma(a_j) x^j$$

é um homomorfismo de anéis. Logo, pelo item 2. do Lema 1.2, obtemos

$$(\sigma^*(g(x)))^p = \sigma^*(g(x)^p) = \sigma^*(g(x^p)) = \sigma^*(\widehat{g}(x)).$$

Assim,

$$(\sigma^*(g(x)))^p = \sigma^*(f(x))\sigma^*(h(x)).$$

Sendo $\mathbb{Z}_p[x]$ um domínio de fatoração única temos que $\sigma^*(g(x))$ e $\sigma^*(f(x))$ possui um fator comum próprio. Portanto,

$$\sigma^*(\Phi_n) = \sigma^*(f(x))\sigma^*(g(x))$$

tem uma raiz múltipla o que é uma contradição, pois $x^n - 1$ é separável sobre $\mathbb{Z}_p$. ■

Teorema 2.4 *Todos os polinômios ciclotômico sobre $\mathbb{Q}$ são irredutíveis*

Prova. Sejam $\Phi_n \in \mathbb{Z}[x]$ o n-ésimo polinômio ciclotômico, $\zeta_n \in P(n, \mathbb{C})$ e $f = \text{irr}(\zeta_n, \mathbb{Q}) \in \mathbb{Q}[x]$. Então f divide Φ_n.

Afirmação. $f = \Phi_n$.

De fato, se $\alpha \in P(n, \mathbb{C})$, então $\alpha = \zeta_n^k$ com $\text{mdc}\,(k, n) = 1$. Seja

$$k = p_1 p_2 \cdots p_r$$

a fatoração de k em números primos (não necessariamente distintos). Pelo Lema 2.2, obtemos $f(\zeta_n^{p_1}) = 0$. Novamente, pelo Lema 2.2, obtemos $f((\zeta_n^{p_1})^{p_2}) = 0$. Continuando este procedimento, obtemos

$$f(\zeta_n^{p_1 p_2 \cdots p_r}) = 0 = f(\zeta_n^k).$$

Logo, qualquer raiz n-ésima primitiva da unidade é raiz de f. Portanto, $f = \Phi_n$. ■

Teorema 2.5 *Seja $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$. Então*

$$\mathrm{Gal}(F/\mathbb{Q}) \simeq U(\mathbb{Z}_n).$$

Prova. Pela prova do Teorema 2.3 sabemos que a função $\psi : \mathrm{Gal}(F/K) \to U(\mathbb{Z}_n)$ definida por

$$\psi(\sigma) = \overline{k},$$

onde $\sigma(\zeta_n) = \zeta_n^k$ e $\mathrm{mdc}(k, n) = 1$, é um homomorfismo de grupos injetor. Assim, basta mostrar que ψ é sobrejetor. Como Φ_n é irredutível sobre $\mathbb{Q}$ temos que $\mathrm{Gal}(F/\mathbb{Q})$ age transitivamente nas raízes de Φ_n. Assim, dado $\overline{k} \in U(\mathbb{Z}_n)$, existe $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ tal que $\psi(\sigma) = \overline{k}$, isto é, ψ é sobrejetor. Portanto,

$$\mathrm{Gal}(F/\mathbb{Q}) \simeq U(\mathbb{Z}_n).$$

■

Corolário 2.3 *Seja $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$. Então* $\mathrm{Gal}(F/\mathbb{Q})$ *é cíclico se $n = 4$ ou p^e ou $2p^e$ com p primo ímpar. Além disso,* $\mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle$, *onde $\sigma(\zeta_n) = \zeta_n^{-1}$ e $\tau(\zeta_n) = \zeta_n^5$ se $n = 2^t$, $t \geq 3$.* ■

Teorema 2.6 *[14, 7-5-4 Theorem.] Seja $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$. Então o conjunto*

$$\{1, \zeta_n, \ldots, \zeta_n^{d-1}\}$$

é uma base integral para $\mathcal{O}_n$, onde $d = \varphi(n)$. Neste caso, $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$. ■

Teorema 2.7 *[14, 7-2-4 Theorem.] Sejam $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$ e p um número primo tal que $p \nmid n$, Então o ideal $p\mathbb{Z}[\zeta_n]$ em $\mathcal{O}_n$ fatora-se como*

$$p\mathbb{Z}[\zeta_n] = P_1 \cdots P_r,$$

onde $P_1, \ldots, P_r$ são ideais primos distintos de $\mathbb{Z}[\zeta_n]$ de grau de inércia h, com $hr = \varphi(n)$ e h o menor inteiro positivo tal que

$$p^h \equiv 1 (\mathrm{mod}\, n).$$

■

Teorema 2.8 *[14, 7-4-3 Theorem.] Sejam $F = \mathbb{Q}(\zeta_n)$, onde $\zeta_n \in P(n, \mathbb{C})$ e $n = p^e m$ com $\mathrm{mdc}(m, p) = 1$. Então o ideal $p\mathbb{Z}[\zeta_n]$ em $\mathcal{O}_n$ fatora-se como*

$$p\mathbb{Z}[\zeta_n] = (P_1 \cdots P_r)^{\varphi(p^e)},$$

onde $P_1, \ldots, P_r$ são ideais primos distintos de $\mathbb{Z}[\zeta_n]$ de grau inércia h, com $hr = \varphi(m)$ e h o menor inteiro positivo tal que

$$p^h \equiv 1 (\mathrm{mod}\, m).$$

Neste caso, a função

$$\sigma : \frac{\mathbb{Z}[\zeta_n]}{P_j} \to \mathbb{Z}_p(\zeta_m) = \mathbb{F}$$

definida por $\sigma(\zeta_n + P_j) = \zeta_m$, $j = 1, \ldots, r$, é um isomorfismo de corpos e

$$\sigma\left(\sum_{i=0}^{d-1} a_i(\zeta_n + P_j)^i\right) = \sum_{i=0}^{d-1} a_i \zeta_m^i.$$

Mais ainda,

$$\sum_{i=0}^{d-1} a_i \zeta_m^i \leftrightarrow (a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d.$$

■

Capítulo 3

Códigos

O objetivo deste capítulo é estudar, sobre certas condições, o peso de Mannheim de um código sob um grupo abeliano qualquer.

3.1 Distâncias

Seja A um grupo abeliano (aditivo) qualquer. Um *peso* sobre A é uma função

$$\omega : A \to \mathbb{R}$$

tal que as seguintes condições são satisfeitas:

1. $\omega(a) \geq 0$, para todo $a \in A$;
2. $\omega(a) = 0$ se, e somente se, $a = 0$;
3. $\omega(-a) = \omega(a)$, para todo $a \in A$;
4. $\omega(a + b) \leq \omega(a) + \omega(b)$, para todos $a, b \in A$.

A *distância* entre dois elementos $a, b \in A$ é definida por

$$d(a, b) = \omega(a - b).$$

É fácil verificar que:

1. $d(a, b) \geq 0$, para todos $a, b \in A$;
2. $d(a, b) = 0$ se, e somente se, $a = b$;

3. $d(a,b) = d(b,a)$, para todos $a, b \in A$;

4. $d(a,b) \leq d(a,c) + d(c,b)$, para todos $a, b, c \in A$.

Seja $G = A^l$ o produto (a soma) direta de l cópias de A. Então é fácil verificar que a função $\widetilde{\omega} : G \to \mathbb{R}$ definida por

$$\widetilde{\omega}(\mathbf{a}) = \sum_{i=1}^{l} \omega(a_i), \mathbf{a} = (a_1, \ldots, a_l) \in G,$$

é um peso sobre G. Portanto,

$$d(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{l} d(a_i, b_i)$$

é uma distância entre $\mathbf{a} = (a_1, \ldots, a_l), \mathbf{b} = (b_1, \ldots, b_l) \in G$.

Exemplo 3.1 *Sejam A um grupo abeliano qualquer e $\omega_H : A \to \mathbb{R}$ a função definida por*

$$\omega_H(a) = \begin{cases} 0 & se\ a = 0 \\ 1 & se\ a \neq 0 \end{cases}.$$

Então ω_H é um peso sobre A, o qual será chamado de peso de Hamming.

Sejam A um grupo abeliano qualquer e ω um peso sobre A. Dizemos que ω é *consecutivo* se para qualquer $a \in A$ existe uma cadeia

$$0 = a_0, a_1, \ldots, a_{\omega(a)} = a, \text{ com } \omega(a) \in \mathbb{Z}_+,$$

tal que

$$\omega(a_j - a_{j-1}) = 1, \text{ para todo } j = 1, \ldots, \omega(a).$$

Proposição 3.1 *Sejam A um grupo abeliano qualquer e ω um peso sobre A. Então as seguintes condições são equivalentes*:

1. *ω é consecutivo.*

2. *Para qualquer $a \in A$, com $\omega(a) > 0$, existe $b \in A$ tal que $\omega(a - b) = 1$ e $\omega(b) = \omega(a) - 1$;*

3. *Para quaisquer $a, b \in A$, e $d = \omega(a - b)$, existe uma cadeia*

$$a = a_0, a_1, \ldots, a_d = b \in A$$

tal que $\omega(a_j - a_{j-1}) = 1$, $j = 1, \ldots, d$;

4. *Para quaisquer $a, b \in A$, com $d = \omega(a-b)$, e qualquer inteiro g com $0 \leq g \leq d$, existe $c \in A$ tal que $\omega(a-c) = g$ e $\omega(c-b) = d-g$.*

Prova. (1. $\Rightarrow$ 2.) Dado $a \in A$ existe, por hipótese, uma cadeia

$$0 = a_0, a_1, \ldots, a_d = a,$$

onde $d = \omega(a) > 0$. Assim, é suficiente provar que

$$\omega(a_{d-1}) = d - 1,$$

pois $\omega(a_d - a_{d-1}) = 1$. Como

$$a_{d-1} = a_1 + (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_{d-1} - a_{d-2})$$

e $\omega(c) = \omega(-c)$ temos que

$$\omega(a_{d-1}) \leq \omega(a_1) + \omega(a_2 - a_1) + \cdots + \omega(a_{d-1} - a_{d-2}) = d - 1$$

Por outro lado,

$$d = \omega(a) = \omega(a - a_{d-1} + a_{d-1}) \leq \omega(a - a_{d-1}) + \omega(a_{d-1}) = 1 + \omega(a_{d-1}),$$

isto é, $d - 1 \leq \omega(a_{d-1})$. Portanto,

$$\omega(a_{d-1}) = d - 1$$

(2 $\Rightarrow$ 1.) Dado $a \in A$ com $d = \omega(a) > 0$ existe, por hipótese, $b \in A$ tal que

$$\omega(a - b) = 1 \text{ e } \omega(b) = \omega(a) - 1.$$

Agora, vamos usar indução sobre $\omega(a) = d$. Se $d = 1$, então existe uma cadeia

$$0 = b = a_0, a_1 = a$$

tal que

$$\omega(a_1 - a_0) = 1.$$

Suponhamos que $d \geq 2$ e que o resultado seja válido para todo k com $1 \leq k \leq d - 1$. Como $\omega(b) = \omega(a) - 1 = d - 1$ temos, por hipótese de indução, que existe uma cadeia

$$0 = a_0, a_1, \ldots, a_{d-1} = b$$

tal que

$$\omega(a_j - a_{j-1}) = 1, j = 1, \ldots, d-1.$$

Assim, fazendo $a_d = a$, obtemos a cadeia

$$0 = a_0, a_1, \ldots, a_{d-1}, a_d = a$$

tal que

$$\omega(a_j - a_{j-1}) = 1, j = 1, \ldots, d.$$

(1. $\Rightarrow$ 3.) Dados $a, b \in A$ com $d = \omega(a - b)$. Então, fazendo $c = b - a$, obtemos por hipótese uma cadeia

$$0 = c_0, c_1, \ldots, c_d = c$$

tal que

$$\omega(c_j - c_{j-1}) = 1, j = 1, \ldots, d$$

Definido $a_j = c_j + a$, $j = 1, \ldots, d$, obtemos a cadeia

$$a = a_0, a_1, \ldots, a_{d-1}, a_d = b$$

tal que

$$\omega(a_j - a_{j-1}) = 1, j = 1, \ldots, d.$$

(3. $\Rightarrow$ 1.) Basta tomar $b = 0$.

(3. $\Rightarrow$ 4.) Sejam $a, b \in A$ com $\omega(a - b) = d$ e $g \in \mathbb{Z}$ tal que $0 \leq g \leq d$. Então por hipótese existe uma cadeia

$$a = a_0, a_1, \ldots, a_d = b$$

tal que

$$\omega(a_j - a_{j-1}) = 1, j = 1, \ldots, d.$$

Seja $c = a_g \in A$. Então

$$a - c = a - a_1 + a_1 - a_2 + \cdots + a_{g-1} - a_g.$$

Logo,

$$\omega(a - c) \leq \omega(a - a_1) + \omega(a_1 - a_2) + \cdots + \omega(a_{g-1} - a_g) = g.$$

Portanto,

$$\omega(a - c) \leq g.$$

De modo análogo

$$\omega(b-c) \leq d-g,$$

fazendo

$$a-b = a-c+c-b,$$

obtemos

$$\begin{aligned} d &= \omega(a-b) \\ &= \omega(a-c+c-b) \\ &\leq \omega(a-c)+\omega(c-b) \\ &\leq \omega(a-c)+d-g \\ &\Rightarrow \omega(a-c) \geq g. \end{aligned}$$

Portanto,

$$\omega(a-c) = g,$$

e também

$$\begin{aligned} d &= \omega(a-b) \\ &= \omega(a-b+c-c) \\ &\leq \omega(b-c)+\omega(a-c) \\ &= \omega(b-c)+g \\ &\Rightarrow \omega(b-c) \geq d-g. \end{aligned}$$

Portanto,

$$\omega(b-c) = d-g$$

(4. $\Rightarrow$ 2.) Basta tomar $b=0$ e $g=1$. ■

Corolário 3.1 *Sejam A um grupo abeliano qualquer e ω um peso consecutivo sobre A. Então a função $\widetilde{\omega} : A^l \to \mathbb{R}$ definida por*

$$\widetilde{\omega}(\mathbf{a}) = \sum_{i=1}^{l} \omega(a_i), \mathbf{a} = (a_1, \ldots, a_l) \in A^l,$$

é um peso consecutivo sobre A^l.

Prova. Dado

$$\mathbf{a} = (a_1, \ldots, a_l) \in A^l,$$

obtemos por definição

$$d = \widetilde{\omega}(\mathbf{a}) = \sum_{j=1}^{l} \omega(a_j) > 0.$$

Logo, existe $j \in \{1, 2, \ldots, l\}$ tal que $\omega(a_j) > 0$. Podemos supor, sem perda de generalidade, que $\omega(a_1) > 0$. Assim, pelo item 2 da Proposição 3.1, existe $b_1 \in A$ tal que

$$\omega(a_1 - b_1) = 1 \text{ com } \omega(b_1) = \omega(a_1) - 1.$$

Logo, existe

$$\mathbf{b} = (b_1, a_2, \ldots, a_n) \in A^l$$

tal que

$$\widetilde{\omega}(\mathbf{a} - \mathbf{b}) = 1 \text{ com } \widetilde{\omega}(\mathbf{b}) = \widetilde{\omega}(\mathbf{a}) - 1.$$

Portanto, $\widetilde{\omega}$ é um peso consecutivo sobre A^l. ■

Agora vamos estender as definições de peso e distância para $\mathbb{Z}[\zeta_n]$. É claro que a função $\omega_M : \mathbb{Z}[\zeta_n] \to \mathbb{R}$ definida por

$$\omega_M(\mathbf{a}) = \sum_{j=0}^{d-1} |a_j|,$$

onde

$$\mathbb{Z}[\zeta_n] \ni \mathbf{a} = \sum_{j=0}^{d-1} a_j \zeta_n^j \leftrightarrow (a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d \text{ e } d = \varphi(n),$$

é um peso sobre $\mathbb{Z}[\zeta_n]$, o qual será chamado de *peso de Manhattan*. A distância associada a este peso será chamada de *distância de Manhattan*. Note que o peso e a distância de Manhattan são inteiros positivos.

Sejam $P = P_1$ um ideal primo fixado em $\mathbb{Z}[\zeta_n]$,

$$\mathbb{F} = \mathbb{Z}_p(\zeta_m) \simeq \frac{\mathbb{Z}[\zeta_n]}{P} \text{ e } \overline{\mathbf{a}} \leftrightarrow \mathbf{a} + P.$$

Proposição 3.2 *A função $\omega_{\overline{M}} : \mathbb{F} \to \mathbb{R}$ definida por*

$$\omega_{\overline{M}}(\overline{\mathbf{a}}) = \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\}$$

é um peso sobre $\mathbb{F}$.

Prova. Note que o conjunto

$$\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\} \neq \emptyset.$$

É claro que $\omega_{\overline{M}}(\overline{\mathbf{a}}) \geq 0$ e $\omega_{\overline{M}}(\overline{\mathbf{a}}) = 0$ se, e somente se, $\overline{\mathbf{a}} = \overline{\mathbf{0}}$. Como $-\mathbf{a} + P = -(\mathbf{a} + P)$ temos que $-\overline{\mathbf{a}} = \overline{(-\mathbf{a})} \in \mathbb{F}$. Logo,

$$\begin{aligned} \omega_{\overline{M}}(-\overline{\mathbf{a}}) &= \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in -\mathbf{a} + P\} \\ &= \min\{\omega_M(-\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\} \\ &= \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\} \\ &= \omega_{\overline{M}}(\overline{\mathbf{a}}) \end{aligned}$$

Pelo Corolário 2.1, é possível escolher um sistema completo de representantes de classes laterais R de P em $\mathbb{Z}[\zeta_n]$ tal que $\mathbf{r} \in R$ com

$$\omega_{\overline{M}}(\overline{\mathbf{r}}) = \omega_M(\mathbf{r}) \text{ e } \omega_M(\mathbf{r}) \leq \omega_M(\mathbf{x}), \ \forall \ \mathbf{x} \in \mathbf{r} + P.$$

Assim, dados $\mathbf{r}, \mathbf{s} \in R$, temos dois casos a ser considerado:

1º **Caso**. Se $\mathbf{r} + \mathbf{s} \in R$, então

$$\omega_{\overline{M}}(\overline{\mathbf{r}} + \overline{\mathbf{s}}) = \omega_{\overline{M}}(\overline{\mathbf{r} + \mathbf{s}}) = \omega_M(\mathbf{r} + \mathbf{s}) \leq \omega_M(\mathbf{r}) + \omega_M(\mathbf{s}) = \omega_{\overline{M}}(\overline{\mathbf{r}}) + \omega_{\overline{M}}(\overline{\mathbf{s}}).$$

2º **Caso**. Se $\mathbf{r} + \mathbf{s} \notin R$, então existe $\mathbf{t} \in R$ tal que $\overline{\mathbf{r} + \mathbf{s}} = \overline{\mathbf{t}}$. Logo,

$$\omega_{\overline{M}}(\overline{\mathbf{r}} + \overline{\mathbf{s}}) = \omega_{\overline{M}}(\overline{\mathbf{t}}) = \omega_M(\mathbf{t}) \leq \omega_M(\mathbf{r} + \mathbf{s}) \leq \omega_M(\mathbf{r}) + \omega_M(\mathbf{s}) = \omega_{\overline{M}}(\overline{\mathbf{r}}) + \omega_{\overline{M}}(\overline{\mathbf{s}}).$$

■

A função $\omega_{\overline{M}} : \mathbb{F} \to \mathbb{R}$ definida por

$$\omega_{\overline{M}}(\overline{\mathbf{a}}) = \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\},$$

será chamada de *peso de Mannheim* sobre $\mathbb{F}$. A distância associada a este peso será chamada de *distância de Mannheim*.

Lema 3.1 *Seja $\omega_{\overline{M}} : \mathbb{Z}[\zeta_n] \to \mathbb{R}$ um peso de Manhattan sobre $\mathbb{Z}[\zeta_n]$. Então*:

1. *$\mathbf{a} \in \mathbb{Z}[\zeta_n]$ com $\omega_M(\mathbf{a}) = 1$ se, e somente se, $\mathbf{a} = \pm 1, \pm\zeta_n, \ldots, \pm\zeta_n^{d-1}$ e, nesse caso,*

$$\omega_{\overline{M}}(\overline{\mathbf{a}}) = \omega_M(\mathbf{a}) = \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{a} + P\}.$$

2. *Se p e m são ímpares, então $\pm 1, \pm\zeta_m, \ldots, \pm\zeta_m^{\varphi(m)-1}$ são os únicos elementos em $\mathbb{F}$ tais que $\omega_{\overline{M}}(\pm\zeta_m^j) = 1$, $j = 0, 1, \ldots, \varphi(m) - 1$.*

Prova. 1. Seja

$$\mathbf{a} = \sum_{j=0}^{d-1} a_j \zeta_n^j \in \mathbb{Z}[\zeta_n]$$

tal que $\omega_M(\mathbf{a}) = 1$. Então

$$1 = \omega_M(\mathbf{a}) = \sum_{j=0}^{d-1} |a_j| .$$

Logo, existe $j \in \{0, 1, \ldots, d-1\}$ tal que $|a_j| = 1$ e $|a_s| = 0$, $s \neq j$, isto é, $a_j = \pm 1$ e $|a_s| = 0$, $s \neq j$. Portanto, $\mathbf{a} = \pm 1, \pm\zeta_n, \ldots, \pm\zeta_n^{d-1}$. A recíproca é claro.

2. É claro que $\omega_{\overline{M}}(\pm\zeta_m^j) = 1$, $j = 0, 1, \ldots, \varphi(m) - 1$. Por outro lado, dado $\overline{\mathbf{a}} \in \mathbb{F}$ com $\omega_{\overline{M}}(\overline{\mathbf{a}}) = 1$. Então existe $g \in \mathbb{Z}$ tal que $\overline{\mathbf{a}} = \zeta_m^g$. Como $n = p^e m$ e $p \nmid m$, temos que $\zeta_n + P \leftrightarrow \overline{\zeta_n} = \zeta_m \in \mathbb{Z}_p(\zeta_m)$ é uma raiz m-ésima primitiva da unidade e

$$(-\overline{\zeta_n})^m = -1 \neq 1 = \overline{\zeta_n}^m,$$

pois p e m são ímpares. Portanto, pelo item 1.

$$\overline{\mathbf{a}} = \pm 1, \pm\zeta_m, \ldots, \pm\zeta_m^{\varphi(m)-1}.$$

■

Proposição 3.3 *Seja $\omega_M : \mathbb{F} \to \mathbb{R}$ um peso de Mannheim sobre $\mathbb{F}$. Então $\omega_{\overline{M}}$ é consecutivo.*

Prova. Para qualquer $\overline{\mathbf{a}} \in \mathbb{F}$ com $\omega_{\overline{M}}(\overline{\mathbf{a}}) = \omega_M(\mathbf{a}) > 0$, devemos encontrar um $\overline{\mathbf{b}} \in \mathbb{F}$ tal que $\omega_{\overline{M}}(\overline{\mathbf{a}} - \overline{\mathbf{b}}) = 1$ e $\omega_{\overline{M}}(\overline{\mathbf{b}}) = \omega_{\overline{M}}(\overline{\mathbf{a}}) - 1$. Pelo item 1. do Lema 3.1, basta encontrar um elemento $\mathbf{b} \in \mathbb{Z}[\zeta_n]$ tal que

$$\omega_M(\mathbf{b}) = \omega_M(\mathbf{a}) - 1 \text{ e } \omega_M(\mathbf{a} - \mathbf{b}) = 1$$

Seja

$$\mathbf{a} = (a_0, \ldots, a_{d-1}) \in \mathbb{Z}[\zeta_n].$$

Então existe $j \in \{0, 1, \ldots, d-1\}$ tal que $a_j \neq 0$, pois $\omega_M(\mathbf{a}) > 0$. Podemos supor, sem perda de generalidade, que $a_0 \neq 0$. Então $a_0 > 0$ ou $a_0 < 0$. Basta considerar o caso $a_0 > 0$, pois se $a_0 < 0$, então tomando $\mathbf{c} = -\mathbf{a}$, aplica-se o caso anterior. Existe

$$\mathbf{b} = (a_0 - 1, a_1, \ldots, a_{d-1}) \in \mathbb{Z}[\zeta_n]$$

tal que

$$\omega_M(\mathbf{b}) = \omega_M(\mathbf{a}) - 1 \text{ e } \omega_M(\mathbf{a} - \mathbf{b}) = 1.$$

Assim, resta provar que

$$\omega_{\overline{M}}(\overline{\mathbf{b}}) = \omega_M(\mathbf{b}).$$

Suponhamos, por absurdo, que $\omega_{\overline{M}}(\overline{\mathbf{b}}) < \omega_M(\mathbf{b})$. Então existe

$$\mathbf{u} = (u_0, u_1, \ldots, u_{d-1}) \in P$$

tal que $\overline{\mathbf{b}} = \mathbf{b} + \mathbf{u}$. Logo,

$$|a_0 - 1 + u_0| + \sum_{j=1}^{d-1} |a_j + u_j| < |a_0 - 1| + \sum_{j=1}^{d-1} |aj|$$

ou, ainda,

$$|a_0 - 1 + u_0| - |a_0 - 1| < \sum_{j=1}^{d-1} (|a_j| - |a_j + u_j|)$$

Por outro lado, pela desigualdade triangular, obtemos

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

Como $a_0 - 1 \geq 0$ temos que

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

Logo,

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

Assim,

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

Portanto,

$$|a_0 + u_0| - |a_0| \leq |a_0 - 1 + u_0| - |a_0 - 1| < \sum_{j=1}^{d-1} (|a_j| - |a_j + u_j|)$$

ou, equivalentemente,

$$\sum_{j=0}^{d-1} |a_j + u_j| < \sum_{j=0}^{d-1} |a_j|\,.$$

Logo,

$$\omega_M(\mathbf{a}) = \omega_{\overline{M}}(\overline{\mathbf{a}}) = \omega_M(\mathbf{a} + \mathbf{u}) < \omega_M(\mathbf{a}),$$

o que é uma contradição. ■

3.2 Códigos

Nesta seção apresentaremos a teoria de códigos corretores de erros baseada em $\mathbb{F}^l$ equipado com uma métrica consecutiva, onde o alfabeto $\mathbb{F}$ é um corpo com p^h elementos.

Um *código* $\mathcal{C}$ sobre $\mathbb{F}$ é qualquer subconjunto não vazio de $\mathbb{F}^l$. Os elementos de $\mathcal{C}$ são chamados de *vetores* ou *palavras código*.

Um *código de bloco* $\mathcal{C}$ de comprimento l sobre $\mathbb{F}$ é qualquer subconjunto não vazio de $\mathbb{F}^l$. A *dimensão* do código $\mathcal{C}$ é o número

$$k = \log_{p^h} |\mathcal{C}| .$$

Note que k não necessariamente é um número inteiro. Um código de bloco $\mathcal{C}$ de comprimento l e dimensão k será chamado um $[l, k]$-código. A *taxa de informação* do $[l, k]$-código é o número

$$R = \frac{k}{l},$$

que pode ser interpretado como o número de símbolos de informação que entrou no codificador por símbolos transmitido.

Se $|\mathcal{C}| \geq 2$, então a *distância consecutiva mínima* $d_\omega(\mathcal{C})$ de $\mathcal{C}$ é definida por

$$d_\omega(\mathcal{C}) = \min\{d_\omega(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\}$$

Note que $1 \leq d_\omega(\mathcal{C}) \leq l$. Se $|\mathcal{C}| = 1$, então $d_\omega(\mathcal{C}) = \infty$ por convenção.

Um código de bloco de comprimento l com dimensão k e distância consecutiva mínima $d_\omega = d_\omega(\mathcal{C})$ será chamado um $[l, k, d_\omega]$-código.

Sejam ρ um inteiro positivo e $\mathbf{c} \in \mathbb{F}^l$, a *bola* de raio ρ e centro $\mathbf{c}$ é definida como

$$B_\rho(\mathbf{c}) = \left\{\mathbf{x} \in \mathbb{F}^l : d_\omega(\mathbf{x}, \mathbf{c}) \leq \rho\right\}.$$

Suponhamos que uma palavra código

$$\mathbf{c} = (c_1, c_2, \ldots c_l)$$

foi enviada através de um canal. Devido ao ruído introduzido pelo canal, o vetor recebido

$$\mathbf{r} = (r_1, r_2, \ldots, r_l)$$

pode ou não ser a palavra código enviada. Com base nesta hipótese, definimos o *vetor erro* por

$$\mathbf{e} = \mathbf{r} - \mathbf{c} = (e_1, e_1, \ldots, e_t) .$$

Dizemos que um código $\mathcal{C}$ *detecta* qualquer padrão de t erros se ele é capaz de decidir que qualquer palavra recebida com t erros não é uma palavra código. Se, além de detectar, ele também é capaz de corrigí-los, dizemos que ele *corrige* qualquer padrão de t erros.

Dizemos que um $[l, k, d_\omega]$-código corrige qualquer padrão de t ou menos erros se

$$B_t(\mathbf{c}) \cap \mathcal{C} = \{\mathbf{c}\}, \ \forall \ \mathbf{c} \in \mathcal{C}.$$

Teorema 3.1 *Seja $\mathcal{C}$ um $[l, k, d_\omega]$-código sobre $\mathbb{F}^l$. Se*

$$t = \left\lfloor \frac{d_\omega - 1}{2} \right\rfloor,$$

então $\mathcal{C}$ corrige qualquer padrão de t ou menos erros mas não $t+1$.

Prova. Como $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ temos que

$$2t + 1 \leq d_\omega < 2t + 2 \text{ ou } t \leq d_\omega - (t+1) < t + 1.$$

Suponhamos, por absurdo, que

$$B_t(\mathbf{c}) \cap B_t(\mathbf{c}') \neq \emptyset, \text{ com } \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'.$$

Então existe $\mathbf{x} \in \mathbb{F}^l$ tal que $\mathbf{x} \in B_t(\mathbf{c}) \cap B_t(\mathbf{c}')$. Logo,

$$d_\omega(\mathbf{x}, \mathbf{c}) \leq t \text{ e } d_\omega(\mathbf{x}, \mathbf{c}') \leq t.$$

Pela desigualdade triangular, obtemos

$$d_\omega(\mathbf{c}, \mathbf{c}') \leq d_\omega(\mathbf{x}, \mathbf{c}) + d_\omega(\mathbf{x}, \mathbf{c}') \leq 2t.$$

Logo,

$$2t \geq d_\omega(\mathbf{c}, \mathbf{c}') \geq d_\omega \geq 2t + 1,$$

o que é uma contradição.

Finalmente, sejam $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ tais que $d_\omega(\mathbf{c}, \mathbf{c}') = d_\omega$. Então, pelo item 2. da Proposição 3.1, existe $\mathbf{r} \in \mathbb{F}^l$ tal que $d_\omega(\mathbf{c}, \mathbf{r}) = t+1$ e $d_\omega(\mathbf{r}, \mathbf{c}') = d_\omega - (t+1)$. Assim, se $\mathbf{c}$ é a palavra código enviada e $\mathbf{r}$ a palavra recebida com $d_\omega(\mathbf{c}, \mathbf{r}) = t + 1$, então um decodificador (com máxima verossimilhaça) decide pela palavra código $\mathbf{c}'$, pois

$$d_\omega(\mathbf{r}, \mathbf{c}') = d_\omega - (t+1) \Rightarrow t \leq d_\omega(\mathbf{r}, \mathbf{c}') < t + 1 \Rightarrow d_\omega(\mathbf{r}, \mathbf{c}') = t.$$

Portanto, $\mathcal{C}$ não corrige qualquer padrão de $t+1$. ■

Corolário 3.2 *Seja $\mathcal{C}$ um $[l, k, d_{\overline{\omega}}]$-código sobre $\mathbb{F}$, onde $d_{\overline{\omega}}$ é a distância de Mannheim mínima. Se*

$$t = \left\lfloor \frac{d_{\overline{\omega}} - 1}{2} \right\rfloor,$$

então $\mathcal{C}$ é capaz de corrigir qualquer padrão de t ou menos erros. ■

3.3 Códigos Lineares

Um código $\mathcal{C}$ sobre $\mathbb{F}$ de comprimento l é chamado um *código linear* se ele é um subespaço vetorial de $\mathbb{F}^l$. Neste caso, o peso consecutivo $\omega(\mathbf{c})$ de uma palavra código não nula $\mathbf{c} \in \mathbb{F}^l$ é o número de componentes diferentes de zero. Assim,

$$d_\omega(\mathbf{c}, \mathbf{c}') = d_\omega(\mathbf{c} - \mathbf{c}', \mathbf{0}) = \omega(\mathbf{c} - \mathbf{c}')$$

e a dimensão do código é um número inteiro.

Seja $\mathcal{C}$ um $[l, k, d_\omega]$-código linear sobre $\mathbb{F}$. Se $\{\mathbf{c}_1, \ldots, \mathbf{c}_k\}$ é uma base de $\mathcal{C}$, então a função $g : \mathbb{F}^k \to \mathbb{F}^l$ dada por,

$$\begin{aligned} g((u_1, \ldots, u_k)) &= \left(\sum_{j=1}^{k} c_{j1} u_j, \ldots, \sum_{j=1}^{k} c_{jl} u_j \right) \\ &= u_1 \mathbf{c}_1 + \cdots + u_k \mathbf{c}_k, \end{aligned}$$

onde $\mathbf{c}_i = (c_{i1}, \ldots, c_{il})$, $1 \leq i \leq k$, é um *codificador* para o código $\mathcal{C}$. A matriz $k \times l$ $\mathbf{G} = [c_{ij}]$ que descreve a transformação linear g é chamada uma *matriz geradora* do código $\mathcal{C}$. Assim, $\mathcal{C}$ consiste de q^k, onde $q = p^h$, combinações lineares $\mathbf{c} = \mathbf{uG}$, onde $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}^k$ é chamada uma *seqüência de informação* ou *mensagem*.

Observação 3.1 *Como a base para um $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$ não é única temos que a matriz geradora $\mathbf{G}$ para $\mathcal{C}$ também não é única. Desde que operações elementares de linhas deixam o código $\mathcal{C}$ invariante, podemos escolher uma base para $\mathcal{C}$ tal que a matriz geradora $\mathbf{G}'$ é da forma*

$$\mathbf{G}' = \begin{bmatrix} \mathbf{P} & \mathbf{I}_k \end{bmatrix},$$

onde $\mathbf{I}_k$ é a matriz $k \times k$ identidade e $\mathbf{P}$ é uma matriz $k \times (l - k)$. Neste caso, dizemos que $\mathbf{G}'$ está na forma canônica.

Se a matriz geradora $\mathbf{G}$ de um $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$ está na forma canônica, então as últimas k componentes de uma palavra código $\mathbf{c} \in \mathcal{C}$ são chamadas de *símbolos*

de informações, os quais são escolhidos arbitrariamente e o restante, chamados *símbolos de verificação de paridade*, são determinados. Em outras palavras, se

$$\mathbf{c} = (c_1, \ldots, c_l) = (u_1, \ldots, u_k)\mathbf{G},$$

então

$$c_{l-k+i} = u_i, 1 \leq i \leq k,$$

e

$$c_j = \sum_{i=1}^{k} u_i p_{ij}, 1 \leq j \leq l-k,$$

a qual é chamada de *equação de verificação de paridade*.

Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ dois $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$. Dizemos que $\mathcal{C}_1$ e $\mathcal{C}_2$ são *equivalentes* se existirem matrizes geradoras $\mathbf{G}_1$ e $\mathbf{G}_2$ para $\mathcal{C}_1$ e $\mathcal{C}_2$, respctivamente, e uma matriz de permutação $\mathbf{Q}$ tal que

$$\mathbf{G}_2 = \mathbf{G}_1\mathbf{Q}.$$

Um $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$ é *sistemático* se ele possui um conjunto de informação, isto é, se existir exatamente uma palavra código para todas as possíveis escolhas de coordenadas nas k-posições, isto é, a matriz geradora $\mathbf{G}$ do código $\mathcal{C}$ é da forma

$$\mathbf{G} = \left[\begin{array}{cc} \mathbf{P} & \mathbf{I}_k \end{array} \right].$$

Seja $g : \mathbb{F}^k \to \mathbb{F}^l$ um codificador para o $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$, com matriz geradora

$$\mathbf{G} = \left[\begin{array}{cc} \mathbf{P} & \mathbf{I}_k \end{array} \right]$$

Então a transformação linear $h : \mathbb{F}^l \to \mathbb{F}^{l-k}$ definida pela matriz $(l-k) \times l$

$$\mathbf{H} = \left[\begin{array}{cc} \mathbf{I}_{l-k} & -\mathbf{P} \end{array} \right]$$

possui as seguintes propriedades:

1. $\ker h = \operatorname{Im} g$;

2. $\mathbf{c} \in \mathcal{C}$ se, e somente se, $\mathbf{H}\mathbf{c}^t = \mathbf{0}$.

De fato, a transformação linear $h \circ g : \mathbb{F}^k \to \mathbb{F}^{l-k}$ é identicamente nula, pois

$$\mathbf{G}\mathbf{H}^t = \left[\begin{array}{cc} \mathbf{P} & \mathbf{I}_k \end{array} \right] \left[\begin{array}{c} \mathbf{I}_{l-k} \\ -\mathbf{P} \end{array} \right] = \mathbf{I}_{l-k}\mathbf{P} + (-\mathbf{P})\mathbf{I}_k = \mathbf{P} - \mathbf{P} = \mathbf{0}.$$

Logo, $\operatorname{Im} g \subseteq \ker h$. Desde que as primeiras $l-k$ colunas de $\mathbf{H}$ formam a base canônica do espaço vetorial $\mathbb{F}^{l-k}$ temos que $\operatorname{Im} h$ gera $\mathbb{F}^{l-k}$ e contém q^{l-k} elementos. Assim, pelo Primeiro Teorema de Homomorfismos,

$$|\ker h| = \frac{\left|\mathbb{F}^l\right|}{|\operatorname{Im} h|} = \frac{q^l}{q^{l-k}} = q^k.$$

Portanto, $\ker h = \operatorname{Im} g$, pois $|\operatorname{Im} g| = q^k$.

A matriz $\mathbf{H}$ é chamada de *matriz de verificação de paridade* para o $[l, k, d_\omega]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$. Se

$$\mathbf{c} = (c_1, \ldots, c_k, c_{k+1}, \ldots, c_l) \in \mathcal{C},$$

então temos o sistema de equações $\mathbf{H}\mathbf{c}^t = \mathbf{0}$ ou, equivalentemente,

$$c_j = \sum_{i=1}^{l-k} c_{k+i} h_{j(k+i)}, 1 \leq j \leq k,$$

onde h_{ij} são as entradas da matriz $\mathbf{P}$. Portanto, *codificamos* uma mensagem $\mathbf{u} \in \mathbb{F}^k$ calculando $\mathbf{uG}$ e podemos *detectar erros* em uma palavra código recebida $\mathbf{r} \in \mathbb{F}^l$ calculando $\mathbf{H}\mathbf{r}^t$.

Sejam $\mathcal{C}$ um $[l, k, d_\omega]$-código linear com matriz de verificação de paridade $\mathbf{H}$ e $\mathbf{x} \in \mathbb{F}^l$. Então o vetor

$$\mathbf{s}(\mathbf{x}) = \mathbf{H}\mathbf{x}^t$$

é chamado a *síndrome* de $\mathbf{x}$. Note que $\mathbf{s}(\mathbf{x}) = \mathbf{0}$ se, e somente se, $\mathbf{x} \in \mathcal{C}$. Agora, sejam $\mathbf{c} \in \mathcal{C}$ uma palavra código, $\mathbf{e}$ o erro introduzido e $\mathbf{r}$ a palavra recebida. Assim, a síndrome de $\mathbf{r}$ é

$$\mathbf{s}(\mathbf{r}) = \mathbf{H}\mathbf{r}^t = \mathbf{H}(\mathbf{c}+\mathbf{e})^t = \mathbf{H}\mathbf{c}^t + \mathbf{H}\mathbf{e}^t = \mathbf{H}\mathbf{e}^t = \mathbf{s}(\mathbf{e}),$$

ou seja, a síndrome de $\mathbf{s}(\mathbf{r})$ é igual a síndrome de $\mathbf{e}$. Portanto,

1. Se $\mathbf{s} \neq \mathbf{0}$, então ocorreu um erro durante a transmissão da mensagem.

2. Se $\mathbf{s} = \mathbf{0}$, segue que a palavra recebida é uma palavra código.

Proposição 3.4 *Sejam $\mathbb{F} = \mathbb{Z}_p(\alpha)$, onde $p^h - 1 = lk$, e $\mathcal{C}$ um código linear sobre $\mathbb{F}$ com matriz de verificação de paridade*

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{l-1} \end{bmatrix}$$

Então $\mathcal{C}$ pode corrigir um erro de Mannheim, o qual pertence ao subgrupo cíclico

$$E = \{1, \alpha^l, \alpha^{2l}, \ldots, \alpha^{(k-1)l}\} = \langle \alpha^l \rangle$$

de $\mathbb{F}^*$.

Prova. Sejam $\mathbf{c} = (c_0, \ldots, c_{l-1}) \in \mathcal{C}$ e $\mathbf{e} = (0, \ldots, 0, \alpha^{jl}, 0, \ldots, 0) \in \mathbb{F}^l$ com uma única componente não-nula α^{jl} na posição s, $0 \leq s \leq l-1$. Então a síndrome da palavra recebida $\mathbf{r} = \mathbf{c} + \mathbf{e}$ é

$$\mathbf{H}\mathbf{r}^t = \mathbf{H}(\mathbf{c}^t + \mathbf{e}^t) = \mathbf{H}\mathbf{e}^t = \alpha^s \alpha^{jl} = \alpha^{jl+s} = \alpha^e.$$

Como $e = s + jl$ temos que conhecendo a posição do erro $s \equiv e (\mathrm{mod}\, l)$, podemos determinar o seu valor α^e. ■

Observação 3.2 *Como*

$$\frac{\mathbb{F}^*}{E} = \{E, \alpha E, \ldots, \alpha^{l-1} E\}$$

temos que o conjunto

$$\{1, \alpha, \ldots, \alpha^{l-1}\}$$

é um sistema completo de representantes de classes laterais de E em $\mathbb{F}^*$. Portanto, os elementos da matriz de verificação de paridade H podem ser representados por qualquer sistema de representantes de classes laterais de E em $\mathbb{F}^*$.

Lema 3.2 *Sejam $m, p, h \in \mathbb{N}$ com p primo. Se m e p são ímpares e $m \mid p^h - 1$, então $2m \mid p^h - 1$.* ■

Teorema 3.2 *Sejam $\mathbb{F} = \mathbb{Z}_p(\alpha)$, onde*

$$l = \begin{cases} \frac{p^h-1}{2m} & , se\ m\ e\ p\ são\ ímpares \\ \frac{p^h-1}{m} & , caso\ contrário \end{cases}$$

e $\mathcal{C}$ um código linear sobre $\mathbb{F}$ com matriz de verificação de paridade

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{l-1} \end{bmatrix}$$

Então $\mathcal{C}$ pode corrigir um erro de Mannheim. Em particular, o peso de Mannheim mínimo de $\mathcal{C}$ é

$$d_{\overline{M}}(\mathcal{C}) \geq 3.$$

Prova. Pelo Lema 3.2 l é inteiro. Pelo item 1. do Lema 3.1, os elementos $\mathbf{a}$ em $\mathbb{F}$ com $\omega_{\overline{M}}(\mathbf{a}) = 1$ são

$$\mathbf{a} = \pm 1, \pm\zeta_m, \ldots, \pm\zeta_m^{\varphi(m)-1}.$$

Se $p^h - 1 = kl$, então em ambos os casos o elemento $-\zeta_m$ tem ordem k, ou seja,

$$-\zeta_m \in \langle \alpha^l \rangle,$$

onde $\langle \alpha^l \rangle$ é um subgrupo cíclico de ordem k de $\mathbb{F}^*$. Assim, todo elemento em $\mathbb{F}$ do peso de Mannheim mínimo, isto é,

$$\omega_{\overline{M}}(\mathbf{a}) = 1,$$

pertence ao subgrupo cíclico de ordem k gerado por α^l. Então, pela Proposição 3.4, o código $\mathcal{C}$ pode corrigir um erro de Mannheim. ■

Exemplo 3.2 *Sejam $p = 13$ e $\mathbb{F} = \mathbb{Z}_p(\alpha)$, onde $\alpha = 1 + i$. Então $h = 1$, $lk = p - 1 = 3 \cdot 4$*

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & 1+i & 2i \end{bmatrix}$$

é matriz de verificação de paridade de um $[3, 2, 3]$-código linear $\mathcal{C}$ sobre $\mathbb{F}$ com matriz geradora

$$\mathbf{G} = \begin{bmatrix} -(1+i) & 1 & 0 \\ -2i & 0 & 1 \end{bmatrix}.$$

Suponhamos que a palavra recebida seja

$$\mathbf{r} = (1 + i, i, -1 + i).$$

Então, usando a Tabela abaixo, encontramos

$$\mathbf{s} = \mathbf{H}\mathbf{r}^t = -2 = \alpha^{11}.$$

Como $11 = 3 \cdot 3 + 2$ temos na posição $s = 2$ um erro de valor

$$\alpha^{11}\alpha^{-2} = \alpha^9 = i.$$

Portanto,

$$\mathbf{e} = (0, 0, i).$$

Assim,

$$\mathbf{c} = \mathbf{r} - \mathbf{e} = (1 + i, i, -1)$$

é uma estimativa da palavra código enviada.

u	α^u	u	α^u	u	α^u	u	α^u
0	1	3	$-i$	6	-1	9	i
1	$1+i$	4	$1-i$	7	$-1-i$	10	$-1+i$
2	$2i$	5	2	8	$-2i$	11	-2

Capítulo 4

Aplicações

Neste capítulo apresentaremos um método geométrico para determinar um sistema completo de representantes de classes laterais de um ideal primo P em $\mathbb{Z}[\zeta_n]$, quando $n = m = 4$.

4.1 Linhas Eqüidistantes

Dados $A, B \in \mathbb{R}^2$, a *linha eqüidistante* de extremos A e B é o conjunto

$$[A, B] = \{Q \in \mathbb{R}^2 : d_M(Q, A) = d_M(Q, B)\}.$$

Lema 4.1 *Seja $ABCD$ um retângulo em $\mathbb{R}^2$. Então*

$$[A, C] = \overline{GE} \cup \overline{EF} \cup \overline{FH},$$

onde E e F são pontos dos segmentos $\overline{AB}$ e $\overline{CD}$, respectivamente, tais que

$$d_M(E, A) = d_M(F, C).$$

Além disso, os segmentos $\overline{EG}$ e $\overline{FH}$ são ortogonais aos segmentos $\overline{AB}$ e $\overline{CD}$, respectivamente. Note que $Z = \overline{AC} \cap \overline{EF}$ é o ponto médio do segmento $\overline{AC}$.

Prova. Não há perda de generalidade, em supor, que as arestas do retângulo $ABCD$ sejam paralelas aos eixos coordenados. Assim, se $A = (a, b), C = (c, d) \in \mathbb{R}^2$, então $B = (c, b)$ e $D = (a, d)$. Logo,

$$d_M(Q, A) = d_M(Q, C) \Leftrightarrow |x - a| + |y - b| = |x - c| + |y - d|\,, \ \forall\ Q = (x, y) \in \mathbb{R}^2.$$

Assim, há três casos a ser considerado:

1º **Caso**. Se Q está abaixo do retângulo e entre A e B, então $x > a$, $y < b$, $x < c$ e $y < d$. Logo,

$$(x-a)-(y-b) = -(x-c)-(y-d) \Rightarrow x = \frac{a-b+c+d}{2}.$$

Neste caso,

$$E = \left(\frac{a-b+c+d}{2}, b\right) \text{ e } d_M(E,A) = \left|\frac{-a-b+c+d}{2}\right|,$$

pois $a < x < c$, e o segmento $\overline{EG}$ é ortogonal ao segmento $\overline{AB}$, onde

$$G = \left(\frac{a-b+c+d}{2}, g\right) \text{ comj } g < b.$$

2º **Caso**. Se Q está acima do retângulo e entre C e D, então $x > a$, $y > b$, $x < c$ e $y > d$. Logo,

$$(x-a)+(y-b) = -(x-c)+(y-d) \Rightarrow x = \frac{a+b+c-d}{2}.$$

Neste caso,

$$F = \left(\frac{a+b+c-d}{2}, d\right) \text{ e } d_M(F,C) = \left|\frac{-a-b+c+d}{2}\right| = d_M(E,A),$$

pois $a < x < c$, e o segmento $\overline{FH}$ é ortogonal ao segmento $\overline{CD}$, onde

$$H = \left(\frac{a+b+c-d}{2}, h\right) \text{ comj } h > d.$$

3º **Caso**. Se Q está dentro do retângulo, então $x > a$, $y > b$, $x < c$ e $y < d$. Logo,

$$(x-a)+(y-b) = -(x-c)-(y-d) \Rightarrow y = -x + \left(\frac{a+b+c+d}{2}\right).$$

É fácil verificar que esta reta contém os pontos E e F. Portanto,

$$[A,C] = \overline{GE} \cup \overline{EF} \cup \overline{FH}.$$

■

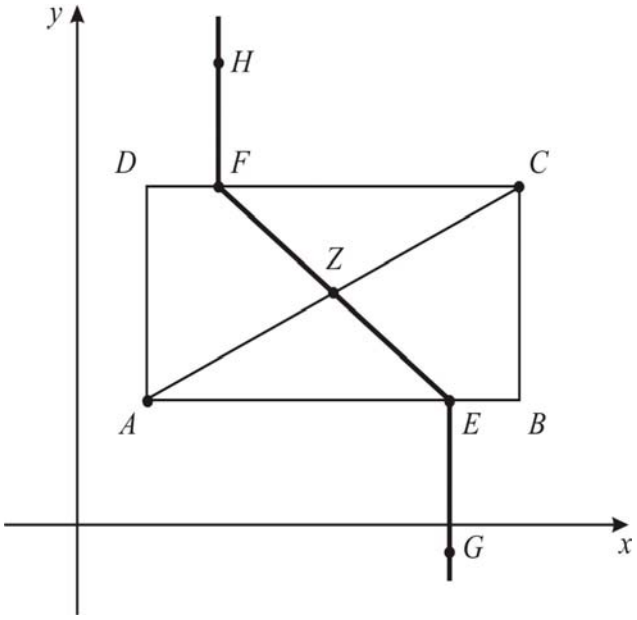

Figura 4.1: Linha eqüidistante.

Observação 4.1 *Seja $ABCD$ um retângulo em $\mathbb{R}^2$. Então $\mathbb{R}^2 = V_{\overrightarrow{AC}} \cup V_{\overrightarrow{CA}}$, onde*

$$V_{\overrightarrow{AC}} = \{Q \in \mathbb{R}^2 : d_M(Q, A) \leq d_M(Q, C)\}$$

e

$$V_{\overrightarrow{CA}} = \{Q \in \mathbb{R}^2 : d_M(Q, A) \geq d_M(Q, C)\}.$$

Note que $V_{\overrightarrow{AC}} \cap V_{\overrightarrow{CA}} = [A, C]$ e que $V_{\overrightarrow{AC}}$ é o conjunto de todos os pontos de $\mathbb{R}^2$ que estão mais próximo de A do que de C.

Lema 4.2 *Seja $ABCD$ um retângulo em $\mathbb{R}^2$. Se $A, C \in \mathbb{Z}^2$ e $d_M(A, C)$ é um número ímpar, então não existe $Q \in \mathbb{Z}^2$ tal que*

$$d_M(A, Q) = d_M(C, Q).$$

Prova. Suponhamos, por absurdo, que exista $Q \in \mathbb{Z}^2$ tal que

$$d_M(A, Q) = d_M(C, Q).$$

Se Q está dentro do retângulo, então

$$d_M(A, Q) + d_M(Q, C) = d_M(A, C) \Rightarrow d_M(A, C) = 2d_M(A, Q),$$

o que é uma contradição, pois $d_M(A, C)$ é ímpar.

Consideremos agora Q fora e abaixo do retângulo e entre os pontos A e B, com $A = (a, b)$, $B = (c, b)$, $C = (c, d)$, $S = (s, b)$, $Q = (s, t)$ e $E = (x, b)$. Sem perda de generalidade, podemos supor que Q está entre A e E. Assim, obtemos

$$d_M(A, Q) = |t - b| + |s - a|$$

e

$$d_M(C, Q) = |t - b| + |x - s| + |c - x| + |b - d| .$$

Portanto,

$$d_M(A, Q) \leq d_M(C, Q),$$

o que é uma contradição, pois $d_M(A, Q) = d_M(C, Q)$. ■

Lema 4.3 *Não existem pontos inteiros entre dois vértices eqüidistantes do quadrado $OACB$.*

Prova. Sejam $O = (0, 0)$, $A = (a, b)$, $B = (-b, a)$, $C = (a - b, a + b)$ e $H = (n, m)$ como na Figura 4.2, com

$$a^2 + b^2 = p, \text{com } \ a, b \in \mathbb{Z}$$

e H entre O e A. É claro que

$$n^2 + m^2 < a^2 + b^2 = p$$

Assim, obtemos

$$\frac{b}{a} = \frac{m}{n} \Rightarrow a = \frac{n}{m}b.$$

Logo,

$$p = \frac{n^2}{m^2}b^2 + b^2 = b^2(\frac{n^2}{m^2} + 1) = b^2(\frac{n^2 + m^2}{m^2}),$$

ou seja,

$$m^2 p = b^2(m^2 + n^2).$$

Como

$$p = a^2 + b^2 \Rightarrow p > b$$

temos que

$$p \mid n^2 + m^2,$$

o que é uma contradição, pois $p = a^2 + b^2 > n^2 + m^2$ ■

4.2 Métodos Geométricos

Nesta seção apresentaremos um método geométrico para determinar um sistema completo de representantes para o conjunto quociente

$$\frac{\mathbb{Z}[\zeta_n]}{P} \simeq \mathbb{Z}_p(\zeta_m) = \mathbb{F},$$

quando $n = m = 4$ e p é um número primo ímpar. Então

$$\mathbb{F}_{p^h} = \mathbb{Z}_p(\zeta_4) = \mathbb{F},$$

onde

$$h = \begin{cases} 1 & \text{se } p \equiv 1 (\mathrm{mod}\, 4) \\ 2 & \text{se } p \equiv 3 (\mathrm{mod}\, 4) \end{cases}.$$

Em todo esta seção trataremos apenas do caso em que $h = 1$. O leitor interessado no caso $h = 2$, pode consultar [13]. Assim,

$$\mathcal{O}_4 = \mathbb{Z}[\zeta_4] = \mathbb{Z}[i] \text{ e } \mathbb{F} = \mathbb{Z}_p.$$

Portanto, pelo item 1. do Lema 2.1, todo ideal primo P de $\mathbb{Z}[i]$ é gerado por um elemento da forma $a + bi \in \mathbb{Z}[i]$ com

$$a^2 + b^2 = p.$$

Como p é um número primo ímpar temos que $a + b$ é impar. Assim, podemos supor, sem perda de generalidade, que $a > b > 0$, pois

$$P = \langle a + bi \rangle = \langle u(a + bi) \rangle, \ \forall \ u \in U(\mathbb{Z}[i]).$$

Assim, pela Proposição 2.2

$$\Lambda = \psi(P)$$

é um sub-reticulado de $\mathbb{Z}^2$. Como

$$P = (a + bi)\mathbb{Z}[i].$$

Se $z \in P$, então existe $c + di \in \mathbb{Z}[i]$ tal que

$$\begin{aligned} z &= (a + bi)(c + di) \\ &= c(a + bi) + di(a + bi) \\ &= c(a + bi) + d(-b + ai) \\ &= cv_1 + dv_2, \end{aligned}$$

onde $v_1 = a + bi$ e $v_2 = -b + ai$. Assim,

$$\psi(v_1) = (a, b) \text{ e } \psi(v_2) = (-b, a).$$

Logo, $\{v_1, v_2\}$ é uma $\mathbb{Z}$-base para P e

$$\Lambda = \psi(P) = \{c\psi(v_1) + d\psi(v_2) \text{ e } c, d \in \mathbb{Z}\}$$

e

$$S = \{t\psi(v_1) + s\psi(v_2) : 0 \leq t < 1 \text{ e } 0 \leq s < 1\}$$

é um quadrado em $\mathbb{R}^2$, onde $O = (0, 0)$, $A = (a, b)$, $B = (-b, a)$ e $C = (a - b, a + b)$.

Pelo Lema 4.3, temos que não existem pontos inteiros entre dois vértices eqüidistantes do quadrado $OACB$ e os pontos A, B, C estão na mesma classe de equivalência de O. Portanto,

$$R = S \cap \mathbb{Z}^2$$

é um sistema completo de representantes de classes laterais de Λ em $\mathbb{Z}^2$.

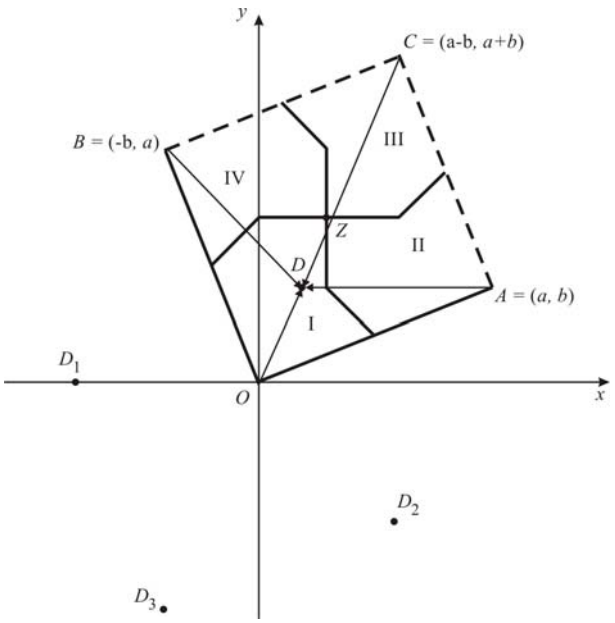

Figura 4.2: Regiões congruentes.

Lema 4.4 *Considere o sub-reticulado $\Lambda = \psi(P)$ de $\mathbb{Z}^2$ e $R = S \cap \mathbb{Z}^2$ o sistema completo de representantes de classes laterais de Λ em $\mathbb{Z}^2$. Se $D = (x, y) \in R$, então os pontos $D_1 = (x - a, y - b)$, $D_2 = (x + b, y - a)$ e $D_3 = (x - a + b, y - a - b)$ estão na classe lateral $D + \Lambda$. Neste caso, um dos pontos D, D_1, D_2 e D_3 têm distância de Manhattan mínima*

em R, isto é, um dos vértice do quadrado O, A, C e B têm distância de Manhattan mínima de D.

Prova. Note que

$$\begin{aligned} D_1 &= D - v_1 \in D + \Lambda \\ D_2 &= D - v_2 \in D + \Lambda \\ D_3 &= D - (v_1 + v_2) \in D + \Lambda. \end{aligned}$$

Logo, D_1, D_2 e D_3 estão na mesma classe de D. Pelo Lema 4.2, temos que não existem pontos com coordenadas inteiras sobre as linhas eqüidistantes. Assim,

$$\omega_M(D_i) \neq \omega_M(D_j) \text{ se } i \neq j.$$

Portanto, , existe um único $i_0 \in \{1, 2, 3\}$ tal que

$$\min\{\omega_M(D + \gamma : \gamma \in \Lambda\} = \omega_M(D_{i_0})$$

■

Proposição 4.1 *Seja P um ideal primo de $\mathbb{Z}[i]$ gerado por um elemento da forma $a+bi \in \mathbb{Z}[i]$ com*

$$a^2 + b^2 = p.$$

1. *Em qualquer classe equivalência de*

$$\frac{\mathbb{Z}[i]}{P}$$

existe um único elemento $\mathbf{r}$ tal que

$$\omega_M(\mathbf{r}) = \min\{\omega_M(\mathbf{x}) : \mathbf{x} \in \mathbf{r} + P\}.$$

2. *Se R é um sistema completo de representantes de classes laterais de P em $\mathbb{Z}[i]$ dado pelo item 1., então*

$$\max\{\omega_{\overline{M}}(\mathbf{r}) : \mathbf{r} \in R\} = \max\{|a|, |b|\} - 1.$$

Prova. Provaremos aprenas o item 1., o item 2. pode ser verificado no Artigo.

1. Seja $OACB$ o quadrado em $\mathbb{R}^2$ com $O = (0,0)$, $A = (a,b)$, $B = (-b,a)$ e $C = (a-b, a+b)$. É fácil verificar que

$$d_M(O,A) = a+b \text{ e } d_M(O,Z) = d_M(A,Z) = d_M(B,Z) = d_M(C,Z) = a,$$

onde

$$Z = \left(\frac{a-b}{2}, \frac{a+b}{2}\right)$$

é o centro do quadrado. Sejam $[O,A]$, $[O,B]$, $[A,C]$ e $[B,C]$ as linhas eqüidistantes a partir do ponto Z (confira Figura 4.2). Então elas dividem o quadrado em quatro regiões congruentes e, pelo Lema 4.2, nenhum dos pontos das linhas eqüidistantes têm coordenadas inteiras, pois

$$d_M(O,A) = a+b$$

é um número ímpar.

Sejam $R_1 = OACB \cap V_{\overrightarrow{OA}} \cap V_{\overrightarrow{OB}}$ e $D \in R_1 \cap \mathbb{Z}^2$. Então

$$d_M(O,D) \leq d_M(O,Q)$$

para todo ponto Q nas outras três regiões. Como não existem pontos de coordenadas inteiras nas linhas eqüidistantes temos que não existe um ponto de coordenadas inteiras no quadrado tendo a menor distância de dois vértices. ■

Como a função $T_2 : \mathbb{R}^2 \to \mathbb{R}^2$ definida por

$$T_2(x,y) = (x-a, x-b)$$

é um movimento rígido temos que

$$R_2' = T_2(R_2)$$

é uma região congruente a R_2. De modo inteiramente análogo, as regiões $R_3' = T_3(R_3)$ e $R_4' = T_4(R_4)$ são regiões congruentes a R_3 e R_4, respectivamente. Portanto, obtemos a Figura 4.3.

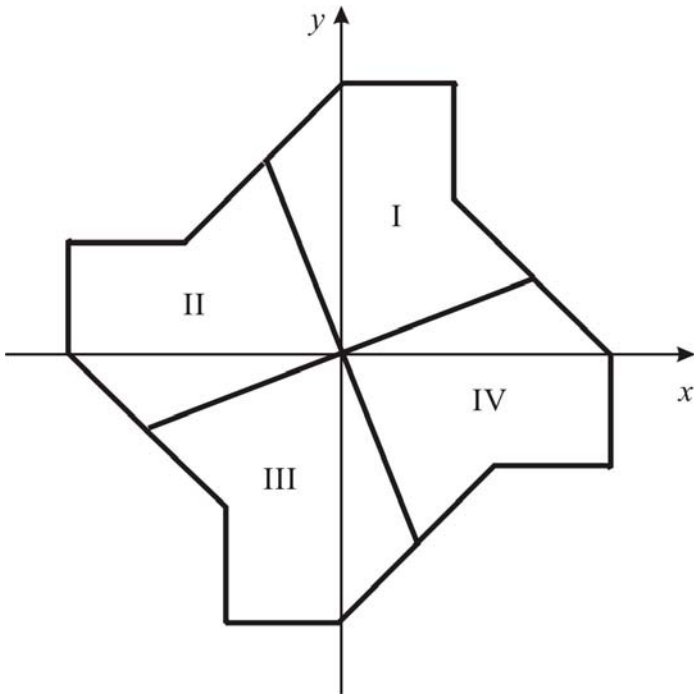

Figura 4.3: Cata-vento.

4.3 Exemplo

Nesta seção apresentaremos um exemplo para provarmos que o nosso método geométrico é mais eficiente do que o método de Huber, para obtermos um sistema completo de representates de classe laterais de P em $\mathbb{Z}[i]$.

Seja P um ideal primo de $\mathbb{Z}[i]$ gerado por $5+2i \in \mathbb{Z}[i]$ com

$$5^2 + 2^2 = 29.$$

Pela Proposição 2.2

$$\Lambda = \psi(P)$$

é um sub-reticulado de $\mathbb{Z}^2$. Como

$$P = (5+2i)\mathbb{Z}[i]$$

temos, para todo $z \in P$, que que existe $c+di \in \mathbb{Z}[i]$ tal que

$$\begin{aligned} z &= (5+2i)(c+di) \\ &= c(5+2i) + d(5+2i) \\ &= c(5+2i) + d(-2+5i), \end{aligned}$$

onde $v_1 = 5 + 2i$ e $v_2 = -2 + 5i$. Assim, $\psi(v_1) = (5, 2)$, $\psi(v_2) = (-2, 5)$ e

$$\{v_1, v_2\}$$

é uma $\mathbb{Z}$-base para P. Como

$$\begin{aligned} \psi(z) &= \{c\psi(v_1) + d\psi(v_2) \text{ com } c, d \in \mathbb{Z}\} \\ &= \{c(5, 2) + d(-2, 5) \text{ com } c, d \in \mathbb{Z}\} \end{aligned}$$

e

$$S = \{t(5, 2) + s(-2, 5) : 0 \leq t < 1 \text{ e } 0 \leq s < 1\}$$

é um quadrado em $\mathbb{R}^2$, onde $O = (0, 0)$, $A = (5, 2)$, $B = (-2, 5)$ e $C = (3, 7)$, temos que

$$R = S \cap \mathbb{Z}^2$$

é um sistema completo de representantes de classes laterais de Λ em $\mathbb{Z}^2$, conforme Figura 4.4.

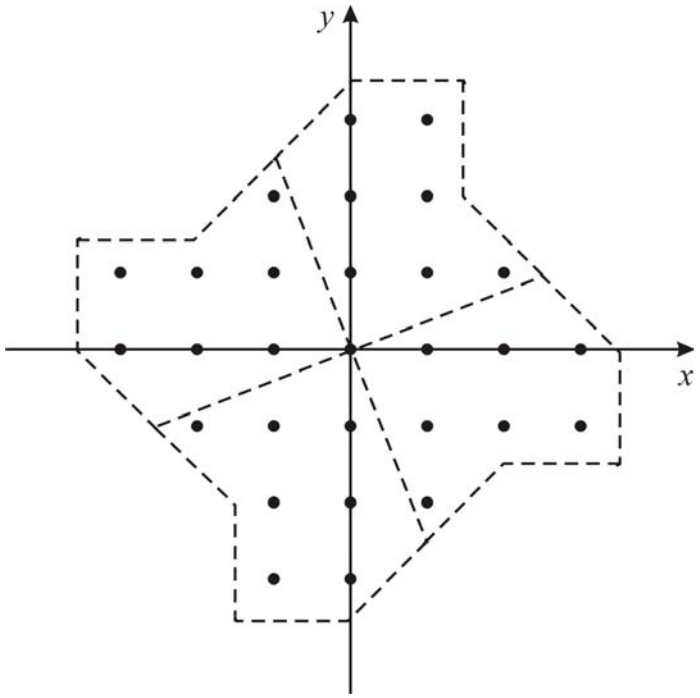

Figura 4.4: Cata-vento.

O método de Huber para obter um sistema completo de representantes para o conjunto quociente

$$\frac{\mathbb{Z}[i]}{\langle a + bi \rangle} \simeq \mathbb{Z}_p = \mathbb{F},$$

onde $a^2 + b^2 = p$, consiste no seguinte:

1. Seja s a solução da equação

$$a + bs \equiv 0 \pmod{p}, \quad 0 \leq s \leq p-1.$$

2. Um ponto $\alpha = x + yi \in \mathbb{Z}[i]$ é rotulado por um elemento $l \in \mathbb{Z}_p$ se

$$x + ys \equiv l \pmod{p}$$

com norma de Galois

$$x^2 + y^2$$

mínima.

Note que $s = 12$ é solução da equação

$$5 + 2s \equiv 0 \pmod{29}.$$

Agora, vamos determinar o elemento de

$$\frac{\mathbb{Z}[i]}{\langle 5 + 2i \rangle}$$

correspondente ao elemento 26 de $\mathbb{Z}_{29}$, isto é, um ponto (x, y) tal que

$$x + 12y = 26 \pmod{29}.$$

Note que os pontos $D = (2, 2)$, $D_1 = (-3, 0)$, $D_2 = (4, -3)$ e $D_3 = (-1, -5)$ satisfazem a equação mas o ponto $D = (2, 2)$ é o de norma de Galois mínima. No entanto, o ponto $D_1 = (-3, 0)$ tem distância de Manhattan mínima em R no nosso sistema de representantes. Observando as Figuras 4.4 e 4.5, notamos que nosso sistema de representantes é mais compacto e convexo do que o de Huber.

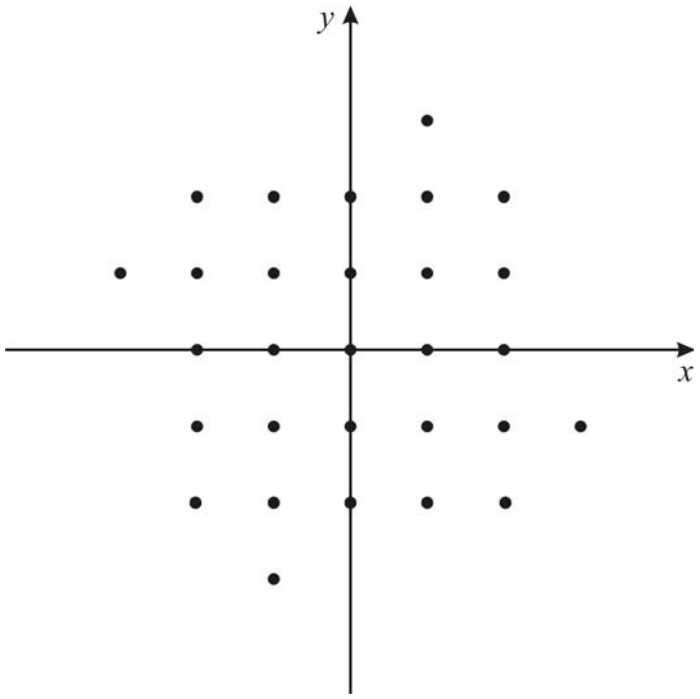

Figura 4.5: Huber.

Referências Bibliográficas

[1] Endler, O. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 1985.

[2] Fan, Y. and Gao, Y., "Codes over Algebraic Integer Rings of Cyclotomic Fields," IEEE. Trans. Inform. Theory, Vol - 50. Nº.1, 2004.

[3] Garcia, A. L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[4] Gonçalves, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 1979.

[5] Hungerford, T. W., *Algebra*. Springer-Verlag, 1996.

[6] Lang, S., *Algebraic Number Theory*. Springer-Verlag, 1986.

[7] Rotman, J. J., *Galois Theory*. Springer, New York, 1998.

[8] Samuel, P., *Algebraic Theory of Numbers.* Hermann, Paris 1970.

[9] Vanstone, S. A and van Oorschot, P. C., *An introdution to error Correting codes with Applications*. Massachusetts: Kluwer Academic Publishers. Second Printing, 1992.

[10] Silva, A. A., *Notas de Aulas*, Depto de Matemática, UFPB - Campus I.

[11] Silva, R. V., *Códigos de Bloco Lineares em Inteiros Algébricos de Corpos Ciclotômicos*. Dissertação de Mestrado, UFPB, 2003.

[12] Stewart, I. N. and Tall, D. O., *Algebraic Number Theory*. Chapman and Hall, London, 1987.

[13] Vieira, V. L., *Códigos sobre Inteiros Algébricos de Corpos Quadráticos*. Dissertação de Mestrado, UFPB, 2000.

[14] Weiss, E., *Algebraic Number Theory*, Dover, 1998.