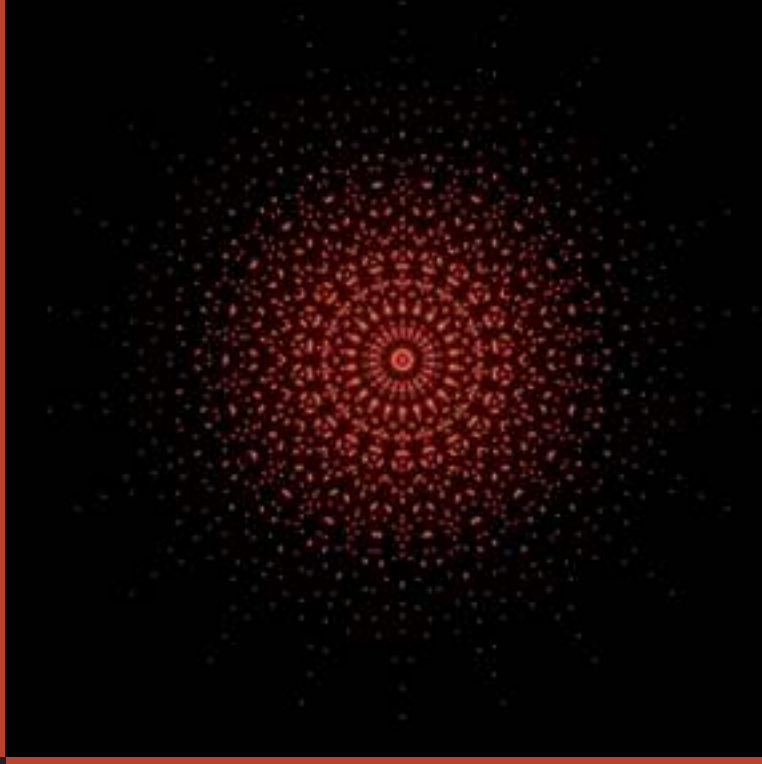
Reticulados via Corpos Ciclotômicos

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, 191 p. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.



editora unesp DIGITAL

Carina Alves
Antonio Aparecido de Andrade

Reticulados via corpos ciclotômicos

Reticulados via Corpos Ciclotômicos

CARINA ALVES
ANTONIO APARECIDO DE ANDRADE

Reticulados via Corpos Ciclotômicos

editora unesp DIGITAL

Praça da Sé, 108
01001-900 – São Paulo – SP
Tel.: (0xx11) 3242-7171
Fax: (0xx11) 3242-7172
www.editoraunesp.com.br
www.livrariaunesp.com.br
feu@editora.unesp.br

CIP – Brasil. Catalogação na fonte
Sindicato Nacional dos Editores de Livros, RJ

A478r

Alves, Carina
Reticulados via corpos ciclotômicos / Carina Alves, Antonio Aparecido de Andrade. São Paulo: Editora Unesp Digital, 2014.

Recurso digital
Formato: ePDF
Requisitos do sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
ISBN 978-85-68334-39-3 (recurso eletrônico)

1. Álgebra. 2. Engenharia. 3. Livros eletrônicos. I. Andrade, Antonio Aparecido de. II. Título.

15-20467 CDD: 512.5
CDU: 512.64

Este livro é publicado pelo projeto *Edição de Textos de Docentes e Pós-Graduados da UNESP* – Pró-Reitoria de Pós-Graduação da UNESP (PROPG) / Fundação Editora da UNESP (FEU)

Editora afiliada:

Asociación de Editoriales Universitarias de América Latina y el Caribe

Associação Brasileira de Editoras Universitárias

Agradecimentos

A Deus.

Ao professor Antonio Aparecido de Andrade, pela amizade tão sincera, pela paciência, pela dedicação e pelo desprendimento durante a valiosa orientação.

Aos professores do Departamento de Matemática da Unesp, *campus* de São José do Rio Preto, pela excelente formação e amizade.

Aos professores da banca examinadora: Ali Messaoudi (Ibilce/ Unesp, *campus* de São José do Rio Preto), Raul Antonio Ferraz (IME/USP, São Paulo), Trajano P. N. Neto (Ibilce/ Unesp, *campus* de São José do Rio Preto) e Marcelo Muniz da Silva Alves (UFPR, Curitiba, PR).

Aos meus colegas do curso de pós-graduação, pelo agradável convívio.

À minha amiga Cristiane, por compartilhar as alegrias, tris-

tezas e dificuldades durante nossa caminhada que ora completamos.

Aos meus pais Vanir Caldeira Alves e Atamir José Alves, que me ensinam, me incentivam e me possibilitam sonhar e crer que tudo é possível. Que a todo momento, através de um abraço forte e um sorriso sincero, me fazem ver a vida com outros olhos.

À minha irmã Luciana Alves, por me apoiar principalmente nos momentos difíceis e por compartilhar os momentos de alegria.

Aos meus avós que plantaram em meu coração a semente de perseverança e solidariedade, humildade e confiança, de amor e paz.

À Fapesp pelo auxílio financeiro.

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

"É graça divina começar bem e persistir na caminhada certa.
Graça maior é diante das dificuldades não desistir nunca,
pois provavelmente aquele que nunca cometeu um erro
nunca fez uma descoberta."

D. Hélder Câmara e Samuel Smiles

Aos meus pais Atamir José Alves e Vanir Caldeira Alves
e à minha irmã Luciana Alves,
dedico.

Lista de símbolos

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

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

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

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

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

∂f: grau do polinômio f

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

$\prod$: produtório

$\sum$: somatório

$det\ A$: determinante de A

(a_{ij}): matriz

$f_\alpha(X)$: polinômio característico de α

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

$\mathbb{A}_\mathbb{K}$: anel dos inteiros de $\mathbb{K}$

$\#X$: cardinalidade do conjunto X

$\mathfrak{a}, \mathfrak{b}, \ldots$: ideais

$\varphi(n)$: função de Euler para o inteiro n

$A[X]$: anel dos polinômios sobre A em X

$K(\alpha_1, \ldots, \alpha_n)$: corpo obtido pela adjunção de $\alpha_1, \ldots, \alpha_n$ a K

$\frac{A}{I}$: quociente de A por I

$\forall$: para todo

$\exists$: existe

ξ_n: $e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, raiz n-ésima primitiva da unidade

$\overline{x}$: conjugado complexo do elemento x

$D_{\mathbb{K}}$: discriminante absoluto do corpo $\mathbb{K}$

$Tr_{\mathbb{L}/\mathbb{K}}$: traço em relação à extensão $\mathbb{L}/\mathbb{K}$

$N_{\mathbb{L}/\mathbb{K}}$: norma em relação à extensão $\mathbb{L}/\mathbb{K}$

$irr(\alpha, \mathbb{K})$: polinômio irredutível de α sobre $\mathbb{K}$

$\ker(f)$: núcleo do homomorfismo f

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

$Gal(\mathbb{L}/\mathbb{K})$: grupo de Galois de $\mathbb{L}/\mathbb{K}$

$a|b$: a divide b

$O_m(a)$: ordem de a módulo m, com $mdc(a, m) = 1$

$D(\mathfrak{p})$: grupo de decomposição com relação a $\mathfrak{p}$

$E(\mathfrak{p})$: grupo de inércia com relação a $\mathfrak{p}$

$min(X)$: mínimo do conjunto X

$\delta(\Lambda)$: densidade de centro do reticulado Λ

$\overline{\sigma}$: conjugação complexa ($\overline{\sigma}(x) = \overline{x}$)

$\underline{X} = (X_1, \cdots, X_n)$ em $\mathbb{R}^n$

$v_p(m)$: valorização p-ádica de m

$[z]$: o inteiro mais próximo de z

d_{min} : distância mínima

γ : ganho fundamental de codificação

Δ : densidade de empacotamento esférico

η : eficiência espectral

E : energia da constelação

E_b : energia por bit

N_0 : potência do ruído

L : diversidade

G_a : ganho assintótico

$erfc$: função erro

Sumário

Introdução

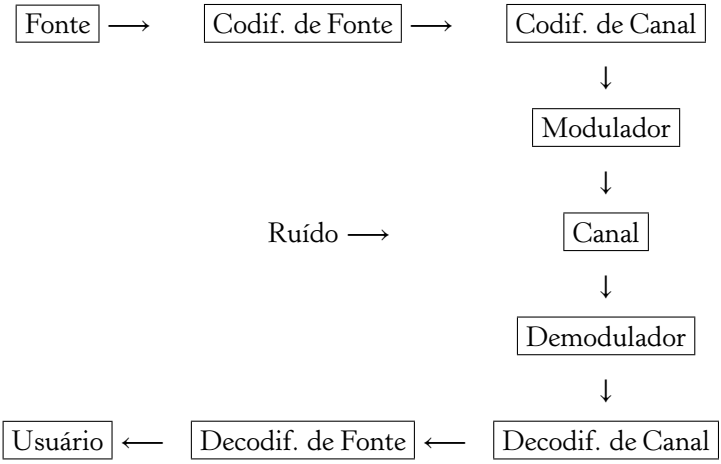
Em um sistema de comunicação digital, o objetivo é transmitir dados de uma fonte até um usuário. O meio usado para esta transmissão é chamado de canal e pode ser um cabo coaxial, fibra óptica, a atmosfera (no caso de ondas de rádio) etc.

Em um sistema tradicional, os dados gerados pela fonte são símbolos de um alfabeto A. Como cada símbolo tem sua probabilidade de ocorrência, estes dados são processados pelo codificador de fonte, com o objetivo de eliminar redundância, ou seja, tornar os símbolos equiprováveis e desta forma compactar a informação.

As sequências geradas pelo codificador de fonte são então processadas pelo codificador de canal, que introduz redundância, gerando sequências de símbolos de A que são chamadas de palavras código. Para a transmissão, o modulador associa a cada palavra código x um símbolo analógico, que é então enviado pelo canal.

A imperfeição do canal gera distorções e o sinal recebido nem

sempre coincide com o enviado. O demodulador faz então a melhor estimativa, fornecendo uma sequência r de símbolos de A. Devido ao ruído, é possível que r não seja uma palavra código. Então o decodificador de canal associará uma palavra código, que é a melhor estimativa. Finalmente, o decodificador de fonte associará a esta palavra código a suposta sequência original de símbolos enviada. O diagrama abaixo ilustra o processo.



Cada uma destas etapas gerou grandes áreas de pesquisa, que se desenvolveram, de certa forma, independentemente.

A teoria dos códigos corretores de erros nasceu em 1948, com o famoso trabalho de Shannon (1948), no qual foi demonstrado o Teorema da Capacidade de Canal. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico δ satisfazendo

$$\delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde ζ é a função zeta de Riemann. Como consequência, obtém-se

$$\frac{1}{n} log_2 \delta \geq -1. \tag{1}$$

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$, Conway e Sloane (199) provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (1) são equivalentes a códigos atingindo a capacidade do canal.

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando teoria algébrica dos números, Craig (1978) reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal no anel de inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Embora os resultados apresentados aqui não sejam traduções fiéis dos originais, eles são equivalentes ou consequências dos mesmos. Des-
sa forma, o restante do livro está delineado na sequência que segue.

O Capítulo 1, visa atender aos leitores com menos conhecimentos em teoria algébrica dos números. Sendo assim, introduzimos os conceitos de módulo, inteiro algébrico, norma e traço de um elemento, discriminante, base integral, anel de Dedekind e outros conceitos indispensáveis ao desenvolvimento dos demais capítulos. Além disso, estudamos formas quadráticas, cuja aplicação se faz quando tentamos determinar o raio de empacotamento da realização geométrica de um ideal em questão. No Capítulo 2, apresentamos um estudo sobre corpos de números, dando ênfase ao estudo dos anéis dos inteiros e discriminantes de corpos quadráticos e ciclotômicos. Também apresentamos a decomposição de um ideal primo em uma extensão fazendo uso do Teorema de Kummer.

No Capítulo 3, apresentamos as definições de reticulado, empacotamento esférico, volume e densidade de centro. Além disso,

apresentamos o método de Minkowski para obtenção de reticulados via a representação geométrica de ideais dos anéis de inteiros algébricos.

O estudo desses capítulos proporcionou-nos ferramentas necessárias para o estudo do Capítulo 4, no qual apresentamos o tema central desse livro. Este capítulo traz um método para o cálculo da densidade de centro de reticulados gerados através de ideais dos anéis de inteiros de $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$, onde p e q são números primos distintos e r é um inteiro maior ou igual a 1.

No Capítulo 5, no qual finalizamos nosso trabalho, apresentamos através do trabalho de Boutros; Viterbo; Rastello; Belfiori (1996), constelações de reticulados que são eficientes para ambos os canais Gaussianos e Rayleigh com desvanecimento, enfocando as construções das versões rotacionadas dos reticulados já conhecidos na literatura, tais como, $\boldsymbol{D}_4$, $\boldsymbol{K}_{12}$ e Λ_{16}, através da matriz mudança de base de um ideal contido no anel dos inteiros de um corpo de números.

1
Corpos de números

1.1 Introdução

Neste capítulo, apresentamos uma coletânea de resultados básicos de teoria algébrica dos números. O objetivo é fornecer a base teórica para o desenvolvimento dos demais capítulos. Aqui introduzimos os conceitos de módulos, elementos inteiros sobre um anel, elementos algébricos sobre um corpo e extensões algébricas, norma e traço em uma extensão, discriminante, anéis noetherianos e anéis de Dedekind, norma de um ideal e formas quadráticas sobre o $\mathbb{R}^n$.

1.2 Módulos

Iniciamos esta seção com as definições de módulos e submódulos. Em seguida apresentamos um teorema que será de grande utilidade posteriormente.

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

i) $a(x + y) = ax + ay$;

ii) $(a + b)x = ax + bx$;

iii) $(ab)x = a(bx)$;

iv) $1x = x$.

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

Um A-módulo M é dito **finitamente gerado** se existem $x_1, \cdots, x_r \in M$ tais que $M = Ax_1 + \cdots + Ax_r$ e, neste caso, dizemos que $x_1, \cdots, x_r$ formam um **sistema de geradores** de M. Um conjunto de elementos $y_1, \cdots, y_s \in M$ são linearmente independentes (sobre A) se a igualdade $\sum_{j=1}^{s} a_j y_j = 0$, com $a_j \in A$, implicar que $a_1 = \cdots = a_s = 0$. Mas, se além disso, $y_1, \cdots, y_s$ formarem um sistema de geradores de M, então eles formam uma base de M. Porém, é importante notar que nem todo módulo finitamente gerado possui um base. Um A-módulo que possui uma base é chamado de um A-**módulo livre**, e o número de elementos da base é chamado de **posto** de M.

Teorema 1.2.1. *Sejam A um anel principal, M um A-módulo livre de posto n, e M' um A-submódulo de M. Então:*

i) M' é livre de posto q, $0 \leq q \leq n$.

ii) Se $M' \neq 0$, então existe uma base $\{e_1, \cdots, e_n\}$ de M e elementos

não nulos $a_1, \cdots, a_q \in A$ *tais que* $\{a_1e_1, \cdots, a_qe_q\}$ *é uma base de* M' *e que* a_i *divide* a_{i+1}, $1 \leq i \leq q-1$.

Demonstração. (Samuel, 1976, p.21, Teo.1). ■

1.3 Elementos inteiros sobre um anel

Nesta seção apresentamos as definições de elemento algébrico, extensão algébrica e polinômio minimal.

Definição 1.3.1. *Sejam* B *um anel e* $A \subset B$ *um subanel. Um elemento* $\alpha \in B$ *é chamado* **inteiro** *sobre* A *se* α *é raiz de um polinômio mônico com coeficientes em* A. *Se* $A = \mathbb{Z}$ *e* $B \subset \mathbb{C}$, *dizemos que* α *é um* **inteiro algébrico**.

Observação 1.3.1. *Denotaremos o conjunto dos elementos que estão em* B *e são inteiros sobre* A *por* $\mathbb{A}_B$, *ou seja,* $\mathbb{A}_B = \{\alpha \in B : \alpha \text{ é inteiro sobre } A\}$.

Observação 1.3.2. $\mathbb{A}_B$ *é chamado* **fecho inteiro** *de* A *em* B *ou anel dos inteiros de* A *em* B. *Se* A *é um domínio e* $B = \mathbb{K}$ *é o corpo de frações de* A, *dizemos que* $\mathbb{A}_{\mathbb{K}}$ *é o fecho inteiro de* A *em* $\mathbb{K}$.

Exemplo 1.3.1. *O elemento* $\alpha = \sqrt{2} + \sqrt{3}$ *é inteiro sobre* $\mathbb{Z}$, *pois é raiz do seguinte polinômio* $X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$.

Definição 1.3.2. *Sejam* B *um anel e* $A \subset B$ *um subanel. Seja* $p(X) \in B[X]$ *um polinômio mônico tal que* $p(\alpha) = 0$, *com* $\alpha \in B$. *A relação* $p(\alpha) = 0$ *é chamada uma* **equação de dependência inteira** *de* α *sobre* A.

Exemplo 1.3.2. *O elemento* $\alpha = \sqrt{2} \in \mathbb{R}$ *é inteiro sobre* $\mathbb{Z}$. *A relação* $\alpha^2 - 2 = 0$ *é uma equação de dependência inteira.*

Teorema 1.3.1. *(*Samuel,1967, p.27, Teo.1*) Sejam B um anel, A um subanel de B e α um elemento de B. Então as seguintes condições são equivalentes:*

1) *α é inteiro sobre A.*

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

3) *Existe um subanel R de B tal que R é um A-módulo finitamente gerado contendo A e α.*

Demonstração (1) $\Longrightarrow$ (2) Como $\alpha \in B$ é inteiro sobre A, então $\alpha \in \mathbb{A}_B$, ou seja, α é raiz de um polinômio mônico com coeficientes em A. Logo existem $a_0, a_1, \cdots, a_{n-1} \in A$ não todos nulos tal que

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

Seja $M = [1, \alpha, \alpha^2, \cdots, \alpha^{n-1}]$ o A-módulo finitamente gerado. Vamos mostrar que $A[\alpha] = M$. Por definição

$$A[\alpha] = \left\{ \sum_i a_i\alpha^i \ : \ a_i \in A \right\}$$

e assim, pelo modo como definimos M, segue que $M \subset A[\alpha]$. Por outro lado,

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \tag{1.1}$$

e assim $\alpha^n \in M$. Portanto $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n \in M$. Agora provaremos por indução sobre j que $\alpha^j \in M$, $\forall\, j = n+1, n+2, \cdots$. Para $j = 0, \cdots, n$ vimos acima que o resultado é válido. Agora suponhamos que o resultado seja válido para $j > n$ e provemos que o resultado vale para $j+1$. Sendo $\alpha^j = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ com $b_i \in A$, então

$$\alpha^{j+1} = b_0\alpha + b_1\alpha^2 + \cdots + b_{n-2}\alpha^{n-1} + b_{n-1}\alpha^n. \tag{1.2}$$

Substituindo (1.1) em (1.2) temos

$$\alpha^{j+1} = -b_{n-1}a_0 + (b_0 - b_{n-1}a_1)\alpha + \cdots + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1}$$

e assim $\alpha^{j+1} \in M$. Portanto $A[\alpha] \subseteq M$. Portanto $A[\alpha] = M$.

(2) $\Longrightarrow$ (3) Como $A \subset A[\alpha]$, $\alpha \in A[\alpha]$ e, por hipótese, $A[\alpha]$ é um A-módulo finitamente gerado, então é suficiente tomar $R = A[\alpha]$.

(3) $\Longrightarrow$ (1) Seja R um A-módulo finitamente gerado que contém A e α e sejam $\{y_1, y_2, \cdots, y_n\}$ os geradores de R, ou seja, $R = Ay_1 + \cdots + Ay_n$. Como $\alpha \in R$ e como R é um subanel de B segue que $\alpha y_i \in R$, $\forall\, i = 1, \cdots, n$. Assim,

$$\begin{cases} \alpha y_1 = a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n \\ \alpha y_2 = a_{21}y_1 + a_{22}y_2 + \cdots + a_{2n}y_n \\ \vdots \\ \alpha y_n = a_{n1}y_1 + a_{n2}y_2 + \cdots + a_{nn}y_n \end{cases}, \quad a_{ij} \in A.$$

Daí segue que $\sum_{j=1}^{n}(\delta_{ij}\alpha - a_{ij})y_j = 0$; onde $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$.

Considere o sistema linear homogêneo definido pelas n equações nas variáveis $y_1, \cdots, y_n$. Ou seja,

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

Seja $d = det(\delta_{ij}\alpha - a_{ij})$. Por Cramer $dy_i = 0$, $\forall\, i = 1, \cdots, n$. Portanto $db = 0$, $\forall\, b \in R$. Em particular $d \cdot 1 = d = 0$. Mas d é uma expressão polinomial em α e o coeficiente da maior potência de α é 1, pois o termo de maior grau aparece na expansão do produto $\prod_{i=1}^{n}(\alpha - a_{ii})$ das entradas da diagonal principal. Portanto α é inteiro sobre A.

■

Corolário 1.3.1. *(*Samuel, 1967, p.28, Prop.1*) Sejam B um anel, A um subanel de B e $\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subset B$. Se α_i é inteiro sobre $A[\alpha_1, \alpha_2, \cdots,$*

$\alpha_{i-1}]$, em particular, se α_i é inteiro sobre A para todo $i = i, \cdots, n$, então $A[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um A-módulo finitamente gerado.

Demonstração. A demonstração será feita por indução sobre n. Para $n = 1$ segue do Teorema 1.3.1, pois se α_1 é inteiro sobre A, então $A[\alpha_1]$, é um A-módulo finitamente gerado. Assim, suponhamos que o teorema seja verdadeiro para $n-1$ elementos e provaremos que o teorema é válido para n elementos. Por hipótese de indução temos que $R = A[\alpha_1, \cdots, \alpha_{n-1}]$ é um A-módulo finitamente gerado, isto é, $R = \sum_{j=1}^{n} Av_j$, onde $v_1, \cdots, v_n \in R$. Visto que α_n é inteiro sobre R temos, pelo Teorema 1.3.1, que $R[\alpha_n]$ é um R-módulo finitamente gerado, isto é, $R[\alpha_n] = \sum_{i=1}^{s} Rw_i$, onde $w_1, \cdots, w_s \in R[\alpha_n]$. Então $A[\alpha_1, \cdots, \alpha_n] = R[\alpha_n] = \sum_{i=1}^{s} Rw_i = \sum_{i=1}^{s}\left(\sum_{j=1}^{n} Av_j\right) w_i = \sum_{i,j} Av_j w_i$. Portanto $\{v_j w_i\}$ gera $A[\alpha_1, \cdots, \alpha_n]$ como um A-módulo. Portanto $A[\alpha_1, \cdots, \alpha_n]$ é um A-módulo finitamente gerado. ■

Teorema 1.3.2. *(*Stewart; Tall, 1987, p.47, Teo.2.9*) Se α é uma raiz de um polinômio mônico, onde os coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Demonstração. Seja $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$, tal que a_i, $i = 1, \cdots, n-1$ pertença ao conjunto de todos os números complexos que são raízes de polinômios mônicos com coeficientes em $\mathbb{Z}$. Fazendo $B = \mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ e $b_0 = a_0, \cdots, b_{n-1} = a_{n-1}$ e $b_n = \alpha$ e temos, pelo Corolário 1.3.1, que $\mathbb{Z}[b_0, \cdots, b_n]$ é um $\mathbb{Z}$-módulo finitamente gerado e portanto α é um inteiro algébrico. ■

Corolário 1.3.2. *(*Samuel, 1967, p.29, Corol.1 *) Sejam B um anel e A um subanel de B. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\mathbb{A}, \alpha\beta \in \mathbb{A}_B$.*

Demonstração. Pela Observação 1.3.1, temos que mostrar que $\mathbb{A}, \alpha\beta$ são inteiros sobre A. Temos que $\mathbb{A}, \alpha\beta \in A[\alpha, \beta]$. Como α, β são inteiros sobre A temos então, pelo Corolário 1.3.1, que $A[\alpha, \beta]$ é um A-módulo finitamente gerado. Assim, existe um A-módulo finitamente gerado, $A[\alpha, \beta]$, que contém $\mathbb{A}$ e $\alpha\beta$. Deste modo, pelo Teorema 1.3.1, $\mathbb{A}$ e $\alpha\beta$ são inteiros sobre A, isto é, $\mathbb{A}, \alpha\beta \in \mathbb{A}_B$. ■

Corolário 1.3.3. *(*Samuel, 1967, p.29, Corol.2*) Sejam B um anel e A um subanel de B. O conjunto $\mathbb{A}_B$ dos elementos de B que são inteiros sobre A é um subanel de B que contém A.*

Demonstração. Pelo Corolário 1.3.2, segue que $\mathbb{A} \in \mathbb{A}_B$ e $\alpha\beta \in \mathbb{A}_B$,

$\forall\, \alpha, \beta \in \mathbb{A}_B$, assim $\mathbb{A}_B$ é subanel de B. Por outro lado $A \subset \mathbb{A}_B$, pois se $a \in A$, então a é raiz do polinômio mônico $p(X) = X - a$, que tem coeficientes em A, isto é, a é inteiro sobre A e assim $a \in \mathbb{A}_B$. ■

Definição 1.3.3. *Sejam B um anel e A um subanel de B. Dizemos que B é inteiro sobre A, se todo elemento de B é inteiro sobre A, isto é, se $\mathbb{A}_B = B$.*

Exemplo 1.3.3. *Dentre os anéis que satisfazem esta condição, citamos o anel dos inteiros de Gauss contendo $\mathbb{Z}$, pois todo elemento $a+bi$ de $\mathbb{Z}[i]$ é raiz do polinômio $X^2-2aX+(a^2+b^2) \in \mathbb{Z}[X]$.*

Proposição 1.3.1. *(*Samuel, 1967, p.29, Prop.2*) Sejam R um anel, B um subanel de R e A um subanel de B. Então R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

Demonstração. Suponhamos R inteiro sobre A e seja $\alpha \in B$. Como $B \subset R$, segue que α é inteiro sobre A, ou seja, B é inteiro sobre A. Para mostrar que R é inteiro sobre B, seja $\alpha \in R$. Então existem $a_0, a_1, \ldots, a_{n-1} \in A$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Como $A \subset B$, segue que α é inteiro sobre B, ou seja, R é inteiro sobre B. Por outro lado, seja $\alpha \in R$. Como R é inteiro sobre B, então existem $b_0, b_1, \cdots, b_{n-1} \in B$, não todos nulos tal que $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Seja $C = A[b_0, b_1, \cdots, b_{n-1}]$. Logo α é inteiro sobre C, pois α é raiz de um polinômio mônico com coeficientes em C. Como B é inteiro sobre A, segue que os $b_i^{'}s \in B$ são inteiros sobre A. Daí pelo Corolário 1.3.1 temos que $A[b_0, \cdots, b_{n-1}, \alpha] = C[\alpha]$ é um A-módulo finitamente gerado e pela parte (c) do Teorema 1.3.1, segue que α é inteiro sobre A. Portanto R é inteiro sobre A. ■

Proposição 1.3.2. *(*Samuel, 1967, p.29, Prop.3*) Sejam $A \subseteq B$ anéis com B um domínio e inteiro sobre A. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração. Suponha que A seja um corpo. Seja $\alpha \in B$, $\alpha \neq 0$. Como B é inteiro sobre A então α é inteiro sobre A e portanto pelo Teorema 1.3.1 segue que $A[\alpha]$ é um espaço vetorial finitamente gerado sobre A, pois A é um corpo. Seja

$$\begin{aligned} \phi : A[\alpha] &\longrightarrow A[\alpha] \\ b &\longrightarrow b\alpha, \quad \forall\, b \in A[\alpha]. \end{aligned}$$

Temos que ϕ é A-linear e $Ker(\phi) = \{b \in A[\alpha] : \phi(b) = 0\} = \{0\}$, pois $\phi(b) = 0$ se, e somente se, $b\alpha = 0$ e como B é um domínio e $\alpha \neq 0$ segue que b=0. Deste modo, ϕ é injetora e como estamos considerando espaços de mesma dimensão finita, segue que ϕ é sobrejetora. Portanto ϕ é bijetora. Assim, como $1 \in A[\alpha]$ segue

que exite $b' \in A[\alpha]$ tal que $b'\alpha = 1$, ou seja, α é inversível em B. Portanto B é um corpo. Por outro lado, seja $\alpha \in A$, $\alpha \neq 0$. Como $A \subset B$ então $\alpha \in B$ e como B é um corpo segue que $\alpha^{-1} \in B$. Como B é inteiro sobre A, e $\alpha^{-1} \in B$ segue que

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

com $a_i \in A$ não todos nulos. Multiplicando por α^{n-1}, obtemos

$$\alpha^{-1} + a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1} = 0$$

e então $\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1}) \in A$.

Portanto A é um corpo. ■

Definição 1.3.4. *Um anel A é chamado* **integralmente fechado** *quando A é um domínio e é seu próprio fecho inteiro. Em outras palavras, um anel A é integralmente fechado se todo elemento do seu corpo de frações que é inteiro sobre A está em A.*

Proposição 1.3.3. *(*Samuel, 1967, p.30, Ex.1*) Se A é domínio, então $\mathbb{A}_B$ é integralmente fechado.*

Demonstração. Segue do fato de que o fecho inteiro de $\mathbb{A}_B$ é inteiro sobre $\mathbb{A}_B$, portanto sobre A. ■

Proposição 1.3.4. *(*Samuel, 1967, p.30, Ex.2*) Se A é um domínio principal então A é integralmente fechado.*

Demonstração. Seja $\mathbb{K}$ o corpo de frações de A. Seja $\alpha \in \mathbb{K}$ inteiro sobre A, isto é, $\alpha \in \mathbb{A}_{\mathbb{K}}$ tal que $\alpha = \frac{a}{b}$, $a, b \in A$, $b \neq 0$ e $mdc(a, b) = 1$. Então existem $a_i \in A$, $i = 0, 1, \cdots, n-1$, não todos nulos, tal que

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

Substituindo α por $\frac{a}{b}$ temos

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_1\left(\frac{a}{b}\right) + a_0 = 0.$$

Multiplicando por b^n ambos os lados, obtemos

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n = 0,$$

e assim

$$a^n = -b(a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1}).$$

Portanto $b|a^n$ e como $mdc(a,b) = 1$ segue que $b|a$, ou seja, $a = bc$. Sendo $mdc(a, b) = 1$ então existe x_0, $y_0 \in A$ tal que $ax_0 + by_0 = 1 \Longrightarrow bcx_0 + by_0 = 1 \Longrightarrow b(cx_0 + y_0) = 1$. Portanto b é inversível em A. Assim, $\alpha = ab^{-1} \in A$. Portanto $\mathbb{A}_{\mathbb{K}} \subset A$ e como $A \subset \mathbb{A}_{\mathbb{K}}$ segue que $A = \mathbb{A}_{\mathbb{K}}$. Portanto A é integralmente fechado. ■

Exemplo 1.3.4. *O anel $\mathbb{Z}$ dos números inteiros é integralmente fechado, pois é principal.*

Exemplo 1.3.5. *Todo domínio fatorial é integralmente fechado, uma vez que é principal.*

1.4 Elementos algébricos sobre um corpo e extensões algébricas

Nesta seção apresentamos as definições de elemento algébrico, extensão algébrica e polinômio minimal.

Para isso, sejam A um anel e $\mathbb{K}$ um corpo de A. Dizemos que um elemento $\alpha \in A$ é **algébrico** sobre $\mathbb{K}$, se α é raiz de um polinômio não nulo, com coeficientes em $\mathbb{K}$. Se todo elemento de A for algébrico sobre $\mathbb{K}$, dizemos que A é algébrico sobre $\mathbb{K}$. Um elemento de A que não é algébrico sobre $\mathbb{K}$ é dito transcendente sobre

$\mathbb{K}$. Se A é um corpo então A é chamado uma extensão algébrica de $\mathbb{K}$. Um corpo de números é uma extensão finita dos racionais. Sabemos, pelo Teorema do Elemento Primitivo, que um corpo de números $\mathbb{K}$ de grau n é da forma $\mathbb{Q}(\alpha)$ para algum elemento $\alpha \in \mathbb{K}$. Como o polinômio minimal de α sobre $\mathbb{Q}$ é de grau n, segue que $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, i = 0, \cdots, n-1\}$, e esta representação é única, ou seja, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base para o espaço vetorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Segundo a definição, sendo α um elemento algébrico sobre um corpo $\mathbb{K}$, α satisfaz uma equação do tipo, $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, com $a_i \in \mathbb{K}$, $a_n \neq 0$. Multiplicando essa equação por a_n^{-1}, obtemos uma equação de dependência inteira, $\alpha^n + a_n^{-1}a_{n-1}\alpha^{n-1} + \cdots + a_n^{-1}a_1\alpha + a_n^{-1}a_0 = 0$, e portanto, sobre um corpo, o conceito de elemento algébrico coincide com o de elemento inteiro.

Exemplo 1.4.1. *O elemento* $\alpha = \sqrt{3} + \sqrt{-5}$ *é algébrico sobre* $\mathbb{Q}$, *pois é raiz do polinômio* $X^4 + 4X^2 + 64 \in \mathbb{Q}[X]$.

Definição 1.4.1. *Sejam* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos e* α *um elemento de* $\mathbb{L}$. *O polinômio mônico e de menor grau em* $\mathbb{K}[X]$ *que tem* α *como raiz é chamado de* **polinômio minimal** *de* α *sobre* $\mathbb{K}$ *e seu grau é* $[\mathbb{K}(\alpha) : \mathbb{K}]$.

1.5 Norma e traço em uma extensão

Nesta seção apresentamos os conceitos de norma e traço, onde a Proposição 1.5.2 e o Corolário 1.5.1 são os principais resultados.

Sejam A um anel e B um A-módulo livre de posto n. Sejam $\psi : B \longrightarrow B$ um homomorfismo de anéis e $\{e_1, e_2, \cdots, e_n\}$ uma

base de B sobre A. Então

$$\begin{cases} \psi(e_1) = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n \\ \psi(e_2) = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n \\ \vdots \\ \psi(e_n) = a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n, \end{cases}$$

com $a_{ij} \in A$, para todo $i, j = 1, \cdots, n$. Assim

$$\begin{bmatrix} \psi(e_1) \\ \psi(e_2) \\ \vdots \\ \psi(e_n) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}.$$

Definição 1.5.1. *Definimos o* **traço** *de* ψ *por* $Tr(\psi) = \sum_{i=1}^{n} a_{ii}$, *a* **norma** *de* ψ *por* $N(\psi) = \det(a_{ij})$ *e o* **polinômio característico** *de* ψ *por* $g(X) = \det(X.I - \psi) = \det(X\delta_{ij} - a_{ij})$.

Como consequência imediata desta definição tem-se:

$$Tr(\psi + \psi') = Tr(\psi) + Tr(\psi'),$$
$$N(\psi\psi') = N(\psi)N(\psi'),$$
$$\det(X.I - \psi) = X^n - Tr(\psi)X^{n-1} + \cdots + (-1)^n \det(\psi).$$

Definição 1.5.2. *Sejam* A *um anel e* B *um* A*-módulo livre. Seja o endomorfismo* $\psi_\alpha : B \longrightarrow B$ *definido por* $\psi_\alpha(x) = \alpha x$, *para todo* $x \in B$. *Definimos o traço (respectivamente, norma e polinômio característico) de* $\alpha \in B$ *relativo a* A, *como o traço (respectivamente, determinante e polinômio característico) do endomorfismo* ψ_α.

Usaremos as notações $Tr_{B/A}(\alpha)$, $N_{B/A}(\alpha)$, ou simplesmente, $Tr(\alpha)$, $N(\alpha)$ quando não houver possibilidade de confusão.

Observação 1.5.1. i) *O traço e a norma são elementos de* A.

ii) *O polinômio característico é um polinômio mônico com coeficientes em* A.

iii) *Para* $\alpha, \alpha' \in B$ *e* $a \in A$ *temos que* $\psi_\alpha + \psi_{\alpha'} = \psi_{\alpha+\alpha'}$ *e* $\psi_\alpha \circ \psi_{\alpha'} = \psi_{\alpha\alpha'}$ *e* $\psi_{a\alpha} = a\psi_\alpha$. *Além disso, a matriz de* ψ_a *com respeito a uma base de* B *sobre* A *é a matriz diagonal cujas entradas não nulas são* a.

Proposição 1.5.1. *(*Samuel, 1967, p.36, Prop.1*) Sejam* $\mathbb{K}$ *um corpo de característica zero ou um corpo finito,* $\mathbb{L}$ *uma extensão algébrica de* $\mathbb{K}$ *de grau* n, α *um elemento de* $\mathbb{L}$ *e* $\alpha_1, \cdots, \alpha_n$ *as raízes do polinômio minimal de* α *sobre* $\mathbb{K}$. *Então* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n$, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n$ *e* $g(X) = (X - \alpha_1) \cdots (X - \alpha_n)$.

Demonstração. Consideraremos primeiramente o caso em que α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $f(X)$ o polinômio minimal de α sobre $\mathbb{K}$. Então $\mathbb{L}$ é $\mathbb{K}$-isomorfo a $\mathbb{K}[X]/ < f(X) >$ e $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Tomando $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, com $a_i \in \mathbb{K}$, temos que a matriz do endomorfismo ψ_α com respeito a esta base é dada por

$$\begin{cases} \psi_\alpha(1) = \alpha \\ \psi_\alpha(\alpha) = \alpha^2 \\ \vdots \\ \psi_\alpha(\alpha^{n-1}) = \alpha^n \end{cases} \Longrightarrow M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{bmatrix}.$$

Assim, $det(X.I - \psi_\alpha)$ é o determinante da matriz

$$X.I_n - M = \begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & \vdots \\ \vdots & 0 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & X & a_{n-2} \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{bmatrix}.$$

Expandindo esse determinante como um polinômio em X, obtemos o polinômio característico de α, que é igual a $f(X)$ e temos que $Tr(\alpha) = -a_{n-1}$ e $N(\alpha) = (-1)^n a_0$. Como α é primitivo, segue que $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ e igualando os coeficientes vemos que $Tr(\alpha) = \alpha_1 + \cdots + \alpha_n$ e $N(\alpha) = \alpha_1 \cdots \alpha_n$.

Consideremos agora o caso geral. Se $r = [\mathbb{L} : \mathbb{K}[\alpha]]$, é suficiente mostrarmos que o polinômio característico $g(X)$ de α, com relação a $\mathbb{L}$ sobre $\mathbb{K}$, é igual a r-ésima potência do polinômio minimal de α sobre $\mathbb{K}$. Seja $\{y_i\}_{i=1,\cdots,q}$ uma base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ e seja $\{z_j\}_{j=1,\cdots,r}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}[\alpha]$. Então $\{y_i z_j\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $n = qr$. Se $M = (a_{ih})$ é a matriz de multiplicação por α em $\mathbb{K}[\alpha]$ com relação a base $\{y_i\}$, temos que $\alpha y_i = \sum_h a_{ih} y_h$. Então temos, $\alpha(y_i z_j) = \left(\sum_h a_{ih} y_h \right) z_j = \sum_h a_{ih} \left(y_h z_j \right)$. Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{12} y_2 z_1 + \cdots + a_{1q} y_q z_1 \\ \alpha y_2 z_1 = a_{21} y_1 z_1 + a_{22} y_2 z_1 + \cdots + a_{2q} y_q z_1 \\ \vdots \\ \alpha y_q z_1 = a_{q1} y_1 z_1 + a_{q2} y_2 z_1 + \cdots + a_{qq} y_q z_1. \end{cases}$$

Assim, a matriz do endomorfismo de α em $\mathbb{L}$ com relação a base $\{y_i z_j\}$, ordenada lexicograficamente é dada por

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & M \end{bmatrix},$$

isto é, M aparece r-vezes na diagonal como blocos na matriz M_1. Daí, a matriz $XI_n - M_1$ consiste de r blocos diagonais, cada um tem a forma $XI_q - M$, e consequentemente, $det(XI_n - M_1) = det(XI_q -$

$M_1)^r$. Assim $g(X) = det(XI_q - M)$ e $det(XI_q - M)$ é o polinômio característico de α sobre $\mathbb{K}$, de acordo com a primeira parte da demonstração. ■

Proposição 1.5.2. *(*Samuel, 1967, p.38, Prop.2*) Sejam A um domínio, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e α um elemento de $\mathbb{L}$ inteiro sobre A. Então os coeficientes do polinômio característico $g(X)$ de α relativo a $\mathbb{L}$ sobre $\mathbb{K}$, em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$, são inteiros sobre A.*

Demonstração. Pela Proposição 1.5.1, temos que $g(X) = (X - \alpha_1) \cdots$

$(X - \alpha_n)$. Como os coeficientes de $g(X)$ a menos de sinal, são somas de produtos dos $\alpha_i^{'}s$, é suficiente mostrarmos que cada α_i é inteiro sobre A. Mas cada α_i é um conjugado de α sobre $\mathbb{K}$, ou seja, existe um $\mathbb{K}$-isomorfismo $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$ tal que $\sigma_i(\alpha) = \alpha_i$. Como α é inteiro sobre A, então

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

com $a_i \in A$ não todos nulos. Aplicando σ_i, obtemos

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

ou seja, $\sigma_i(\alpha) = \alpha_i$ é inteiro sobre A, portanto $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$, são inteiros sobre A. ■

Corolário 1.5.1. *(*Samuel, 1967, p.38, Corol.1*) Nas condições da Proposição 1.5.2, se A é um anel integralmente fechado, então os coeficientes do polinômio característico de α, e em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A.*

Demonstração. Por definição esses coeficientes são elementos de $\mathbb{K}$. Pela Proposição 1.5.2 são inteiros sobre A. Logo, são elementos de A, pois A é integralmente fechado. ■

Observação 1.5.2. *Observando a Proposição 1.5.2 temos que* $Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$, $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ *e* $g_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$, *onde* σ_i, $i = 1, \cdots, n$ *são os* $\mathbb{K}$*- monomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$.

Sejam $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ corpos de números, α, $\alpha' \in \mathbb{M}$ e $a \in \mathbb{K}$. Então valem as seguintes propriedades:

1. $Tr_{\mathbb{M}/\mathbb{K}}(\alpha + \alpha') = Tr_{\mathbb{M}/\mathbb{K}}(\alpha) + Tr_{\mathbb{M}/\mathbb{K}}(\alpha')$
2. $Tr_{\mathbb{M}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{M}/\mathbb{K}}(\alpha)$
3. $Tr_{\mathbb{M}/\mathbb{K}}(a) = [\mathbb{M} : \mathbb{K}]a$
4. $Tr_{\mathbb{M}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\alpha))$.
5. $N_{\mathbb{M}/\mathbb{K}}(\alpha\alpha') = N_{\mathbb{M}/\mathbb{K}}(\alpha)N_{\mathbb{M}/\mathbb{K}}(\alpha')$
6. $N_{\mathbb{M}/\mathbb{K}}(a) = a^{[\mathbb{M}:\mathbb{K}]}$
7. $N_{\mathbb{M}/\mathbb{K}}(a\alpha) = a^{[\mathbb{M}:\mathbb{K}]}N_{\mathbb{M}/\mathbb{K}}(\alpha)$
8. $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$.

1.6 Discriminante

Nesta seção apresentamos o conceito de discriminante enfocando suas principais propriedades, e o Teorema 1.6.1 é o principal resultado.

Definição 1.6.1. *Sejam* B *um anel e* A *um subanel de* B *tal que* B *é um* A*-módulo livre de posto finito* n. *Dado* $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in B^n$, *definimos o seu* **discriminante** *por*

$$D_{B/A}(\alpha_1, \alpha_2, \cdots, \alpha_n) = det(Tr(\alpha_i\alpha_j)).$$

Exemplo 1.6.1. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *um corpo de números e* $\{1, \sqrt{3}\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$. *Então*

$$D_{B/A}(1, \sqrt{3}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{3}) \\ Tr(\sqrt{3}) & Tr(\sqrt{3})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 6 \end{vmatrix} = 12.$$

Proposição 1.6.1. *(*Samuel, 1967, p.38, Prop.1*) Seja* $(\alpha_1, \cdots, \alpha_n) \in B^n$. *Se* $(\beta_1, \cdots, \beta_n) \in B^n$ *é um conjunto de elementos de* B *tais que* $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, *com* $a_{ij} \in A$, *então*

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

Demonstração. Sejam $\beta_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^{n} a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in A$. Assim, $\beta_p\beta_q = \sum_{i=1}^{n} a_{pi}\alpha_i \sum_{j=1}^{n} a_{qj}\alpha_j = \sum_{i,j=1}^{n} a_{pi}a_{qj}\alpha_i\alpha_j$, e então $Tr(\beta_p\beta_q) = Tr(\sum_{i,j}^{n} a_{pi}a_{qj}\alpha_i\alpha_j) = \sum_{i,j}^{n} a_{pi}a_{qj}Tr(\alpha_i\alpha_j)$. Na forma matricial, temos $(Tr(\beta_p\beta_q)) = (a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t$. Pela Definição 1.6.1 temos que $D_{B/A}(\beta_1, \cdots, \beta_n) = det(Tr(\beta_p\beta_q))$. Logo

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

Exemplo 1.6.2. *Pelo exe 1.6.1 vimos que o discriminante da base* $\{1, \sqrt{3}\}$ *do corpo de números* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *é igual a* 12. *Agora, considerando uma outra base para o corpo* $\mathbb{K}$, *por exe,* $\{2-\sqrt{3}, 3+4\sqrt{3}\}$, *segue pela Proposição 1.6.1, que* $2-\sqrt{3} = 2\cdot 1 + (-1)\cdot\sqrt{3}$ *e* $3+4\sqrt{3} = 3\cdot 1 + 4\cdot\sqrt{3}$. *Assim*

$$D_{\mathbb{K}/\mathbb{Q}}(2-\sqrt{3}, 3+4\sqrt{3}) = \left(det\begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}\right)^2 D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{3}) = (11)^2 12.$$

Observação 1.6.1. *A Proposição 1.6.1 implica que o discriminante das bases de* B *sobre* A *são associados, isto é, a matriz* (a_{ij}) *que expressa uma base em termos da outra tem uma matriz inversa com entradas em* A. *Portanto, ambos* $det(a_{ij})$ *e* $det(a_{ij})^{-1}$ *são inversíveis em* A.

Definição 1.6.2. *Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. O discriminante de B sobre A é um ideal de A, dado por*

$$\mathfrak{D}_{B/A} = \langle D_{B/A}(\alpha_1, \cdots, \alpha_n) \rangle,$$

onde $\{\alpha_1, \cdots, \alpha_n\}$ é base de B sobre A.

Proposição 1.6.2. *(*Samuel, 1967, p.39, Prop.2*) Suponhamos que $\mathfrak{D}_{B/A}$ contém um elemento que não é um divisor de zero. Então, para que $(\alpha_1, \cdots, \alpha_n) \in B^n$ seja uma base de B sobre A, é necessário e suficiente que, $D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$.*

Demonstração. Se $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ é uma base de B sobre A, então pela Proposição 1.6.1, segue que $D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$. Reciprocamente, suponhamos que $d = D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$. Sejam $\{e_1, \cdots, e_n\}$ uma base de B sobre A, $d' = D_{B/A}(e_1, \cdots, e_n)$ e $\alpha_i = \sum_{j=1}^{n} a_{ij} e_j$ com $a_{ij} \in A$, $1 \leq i \leq n$. Pela Proposição 1.6.1, segue que $d = det(a_{ij})^2 d'$. Por hipótese, $Ad = \mathfrak{D}_{B/A} = Ad'$. Logo, existe um elemento $b \in A$ tal que $d' = bd$. Então $d = det(a_{ij})^2 bd$, e portanto $d(1 - det(a_{ij})^2 b) = 0$. Temos que d não é um divisor de zero, pois se fosse todo elemento de $Ad = \mathfrak{D}_{B/A}$ seria um divisor de zero, contrariando a hipótese. Logo, $1 - det(a_{ij})^2 b = 0$, e portanto $det(a_{ij})$ é inversível. Assim, a matriz $M = [a_{ij}]$ é inversível. Portanto, $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de B sobre A. ■

Lema 1.6.1. *(***Lema de Dedekind***) (*Samuel, 1967,p.39*) Sejam G um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \cdots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$. Então $\{\sigma_1, \cdots, \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.*

Demonstração. Suponhamos que os σ_i's sejam linearmente dependentes. Seja $\sum_{i=1}^{m} a_i \sigma_i = 0$, $a_i \in \mathbb{K}$ uma combinação linear mí-

nima com $a_i \neq 0, \forall i$. Logo, para qualquer $x \in G$, temos que

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_m\sigma_m(x) = 0. \tag{1.3}$$

Como os homomorfismos são distintos, então existe $c \in G$ tal que $\sigma_1(c) \neq \sigma_m(c)$. Agora, como $cx \in G$, segue que

$$a_1\sigma_1(cx) + a_2\sigma_2(cx) + \cdots + a_m\sigma_m(cx) = 0 \tag{1.4}$$

e então

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_2(c)\sigma_2(x) + \cdots + a_m\sigma_m(c)\sigma_m(x) = 0. \tag{1.5}$$

Multiplicando (1.3) por $\sigma_1(c)$, obtemos

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_1(c)\sigma_2(x) + \cdots + a_m\sigma_1(c)\sigma_m(x) = 0. \tag{1.6}$$

Subtraindo (1.5) de (1.6) obtemos

$$a_2\sigma_2(x)(\sigma_2(c) - \sigma_1(c)) + \cdots + a_m\sigma_m(x)(\sigma_m(c) - \sigma_1(c)) = 0. \tag{1.7}$$

Como isso vale para todo $x \in G$ e m é mínimo, segue que $a_m(\sigma_m(c) - \sigma_1(c)) = 0$, ou seja, $\sigma_m(c) = \sigma_1(c)$ para todo $c \in G$, visto que $a_m \neq 0$, o que contradiz a hipótese de que os homomorfismos são distintos. ■

Proposição 1.6.3. *(*Samuel, 1967, p.39, Prop.3*) Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\sigma_1, \cdots, \sigma_n$ os n $\mathbb{K}$-isomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado F contendo $\mathbb{K}$. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \cdots, \alpha_n) = (\det(\sigma_i(\alpha_j)))^2 \neq 0.$$

Demonstração. Temos que $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \cdots, \alpha_n) = \det(Tr(\alpha_i\alpha_j))$. Como o traço de $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \cdots$

$$\alpha_n) = \det(Tr(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j)\right) = \det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) =$$

$\det(\sigma_k(\alpha_i))\det(\sigma_k(\alpha_j)) = (\det(\sigma_i(\alpha_j)))^2$, uma vez que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} =$$

$$= \sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j).$$

Suponha por absurdo que $\det(\sigma_k(\alpha_j)) = 0$. Então existem $a_1, \cdots, a_n \in F$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$ para todo j. Se $\alpha \in \mathbb{L}$, então $\alpha = \sum_{i=1}^{n} b_i\alpha_i$, com $b_i \in \mathbb{K}$, e por linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$. Mas isto contradiz o Lema de Dedekind e portanto $\det(\sigma_k(\alpha_j)) \neq 0$. ■

Corolário 1.6.1. *(*Ribeiro, 2013, p.21, Corol.2.4.1*) Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\sigma_1, \sigma_2, \cdots, \sigma_n$ *os* n $\mathbb{K}$*-isomorfismos distintos de* $\mathbb{L}$ *em um corpo algebricamente fechado* F *contendo* $\mathbb{K}$*. Então a forma bilinear* $\psi : \mathbb{L}\times\mathbb{L} \longrightarrow \mathbb{R}$ *definida por* $\psi(\alpha,\beta) = Tr(\alpha\beta)$ *é não degenerada, isto é, se* $Tr(\alpha\beta) = 0$ *para todo* $\beta \in \mathbb{L}$*, então* $\alpha = 0$*.*

Demonstração. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. É suficiente mostrar que se $Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \cdots, n$, então $\alpha = 0$. Temos que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, com $a_i \in \mathbb{K}$, $i = 1, \cdots, n$. Assim, se $a_1Tr(\alpha_1\alpha_j) + a_2Tr(\alpha_2\alpha_j) + \cdots + \alpha_nTr(\alpha_n\alpha_j) = Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \cdots, n$, então obtemos o seguinte sistema linear

homogêneo

$$\begin{bmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) & \cdots & Tr(\alpha_1\alpha_n) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) & \cdots & Tr(\alpha_2\alpha_n) \\ \vdots & \vdots & \dots & \vdots \\ Tr(\alpha_n\alpha_1) & Tr(\alpha_n\alpha_2) & \cdots & Tr(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Da Proposição 1.6.3, temos que $\det(Tr(\alpha_i\alpha_j)) \neq 0$, e portanto o sistema possui solução única dada por $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ■

Corolário 1.6.2. *(*Ribeiro, 2013, p.22, Obs.2.4.1*) A aplicação* $\psi : \mathbb{L} \longrightarrow Hom_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$ *definida por* $\psi(\alpha) = S_\alpha$, *onde* $S_\alpha(\beta) = Tr(\alpha\beta)$, $\beta \in \mathbb{L}$, *é um isomorfismo. Assim, se* $\{\alpha_1, \cdots, \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *então existe* $\{\psi_{\beta_1}, \cdots, \psi_{\beta_n}\}$ *base dual de* $Hom_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$ *tal que* $Tr(\alpha\alpha_j) = \psi_{\beta_i}(\alpha_j) = \delta_{ij}$.

Demonstração.

i) ψ é $\mathbb{K}$-linear, uma vez que para $\beta \in \mathbb{L}$ temos que $S_{\alpha_1+\alpha_2}(\beta) = Tr((\alpha_1+\alpha_2)\beta) = Tr(\alpha_1\beta) + Tr(\alpha_2\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (S_{\alpha_1} + S_{\alpha_2})(\beta)$. Portanto $\psi(\alpha_1+\alpha_2) = S_{\alpha_1+\alpha_2} = S_{\alpha_1} + S_{\alpha_2} = \psi(\alpha_1) + \psi(\alpha_2)$. Por outro lado, $S_{k\alpha}(\beta) = Tr((k\alpha)\beta) = Tr(k\alpha\beta) = kTr(\alpha\beta) = kS_\alpha(\beta)$. Portanto $\psi(k\alpha) = S_{k\alpha} = kS_\alpha = k\psi(\alpha)$.

ii) ψ é injetora: Seja $\alpha \in \mathbb{L}$ tal que $\psi(\alpha) = 0$. Então $\psi(\alpha) = S_\alpha = 0$, e isto implica que $S_\alpha(\beta) = Tr(\alpha\beta) = 0$, $\forall \beta \in \mathbb{L}$. Pelo Corolário 1.6.1 segue que $\alpha = 0$. Portanto $Ker(\psi) = \{0\}$, ou seja, ψ é injetora.

iii) ψ é sobrejetora: Como $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}\mathbb{L}^*$, onde $\mathbb{L}^* = Hom(\mathbb{L}, \mathbb{K})$, segue que ψ é sobrejetora.

Por (i), (ii), *e* (iii) concluímos que ψ é um isomorfismo. ■

Teorema 1.6.1. *(*Samuel, 1967, p.40, Teo.1*) Sejam* A *um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações com característica*

zero, $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\mathbb{A}_{\mathbb{L}}$ *o fecho inteiro de* $\mathbb{A}$ *em* $\mathbb{L}$*. Então* $A_{\mathbb{L}}$ *é um* A*-submódulo de um* A*-módulo livre de posto* n*.*

Demonstração. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como toda extensão finita é algébrica, segue que cada α_i é algébrico sobre $\mathbb{K}$ e assim existem $a_i \in A$, $i = 1, \cdots, n$, não todos nulos tal que

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

Suponhamos que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1}, temos que

$$a_n^{n-1}(a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_1\alpha_i + a_0) = 0,$$

ou seja,

$$(a_n\alpha_i)^n + a_{n-1}(a_n\alpha_i)^{n-1} + \cdots + a_1a_n^{n-2}(a_n\alpha_i) + a_n^{n-1}a_0.$$

Portanto $a_n\alpha_i \in \mathbb{A}_{\mathbb{L}}$, ou seja, $a_n\alpha_i$ é inteiro sobre A. Logo, $a_n\alpha_i = z_i$, com $z_i \in \mathbb{A}_{\mathbb{L}}$. Portanto $\{z_1, \cdots, z_n\}$ forma uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathbb{A}_{\mathbb{L}}$, uma vez que se $b_1z_1 + \cdots + b_nz_n = 0$ com $b_i \in \mathbb{K}$, então $b_1(a_n\alpha_1) + \cdots + b_n(a_n\alpha_n) = 0$, ou seja, $(b_1a_n)\alpha_1 + \cdots + (b_na_n)\alpha_n = 0$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_ia_n = 0$, para todo i, e como $a_n \neq 0$, segue que $b_i = 0$, para todo i, o que prova que $\{z_1, \cdots, z_n\}$ é linearmente independente, e como possui n elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.6.2 existe uma base $\{\beta_1, \cdots, \beta_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, tal que $Tr(z_i\beta_j) = \delta_{ij}$. Tomando $\rho \in \mathbb{A}_{\mathbb{L}}$, e como $\{\beta_1, \cdots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, escrevemos $\rho = \sum_{j=1}^{n} c_j\beta_j$ com $c_j \in \mathbb{K}$. Para todo i temos $z_i\rho \in \mathbb{A}_{\mathbb{L}}$, uma vez que $z_i \in A$. Portanto, pelo Corolário 1.5.1, temos que $Tr(z_i\rho) \in A$. Assim, como $Tr(z_i\rho) = Tr\left(\sum_j c_jz_i\beta_j\right) =$

$\sum_j c_j Tr(z_i\beta_j) = \sum_j c_j\delta_{ij} = c_i$, concluímos que $c_i \in A$, para todo i, o que implica que $\mathbb{A}_{\mathbb{L}}$ é um submódulo do A-módulo livre $\sum_{j=1}^{n} A\beta_j$. ■

Corolário 1.6.3. *(*Samuel, 1967, p.40, Corol.1*) Considerando as hipóteses do Teorema 1.6.1, se A é um anel principal, então $\mathbb{A}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Demonstração. Pelo Teorema 1.2.1 temos que um submódulo de um A-módulo livre com A principal, é livre com posto $\leq n$. Pelo Teorema 1.6.1 vimos que $\mathbb{A}_{\mathbb{L}}$ contém uma base com n elementos de $\mathbb{L}$ sobre $\mathbb{K}$. Logo $\mathbb{A}_{\mathbb{L}}$ tem posto n. ■

Exemplo 1.6.3. *Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ e $A = \mathbb{Z}$. O anel $\mathbb{A}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{L} : \mathbb{Q}]$, visto que $\mathbb{Z}$ é principal.*

Definição 1.6.3. *Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$, $A = \mathbb{Z}$ e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Temos que $\mathbb{A}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de* **base integral**, *e seu discriminante é chamado de* **discriminante absoluto** *e denotamos por $D_{\mathbb{K}}$.*

Observação 1.6.2. *Qualquer base integral de $\mathbb{A}_{\mathbb{K}}$ é uma $\mathbb{Q}$-base de $\mathbb{K}$ mas nem toda $\mathbb{Q}$-base de $\mathbb{K}$ consistindo de inteiros algébricos é uma base integral de $\mathbb{A}_{\mathbb{K}}$.*

Exemplo 1.6.4. *Temos que $\{1, \sqrt{5}\}$ é uma $\mathbb{Q}$-base de $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, mas não é uma base integral de $\mathbb{A}_{\mathbb{K}}$, pois o elemento $\frac{1+\sqrt{5}}{2}$ é raiz de $X^2 - X + 1$ e portanto inteiro algébrico, mas não é combinação linear, com coeficientes em $\mathbb{Z}$, de 1 e $\sqrt{5}$.*

Proposição 1.6.4. *(*Ribeiro, 2013, p.23, Prop.2.4.4*) Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L} = \mathbb{K}[\alpha]$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $f(X)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$*. Então,*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(f'(\alpha)),$$

onde $f'(\alpha)$ *é a derivada de* $f(\alpha)$*.*

Demonstração. Se $\alpha_1, \cdots, \alpha_n$ são as raízes de $f(X)$ em alguma extensão de $\mathbb{K}$, então são conjugados de α. Pela Proposição 1.6.3 temos que $D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \cdots, \alpha^{n-1}) = \left(det(\sigma_i(\alpha^j))\right)^2 = det(\alpha_i^j)^2$, com $i = 1, \cdots, n$ e $j = 0, \cdots, n-1$. Como $det(\alpha_i^j)$ é um determinante de Vandermonde segue que $\det(\alpha_i^j)^2 = \left[\prod_{1\leq k<i\leq n} (\alpha_i - \alpha_k)\right]^2 = \prod_{1\leq k<i\leq n} [(\alpha_i - \alpha_k)(\alpha_i - \alpha_k)] = (-1)^{\frac{1}{2}n(n-1)} \prod_{1\leq k<i\leq n,\, i\neq k} (\alpha_i - \alpha_k) = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \left[\prod_{k=1,\, k\neq i}^{n} (\alpha_i - \alpha_k)\right] = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(f'(\alpha))$. ■

Exemplo 1.6.5. *Sejam* $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{3})$ *e* $f(X) = X^2 - 3$ *o polinômio minimal de* $\sqrt{3}$ *sobre* $\mathbb{Q}$*. Então* $D_{\mathbb{L}/\mathbb{K}}(1, \sqrt{3}) = (-1)^{\frac{2\cdot 1}{2}} N_{\mathbb{L}/\mathbb{K}}(f'(\sqrt{3})) = -N_{\mathbb{L}/\mathbb{K}}(2\sqrt{3}) = -2^2 N_{\mathbb{L}/\mathbb{K}}(\sqrt{3}) = -4(\sqrt{3})(-\sqrt{3}) = 12$.

1.7 Anéis Noetherianos e anéis de Dedekind

Os principais objetivos desta seção são provar que o anel dos inteiros algébricos de um corpo de números é um domínio de Dedekind e mostrar a unicidade da fatoração de um ideal não nulo como um produto de ideais primos neste domínio.

Definição 1.7.1. *Sejam* A *um anel e* M *um* A*-módulo. Dizemos*

que M é um A-módulo **Noetheriano** *se satisfaz uma das seguintes condições:*

i) *Todo conjunto não vazio de submódulos de* M *contém um elemento maximal.*

ii) *Toda sequência crescente de submódulos de M é estacionária.*

iii) *Todo submódulo de M é finitamente gerado.*

Um anel A é chamado Noetheriano se quando considerado como um A-módulo for Noetheriano.

Exemplo 1.7.1. *Todo anel principal é Noetheriano, uma vez que seus ideais são submódulos gerados por um elemento.*

Proposição 1.7.1. *(*Samuel, 1967, p.46, Prop.1*) Sejam A um anel, M um A-módulo e* M' *um submódulo de* M*. Então M é Noetheriano se, e somente se,* M' *e* $\frac{M}{M'}$ *são Noetherianos.*

Demonstração. Suponhamos que M é Noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M', que também é uma sequência de submódulos de M. Como M é Noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária, ou seja, M' é Noetheriano. Para mostrarmos que $\frac{M}{M'}$ é Noetheriano, sejam $S = \{$conjunto dos submódulos de M contendo $M'\}$ e $S' = \{$conjunto dos submódulos de $\frac{M}{M'}\}$. Temos que existe uma aplicação bijetora $\phi : S \longrightarrow S'$ definida por $\phi(H) = \varphi(H)$ onde $\varphi : M \longrightarrow \frac{M}{M'}$ é o homomorfismo canônico. A inversa de ϕ é dada por $\theta : S' \longrightarrow S$, onde $\theta(H') = \varphi^{-1}(H')$. Através do isomorfismo φ temos que $\frac{M}{M'}$ também é Noetheriano, uma vez que se $(H'_n)_{n\geq 0}$ é uma sequência crescente de submódulos de $\frac{M}{M'}$, então $(\theta(H'_n))_{n\geq 0}$ é uma sequência crescente de submódulos de M e como M é Noetheriano, segue que $(\theta(H'_n))_{n\geq 0}$ é estacionária, o que implica que $(H'_n)_{n\geq 0}$ é estacionária, ou seja, $\frac{M}{M'}$ é Noetheriano.

Reciprocamente, suponha que M' e $\frac{M}{M'}$ são Noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M. Como M' é Noetheriano, segue que a sequência $(M' \cap M_n)_{n\geq 0}$ é estacionária, e como $\frac{M}{M'}$ é Noetheriano, segue que a sequência $\left(\frac{M_n + M'}{M'}\right)_{n\geq 0}$ é estacionária. Assim, a sequência $(M_n + M')_{n\geq 0}$ é estacionária e portanto $(M_n)_{n\geq 0}$ é estacionária, ou seja, M é Noetheriano. ■

Corolário 1.7.1. *(*Samuel, 1967, p.47, Corol.1*) Sejam A um anel e $M_1, \cdots, M_n$ A-módulos Noetherianos. Então $M_1 \times \cdots \times M_n$ é um A-módulo Noetheriano.*

Demonstração. Faremos a prova por indução sobre n. Para $n = 2$ identificando $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$ e $M_2 \simeq \{0\} \times M_2 \subseteq M_1 \times M_2$, temos que $\frac{M_1 \times M_2}{M_1 \times \{0\}}$ é isomorfo a M_2. Como M_2 e $M_1 \times \{0\}$ são Noetherianos, segue da Proposição 1.7.1 que $M_1 \times M_2$ é Noetheriano. Agora, suponha por hipótese de indução que $M = M_1 \times \cdots \times M_{n-1}$ é Noetheriano. Como M_n é Noetheriano, segue do caso $n = 2$ que $M = M_1 \times \cdots \times M_n$ é Noetheriano. ■

Corolário 1.7.2. *(*Samuel, 1967, p.47, Corol.2*) Sejam A um anel Noetheriano e M um A-módulo finitamente gerado. Então M é um A-módulo Noetheriano.*

Demonstração. Seja $\{e_1, \cdots, e_n\}$ um conjunto de geradores de M sobre A. Temos que a aplicação $\phi : A^n \longrightarrow M$ definida por $\phi(a_1, a_2, \cdots, a_n) = \sum_{i=1}^{n} a_i e_i$ é um homomorfismo sobrejetor e que $\frac{A^n}{Ker(\phi)}$ é isomorfo a M. Pelo Corolário 1.7.1 temos que A^n é Noetheriano, e da Proposição 1.7.1, segue que $Ker(\phi)$ e M são Noetherianos. ■

Proposição 1.7.2. *(*Samuel, 1967, p.47, Prop.1*) Sejam A um anel Noetheriano e integralmente fechado, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $A_{\mathbb{L}}$ o fecho inteiro de A em $\mathbb{L}$. Então $A_{\mathbb{L}}$ é um A-módulo finitamente gerado e um anel Noetheriano.*

Demonstração. Segue do Teorema 1.6.1 que $\mathbb{A}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre de posto n, e portanto A' é um A-módulo finitamente gerado. Pelo Corolário 1.7.2, segue que $\mathbb{A}_{\mathbb{L}}$ é um A-módulo Noetheriano. Como os ideais de $\mathbb{A}_{\mathbb{L}}$ são A-submódulos de $\mathbb{A}_{\mathbb{L}}$, e sendo $\mathbb{A}_{\mathbb{L}}$ um A-módulo Noetheriano segue que os ideais de $\mathbb{A}_{\mathbb{L}}$ são Noetherianos. Portanto, $\mathbb{A}_{\mathbb{L}}$ é um anel Noetheriano. ■

Proposição 1.7.3. *(*Samuel, 1967, p.47, Lema 1*) Sejam B um anel, A um subanel de B e $\mathfrak{p}$ um ideal primo de B. Então $\mathfrak{p} \cap A$ é um ideal primo de A.*

Demonstração. Consideremos os seguintes homomorfismos $A \xrightarrow{i} B \xrightarrow{\pi} \frac{B}{\mathfrak{p}}$, onde i é a inclusão e π a projeção, e seja o homomorfismo $\theta = \pi \circ i : A \longrightarrow B/\mathfrak{p}$, definido por $\theta(a) = a + \mathfrak{p}$, $\forall a \in A$. Temos que θ é um homomorfismo, pois é composição de homomorfismos, e que $Ker(\theta) = A \cap \mathfrak{p}$, pois se $x \in Ker(\theta)$ então $x \in A$ e $\theta(x) = \overline{0}$ o que implica que $x \in A$ e $x + \mathfrak{p} = \overline{0}$, ou seja, $x \in A \cap \mathfrak{p}$. Logo, $Ker(\theta) \subset A \cap \mathfrak{p}$. Por outro lado, se $y \in A \cap \mathfrak{p}$ então $\theta(y) = (\pi \circ i)(y) = \pi(y) = y + \mathfrak{p} = \overline{0}$ e assim $y \in Ker(\theta)$, ou seja, $A \cap \mathfrak{p} \subset Ker(\theta)$. Portanto, $Ker(\theta) = A \cap \mathfrak{p}$. Logo, pelo Teorema do Isomorfismo de anéis, temos que $A/A \cap \mathfrak{p} \simeq Im(\theta) \subset B/\mathfrak{p}$. Mas como $B/\mathfrak{p}$ é um domínio, $Im(\theta)$ é um domínio. Portanto, $A/A \cap \mathfrak{p}$ é um domínio, ou seja, $A \cap \mathfrak{p}$ é um ideal primo. ■

Proposição 1.7.4. *(*Samuel, 1967, p.48, Lema 2*) Se um ideal primo $\mathfrak{p}$ de um anel A contém um produto $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ de ideais de A, então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.*

Demonstração. Suponhamos que $\mathfrak{a}_i \not\subset \mathfrak{p}$, $\forall\, i = 1, \cdots, n$. Então para cada $i = 1, \cdots, n$ existe um elemento $\alpha_j \in \mathfrak{a}_i - \mathfrak{p}$. Assim $\alpha_1 \cdots \alpha_n \notin \mathfrak{p}$, pois $\mathfrak{p}$ é um ideal primo, e $\alpha_1 \cdots \alpha_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}$ o que é um absurdo uma vez que $\alpha_i \notin \mathfrak{p}$, $\forall\, i = 1, \cdots, n$. Portanto, $\mathfrak{a}_i \subset \mathfrak{p}$, para algum $i = 1, \cdots, n$. ■

Proposição 1.7.5. *(*Samuel, 1967, p.48, Lema 3*) Se A é um anel Noetheriano, então todo ideal não nulo de A contém um produto de ideais primos não nulos de A.*

Demonstração. Sendo A Noetheriano, seus ideais são A-módulos Noetherianos. Seja F o conjunto de todos os ideais não nulos de A que não contém um produto de ideais primos não nulos de A. Suponha que $F \neq \emptyset$. Como A é Noetheriano segue que F possui um elemento maximal M. Temos que M não é primo, pois caso contrário, M não pertenceria a F. Além disso, temos que $M \neq A$. Por M não ser um ideal primo, existem elementos $x, y \in A - M$ tais que $xy \in M$, e que os ideais $< x > +M$ e $< y > +M$ contém M propriamente. Pela maximalidade de M estes ideais não estão em F, e assim existem ideais $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ primos não nulos de A, tais que $< x > +M \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ e $< y > +M \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Assim, $M \supset < xy > +M \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s$, o que é um absurdo. Assim $F = \emptyset$ e portanto todo ideal não nulo de A contém um produto de ideais primos não nulos de A. ■

Definição 1.7.2. *Um anel A é chamado um* **anel de Dedekind**, *se A é Noetheriano, integralmente fechado e se todo ideal primo não nulo de A é maximal.*

Exemplo 1.7.2. *Todo domínio A de ideais principais é um domínio de Dedekind. De fato, do exe 1.7.1 segue que A é Noetheriano. Da Proposição 1.3.4 segue que é A integralmente fechado. Além*

disso, em um domínio de ideais principais todo ideal primo não nulo é maximal. Portanto A é um domínio de Dedekind.

Teorema 1.7.1. *(*Samuel, 1967, p.49, Teo.1*) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de grau finita de $\mathbb{K}$ e $\mathbb{A}_{\mathbb{L}}$ o fecho inteiro de A em $\mathbb{L}$. Então $\mathbb{A}_{\mathbb{L}}$ é um anel de Dedekind.*

Demonstração. Sabemos que $\mathbb{A}_{\mathbb{L}}$ é integralmente fechado, Noetheriano e é um A-módulo finitamente gerado. Falta mostrar que todo ideal primo $\mathfrak{p} \neq \langle 0 \rangle$ de $\mathbb{A}_{\mathbb{L}}$ é maximal. Pela Proposição 1.7.3, temos que $\mathfrak{p} \cap A$ é um ideal primo de A. Seja $x \in \mathfrak{p} - \langle 0 \rangle$ e consideremos a equação de dependência inteira de x sobre A dada por $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, com $a_i \in A$, $i = 1, \cdots, n-1$, não todos nulos, de grau mínimo. Assim $a_0 \neq 0$, pois caso contrário obteríamos uma equação de grau menor. Portanto temos que $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in \mathbb{A}_{\mathbb{L}}x \cap A \subset \mathfrak{p} \cap A$, ou seja, $\mathfrak{p} \cap A \neq \langle 0 \rangle$. Como A é Dedekind, segue que $\mathfrak{p} \cap A$ é um ideal maximal de A e portanto $A/(\mathfrak{p} \cap A)$ é um corpo. Além disso, $A/\mathfrak{p} \cap A$ pode ser identificado com um subanel de $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$, e como $\mathbb{A}_{\mathbb{L}}$ é inteiro sobre A, segue que $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$ é inteiro sobre $A/\mathfrak{p} \cap A$. Assim, pela Proposição 1.3.2 temos que $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$ é corpo e portanto $\mathfrak{p}$ é maximal. ∎

Exemplo 1.7.3. *Segue do Teorema 1.7.1 que o anel do inteiros de um corpo de números é um anel de Dedekind.*

Exemplo 1.7.4. *Seja o anel $Z[\sqrt{-5}]$. Temos que $Z[\sqrt{-5}]$ não é fatorial, uma vez que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Além disso, $Z[\sqrt{-5}]$ não é um anel principal. De fato, temos que $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, $N(2) = 4$ e $N(3) = 9$, e que $1 + \sqrt{-5}$ não possui um divisor não trivial em $Z[\sqrt{-5}]$ pois se $a + b\sqrt{-5}$ é um*

divisor não trivial de $1+\sqrt{-5}$*, ou seja, se* $1+\sqrt{-5} = (a+b\sqrt{-5})y$*, com* $y \in Z[\sqrt{-5}]$*,* $y \neq \pm 1$ *e* $y \neq 1+\sqrt{-5}$*, então* $6 = N(1+\sqrt{-5}) = N(a+b\sqrt{-5})N(y)$ *e que* $N(a+b\sqrt{-5})$ *seria um divisor não trivial de 6, mas isto é impossível, pois* $a^2+5b^2 = 2$ *e* $a^2+5b^2 = 3$*, não possui solução em* $\mathbb{Z}$*. Assim,* $1+\sqrt{-5}$ *é um elemento primo. Agora, se* $Z[\sqrt{-5}]$ *fosse principal e como* $1+\sqrt{-5}$ *divide* $6 = 2\cdot 3$*, segue que* $1+\sqrt{-5}$ *divide 2 ou 3. Tomando as normas temos que 6 divide 4 ou 9, o que é um absurdo. Portanto* $Z[\sqrt{-5}]$ *não é um anel principal.*

Definição 1.7.3. *Sejam* A *um domínio e* $\mathbb{K}$ *seu corpo de frações. Um* A*-submódulo* I *de* $\mathbb{K}$ *é chamado de* **ideal fracionário** *de* A *se existe um* $d \in A - \{0\}$ *tal que* $d \cdot I \subset A$*. Quando* $d = 1$ *dizemos que* I *é um ideal inteiro.*

Observação 1.7.1. *Segue da Definição 1.7.3 que os elementos de um ideal fracionário* I *tem um denominador comum* $d \in A$*.*

Proposição 1.7.6. *(*Ribeiro, 2013, p.29*) Se* A *é um domínio Noetheriano então todo ideal fracionário* I *de* A *é um* A*-módulo finitamente gerado.*

Demonstração. Como I é um ideal fracionário, então existe $d \in A - \{0\}$ tal que $d \cdot I \subset A$. Assim, $I \subset d^{-1}A$. Além disso, $d^{-1}A$ é um A-módulo e a função $\phi : A \longrightarrow d^{-1}A$ tal que $\phi(x) = d^{-1}x$ define um isomorfismo entre A e $d^{-1}A$, e como A é Noetheriano então concluímos que $d^{-1}A$ é Noetheriano. Logo, I é um A-módulo finitamente gerado. ■

Proposição 1.7.7. *(*Ribeiro, 2013, p.29*) Sejam A um domínio e* $\mathbb{K}$ *seu corpo de frações. Todo A-submódulo finitamente gerado de* $\mathbb{K}$ *é um ideal fracionário.*

Demonstração. Se $\{x_1, \cdots, x_n\}$ é um conjunto finito de geradores de I, então os $x_i^{'}s$ tem um denominador comum d dado pelo produto dos denominadores d_i, onde $x_i = a_i d_i^{-1}$, com a_i, $d_i \in A$. Assim $dI \subset A$ e portanto I é um ideal fracionário. ■

Observação 1.7.2. *O produto $II^{'}$ de dois ideais fracionários I e $I^{'}$ é definido como o conjunto das somas $\sum_i x_i y_i$ com $x_i \in I$ e $y_i \in I$. Sendo I e $I^{'}$ ideais fracionários com denominadores comuns d e $d^{'}$, então os conjuntos $I \cap I^{'}$, $I + I^{'}$ e $II^{'}$ são ideais fracionários, os quais são A-submódulos de $\mathbb{K}$ e tem denominadores comuns d ou $d^{'}$, $dd^{'}$ e $dd^{'}$, respectivamente.*

Lema 1.7.1. *(*Ribeiro, 2013, p.31, Lema 2.7.1*) Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Seja $\mathfrak{m}$ um ideal maximal de A. Então $\mathfrak{m}^{'} = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$ é um ideal fracionário de $\mathbb{K}$.*

Demonstração. Como A não é um corpo, temos que $\mathfrak{m} \neq \{0\}$ e que $\mathfrak{m}^{'} \neq \emptyset$, pois $0 \in \mathfrak{m}^{'}$. Sejam x, $y \in \mathfrak{m}^{'}$. Então pela definição de $\mathfrak{m}^{'}$, temos que $x\mathfrak{m} \subset A$ e $y\mathfrak{m} \subset A$, e portanto $(x + y)\mathfrak{m} = x\mathfrak{m} + y\mathfrak{m} \subset A$, ou seja, $x + y \in \mathfrak{m}^{'}$. Agora, sejam $x \in \mathfrak{m}^{'}$ e $a \in A$. Assim $x\mathfrak{m} \subset A$, e portanto $(xa)\mathfrak{m} = a(x\mathfrak{m}) \subset A$, ou seja, $xa \in \mathfrak{m}^{'}$. Finalmente, temos que $d\mathfrak{m} \subset A$, para todo $d \in A - \{0\}$, ou seja, $\mathfrak{m}^{'}$ é um ideal fracionário de $\mathbb{K}$. ■

Teorema 1.7.2. *(*Samuel, 1967, p.50, Teo. 2*) Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Todo ideal maximal de A é inversível no conjunto dos ideais fracionários de A.*

Demonstração. Seja $\mathfrak{m}$ um ideal maximal de A. Pelo Lema 1.7.1 temos que $\mathfrak{m}^{'} = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$ é um ideal fracionário de $\mathbb{K}$.

Pela definição de $\mathfrak{m}'$, segue que $\mathfrak{m}'\mathfrak{m} \subset A$, e como $\mathfrak{m}$ é um ideal de A, segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{m}\mathfrak{m}' \subset A$. Desde que $\mathfrak{m}$ é maximal, temos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ ou $\mathfrak{m}\mathfrak{m}' = A$. Vamos mostrar que $\mathfrak{m}\mathfrak{m}' \neq \mathfrak{m}$. Para isto suponhamos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. Seja $x \in \mathfrak{m}'$. Então $x\mathfrak{m} \subset \mathfrak{m}$; $x^2\mathfrak{m} \subset \mathfrak{m}; \cdots; x^n\mathfrak{m} \subset \mathfrak{m}$. Se $d \in \mathfrak{m}$ é não nulo, temos que $x^n d \in A$, para todo $n \in \mathbb{N}$. Assim, $A[x]$ é um ideal fracionário de A, e como A é Noetheriano, segue da Proposição 1.7.6 que $A[x]$ é um A-módulo finitamente gerado. Portanto, pelo Teorema 1.3.1 segue que x é inteiro sobre A, e como A é integralmente fechado, segue que $x \in A$, ou seja, $\mathfrak{m}' \subset A$. Como $A \subset \mathfrak{m}'$, segue que $A = \mathfrak{m}'$. Por outro lado, se $a \in \mathfrak{m} - < 0 >$, então pela Proposição 1.7.5, o ideal aA contém um produto de ideais primos não nulos $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, de A com n o menor possível. Assim, $\mathfrak{m} \supset aA \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Pela Proposição 1.7.4 temos que $\mathfrak{m} \supset \mathfrak{p}_i$, para algum $i = 1, \cdots, n$, e sem perda de generalidade, digamos que $\mathfrak{m} \supset \mathfrak{p}_1$. Como $\mathfrak{p}_1$ é maximal pois A é Dedekind, segue que $\mathfrak{m} = \mathfrak{p}_1$. Tomando $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, temos que $aA \supset \mathfrak{m}\mathfrak{b}$ e $aA \not\supset \mathfrak{b}$ devido a minimalidade de n. Assim, existe $z \in \mathfrak{b}$ tal que $z \notin aA$. Como $\mathfrak{m}\mathfrak{b} \subset aA$ segue que $\mathfrak{m}\frac{z}{a} \subset A$. Assim, $\frac{z}{a} \in \mathfrak{m}'$, e como $z \notin aA$, temos que $\frac{z}{a} \notin A$, ou seja, $\mathfrak{m}' \neq A$, o que contradiz o fato de $\mathfrak{m}' = A$. Portanto, $\mathfrak{m}\mathfrak{m}' = A$, ou seja, $\mathfrak{m}'$ é o inverso de $\mathfrak{m}$. ■

Teorema 1.7.3. *(*Samuel, 1967, p.50, Teo.3(a)*) Sejam A um anel de Dedekind e $\mathfrak{a} \neq A$ um ideal não nulo de A. Então existem ideais primos não nulos $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ de A e inteiros positivos $\mathfrak{e}_1, \cdots, \mathfrak{e}_t$ tal que $\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$, e esta expressão é única.*

Demonstração. Pela Proposição 1.7.5, existem ideais primos $\mathfrak{p}_1, \cdots$

$, \mathfrak{p}_v$ não nulos de A tal que $\mathfrak{p}_1 . \cdots . \mathfrak{p}_v \subset \mathfrak{a}$. Provemos que $\mathfrak{a}$ é um

produto de ideais primos por indução sobre v. Se $v = 1$, temos que $\mathfrak{a} \subset \mathfrak{p}_1$, mas como $\mathfrak{p}_1$ é maximal, pois A é Dedekind, então $\mathfrak{a} = \mathfrak{p}_1$, e assim $\mathfrak{a}$ é primo. Agora, suponhamos que todo ideal que contém um produto com $v-1$ ideais primos não nulos de A é um produto de ideais primos de A. Temos que $\mathfrak{p}_1 \cdots \mathfrak{p}_v \subset \mathfrak{a}$, e como A é Dedekind segue que $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{m}$ de A. Seja $\mathfrak{m}^{-1}$ o ideal fracionário inverso de $\mathfrak{m}$. Como $\mathfrak{m} \supset \mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_v$, segue da Proposição 1.7.4, que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i's$, para $i = 1, \cdots v$. Suponhamos que $\mathfrak{m} \supset \mathfrak{p}_v$, e assim, $\mathfrak{m} = \mathfrak{p}_v$, pois $\mathfrak{p}_v$ é maximal. Portanto $\mathfrak{p}_1 \cdots \mathfrak{p}_{v-1} \subset \mathfrak{a}\mathfrak{m}' \subset \mathfrak{m}\mathfrak{m}' = A$. Da hipótese de indução decorre que $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, com $\mathfrak{q}_j's$, para $j = 1, \cdots, s$, ideais primos não nulos de A, e portanto $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s\mathfrak{p}_v$, como queríamos. Para provar a unicidade suponhamos que $\prod_{i=1}^{t} \mathfrak{p}^{e_i} = \prod_{j=1}^{h} \mathfrak{p}^{e_j}$. Então $A = \prod \mathfrak{p}^{e_i - e_j}$. Se $e_i - e_j \neq 0$, podemos separar os expoentes positivos e os expoentes negativos e reescrevê-los como

$$\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_v^{\beta_v},$$

com $\mathfrak{p}_i$, $\mathfrak{q}_j$ ideais primos não nulos de A e α_i, $\beta_j > 0$ para $\mathfrak{p}_i \neq \mathfrak{q}_j$, $\forall i, j$. Portanto $\mathfrak{p}_1$ contém $\mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_v^{\beta_v}$ e pela Proposição 1.7.4 segue que $\mathfrak{p}_1 \supset \mathfrak{q}_j$, para algum j. Suponhamos sem perda de generalidade que $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Como $\mathfrak{p}_1$ e $\mathfrak{q}_1$ são ideais maximais, segue que $\mathfrak{p}_1 = \mathfrak{q}_1$. Portanto $e_i - e_j = 0$, isto é, $e_i = e_j$, o que é uma contradição pois $\mathfrak{p}_i \neq \mathfrak{q}_j$, $\forall\, i, j$ e assim concluímos que a expressão é única. ■

Corolário 1.7.3. *Se A é um anel de Dedekind, então o conjunto dos ideais fracionários não nulos de A formam um grupo com relação a multiplicação.*

Demonstração. (Samuel, 1967, p.50, Teo.3(b)). ■

1.8 Norma de um ideal

Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Nesta seção apresentamos a norma de um ideal como uma generalização da norma de um elemento de $\mathbb{A}_{\mathbb{K}}$.

Definição 1.8.1. *Seja $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$. A* **norma do ideal $\mathfrak{a}$**, *é definida como o número de elementos do anel quociente $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$, isto é, $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a}) = \#(\mathbb{A}_{\mathbb{K}}/\mathfrak{a})$.*

Observação 1.8.1. *Quando não houver dúvida quanto ao anel que contém o ideal $\mathfrak{a}$, usaremos $N(\mathfrak{a})$ ao invés de $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a})$.*

Exemplo 1.8.1. *Seja $\mathfrak{a}$ um ideal principal de $\mathbb{Z}[i]$, onde $i^2 = -1$, gerado por $2 - i$. Assim, $\frac{\mathbb{Z}[i]}{\mathfrak{a}} = \{x + \mathfrak{a};\ x \in \mathbb{Z}[i]\}$. A norma de $\mathfrak{a}$ é o número das classes laterais de $\mathfrak{a}$. Uma vez que $2 - i \equiv 0 (mod\ \mathfrak{a})$, segue que $2 \equiv i (mod\ \mathfrak{a})$. Assim para $x = a + bi$, com $a, b \in \mathbb{Z}$, temos que $x = a + bi \equiv a + 2b (mod\ \mathfrak{a})$. Como $(2 + i)(2 - i) = 5 \in \mathfrak{a}$, segue que as classes laterais de $\mathfrak{a}$ em $\mathbb{Z}[i]$ são $\{0, 1, 2, -1, -2\}$, ou seja, $N(\mathfrak{a}) = 5$.*

Proposição 1.8.1. *(*Samuel, 1967, p.52, Prop.1*) Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, $\alpha \neq 0$, então $|N(\alpha)| = \#\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha$.*

Demonstração. Seja $\alpha \in \mathbb{A}_{\mathbb{K}}$, $\alpha \neq 0$. Então, pelo Corolário 1.5.1, temos que $N(\alpha) \in \mathbb{Z}$. Pelo Corolário 1.6.3 temos que $\mathbb{A}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Além disso, como $\psi : \mathbb{A}_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$ definida por $\psi(a) = a\alpha$, com $a \in \mathbb{A}_{\mathbb{K}}$, é um isomorfismo, segue que $\mathbb{A}_{\mathbb{K}}\alpha$ é um $\mathbb{Z}$-submódulo livre de posto n de $\mathbb{A}_{\mathbb{K}}$. Pelo Teorema 1.2.1 existe uma base $\{e_1, e_2, \cdots, e_n\}$ do $\mathbb{Z}$-módulo $\mathbb{A}_{\mathbb{K}}$ e elementos $c_i \in \mathbb{N}$ tal que $\{c_1e_1, c_2e_2, \cdots, c_ne_n\}$ é uma base de $\mathbb{A}_{\mathbb{K}}\alpha$. Também temos que o grupo abeliano $\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha$ é isomorfo ao grupo abeliano $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$, cuja ordem é $c_1c_2 \cdots c_n$. Agora seja a aplicação linear

$\phi : \mathbb{A}_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$ definida por $\phi(e_i) = c_i\alpha_i$, $i = 1, \cdots, n$. Temos que $\det(\phi) = c_1c_2\cdots c_n$. Por outro lado, como $\{\alpha e_1, \cdots, \alpha e_n\}$ também é uma base de $\mathbb{A}_{\mathbb{K}}\alpha$, segue que existe um endomorfismo de $\mathbb{Z}$-módulo $\varphi : \mathbb{A}_{\mathbb{K}}\alpha \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$, definido por $\varphi(c_ie_i) = \alpha e_i$, $i = 1\cdots, n$. Logo, como o $\det(\varphi) \in \mathbb{Z}$ e é inversível, segue que $\det(\varphi) = \pm 1$. Mas, a composição $\varphi\phi$ é um homomorfismo, que é a multiplicação por α, e seu determinante é por definição $N(\alpha)$. Portanto, como $\det(\varphi\phi) = \det(\varphi)\det(\phi)$, segue que $N(\alpha) = \pm c_1\cdots c_n = \pm\#(\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha)$. ■

Proposição 1.8.2. *(*Samuel, 1967, p.52*) Se $\mathfrak{a}$ é um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, então o quociente $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$ é finito.*

Demonstração. Seja $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Temos que $\mathbb{A}_{\mathbb{K}}\alpha \subset \mathfrak{a}$. Logo $\mathbb{A}_{\mathbb{K}}/\mathfrak{a} \simeq \dfrac{\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha}{\mathfrak{a}/\mathbb{A}_{\mathbb{K}}\alpha}$. Assim, $\#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathbb{A}_{\mathbb{K}}\alpha} = \#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\#\dfrac{\mathfrak{a}}{\mathbb{A}_{\mathbb{K}}\alpha} < \infty$. Portanto, $N(\mathfrak{a}) = \#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}$ é finito. ■

Proposição 1.8.3. *(*Samuel, 1967, p.52, Prop.2*) Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathbb{A}_{\mathbb{K}}$, então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Demonstração. Pelo Teorema 1.7.3, temos que $\mathfrak{b} = \prod_{i\in I}\mathfrak{p}_i^{\alpha_i}$, onde os $\mathfrak{p}_i's$ são ideais primos não nulos de $\mathbb{A}_{\mathbb{K}}$ e $\alpha_i \geq 0$, $i \in I$. Como $\mathbb{A}_{\mathbb{K}}$ é um domínio de Dedekind, então os ideais $\mathfrak{p}_i, i \in I$, são ideais maximais. Seja $\mathfrak{p}_i = \mathfrak{m}$, para algum $i \in I$. Por indução sobre o número de fatores, é suficiente provar que

$$N(\mathfrak{am}) = N(\mathfrak{a})N(\mathfrak{m}). \tag{1.8}$$

Segue da definição de norma que (1.8) se verifica se

$$\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\right)\cdot\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}\right). \tag{1.9}$$

Mas, do homomorfismo sobrejetor $\varphi : \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}\mathfrak{m}} \longrightarrow \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}$, definido por $\varphi(x+\mathfrak{a}\mathfrak{m}) = x+\mathfrak{a}$, temos que $Ker(\varphi) = \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{p}}$, e pelo Teorema do Isomorfismo temos que, $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}\mathfrak{m}}/\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \simeq \mathbb{A}_{\mathbb{K}}/\mathfrak{a}$. Logo,

$$\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}\mathfrak{m}}\right) = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\right)\cdot\#\left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}\right). \tag{1.10}$$

De (1.9) e (1.10), podemos concluir que (1.8) é verificado se $\#\left(\frac{\mathbb{A}}{\mathfrak{m}}\right) = \#\left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}\right)$. Agora, mostremos que $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$ é um espaço vetorial sobre $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}$ de dimensão 1. De fato, sejam as operações

$$\begin{aligned} + : \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \times \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} &\longrightarrow \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \\ (x+\mathfrak{a}\mathfrak{m}, y+\mathfrak{a}\mathfrak{m}) &\longrightarrow (x+y)+\mathfrak{a}\mathfrak{m}. \end{aligned}$$

$$\begin{aligned} \cdot : \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}} \times \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} &\longrightarrow \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \\ (x+\mathfrak{m}, y+\mathfrak{a}\mathfrak{m}) &\longrightarrow (\alpha x)+\mathfrak{a}\mathfrak{m}. \end{aligned}$$

Estão bem definidas:

Soma: $x+\mathfrak{a}\mathfrak{m} = x^{'}+\mathfrak{a}\mathfrak{m}$ e $y+\mathfrak{a}\mathfrak{m} = y^{'}+\mathfrak{a}\mathfrak{m} \Longrightarrow \overline{x}-\overline{x^{'}} = \overline{0}$ e $\overline{y}-\overline{y^{'}} = \overline{0} \Longrightarrow \overline{x}+\overline{y} = \overline{x^{'}}+\overline{y^{'}} \Longrightarrow (x+\mathfrak{a}\mathfrak{m})+(y+\mathfrak{a}\mathfrak{m}) = (x^{'}+\mathfrak{a}\mathfrak{m})+(y^{'}+\mathfrak{a}\mathfrak{m}) \Longrightarrow (x+y)+\mathfrak{a}\mathfrak{m} = (x^{'}+y^{'})+\mathfrak{a}\mathfrak{m}$.

Produto: $x+\mathfrak{a}\mathfrak{m} = x^{'}+\mathfrak{a}\mathfrak{m}$ e $\alpha+\mathfrak{m} = \alpha^{'}+\mathfrak{m} \Longrightarrow x-x^{'} \in \mathfrak{a}\mathfrak{m}$ e $\alpha-\alpha^{'} \in \mathfrak{m}$. Assim, $\alpha^{'}x^{'}-\alpha x = x^{'}(\alpha^{'}-\alpha)+(x^{'}-x)\alpha \in \mathfrak{a}\mathfrak{m}$. Assim, $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$ é um espaço vetorial sobre $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}$. Temos que os $\mathbb{A}_{\mathbb{K}}$-submódulos de $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$ são ideais e são do tipo $\frac{\mathfrak{b}}{\mathfrak{a}\mathfrak{m}}$, onde $\mathfrak{b}$ é um ideal tal que $\mathfrak{a}\mathfrak{m} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Mas, como todo ideal num domínio de Dedekind admite inverso, segue que

$$\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{m} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \overset{a^{-1}a=\mathbb{A}_{\mathbb{K}}}{\Longrightarrow} \mathfrak{m} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathbb{A}_{\mathbb{K}} \overset{m\ maximal}{\Longrightarrow}$$
$$\mathfrak{m} = \mathfrak{a}^{-1}\mathfrak{b} \text{ ou } \mathfrak{a}^{-1}\mathfrak{b} = \mathbb{A}_{\mathbb{K}} \Longrightarrow \mathfrak{a}\mathfrak{m} = \mathfrak{b} \text{ ou } \mathfrak{b} = \mathfrak{a}.$$

Portanto, não existe $\mathfrak{b}$ tal que $\mathfrak{a}\mathfrak{m} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Assim, os $\mathbb{A}_{\mathbb{K}}$-submódulos de $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$, ou os subespaços do espaço vetorial $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$ são apenas os triviais. Portanto, $dim_{\frac{\mathbb{A}_{\mathbb{K}}}{m}} \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} = 1$ e então $\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}\mathfrak{m}}\right) = \#\left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}\right)$. ■

1.9 Formas quadráticas sobre o $\mathbb{R}^n$

Nesta seção apresentamos as formas quadráticas sobre o $\mathbb{R}^n$, que serão muito útil no estudo das aplicações das formas quadráticas aos corpos ciclotômicos e desta forma calcular a densidade de centro dos reticulados obtidos via esses corpos.

Para cada inteiro n, seja $Q_n(\underline{X})$ a **forma quadrática** sobre o $\mathbb{R}^n$ definida por

$$Q_n(\underline{X}) = Q_n(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_i^2 + \sum_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

Da igualdade

$$\sum_{1 \leq i < j \leq n} (X_i - X_j)^2 = (n-1) \sum_{i=1}^{n} X_i^2 - 2 \sum_{1 \leq i < j \leq n} X_i X_j$$

obtém-se que

$$Q_n(X_1, \cdots, X_n) = n \sum_{i=1}^{n} X_i^2 - 2 \sum_{1 \leq i < j \leq n} X_i X_j.$$

Observamos que $Q_n(\underline{X})$ é uma função positiva definida e totalmente simétrica, isto é, $Q_n(X_1, \cdots, X_n) = Q_n(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$, onde σ é uma permutação qualquer do conjunto $\{1, \cdots, n\}$.

A próxima proposição é de grande importância no cálculo do raio de empacotamento de certos reticulados.

Proposição 1.9.1. *(*Flores, 1996, p.64, Prop.3.4.1*)* **i)** *O menor valor que $Q_n(X_1, \cdots, X_n)$ assume com entradas inteiras não todas*

nulas é n.

ii) *Para $a \in \mathbb{Z}^n$, temos que $Q_n(\underline{a}) = n$ quando $\underline{a} = \pm(1, 1, \cdots, 1)$ ou $\underline{a} = \pm e_i$, $i = 1, \cdots, n$; onde $\{e_1, \cdots, e_n\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$.*

Demonstração. i) Observe que

$$Q_n(X_1, \cdots, X_n) = Q_{n-1}(X_1, \cdots, X_{n-1}) + X_n^2 + \sum_{i=1}^{n-1}(X_i - X_n)^2.$$

Se $a_1 = \cdots = a_{n-1} = 0$, então $Q_n(a_1, \cdots, a_n) = a_n^2 + (n-1)a_n^2 = na_n^2 \geq n$, para $a_n \neq 0$. Caso contrário, por hipótese de indução, tem-se que

$$Q_{n-1}(a_1, \cdots, a_{n-1}) \geq n - 1,$$

e neste caso

$$a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 \geq n - 1.$$

De fato, se $a_n \neq 0$ então $a_n^2 \geq 1$. Caso contrário, pelo menos uma das parcelas $(a_i - a_n)^2$ será não nula.

ii) A prova se faz usando novamente indução sobre n. Para $j = 1$ temos que $Q_1(\underline{a}) = Q_1(a_1) = a_1^2 = 1$, onde $a_1 = \pm 1$. Suponhamos que o resultado seja válido para $j = n - 1$. Observe que $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 > 0$. Assim temos que $Q_n(\underline{a}) = Q_n(a_1, \cdots, a_n) = Q_{n-1}(a_1, \cdots, a_{n-1}) + a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 > n - 1 + 0 = n - 1$. Agora, se $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 \neq 1$ então $Q_n(a_1, \cdots, a_n)$ assumiria um valor maior que $n+1$, o que contraria o item (i). Portanto, $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 = 1$ e assim $Q_n(\underline{a}) = Q_n(a_1, \cdots, a_n) = n - 1 + 1 = n$, se $\underline{a} = \pm(1, \cdots, 1)$ ou $\underline{a} = \pm e_i$, $i = 1, \cdots, n$ onde $\{e_1, \cdots, e_n\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$. ■

Lema 1.9.1. *(*Flores, 1996, p.80, Lema A.1*) Se $Q_n(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_1^2 + \sum_{i<j}(X_i - X_j)^2$, e $a = (a_1, \cdots, a_n) \in \mathbb{R}^n$, então*

$$Q_n(a_1, \cdots, a_n) = d^2(a, 0) + n.d^2(a, \Delta),$$

onde $d^2(a,0)$ *e* $d^2(a,\Delta)$ *são os quadrados das distâncias euclidianas de* a *até a origem e de* a *até a diagonal de* $\mathbb{R}^n$*, respectivamente.*

Demonstração. Se $X = (x, \cdots, x)$ é um elemento qualquer da diagonal de $\mathbb{R}^n$, então

$$d(a, X)^2 = \sum_{i=1}^{n}(a_i - x)^2.$$

Esta distância será mínima quando $\frac{d}{dx}(\sum(a_i - x)^2) = 0$, e isto ocorre para $x = (1/n).\sum_{i=1}^{n} a_i$. Assim

$$\begin{aligned}
d^2(a,\Delta) &= \sum_{j=1}^{n}\left(a_j - (1/n).\left(\sum_{i=1}^{n} a_i\right)\right)^2 \\
&= \sum_{j=1}^{n}\left(a_j^2 - (2/n).a_j.\left(\sum_{i=1}^{n} a_i\right) + \left(\sum_{i=1}^{n} a_i\right)^2/n^2\right) \\
&= \sum_{j=1}^{n} a_j^2 - (2/n).\left(\sum_{j=1}^{n} a_j\right).\left(\sum_{i=1}^{n} a_i\right) + n.\left(\sum_{i=1}^{n} a_i\right)^2/n^2 \\
&= \sum_{j=1}^{n} a_j^2 - (2/n).\left(\sum_{j=1}^{n} a_j\right)^2 + (1/n).\left(\sum_{j=1}^{n} a_j\right)^2 \\
&= \left(\sum_{j=1}^{n} a_j^2\right) - (1/n).\left(\sum_{i=1}^{n} a_i\right)^2.
\end{aligned}$$

Logo,

$$n.d^2(P,a) = (n-1).\left(\sum_{i=1}^{n} a_i^2\right) - 2\left(\sum_{1\le i<j\le n} a_i.a_j\right),$$

e somando $d^2(P,0) = \sum_{i=1}^{n} a_i^2$ em ambos os membros chegamos ao resultado desejado. ∎

Teorema 1.9.1. *(*Flores, 1996, p.81, Teo.A.2*) Sejam os números reais* $a_1, \cdots, a_r$, *com* $r < n$. *Se*

$$F(X_{r+1}, \cdots, X_n) = Q_n(a_1, \cdots, a_r, X_{r+1}, \cdots, X_n),$$

então F *atinge seu mínimo com coordenadas inteiras no ponto*

$$(y, y, \cdots, y), \text{ onde } y = \left[\left(\sum_{i=1}^{r} a_i \right) /(r+1) \right],$$

onde [z] denota o inteiro mais próximo de z. Caso $z + 1/2$ *seja inteiro, então* $[z]$ *denota* $z - 1/2$.

Demonstração. Os pontos da reta, em $\mathbb{R}^{n-r}$, passando por $P = (x, x, \cdots, x)$, onde $x = \left(\sum_{i=1}^{r} a_i \right) /(r+1)$ e tendo $(b_{r+1}, \cdots, b_n)$ como vetor diretor são da forma

$$X = P + t(b_{r+1}, \cdots, b_n) = (x + tb_{r+1}, \cdots, x + tb_n).$$

Assim

$$F(x + tb_{r+1}, \cdots, x + tb_n) = Q(a_1, \cdots, a_r, x + tb_{r+1}, \cdots, x + tb_n) =$$
$$\sum_{i=1}^{r} a_i^2 + \sum_{i=r+1}^{n} (x + tb_i)^2 + \sum_{i<j} (a_i - a_j)^2 + \sum_{i,j} (a_i - x - tb_j)^2 +$$
$$+ \sum_{i<j} t^2 (b_i - b_j)^2 = At^2 + Bt + C,$$

onde

$$A = (r+1) \sum_{j=r+1}^{n} b_i^2 + \sum_{i<j} (b_i - b_j)^2;$$

$$B = 2x(r+1) \sum_{j=r+1}^{n} b_j - 2 \left(\sum_{i=1}^{r} a_i \right) \left(\sum_{j=r+1}^{n} b_j \right) \text{ e}$$

$$C = (n-r+1) \sum_{i=1}^{r} a_i^2 + \sum_{i<j} (a_i - a_j)^2 + (r+1)(n-r)x^2 - 2x(n-r) \sum_{i=1}^{n} a_i.$$

Como esta expressão é uma função de segundo grau na variável t, segue que derivando com relação a t, obtemos que

$$\frac{dF}{dt}(x+tb_{r+1},\cdots,x+tb_n) = 2t(r+1)\sum_{j=r+1}^{n} b_i^2 +$$
$$+2t\sum_{i<j}(b_i-b_j)^2 + 2x(r+1)\sum_{j=r+1}^{n} b_j - 2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right).$$

Em $t=0$, temos que

$$\frac{dF}{dt}(0) = 2x(1+r)\sum_{j=r+1}^{n} b_j - 2(\sum_{i=1}^{r} a_i)(\sum_{j=r+1}^{n} b_j) =$$
$$= -2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right) - 2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right) = 0.$$

Assim, sobre as retas passando por P, o gráfico de F é uma parábola com concavidade voltada para cima, cujo menor valor é assumido em P. Seja $Y_1 = (y, y, \cdots, y)$, onde $y = \left[\frac{\sum_{i=1}^{r} a_i}{r+1}\right]$. Supomos no que segue que $y \leq x$, sendo que para o caso $y \geq x$ a demonstração é análoga. As parábolas descritas acima têm coeficiente dominante

$$r\sum_{i=r+1}^{n} b_i^2 + \left(\sum_{i=r+1}^{n} b_i^2 + \sum_{i<j}(b_i-b_j)^2\right) = r\sum_{i=r+1}^{n} b_i^2 + Q_{n-r}(v),$$

onde $v = (b_{r+1}, \cdots, b_n)$ e Q_{n-r} é a forma quadrática definida no início da seção. Pelo Lema 1.9.1, segue que este coeficiente dominante é

$$r\sum_{i=r+1}^{n} b_i^2 + d^2(v,0) + (n-r)d^2(v,\Delta),$$

onde $d^2(v,0)$ e $d^2(v,\Delta)$ representam os quadrados das distâncias de v até a origem e diagonal de $\mathbb{R}^{n-r}$, respectivamente. Para determinar a direção de menor crescimento destas parábolas, consideremos vetores diretores v com comprimento 1. Na direção de v, o coeficiente dominante da parábola passando por P é dado por

$$(r+1)+(n-r)d^2(v,\Delta).$$

Logo, a direção de menor crescimento dessas parábolas é dada com $d^2(v,\Delta)$ mínimo, ou seja, na direção de Y_1, que é a diagonal. Observe que para outra direção o crescimento dessas parábolas será estritamente maior. Consequentemente, se $Y \in \mathbb{R}^{n-r}$ é tal que $F(Y) = F(Y_1)$, temos que

$$d(Y,P) \leq d(Y_1,P), \tag{1.11}$$

com igualdade se, e somente se, Y estiver na diagonal de $\mathbb{R}^{n-r}$. Agora, dado o conjunto

$$A = \{Y \in \mathbb{R}^{n-r};\ F(Y) \geq F(Y_1)\},$$

vamos calcular $A \cap \mathbb{Z}$. Para isso, vamos escrever A como a união disjunta de dois conjuntos A_1 e A_2, onde

$$A_1 = \{Y \in \mathbb{R}^{n-r};\ F(Y) < F(Y_1)\}$$
$$\text{e}$$
$$A_2 = \{Y \in \mathbb{R}^{n-r};\ F(Y) = F(Y_1)\}$$

Temos que $A_1 \cap \mathbb{Z}^{n-r} = \emptyset$. Para calcular $A_2 \cap \mathbb{Z}$ note, por (1.11), que para todo Y em A_2 temos que $d(Y,P) < d(Y_1,P)$ ou Y está na diagonal de $\mathbb{R}^{n-r}$. Os Y que satisfazem a primeira possibilidade não são inteiros. Caso Y esteja na diagonal de $\mathbb{R}^{n-r}$, novamente, por (1.11), temos $d(Y,P) = d(Y_1,P)$. Para concluir, consideremos dois casos:

1º caso: $x < y + 1/2$. Aqui, $d(Y,P) = d(Y_1,P)$ ocorre apenas para $Y = Y_1$;

2º caso: $x = y + 1/2$. Neste caso, os únicos pontos da diagonal de $\mathbb{Z}^{n-r}$ satisfazendo $d(Y,P) = d(Y_1,P)$ são Y_1 e $Y_2 = (y+1, \cdots, y+1)$.

Assim,

$$A \cap \mathbb{Z}^{n-r} = \begin{cases} Y_1, \ se\ x < y + 1/2; \\ \{Y_1, Y_2\}, \ se\ x = y + 1/2. \end{cases}$$

Para concluir, observe que para todo ponto Y de $\mathbb{Z}^{n-r}$ temos que $F(Y) \geq F(Y_1)$, ou seja, Y_1 é o ponto de mínimo de F em $\mathbb{Z}^{n-r}$. ■

Teorema 1.9.2. *(*Flores, 1996, p.84, Teo.A.3*) Sejam $m \in \mathbb{N}$ e $Q_n^{'}(m) = Q_n(m, t, \cdots, t)$, onde $t = [m/2]$, isto é, $Q^{'}(m)$ é o menor valor que $Q_n(m, X_2, \cdots, X_n)$ assume fazendo $X_2, \cdots, X_n$ variar no conjunto dos números inteiros. Então $Q^{'}$ é uma função crescente de m.*

Demonstração. Se m for par, então $t = \dfrac{m}{2}$, é inteiro e

$$Q^{'}(m) = Q_n(m, m/2, \cdots, m/2) = m^2 + 2(n-1)(m^2/4).$$

Neste caso, $[m+1] = 1/2$, e

$$Q^{'}(m+1) = Q_n(m+1, m/2, \cdots, m/2) = \\ (m+1)^2 + (n-1)(m^2/4) + (n-1)(1 + m/2)^2.$$

Logo, $Q^{'}(m+1) > Q^{'}(m)$. A prova para o caso m ímpar se faz de modo análogo. ■

Denotaremos por I_d o conjunto $\{(a_1, \cdots, a_m) \in \mathbb{Z}^m;\ |a_i| \leq d\}$.

Lema 1.9.2. *(*Flores, 1996, p.76, Lema 3.4.13*) A forma quadrática $Q_n(a_1, \cdots, a_n)$ não atinge o valor $n+1$, para $(a_1, \cdots, a_n) \in \mathbb{Z}^n$.*

Demonstração. Para $a \in I_1 = \{(a_1, \cdots, a_n) \in \mathbb{Z}^n, |a_i| \leq 1\}$ o resultado é verdadeiro. Tomemos $a \in I_2 - I_1$. Sem perda de generalidade, podemos supor que $a = (2, a_2, \cdots, a_n)$, para inteiros $a_2, \cdots, a_n$. Pelo Teorema 1.9.1 temos que

$$Q_n(a) \geq Q_n(2, 1, \cdots, 1) = 4 + n - 1 + n - 1 = 2n + 2 > n + 1,$$

e pelo Teorema 1.9.2, $Q_n(a) > n+1$, $\forall\ j$ e $a \in I_j$. ■

Definição 1.9.1. *Dados p um número primo e m um número inteiro positivo, denotamos por $v_p(m)$ a* **valorização p-ádica** *de m, ou seja, o maior número α para o qual p^α divide m.*

Proposição 1.9.2. *(*Simonato, 2000, p.61, Lema A.1*) Se n é um número inteiro positivo, p um número primo e $b_0, b_1, \cdots, b_s \in \mathbb{Z}$, com $0 \leq b_i \leq p-1$ são tais que $n = b_0 + b_1 p + \cdots + b_s p^s$, então*

$$v_p(n!) = \frac{n - \sum_{i=0}^{s} b_i}{p-1},$$

onde $v_p(n!)$ é a valorização p-ádica de $n!$.

Demonstração. Faremos por indução sobre n.

i) Se n=1, a conclusão é imediata.

ii) Suponhamos verdadeira para n, onde $n = b_0 + b_1 p + \cdots + b_s p^s$ e mostremos que a asserção é verdadeira para $n+1$, onde

$$n+1 = \begin{cases} (b_0+1) + b_1 p + \cdots + b_s p^s, \ \textit{se}\ \ b_0 \neq p-1 \\ (b_r+1)p^r + b_{r+1}p^{r+1} + \cdots + b_s p^s, \ \textit{se}\ \ b_0 = \cdots = b_{r-1} = p-1 \\ \textit{e}\ \ b_r \leq p-2. \end{cases}$$

1º Caso: $n+1 = (b_0+1) + b_1 p + \cdots + b_s p^s$, *se* $b_0 \neq p-1$. Pelo fato de que $p \nmid n+1$ pois $b_0 + 1 \not\equiv 0 (mod\ p)$, e da hipótese de indução segue que

$$v_p((n+1)!) = v_p(n!) = \frac{n - \sum_{i=0}^{s} b_i}{p-1} = \frac{n+1 - \left(\sum_{i=0}^{s} b_i + b_0 + 1\right)}{p-1}.$$

2º Caso: $n+1 = (b_r+1)p^r + b_{r+1}p^{r+1} + \cdots + b_s p^s$, *se* $b_0 = b_1 = \cdots = b_{r-1} = p-1$. Assim

$$n+1 = p^r[(b_r+1) + b_{r+1}p + \cdots + b_s p^{s-r}] \quad \text{e}$$
$$v_p((n+1)!) = r + v_p(n!)$$

Sendo $n = (p-1)+(p-1)p+\cdots+(p-1)p^{r-1}+b_r p^r+b_{r+1}p^{r+1}+\cdots+b_s p^s$, segue que

$$\begin{aligned} r + v_p(n!) &= r + \frac{n - \sum_{i=0}^{s} b_i}{p-1} \\ &= r + \frac{n - (r(p-1) + b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{r(p-1) + n - r(p-1) - (b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{n - (b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{(n+1) - [(b_r+1) + b_{r+1} + \cdots + b_s]}{p-1}. \end{aligned}$$

■

Corolário 1.9.1. *(*Simonato, 2000, p.62, Corol.A.2*) Se p é um número primo e m, n são inteiros positivos com $m \leq n$ tais que*

$$\begin{aligned} n &= a_0 + a_1 p + \cdots + a_s p^s,\ 0 \leq a_i \leq p-1, \\ m &= b_0 + b_1 p + \cdots + b_s p^s,\ 0 \leq b_i \leq p-1, \\ n - m &= c_0 + c_1 p + \cdots + c_s p^s,\ 0 \leq c_i \leq p-1, \end{aligned}$$

então a valorização p-ádica de $\left(\begin{array}{c} n \\ m \end{array}\right)$ *é dada por*

$$v_p\left(\left(\begin{array}{c} n \\ m \end{array}\right)\right) = \frac{\sum_{i=0}^{s} b_i + \sum_{i=0}^{s} c_i - \sum_{i=0}^{s} a_i}{p-1},$$

Demonstração. Aplicação da Proposição 1.9.2. ■

Proposição 1.9.3. *(*Flores, 1996, p.74, Lema 3.4.10*) Sejam p um número primo, r um número inteiro positivo e $m = p^{r-2}$. Então*

$$v_p\left(\left(\begin{array}{c} m \\ i \end{array}\right)\right) \geq 1,\ \textit{onde}\ \left(\begin{array}{c} m \\ i \end{array}\right) = \frac{m!}{i!\,(m-i)!},$$

para $i = 1, \cdots, m-1$.

Demonstração. Sejam $b_1, \cdots, b_m, c_1, \cdots, c_m$, números naturais satisfazendo $0 \leq b_i \leq p-1$, $0 \leq c_i \leq p-1$ e tais que $i = b_0 + b_1 p + \cdots + a_m p^m$ e $(m-i) = c_0 + c_1 p + \cdots + c_m p^m$.

Pela Proposição 1.9.2, temos que

$$v_p(m!) = \frac{p^{r-2}-1}{p-1}, \quad v_p(i!) = \frac{i - \sum_{i=1}^{m} b_i}{p-1}, \quad v_p((m-i)!) = \frac{m-i-\sum_{i=1}^{m} c_i}{p-1},$$

de onde segue que

$$v_p\left(\begin{pmatrix} m \\ i \end{pmatrix}\right) = \frac{-1 + \sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i}{p-1}.$$

Como $\sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i \geq 2$, o resultado segue. ∎

2

Corpos quadráticos e ciclotômicos

2.1 Introdução

Neste capítulo apresentamos os conceitos de corpos quadráticos e corpos ciclotômicos, dando ênfase especialmente aos corpos ciclotômicos. Para isso usamos os resultados de Teoria Algébrica dos Números vistos no capítulo 1. Concluindo o capítulo apresentamos a decomposição de um ideal primo em uma extensão onde fizemos o uso do Teorema de Kummer.

Temos duas classes importantes dos corpos de números que são a classe dos corpos quadráticos e a classe dos corpos ciclotômicos. Nosso objetivo nas próximas seções é determinar o anel dos inteiros algébricos, base integral e discriminante dos corpos quadráticos e dos corpos ciclotômicos.

2.2 Corpos quadráticos

Nesta seção apresentamos os corpos quadráticos juntamente com a teoria necessária para caracterizar seu anel dos inteiros, base integral e discriminante.

Definição 2.2.1. *Uma extensão de corpos de grau 2 sobre o corpo* $\mathbb{Q}$ *é chamado um* **corpo quadrático**.

Proposição 2.2.1. *(*Ribeiro, 2013, p.13, Prop.2.2.1*) Todo corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$, *sendo* d *um inteiro livre de quadrados.*

Demonstração: Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo quadrático, ou seja, um corpo de números de grau 2, e $f(X) = X^2+aX+b$, com $a, b \in \mathbb{Q}$, o polinômio minimal de $\theta \in \mathbb{K}$. Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$ temos que $\theta = \dfrac{-a \pm \sqrt{a^2-4b}}{2}$ são as raízes de $f(X)$. Como $2\theta \pm a = \sqrt{a^2-4b}$ segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2-4b})$. Por outro lado, a^2-4b é um número racional que podemos escrever como $a^2-4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, $mdc(u, v) = 1$ e de forma que u e v não sejam quadrados perfeitos, pois caso contrário, teremos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2-4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Suponhamos que $uv = k^2d$, com $k, d \in \mathbb{Z}$, e d livre de quadrados. Logo, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2d}) = \mathbb{Q}(\sqrt{d})$. ∎

A Proposição 2.2.1 nos diz que todo corpo quadrático $\mathbb{K}$ é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $\{1, \sqrt{d}\}$ é uma base do espaço vetorial $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

Proposição 2.2.2. *(*Samuel, 1967, p.35*) Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *com* d *um inteiro livre de quadrados, um corpo quadrático. Se um*

elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *é um inteiro algébrico, então* $2a$ *e* $a^2 - db^2$ *são números inteiros.*

Demonstração. Seja $\alpha \in \mathbb{K}$ um inteiro algébrico. Então existem $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Assim, considerando σ um automorfismo de $\mathbb{K}$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$, ou seja, $\sigma(\alpha)$ também é um inteiro algébrico de $\mathbb{K}$. Do Corolário 1.3.2, temos que $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ também são inteiros algébricos de $\mathbb{K}$. Além disso, temos que se $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, então $\alpha + \sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é integralmente fechado segue, da Proposição 1.3.4, que $2a$ e $a^2 - db^2$ são números inteiros. ■

Observação 2.2.1. *Se* $d > 0$, *a extensão* $\mathbb{Q}(\sqrt{d})$ *é dita real e se* $d < 0$, *a extensão* $\mathbb{Q}(\sqrt{d})$ *é dita imaginária.*

A seguir determinaremos o anel dos inteiros algébricos de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados.

Teorema 2.2.1. *(*Stewart; Tall, 1987, p.67, Teo.3.2*) Se* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *é um corpo quadrático com* $d \in \mathbb{Z}$ *livre de quadrados, então o anel dos inteiros algébricos* $\mathbb{A}_{\mathbb{K}}$ *de* $\mathbb{Q}(\sqrt{d})$ *é dado por:*

a) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2$ *ou* $d \equiv 3 (mod\ 4)$ *e*

b) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *se* $d \equiv 1 (mod\ 4)$.

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com $a, b \in \mathbb{Q}$, um inteiro algébrico sobre $\mathbb{Z}$. Se $b = 0$ então o polinômio minimal de α sobre $\mathbb{Q}$ é dado por $m(X) = X - a$, e como α é um inteiro algébrico sobre $\mathbb{Z}$, segue que $a \in \mathbb{Z}$. Se $b \neq 0$, então o polinômio minimal $m(X)$ de α sobre $\mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

$$\alpha = a + b\sqrt{d} \Longrightarrow \alpha - a = b\sqrt{d} \Longrightarrow (\alpha - a)^2 = b^2 d \Longrightarrow$$
$$\alpha^2 - 2a\alpha + a^2 = b^2 d \Longrightarrow \alpha^2 - 2a\alpha + (a^2 - b^2 d) = 0.$$

Logo $m(X) = X^2 - 2aX + a^2 - db^2$. Pela Proposição 2.2.2 temos que $2a$, $a^2 - db^2 \in \mathbb{Z}$. Assim, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e daí $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Ainda temos que $2b \in \mathbb{Z}$, pois, caso contrário, no seu denominador existiria um fator primo p que apareceria na forma p^2 no denominador de $(2b)^2$ e como d é livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Logo, $2b \in \mathbb{Z}$. Assim, podemos escrever:

$$a = \frac{u}{2},\ b = \frac{v}{2},\quad com\, u,\ v \in \mathbb{Z}. \tag{2.1}$$

Além disso, temos que

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \tag{2.2}$$

Substituindo a por $\frac{u}{2}$ e b por $\frac{v}{2}$, obtemos $u^2 - dv^2 \in 4\mathbb{Z}$.

a) Se $d \equiv 2$ ou $3(mod\, 4)$, temos que u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1(mod\, 4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$ temos que $u^2 \equiv dv^2 \equiv d(mod\, 4)$, ou seja, $d \equiv 0(mod\, 4)$ ou $d \equiv 1(mod\, 4)$, o que é um absurdo. Portanto, concluímos que v é par, isto é, $v^2 \equiv 0(mod\, 4)$ e assim, $u^2 \equiv dv^2 \equiv 0(mod\, 4)$ o que implica que u é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathbb{A}_{\mathbb{K}}$ temos que $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$, pois pela Proposição 2.2.2, temos que $2a$, $a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathbb{A}_{\mathbb{K}}$. Portanto, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

b) Se $d \equiv 1(mod\, 4)$, temos que $u^2 - dv^2 \in 4\mathbb{Z}$, e que u e v são de mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a, b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u -$

$v)/2 + v((1+\sqrt{d})/2) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ou seja, $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a, b \in \mathbb{Z}$, temos que $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 - d(b/2)^2 = a^2 + ab + (1-d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1(mod\ 4)$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathbb{A}_{\mathbb{K}}$, pois os coeficientes do polinômio minimal de α, $m(X) = X^2 - (2a + b)X + a^2 + ab + (1-d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{A}_{\mathbb{K}}$. ■

Exemplo 2.2.1. *Seja $\mathbb{K}$ o corpo quadrático $\mathbb{Q}(\sqrt{-1})$. O anel dos inteiros algébricos de $\mathbb{K}$ é dado por $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$ pois $d = -1 \equiv 3(mod\ 4)$. O anel dos inteiros algébricos do corpo quadrático $\mathbb{Q}(\sqrt{-3})$é $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

Como os $\mathbb{Q}$-monomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, em $\mathbb{C}$ são σ_1 e σ_2, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$, segue que o discriminante absoluto de um corpo quadrático é obtido do seguinte modo:

i) se $d \equiv 1(mod\ 4)$, então

$$\begin{aligned} D_{\mathbb{K}} &= D_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) \\ &= \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right)^2 \\ &= \left(\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right)^2 = d. \end{aligned}$$

ii) se $d \equiv 2$ ou $3(mod\ 4)$ então

$$D_{\mathbb{K}} = D_{\mathbb{K}/\mathbb{Q}}\left(1, \sqrt{d}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right)^2$$

$$= \left(\det\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right)^2 = 4d.$$

Exemplo 2.2.2. *Dado* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, *tem-se* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, *isto é,* $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ *é uma base integral de* $\mathbb{A}_{\mathbb{K}}$ *e o discriminante absoluto de* $\mathbb{K}$ *é* 5. *Os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são* σ_1 *a inclusão e* σ_2 *a conjugação complexa, isto é,* $\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ *e* $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$. *Logo,* $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{5}) = \sum_{i=1}^{2} \sigma_i(a+b\sqrt{5}) = 2a$ *e* $N_{\mathbb{K}/\mathbb{Q}}(a + b\sqrt{5}) = \prod_{i=1}^{2} \sigma_i(a + b\sqrt{5}) = a^2 + b^2$.

Exemplo 2.2.3. *Dado* $\mathbb{K} = \mathbb{Q}(i)$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$, *isto é,* $\{1, \sqrt{-1}\}$ *é uma base integral para* $\mathbb{A}_{\mathbb{K}}$ *e o discriminante absoluto de* $\mathbb{K}$ *é* -4. *Os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são* σ_1 *a inclusão e* σ_2 *a conjugação complexa, isto é,* $\sigma_1(a + b\sqrt{-1}) = a + b\sqrt{-1}$ *e* $\sigma_2(a + b\sqrt{-1}) = a-b\sqrt{-1}$. *Logo,* $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{-1}) = \sum_{i=1}^{2} \sigma_i(a+b\sqrt{-1}) = 2a$ *e* $N_{\mathbb{K}/\mathbb{Q}}(a + b\sqrt{-1}) = \prod_{i=1}^{2} \sigma_i(a + b\sqrt{-1}) = a^2 + b^2$

2.3 Corpos ciclotômicos

Nesta seção apresentamos os corpos ciclotômicos. Esses corpos desempenham um papel fundamental na Teoria Algébrica dos Números, uma vez que é possível caracterizar o anel dos intei-

ros algébricos de um corpo ciclotômico e, consequentemente, seu discriminante.

Definição 2.3.1. *Seja $\mathbb{K}$ um corpo. Um elemento $\zeta \in \mathbb{K}$ é chamado uma raiz n-ésima da unidade se $\zeta^n = 1$, para $n \geq 1$, um inteiro.*

Segue da Definição 2.3.1 que as raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$. Seja $U = \{\zeta^{r_1}, \cdots, \zeta^{r_n}\}$ o conjunto de todas as raízes distintas de $X^n - 1$ em $\mathbb{K}$. Como $(\zeta^i\zeta^j)^n = (\zeta^i)^n(\zeta^j)^n = (\zeta^n)^i(\zeta^n)^j = 1$ e $\left(\frac{\zeta^i}{\zeta^j}\right)^n = \frac{(\zeta^i)^n}{(\zeta^j)^n} = \frac{(\zeta^n)^i}{(\zeta^n)^j} = 1$, segue que o conjunto U é um grupo multiplicativo. Como todo grupo multiplicativo finito num corpo é cíclico então segue que U é um grupo cíclico. Assim, podemos representar as n raízes n-ésimas da unidade por $\zeta, \zeta^2, \cdots, \zeta^n = 1$, onde ζ é um gerador do grupo U. As raízes n-ésimas primitivas da unidade são os geradores do grupo U, isto é, os elementos ζ^k com $mdc(k, n) = 1$, para $k = 1, 2, \cdots, n$. O número das raízes n-ésimas primitivas da unidade é dado por

$$\phi(n) = \#\{0 < m < n : mdc(m, n) = 1, m \in \mathbb{Z}\},$$

onde ϕ é a função de Euler. Dado n um inteiro positivo, definimos ζ_n como sendo $e^{\frac{2\pi i}{n}}$ e o corpo $\mathbb{Q}(\zeta_n)$ é chamado o $n-$ésimo corpo ciclotômico.

Definição 2.3.2. *O polinômio $\varphi_n(X) = \prod_{j=1,\, mdc(j,n)=1}^{n} (X - \zeta_n^j)$ é chamado de $n-$ésimo polinômio ciclotômico.*

Lema 2.3.1. *(*Lang, 1972, p.206*) Se n é um inteiro positivo, então $X^n - 1 = \prod_{d|n} \varphi_d(X)$.*

Demonstração: Sendo $f(X) = X^n - 1$, temos que as raízes de $f(X)$ são $1, \omega, \omega^2, \cdots, \omega^{n-1}$. Logo $X^n - 1 = (X - 1)(X - \omega)\cdots(X - \omega^{n-1})$.

Analisando os períodos de cada raiz de f(X), e escrevendo todas as raízes de mesmo período como um polinômio da forma $\varphi_d(X) = \prod_{periodo\ \omega=d} (X-\omega)$, segue que $X^n - 1 = \prod_{d|n} \varphi_d(X)$. ■

Exemplo 2.3.1. *Considere o polinômio* $f(X) = X^6 - 1$. *Temos que as raízes de* $f(X)$ *são* ω, ω^2, ω^3, ω^4, ω^5, ω^6. *Deste modo,* ω, ω^2, ω^3, ω^4, *e* ω^5 *tem período* 6, 3, 2, 3 *e* 6, *respectivamente. Assim,* $\varphi_1(X) = (X-\omega^6) = (X-1)$, $\varphi_2(X) = (X-\omega^3)$, $\varphi_3(X) = (X-\omega^2)(X-\omega^4)$, $\varphi_6(X) = (X-\omega)(X-\omega^5)$. *Como os divisores de 6 são 1, 2, 3, 6, temos que* $X^6-1 = \prod_{d|6} \varphi_d(X)$, *ou seja,* $X^6-1 = \varphi_1(X)\varphi_2(X)\varphi_3(X)\varphi_6(X) = (X-1)(X-\omega^3)(X-\omega^2)(X-\omega^4)(X-\omega)(X-\omega^5)$.

Como consequência do Lema 2.3.1 temos que

$$\varphi_n(X) = \frac{X^n - 1}{\prod_{d|n,\, d<n} \varphi_d(X)}. \tag{2.3}$$

Assim $\varphi_1(X) = X-1$, $\varphi_2(X) = \frac{X^2-1}{\varphi_1(X)} = \frac{X^2-1}{X-1} = X+1$, $\varphi_3(X) = \frac{X^3-1}{\varphi_1(X)} = \frac{X^3-1}{X-1} = X^2+X+1$, $\varphi_4(X) = \frac{X^4-1}{\varphi_1(X)\varphi_2(X)} = \frac{(X^2-1)(X^2+1)}{(X-1)(X+1)} = X^2+1$. Quando $n = p$, onde p é um número primo, segue que

$$\varphi_p(X) = \frac{X^p-1}{\varphi_1(X)} = \frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1. \tag{2.4}$$

que é chamado de **p-ésimo polinômio ciclotômico**. Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, de acordo com o Lema 2.3.1,

$$X^{p^r} - 1 = \varphi_1(X)\varphi_p(X)\varphi_{p^2}(X)\cdots\varphi_{p^{r-1}}(X)\varphi_{p^r}(X) \ \ e$$
$$X^{p^{r-1}} - 1 = \varphi_1(X)\varphi_p(X)\varphi_{p^2}(X)\cdots\varphi_{p^{r-1}}(X).$$

Logo $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1} = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1$. Este polinômio é chamado de **p^r-ésimo polinômio ciclotômico**.

Teorema 2.3.1. *(*Lang, 1972, p.204, Teo.6*) Se ζ_n é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Demonstração. Seja $f(X)$ um polinômio mônico, irredutível e de menor grau de ζ_n sobre $\mathbb{Q}$. Logo $X^n - 1 = f(X)h(X)$, com $h(X) \in \mathbb{Q}[X]$. Pelo lema de Gauss segue que $f(X)$, $h(X) \in \mathbb{Z}[X]$. Seja p um número primo tal que $p \nmid n$. Assim, ζ_n^p é raiz n-ésima primitiva da unidade. Logo $(\zeta_n^p)^n - 1 = f(\zeta_n^p)h(\zeta_n^p)$, ou seja, $0 = f(\zeta_n^p)h(\zeta_n^p)$. Assim, se ζ_n^p não for raiz de $f(X)$, então ζ_n^p é raiz de $h(X)$, e portanto ζ_n é raiz de $h(X^p)$. Portanto, pelo modo como tomamos $f(X)$, segue que, $f(X) \mid h(X^p)$, ou seja, $h(X^p) = f(X)g(X)$, com $g(X) \in \mathbb{Z}[X]$ pelo lema de Gauss. Como consequência do pequeno Teorema de Fermat, $a^p \equiv a (mod\ p)$ e daí $h(X^p) \equiv h(X)^p (mod\ p)$. Assim, $f(X)g(X) \equiv h(X)^p (mod\ p)$, e portanto $h(X)^p \equiv f(X)g(X) (mod\ p)$. Logo, $\overline{h(\zeta_n)^p} = \overline{0}$, pois ζ_n é raiz de $f(X)$. E recursivamente chegamos que $\overline{h}(\zeta_n) = 0$. Portanto $\overline{f}$ e $\overline{h}$ tem uma raiz em comum. Assim $X^n - \overline{1} = \overline{f}(X)\overline{h}(X)$, e portanto $X^n - \overline{1}$ tem raízes múltiplas. Logo $nX^{n-1} = \overline{0}$ e assim, para qualquer $\alpha \in \mathbb{Z}_p$, $n\alpha^{n-1} = \overline{0}$. Como a característica de $\mathbb{Z}_p$ é p segue que $p|n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto ζ_n^p é raiz de $f(X)$ $\forall$ $p \nmid n$ e $mdc(p, n) = 1$. Logo $\partial(f(X)) \geq \partial(\varphi_n(X))$, pois toda raiz de $\varphi_n(X)$ é raiz de $f(X)$, e como $f(X)|\varphi_n(X)$, segue que $\partial(\varphi_n(X)) \geq \partial(f(X))$. Portanto $\partial(f(X)) = \partial(\varphi_n(X)) = \phi(n)$. ∎

Observação 2.3.1. *Existe um único polinômio minimal $f(X)$ tal que $f(\zeta_n) = 0$. Pelo Teorema 2.3.1, $\partial(f(X)) = \partial(\varphi_n(X))$, e $\varphi_n(\zeta_n) = 0$. Assim $f(X) = \varphi_n(X)$, e assim $\varphi_n(X)$ é irredutível.*

Lema 2.3.2. *(*Lang, 1972, p.204*) Se* $mdc(m, n) = 1$, *então* $U_{mn} \cong U_m \times U_n$.

Demonstração. Seja a seguinte função:

$$\begin{aligned} \varphi : U_m \times U_n &\longrightarrow U_{mn} \\ (a, b) &\longmapsto ab \end{aligned}$$

i) φ esta bem definida, pois $(ab)^{mn} = (a^m)^n(b^n)^m = 1$

ii) φ é homomorfismo, pois $\forall (a, b), (c, d) \in U_m \times U_n$ temos que $\varphi((a, b) \cdot (c, d)) = \varphi(ac, bd) = (acbd) = (ab)(cd) = \varphi(a, b)\varphi(c, d)$.

iii) φ é injetora: Temos que provar que $Ker(\varphi) = \{(a, b) \in U_m \times U_n : \varphi(a, b) = 1\} = \{1\}$. Deste modo, temos que mostrar que para $\forall (a, b) \in U_m \times U_n$ tal que $\varphi(a, b) = ab = 1 \Longrightarrow a = b = 1$. Para isto, seja $a = \zeta_m^k$, $b = \zeta_n^l$, onde $0 \leq k \leq m-1$ e $0 \leq l \leq n-1$. Assim, $ab = 1 \iff \zeta_m^k\zeta_n^l = 1 \iff \zeta_m^k = \zeta_n^{-l} \iff \zeta_m^{nk} = \zeta_n^{-nl} \iff \zeta_m^{nk} = 1$. Logo, como ζ_m é uma raiz m-ésima primitiva da unidade, segue que $m|nk$, e como $mdc(m, n) = 1$ então $m|k$, e isto implica que $k = mx$. Analogamente $n|l$, e isto implica que $l = ny$. Deste modo, $\zeta_m^k = \zeta_m^{mx} = 1 = \zeta_n^{-ny} = \zeta_n^{-l}$, ou seja, $\zeta_m^k = \zeta_n^{-l} = 1$, e isto implica que $k = l = 0$, pois ζ_m e ζ_n são raízes m-ésima e n-ésima primitivas da unidade, respectivamente. Portanto $ab = 1 \iff a = b = 1$. Portanto $Ker(\varphi) = \{1\}$ e assim φ é injetora.

iv) φ é sobrejetora: Como $o(U_m \times U_n) = o(U_{mn})$ e φ é injetora, segue que φ é sobrejetora. Por *iii*) e *iv*), φ é bijetora. Portanto φ é isomorfismo. ■

Proposição 2.3.1. *(*Lang, 1972, p.205*) Temos que* $\zeta_m^k\zeta_n^l$, *para* $0 \leq k \leq m-1$ *e* $0 \leq l \leq n-1$, *é uma raiz* mn*-ésima primitiva da unidade se, e somente se,* ζ_m^k *é uma raiz* m*-ésima primitiva da unidade e* ζ_n^l *é uma raiz* n*-ésima primitiva da unidade.*

Demonstração. Se ζ_m^k não é uma raiz m-ésima primitiva da unidade, então temos que $mdc(k, m) = d > 1$. Assim, $(\zeta_m^k\zeta_n^l)^{\frac{mn}{d}} = ((\zeta_m^k\zeta_n^l)^{mn})^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1$, o que é absurdo, pois $\frac{mn}{d} < mn$. Reciprocamente, se ζ_m^k é uma raiz m-ésima primitiva da unidade e ζ_n^l é uma raiz n-ésima primitiva da unidade, então $mdc(k, m) = mdc(l, n) = 1$. Assim,

$$(\zeta_m^k\zeta_n^l)^a = 1 \iff \zeta_m^{ka}\zeta_n^{la} = 1 \iff \zeta_m^{ka} = \zeta_n^{-la} \iff \zeta_m^{kan} = \zeta_n^{-lan} \iff$$
$$(\zeta_m^k)^{na} = (\zeta_n^n)^{-la} \iff (\zeta_m^k)^{na} = 1^{-la} \iff (\zeta_m^k)^{na} = 1 \iff m|na.$$

Como $mdc(m, n) = 1$ segue que $m|a$. De modo análogo, $n|a$. Ainda, usando o fato de que $mdc(m, n) = 1$ segue que $mn|a$. Assim temos que, $(\zeta_m^k\zeta_n^l)^{mn} = (\zeta_m^m)^{kn}(\zeta_n^n)^{lm} = 1$. Assim, mn é a menor potência tal que $(\zeta_m^k\zeta_n^l)^{mn} = 1$. Portanto $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. ■

Corolário 2.3.1. *(*Lang, 1972, p.205*)* $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

Sejam p um número primo e ζ_p uma raiz p-ésima primitiva da unidade. Como em $\varphi_p(X)$ o coeficiente a_{p-2} do termo X^{p-2} é igual a 1, segue que

$$\begin{cases} Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) = \left[\mathbb{Q}(\zeta_p) : \mathbb{Q}\right] \cdot 1 = p - 1, \text{ e} \\ Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = -a_{p-2} = -1, \text{ para } j = 1, \cdots, p-1. \end{cases}$$

Consequentemente,

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^j) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) - Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = p, \text{ para } j = 1, \cdots, p-1. \tag{2.5}$$

Os elementos $1 - \zeta_p^j$, para $j = 1, \cdots, p-1$, são todos os conjugados de $1 - \zeta_p^k$, para $k = 1, \cdots, p-1$. Assim, pela Definição 2.3.2, segue que $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p^k) = \varphi_p(1) = p$, para $k = 1, \cdots, p-1$.

Lema 2.3.3. *(*Simonato, 2000, p.18, Lema1.4.4*) Se* $\mathbb{A}_{\mathbb{K}}$ *é o anel dos inteiros algébricos de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *então:*

i) $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

ii) $Tr_{\mathbb{K}/\mathbb{Q}}((1-\zeta_p)y) \in p\mathbb{Z}$, $\forall\, y \in \mathbb{A}_{\mathbb{K}}$.

Demonstração: i) O p-ésimo polinômio ciclotômico de ζ_p é $\varphi_p(X) = X^{p-1} + \cdots + X + 1 = (X-\zeta_p)(X-\zeta_p^2)\cdots(X-\zeta_p^{p-1})$. Como $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^k) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$, segue que $\varphi_p(1) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$. Como $1-\zeta_p^j \in \mathbb{A}_{\mathbb{K}}$, para $j = 1, \cdots, p-1$, segue que $p \in (1-\zeta_p)\mathbb{A}_{\mathbb{K}}$. Portanto $p\mathbb{Z} \subset (1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$. Para mostrar a outra inclusão, vamos supor por absurdo que $p\mathbb{Z}$ está contido propriamente em $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, então $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Como $1 \in \mathbb{Z}$ segue que $1 = (1-\zeta_p)a$, para algum $a \in \mathbb{A}_{\mathbb{K}}$. Logo $1-\zeta_p$ é inversível em $\mathbb{A}_{\mathbb{K}}$, e assim $1-\zeta_p^j$ são inversíveis em $\mathbb{A}_{\mathbb{K}}$, para $j = 2, \cdots, p-1$. Assim, $(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$ é inversível em $\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$, isto é, p é inversível em $\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$, o que é um absurdo. Portanto $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

ii) Cada conjugado $y_i(1-\zeta_p^i)$ de $y(1-\zeta_p)$ é um múltiplo de $1-\zeta_p^i$ em $\mathbb{A}_{\mathbb{K}}$, para $i = 1, 2, \cdots, p-1$. Como $1-\zeta_p^i = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})$ segue que $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathbb{A}_{\mathbb{K}}$. Sendo o traço a soma dos conjugados, $Tr_{\mathbb{K}/\mathbb{Q}}(y(1-\zeta_p)) = y_1(1-\zeta_p) + y_2(1-\zeta_p^2) + \cdots + y_{p-1}(1-\zeta_p^{p-1}) = \alpha(1-\zeta_p)$, $\alpha \in \mathbb{A}_{\mathbb{K}}$. Portanto $Tr(y(1-\zeta_p)) \in \mathbb{A}_{\mathbb{K}}(1-\zeta_p)$. Como, pela Proposição 1.3.4, $\mathbb{Z}$ é integralmente fechado, segue pelo Corolário 1.5.1 que $Tr(y(1-\zeta_p)) \in \mathbb{Z}$. Assim, $Tr(y(1-\zeta_p)) \in \mathbb{A}_{\mathbb{K}}(1-\zeta_p) \cap \mathbb{Z} = p\mathbb{Z}$, onde a igualdade segue de (i). ■

Teorema 2.3.2. *(*Samuel, 1967, p.43, Teo.2*) O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *é* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ *e* $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ *é uma base de* $\mathbb{Z}[\zeta_p]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: Seja $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Como $\mathbb{Z}[\zeta_p] \subset \mathbb{A}_{\mathbb{K}}$, falta mostrar que $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$. Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, então $\alpha \in \mathbb{Q}(\zeta_p)$, e assim podemos escrever

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}, \tag{2.6}$$

com $a_i \in \mathbb{Q}$, para $i = 0, 1, \cdots, p-2$. Multiplicando por $1-\zeta_p$ em ambos os membros temos que

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}).$$

Aplicando o traço nesta equação e usando a sua linearidade, obtemos que

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha(1-\zeta_p)) =$$
$$a_0 Tr(1-\zeta_p) + a_1 Tr(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}Tr(\zeta_p^{p-2} - \zeta_p^{p-1}) \in p\mathbb{Z},$$

pelo Lema 2.3.3. Como $Tr(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \cdots, p-2$, segue que $a_0 Tr(1-\zeta_p) = a_0 p \in p\mathbb{Z}$ e assim $a_0 \in \mathbb{Z}$. Como $\zeta_p^{-1} = \zeta_p^{p-1}$ segue que $\zeta_p^{-1} \in \mathbb{A}_{\mathbb{K}}$, e portanto pela Equação (2.6) segue que

$$(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3}.$$

Multiplicando ambos os membros por $1-\zeta_p$ temos que

$$(\alpha - a_0)\zeta_p^{-1}(1-\zeta_p) = a_1(1-\zeta_p) + a_2(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}(\zeta_p^{p-3} - \zeta_p^{p-2}).$$

Logo

$$Tr((\alpha - a_0)\zeta_p^{-1}(1-\zeta_p)) =$$
$$a_1 Tr(1-\zeta_p) + a_2 Tr(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}Tr(\zeta_p^{p-3} - \zeta_p^{p-2}) \in p\mathbb{Z}.$$

Mas $a_1 Tr(1-\zeta_p) = a_1 p \in p\mathbb{Z}$ e assim $a_1 \in \mathbb{Z}$. Continuando dessa forma, chegamos que $a_i \in \mathbb{Z}$, para todo $i = 0, 1, \cdots p-2$. Portanto $\mathbb{A}_{\mathbb{K}} \subseteq \mathbb{Z} + \mathbb{Z}\zeta_p + \cdots + \mathbb{Z}\zeta_p^{p-2}$, ou seja, $\mathbb{A}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Deste modo concluímos que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Além disso, como $1, \zeta_p, \cdots, \zeta_p^{p-2}$ são

linearmente independentes sobre $\mathbb{Z}$, pois são sobre $\mathbb{Q}$ e como $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}+\mathbb{Z}\zeta_p+\cdots+\mathbb{Z}\zeta_p^{p-2}$ segue que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$. ■

Proposição 2.3.2. *(*Simonato, 2000, p.19, Obs.1.4.6*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é dado por* $D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$.

Demonstração: Sejam p um número primo e ζ_p uma raiz p-ésima da unidade. Vimos que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base integral de $\mathbb{Z}[\zeta_p]$. Pela Proposição 1.6.4 temos que $D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p))$, e deste modo vamos mostrar que $N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p)) = p^{p-2}$. Como o p-ésimo polinômio ciclotômico é dado por $\varphi_p(X) = \dfrac{X^p - 1}{X - 1}$, segue que derivando ambos os lados temos que $\varphi_p^{'}(X) = \dfrac{(X-1)p\,X^{p-1} - (X^p - 1)}{(X-1)^2}$. Substituindo X por ζ_p temos que $\varphi_p^{'}(\zeta_p) = \dfrac{(\zeta_p - 1)p\,\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2}$. Como $\zeta_p^p = 1$, pois ζ_p é uma raiz p-ésima da unidade, temos que $\varphi_p^{'}(\zeta_p) = \dfrac{p\,\zeta_p^{-1}(\zeta_p - 1)}{(\zeta_p - 1)^2}$, ou seja, $\varphi_p^{'}(\zeta_p) = \dfrac{p}{(\zeta_p - 1)\zeta_p}$, e isto implica que $\varphi_p^{'}(\zeta_p) = \dfrac{-p}{(1 - \zeta_p)\zeta_p}$. Aplicando a norma e usando a sua linearidade obtemos que $N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p)) = \dfrac{N_{\mathbb{Q}(\zeta_p)/Q}(-p)}{N_{\mathbb{Q}(\zeta_p)/Q}(1 - \zeta_p)N_{\mathbb{Q}(\zeta_p)/Q}(\zeta_p)} = \dfrac{(-p)^{p-1}}{p \cdot 1} = \dfrac{p^{p-1}}{p} = p^{p-2}$. Portanto $D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$. ■

Sejam p um número primo e $n \geq 1$ um inteiro. O Lema 2.3.3 estende naturalmente para o p^r-ésimo corpo ciclotômico, $\mathbb{Q}(\zeta_{p^r})$, ou seja, valem

$$\begin{cases} i)\ (1 - \zeta_{p^r})\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}. \\ ii)\ Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}((1 - \zeta_{p^r})y) \in p\mathbb{Z},\ \forall\, y \in \mathbb{A}_{\mathbb{K}}. \end{cases}$$

onde $\mathbb{A}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$. Nosso objetivo agora é encontrar o anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$.

Lema 2.3.4. *(*Marcus, 1977, p.30, Lema.1*) Temos que* $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$ *e que*

$$D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1,\, 1-\zeta_{p^r}, \cdots, (1-\zeta_{p^r})^{\phi(p^r)-1}) = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}),$$

onde $p^r \geq 3$.

Demonstração. Por definição, $\mathbb{Z}[\alpha] = \left\{ \sum_i a_i \alpha^i \,:\, a_i \in \mathbb{Z} \right\}$. Logo, para qualquer $\alpha \in \mathbb{Z}[1-\zeta_{p^r}]$ temos que $\alpha = b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1} = (b_0 + b_1 + b_2 + \cdots + b_{(p-1)p^{r-1}-1}) + (-b_1 - 2b_2)\zeta_{p^r} + b_2\zeta_{p^r}^2 + \cdots$. Assim, temos que α é da forma $a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}-1}\zeta_{p^r}^{(p-1)p^{r-1}-1}$, ou seja, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Portanto $\mathbb{Z}[1-\zeta_{p^r}] \subset \mathbb{Z}[\zeta_{p^r}]$. Por outro lado, seja $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Assim, $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}-1}\zeta_{p^r}^{(p-1)p^{r-1}-1}$. Observando que $\zeta_{p^r} = 1-(1-\zeta_{p^r})$, temos que

$$\begin{aligned}
\alpha &= a_0 + a_1(1-(1-\zeta_{p^r})) + \cdots + a_{(p-1)p^{r-1}-1}(1-(1-\zeta_{p^r}))^{(p-1)p^{r-1}-1} \\
&= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2(1-2(1-\zeta_{p^r}) + (1-\zeta_{p^r})^2) + \cdots \\
&= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2 - 2a_2(1-\zeta_{p^r}) + a_2(1-\zeta_{p^r})^2 + \cdots \\
&= (a_0 + \cdots + a_{(p-1)p^{r-1}-1}) + (-a_1 - 2a_2)(1-\zeta_{p^r}) + \cdots .
\end{aligned}$$

Dessa forma, chegamos que α é da forma $b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}$, isto é, $\alpha \in \mathbb{Z}[1-\zeta_{p^r}]$. Assim $\mathbb{Z}[\zeta_{p^r}] \subset \mathbb{Z}[1-\zeta_{p^r}]$. Portanto, das duas inclusões concluímos que $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[1-\zeta_{p^r}]$. Para a segunda parte, como os conjugados de ζ_{p^r} são os elementos $\zeta_{p^r}^k$ tais que $k = 1, \cdots, p^r - 1$ e $mdc(k, p^r) = 1$, segue que os elementos $1-\zeta_{p^r}^k$ são os conjugados de $1-\zeta_{p^r}$. Como

$\det(\sigma_j(\zeta_{p^r}^i))$ é o determinante de uma matriz de Vandermonde,

$$\begin{aligned} D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) &= \prod_{t<k}(\zeta_{p^r}^k - \zeta_{p^r}^t)^2 \\ &= \prod_{t<k}((1-\zeta_{p^r}^k) - (1-\zeta_{p^r}^t))^2 \\ &= D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \cdots, (1-\zeta_{p^r})^{\phi(p^r)-1}). \end{aligned}$$

■

Lema 2.3.5. *(*Marcus, 1977, p.31, Lema 2*) Temos que* $\prod_k(1-\zeta_{p^r}^k) = p$, *onde o produto é tomado sobre todos os* k, *com* $1 \leq k \leq p^r$, *e tal que* $p \nmid k$.

Demonstração. Como $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$, segue que todos os $\zeta_{p^r}^k$, onde $1 \leq k \leq p^r$ e tal que $p \nmid k$ são raízes de $\varphi_{p^r}(X)$ pois são raízes de $X^{p^r}-1$ mas não de $X^{p^{r-1}}-1$. Deste modo, $\varphi_{p^r}(X) = \prod_k(X-\zeta_{p^r}^k)$ e existem exatamente $\phi(p^r) = (p-1)p^{r-1}$ valores de k pois $\partial(\varphi_{p^r}(X)) = (p-1)p^{r-1}$. Tomando $X = 1$, temos que $\varphi_{p^r}(1) = \prod_k(1-\zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p$.

■

Teorema 2.3.3. *(*Marcus, 1977, p.29, Teo.9*) Sejam* $\{\alpha_1, \cdots, \alpha_n\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *consistindo de inteiros algébricos e* $d = D_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$. *Se* $\alpha \in \mathbb{A}_{\mathbb{K}}$, *então* α *pode ser expresso na forma* $\dfrac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$, *com* $m_j \in \mathbb{Z}$ *e* m_j^2 *divisível por* d, *para* $j = 1, 2, \cdots, n$.

Demonstração. Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, então $\alpha \in \mathbb{K}$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n,$$

com $x_j \in \mathbb{Q}$, para $j = 1, \cdots, n$. Sejam $\sigma_1, \cdots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando cada σ_i, para $i = 1, \cdots, n$, em α, obtemos um sistema de n equações dada por

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n),$$

para $i = 1, \cdots, n$. Resolvendo esse sistema pela regra de Cramer, obtemos que as n raízes são dadas por $x_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Temos que os γ_j, para $j = 1, 2, \cdots, n$, e δ são inteiros algébricos pois são obtidos a partir dos $\alpha_i's$, que são, por hipótese, inteiros algébricos. Pela Proposição 1.6.3, temos que $\delta^2 = d$ e portanto $dx_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$ é um inteiro algébrico. Como $\mathbb{Z}$ é integralmente fechado segue que $dx_j \in \mathbb{Z}$, para $j = 1, 2, \cdots, n$. Seja $m_j = dx_j$, para $j = 1, 2, \cdots n$. Se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, teremos que m_j^2 é divisível por d. Mas, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$ então é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico. Como $m_j = dx_j = \delta\gamma_j$ segue que $m_j^2 = d^2x_j^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Logo $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j é um inteiro algébrico. Portanto $\frac{m_j^2}{d} \in \mathbb{Z}$ e assim m_j^2 é divisível por d. ■

Lema 2.3.6. *(*Marcus, 1977, p.31*) Se* $d = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{n-1})$, *onde* $n = \phi(p^r)$, *então* $d = p^s$ *para algum* $s \in \mathbb{N}$.

Demonstração: Pela Equação (2.3) temos que

$$X^{p^r} - 1 = \varphi_{p^r}(X)g(X), \tag{2.7}$$

onde $g(X) = X^{p^{r-1}} - 1$ e $\varphi_{p^r}(X)$ é o polinômio irredutível de ζ_{p^r} sobre $\mathbb{Q}$. Derivando a Equação (2.7) temos que $p^r X^{p^r-1} = \varphi_{p^r}'(X)g(X) + \varphi_{p^r}(X)g'(X)$, e substituindo X por ζ_{p^r} obtemos que

$$p^r\zeta_{p^r}^{p^r-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}) + \varphi_{p^r}(\zeta_{p^r})g^{'}(\zeta_{p^r}).$$

Como $\varphi_{p^r}(\zeta_{p^r}) = 0$ segue que

$$p^r\zeta_{p^r}^{p^r-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}),$$

e isto é equivalente a

$$p^r\zeta_{p^r}^{p^r}\zeta_{p^r}^{-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}),$$

ou seja,

$$p^r = \zeta_{p^r}\varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}).$$

Aplicando a função norma nesta última igualdade obtemos que

$$p^{nr} = N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\varphi_{p^r}^{'}(\zeta_{p^r}))N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Pela Proposição 1.6.4, temos que

$$p^{nr} = \pm D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1,\cdots,\zeta_{p^r}^{n-1})N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Logo, $d|p^{nr}$, ou seja, $d = p^s$, para algum inteiro s. ■

Teorema 2.3.4. *(*Marcus, 1977, p.30, Teo.10*) O anel $\mathbb{A}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ é $\mathbb{Z}[\zeta_{p^r}]$.*

Demonstração. Mostraremos que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}]$, e assim o teorema segue pelo Lema 2.3.4. Suponhamos que $\mathbb{A}_{\mathbb{K}} \neq \mathbb{Z}[1-\zeta_{p^r}]$. Pelo Teorema 2.3.3, todo elemento $\alpha \in \mathbb{A}_{\mathbb{K}}$ pode ser expresso na forma

$$\alpha = \frac{m_1 + m_2(1-\zeta_{p^r}) + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{d},$$

onde $n = \phi(p^r)$, e $m_i \in \mathbb{Z}$, para $i = 1, 2, \cdots, n$. Pelo Lema 2.3.6, temos que $d = p^s$, onde $s \in \mathbb{N}$. Logo, existe $\alpha \in \mathbb{A}_{\mathbb{K}}$ de modo que nem todos os m_j são divisíveis por p^s. Seja $i \leq n$ tal que m_i não seja divisível por p^s. Assim, temos que $m_i = p^s q + r$, onde $q, r \in \mathbb{Z}$ e $r < p^s$. Logo, podemos reescrever α da seguinte forma

$$\alpha = \frac{m_1 + m_2(1-\zeta_{p^r}) + \cdots + (p^s q + r)(1-\zeta_{p^r})^{i-1} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p^s}.$$

Desse modo, $\mathbb{A}_{\mathbb{K}}$ contém um elemento da forma

$$\gamma = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^{i} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p^s}.$$

Multiplicando ambos os lados por p^{s-1}, obtemos que

$$\gamma p^{s-1} = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^{i} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p},$$

que podemos reescrever como

$$\beta = \frac{a_i(1-\zeta_{p^r})^{i-1} + a_{i+1}(1-\zeta_{p^r})^{i} + \cdots + a_n(1-\zeta_{p^r})^{n-1}}{p},$$

com $a_j \in \mathbb{Z}$ e a_i não divisível por p. Pelo Lema 2.3.5, temos que $p/(1-\zeta_{p^r})^n \in \mathbb{Z}[\zeta_{p^r}]$ pois $1-\zeta_{p^r}^k$ é divisível, em $\mathbb{Z}[\zeta_{p^r}]$, por $1-\zeta_{p^r}$. Então $p/(1-\zeta_{p^r})^i \in \mathbb{Z}[\zeta_{p^r}]$ e portanto temos que $\beta p/(1-\zeta_{p^r})^i \in \mathbb{A}_{\mathbb{K}}$. Subtraindo termos que estão em $\mathbb{A}_{\mathbb{K}}$, obtemos que $a_i/(1-\zeta_{p^r}) \in \mathbb{A}_{\mathbb{K}}$. Disto segue que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}) \mid N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(a_i)$. Como $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(a_i) = a_i^n$ e pelo Lema 2.3.5, temos que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}) = p$. Assim $p \mid a_i^n$, o que é impossível pois a_i não é divisível por p. Portanto $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. ∎

Observação 2.3.2. *Como o p^r-ésimo polinômio ciclotômico tem grau $(p-1)p^{r-1}$ e seu termo independente é igual a 1, obtemos pela seção 1.4, que*

$$N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^t) = (-1)^{(p-1)p^{r-1}}, \text{ onde } t = 0, \cdots, p^{r-1} \text{ e } mdc(t, p^r) = 1. \tag{2.8}$$

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^t) = -a_{p-2} = -1, \text{ para } j = 1, \cdots, (p-1)p^{r-1} \tag{2.9}$$

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}. \tag{2.10}$$

Proposição 2.3.3. *(*Simonato, 2000, p.22, Prop.1.4.9*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ *sobre* $\mathbb{Q}$ *é dado por* $D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \pm p^{p^{r-1}\cdot(r(p-1)-1)}$.

Demonstração. Pela Proposição 1.6.4 temos que

$$D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \pm N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\varphi_{p^r}^{'}(\zeta_{p^r})).$$

Derivando ambos os membros de $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1}$, temos que

$$\varphi_{p^r}^{'}(X) = \frac{p^r X^{p^r-1}(X^{p^{r-1}}-1) - (X^{p^r}-1)p^{r-1}X^{p^{r-1}-1}}{(X^{p^{r-1}}-1)^2},$$

e substituindo X por ζ_{p^r} temos que

$$\varphi_{p^r}^{'}(\zeta_{p^r}) = \frac{p^r \zeta_{p^r}^{p^r-1}(\zeta_{p^r}^{p^{r-1}}-1) - (\zeta_{p^r}^{p^r}-1)p^{r-1}\zeta_{p^r}^{p^{r-1}-1}}{(\zeta_{p^r}^{p^{r-1}}-1)^2}.$$

Como $\zeta_{p^r}^{p^r} = 1$ segue que

$$\varphi_{p^r}^{'}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{-1}}{(\zeta_{p^r}^{p^{r-1}}-1)} = \frac{-p^r}{(1-\zeta_{p^r}^{p^{r-1}})\zeta_{p^r}}.$$

Temos que $\zeta_{p^r}^{p^{r-1}} = (e^{\frac{2\pi i}{p^r}})^{p^{r-1}} = e^{\frac{2\pi i}{p}} = \zeta_p$. Aplicando a função norma em ambos os membros e usando sua linearidade temos que

$$N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\varphi_{p^r}^{'}(\zeta_{p^r})) = \frac{N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(-p^r)}{N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_p)N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r})}.$$

Da Equação (2.8) temos que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = \pm 1$. Também $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$ e

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_p) &= N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_p)}(1-\zeta_p)) \\ &= (N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p))^{p^{r-1}} = p^{p^{r-1}}. \end{aligned}$$

Portanto $D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \dfrac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}$.

■

A seguir nosso objetivo é determinar o anel dos inteiros $\mathbb{A}_{\mathbb{K}}$ para qualquer corpo ciclotômico, $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Esta generalização seguirá de um resultado mais geral considerando os inteiros algébricos de um corpo composto $\mathbb{KL}$, onde $\mathbb{K}$ e $\mathbb{L}$ são corpos numéricos.

Se $\mathbb{K}$ e $\mathbb{L}$ são dois corpos numéricos, então o corpo composto $\mathbb{KL}$ (definido como o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{K}$ e $\mathbb{L}$) consistem de todas as somas finitas

$$\alpha_1\beta_1 + \cdots + \alpha_r\beta_r, \text{ onde } \alpha_i \in \mathbb{K}, \text{ e } \beta_i \in \mathbb{L}, \text{ para } i = 1, 2, \cdots, r.$$

Se $\mathbb{A}_{\mathbb{K}}$, $\mathbb{A}_{\mathbb{L}}$ e $\mathbb{A}_{\mathbb{KL}}$ são os anéis dos inteiros algébricos de $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{KL}$, respectivamente, então $\mathbb{A}_{\mathbb{KL}}$ contém o anel

$$\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}} = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r : \alpha_i \in \mathbb{A}_{\mathbb{K}}, \beta_i \in \mathbb{A}_{\mathbb{L}}, \text{ para } i = 1, 2, \cdots, r\}.$$

Em geral, não temos uma igualdade. Entretanto, podemos mostrar que $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$ sob certas condições sobre os corpos ciclotômicos.

Sejam m e n os graus de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, sobre $\mathbb{Q}$, e seja $d = mdc(d_1, d_2)$, onde d_1 e d_2 são o discriminante absoluto de $\mathbb{A}_{\mathbb{K}}$ e $\mathbb{A}_{\mathbb{L}}$, respectivamente.

Teorema 2.3.5. *(*Marcus, 1977, p.33, Teo.12*) Se* $[\mathbb{KL} : \mathbb{Q}] = mn$, *então* $\mathbb{A}_{\mathbb{KL}} \subset \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$.

Demonstração. Sejam $\{\alpha_1, \cdots, \alpha_m\}$ uma base de $\mathbb{A}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $\{\beta_1, \cdots, \beta_n\}$ uma base de $\mathbb{A}_{\mathbb{L}}$ sobre $\mathbb{Z}$. Assim, temos que $\boldsymbol{B} = \{\alpha_i\beta_j,\ i = 1, \cdots, m;\ j = 1, \cdots, n\}$ é uma base de $\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$ sobre $\mathbb{Z}$ e também uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$. Se $\alpha \in \mathbb{A}_{\mathbb{KL}}$, então α pode ser expresso na forma

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j, \tag{2.11}$$

onde r e todos os m_{ij} estão em $\mathbb{Z}$, e que estes $mn+1$ inteiros não tem fatores comuns maiores que 1, ou seja, $mdc(r, mdc(m_{ij})) = 1$. Para mostrar o teorema, temos que mostrar que $r|d$ para qualquer α. Para isto, devemos mostrar que $r|d_1$ e $r|d_2$ pois assim, pela definição de máximo divisor comum, teremos que $r \mid d$. Temos que todo monomorfismo σ de $\mathbb{K}$ em $\mathbb{C}$ estende a um monomorfismo (que também denotamos por σ) de $\mathbb{KL}$ em $\mathbb{C}$, fixando $\mathbb{L}$. Portanto, para cada σ temos que

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r} \sigma(\alpha_i)\beta_j.$$

Tomando $x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$, para cada $i = 1, \cdots, m$, obtemos m equações $\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha)$ para cada σ. Agora, resolvendo este sistema pela regra de Cramer, obtemos que $x_i = \frac{\gamma_i}{\delta}$, onde δ é o determinante da matriz formado pelos coeficientes $\sigma(\alpha_i)$ e γ_i é obtido de δ trocando a i-ésima coluna por $\sigma(\alpha)$, para $i = 1, 2, \cdots, m$. Temos que δ e todos os γ_i são inteiros algébricos, pois todos os $\sigma(\alpha_i)$ e $\sigma(\alpha)$ são, e além disso $\delta^2 = d_1$. Se $e = d_1$, temos que $ex_i = \delta\gamma_i \in \mathbb{A}_{\mathbb{C}}$, onde $\mathbb{A}_{\mathbb{C}}$ é o anel dos inteiros algébricos de $\mathbb{C}$, e portanto $ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j \in \mathbb{A}_{\mathbb{C}} \cap \mathbb{L} = \mathbb{A}_{\mathbb{L}}$. Lembrando que $\{\beta_1, \cdots, \beta_n\}$ forma uma base integral para $\mathbb{A}_{\mathbb{L}}$, concluímos que os números racionais $\frac{em_{ij}}{r}$ devem ser inteiros, e deste modo r divide em_{ij}, para todo i e j. Como assumimos que r é relativamente primo com $mdc(m_{ij})$, segue que $r|e = d_1$. Analogamente, $r|d_2$. Portanto, $r \mid d$ e assim $d = kr$, com $k \in \mathbb{Z}$, ou seja, $r = \frac{d}{k}$. Substituindo na Equação (2.11) temos que $\alpha = \sum_{i,j} \frac{km_{ij}}{d}\alpha_i\beta_j = \frac{1}{d}\sum_{i,j} km_{ij}\alpha_i\beta_j$. Logo $\alpha \in \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. Portanto $\mathbb{A}_{\mathbb{KL}} \subset \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. ■

Corolário 2.3.2. *(*Marcus, 1977, p.34, Corol.1*) Se* $[\mathbb{KL} : \mathbb{Q}] = mn$ *e* $d = 1$, *então* $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$.

Demonstração. Como $\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}} \subset \mathbb{A}_{\mathbb{KL}}$ e como $d = 1$ segue, pelo Teorema 2.3.5, que $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. ■

Teorema 2.3.6. *(*Marcus, 1977, p.34, Corol.2*) O anel dos inteiros de* $\mathbb{Q}(\zeta_n)$ *é* $R = \mathbb{Z}[\zeta_n]$.

Demonstração: O teorema já foi provado se n é primo ou se é uma potência de um primo. Agora, se n não é primo ou não é uma potência de um primo, então podemos escrever $n = n_1 n_2$, para inteiros relativamente primos n_1, n_2 maiores que 1. Vamos mostrar por indução que se o resultado também é válido para n_1 e n_2, então o resultado é válido para n. Assim, suponhamos por hipótese de indução que $R_1 = \mathbb{Z}[\zeta_{n_1}]$ e $R_2 = \mathbb{Z}[\zeta_{n_2}]$. Para aplicar o Corolário 2.3.2, temos que mostrar que

1)$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ e como consequência $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}]$.

2) $\phi(n) = \phi(n_1)\phi(n_2)$.

3) $d = 1$.

A parte (1) segue do Corolário 2.3.1 e a parte (2) segue do fato de n_1 e n_2 serem relativamente primos. Para a parte (3), temos da Proposição 1.6.4 que $D(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha))$. Seja d_{n_1} e d_{n_2} o discriminante absoluto de $\mathbb{Z}[\zeta_{n_1}]$ e $\mathbb{Z}[\zeta_{n_2}]$, respectivamente. Como $f(X) = X^{n_1} - 1$, segue que $f'(X) = n_1 X^{n_1-1}$, e substituindo X por ζ_{n_1} segue que $f'(\zeta_{n_1}) = n_1 \zeta_{n_1}^{n_1-1} = \frac{n_1}{\zeta_{n_1}}$. Assim aplicando a função norma em ambos os lados e usando a sua linearidade temos que

$$N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(f'(\zeta_{n_1})) = \frac{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(n_1)}{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(\zeta_{n_1})} = \frac{n_1^{\phi(n_1)}}{\pm 1}.$$

Portanto $d_{n_1} = \pm n_1^{\phi(n_1)}$, e isto implica que

$$d_{n_1} | n_1^{\phi(n_1)}.$$

Analogamente,

$$d_{n_2} | n_2^{\phi(n_2)}.$$

Sendo $d = mdc(d_{n_1}, d_{n_2})$, temos que

$$\begin{cases} d | d_{n_1} \text{ e } d_{n_1} | n_1^{\phi(n_1)} \Longrightarrow d | n_1^{\phi(n_1)} \\ d | d_{n_2} \text{ e } d_{n_2} | n_2^{\phi(n_2)} \Longrightarrow d | n_2^{\phi(n_2)}. \end{cases}$$

Como $mdc(n_1^{\phi(n_1)}, n_2^{\phi(n_2)}) = 1$ segue que $d|1$, e portanto $d = 1$. Finalmente então concluímos que $R = R_1 R_2 = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_n]$. ■

Teorema 2.3.7. *(*Washington, 1982, p.11*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{Q}$ *é dado por*

$$D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}) = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Demonstração: Por (Ribenboim, 1972, p.217, prop.7O) temos que $D_{\mathbb{LM}} = D_{\mathbb{L}}^{[\mathbb{M}:\mathbb{Q}]} \cdot D_{\mathbb{M}}^{[\mathbb{L}:\mathbb{Q}]}$. Aplicando a função logaritmo em ambos os lados e usando as propriedades do logaritmo segue que $\log|D_{\mathbb{LM}}| = [\mathbb{M} : \mathbb{Q}] \log|D_{\mathbb{L}}| + [\mathbb{L} : \mathbb{Q}] \log|D_{\mathbb{M}}|$. Como toda extensão ciclotômica é Galoisiana, segue que $[\mathbb{LM} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}][\mathbb{M} : \mathbb{Q}]$, e assim

$$\frac{\log|D_{\mathbb{LM}}|}{[\mathbb{LM} : \mathbb{Q}]} = \frac{\log|D_{\mathbb{L}}|}{[\mathbb{L} : \mathbb{Q}]} + \frac{\log|D_{\mathbb{M}}|}{[\mathbb{M} : \mathbb{Q}]}.$$

Portanto, se $n = \prod_i p_i^{a_i}$ temos que

$$\frac{\log|D_{\mathbb{K}}|}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \frac{\log|D_{\mathbb{K}_1}|}{[\mathbb{Q}(\zeta_{p_1^{a_1}}) : \mathbb{Q}]} + \cdots + \frac{\log|D_{\mathbb{K}_r}|}{[\mathbb{Q}(\zeta_{p_r^{a_r}}) : \mathbb{Q}]} = \sum_{i=1}^{n} \frac{\log|D_{\mathbb{K}_i}|}{\phi(p_i^{a_i})},$$

onde $\mathbb{K}_i = \mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \cdots, r$. Assim, pela Proposição 2.3.3, temos que

$$\begin{aligned}
\frac{\log|D_{\mathbb{K}}|}{\phi(n)} &= \sum_{i=1}^{r} \frac{\log p_i^{p_i^{a_i-1}(a_i(p_i-1)-1)}}{p_i^{a_i-1}(p_i-1)} = \sum_{i=1}^{r} \frac{p_i^{a_i-1}(a_i(p_i-1)-1)}{p_i^{a_i-1}(p_i-1)} log p_i = \\
&= \sum_{i=1}^{r} \left(a_i - \frac{1}{p_i-1}\right) log p_i = \sum_{i=1}^{r} a_i log p_i - \sum_{i=1}^{r} \frac{log p_i}{p_i-1} = \\
&= \sum_{i=1}^{r} log p_i^{a_i} - \sum_{i=1}^{r} log p_i^{\frac{1}{p_i-1}} = \\
&= log\left(\prod_{i=1}^{r} p_i^{a_i}\right) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right) = \\
&= log(n) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right),
\end{aligned}$$

e consequentemente,

$$log|D_{\mathbb{K}}| = \phi(n)\left(log(n) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right)\right) = log\left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\phi(n)}.$$

Assim, $|D_{\mathbb{K}}| = \left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\phi(n)}$ e portanto,

$$D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

■

2.4 Decomposição de ideais primos em uma extensão

Nesta seção apresentamos a decomposição de um ideal primo em um extensão. Assim, dados $A \subset B$, anéis e $\mathfrak{a}$ um ideal de A, denotamos por $\mathfrak{a}B$ ao ideal de B formado pelos elementos da forma $\sum_{i=1}^{n} x_i y_i$, com $x_i \in \mathfrak{a}$ e $y_i \in B$. Além disso, consideramos $\mathbb{K} \subset \mathbb{L}$ corpos de números tais que $[\mathbb{L} : \mathbb{K}] = n$.

Se $\mathfrak{p}$ é um ideal primo de B, consideremos a inclusão $i : A \longrightarrow B$, a projeção canônica $h : B \longrightarrow B/\mathfrak{p}$ e a composição $f = h \circ i$. O núcleo de f é $A \cap \mathfrak{p}$ e portanto $A/(A \cap \mathfrak{p}) \simeq f(A) \subset B/\mathfrak{p}$, e deste modo, $A/(A \cap \mathfrak{p})$ é um domínio, isto é, $A \cap \mathfrak{p}$ é um ideal primo de A.

Proposição 2.4.1. *(*Samuel, 1967, p.71, Prop.1*) Sejam $\mathfrak{p}$ um ideal primo não nulo de $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{b}_i^{e_i}$ a decomposição do ideal $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ em ideais primos de $\mathbb{A}_{\mathbb{L}}$. Então os $\mathfrak{b}_i$'s são os únicos ideais primos de $\mathbb{A}_{\mathbb{L}}$ cuja interseção com $\mathbb{A}_{\mathbb{K}}$ coincide com $\mathfrak{p}$ e nestas condições dizemos que $\mathfrak{b}_i$ é um ideal acima de $\mathfrak{p}$.*

Demonstração: Para cada $i = 1, \cdots, g$ temos que $\mathfrak{b}_i \supseteq \mathfrak{p}\mathbb{A}_{\mathbb{L}} \supseteq \mathfrak{p}$, e portanto $\mathfrak{b}_i \cap \mathbb{A}_{\mathbb{K}}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ que contém $\mathfrak{p}$. Sendo $\mathfrak{p}$ maximal resulta que $\mathfrak{p} = \mathfrak{b}_i \cap \mathbb{A}_{\mathbb{K}}$. Agora, se d é um ideal primo de $\mathbb{A}_{\mathbb{L}}$ tal que $d \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, então $d = \mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{b}_i^{e_i}$. Assim, $d \supseteq \mathfrak{b}_i$, para algum i. Como $\mathfrak{b}_i$ é maximal segue que $d = \mathfrak{b}_i$. ■

O anel $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ pode ser considerado como um subanel de $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ através do homomorfismo induzido acima. Além disso, $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ são corpos e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ é um espaço vetorial de dimensão finita sobre $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$, uma vez que $\mathbb{A}_{\mathbb{L}}$ e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ são finitamente gerados como

$\mathbb{A}_{\mathbb{K}}$-módulo e $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$-módulo, respectivamente. A dimensão $[\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i : \mathbb{A}_{\mathbb{K}}/\mathfrak{p}]$, denotada por f_i ou $f(\mathfrak{b}_i, \mathfrak{p})$ é denominada de **grau residual** de $\mathfrak{b}_i$ sobre $\mathbb{A}_{\mathbb{K}}$. O expoente e_i ou $e(\mathfrak{b}_i, \mathfrak{p})$ é denominado **índice de ramificação** de $\mathfrak{b}_i$ sobre $\mathbb{A}_{\mathbb{K}}$. Quando $e_i > 1$, para algum índice i, dizemos que $\mathfrak{p}$ se ramifica em $\mathbb{L}$.

As igualdades $\sum_{i=1}^{g} e_i f_i = [\mathbb{A}_{\mathbb{L}}/\mathfrak{p}\mathbb{A}_{\mathbb{L}} : \mathbb{A}/\mathfrak{p}] = n$ podem ser vistas em ([6], *p.*71, *Teo.*1) e este resultado é conhecido como **Igualdade Fundamental**.

A igualdade fundamental forma alguns tipos de decomposições de $\mathfrak{p}$. Diremos, então, que o ideal primo $\mathfrak{p}$ de $\mathbb{A}_{\mathbb{K}}$ é

(i) totalmente decomposto em $\mathbb{L}$, se $g = n$ e consequentemente, $e_i = f_i = 1$, $i = 1, \cdots, g$.

(ii) inerte em $\mathbb{L}$, se $g = 1$, $e_1 = 1$ e consequentemente $f_1 = n$.

(iii) totalmente ramificado em $\mathbb{L}$, se $g = 1$ e consequentemente $f_1 = 1$ e $e_1 = n$.

Teorema 2.4.1. *(*Lang, 1970, p.27, Prop.25*) (Kummer) Seja A um anel de Dedekind com corpo quociente $\mathbb{K}$. Seja $\mathbb{L}$ uma extensão finita separável de $\mathbb{K}$. Seja $\mathbb{A}_{\mathbb{L}}$ o fecho integral de A em $\mathbb{L}$ e assuma que $\mathbb{A}_{\mathbb{L}} = A[\alpha]$ para algum elemento α. Seja $f(X)$ o polinômio irredutível de α sobre $\mathbb{K}$. Seja $\mathfrak{p}$ um ideal primo de A. Seja $\overline{f}(X)$ a redução de $f(X)$ e $\mathfrak{p}$, e seja*

$$\overline{f}(X) = \overline{\mu}_1(X)^{e_1} \cdots \overline{\mu}_r(X)^{e_r}$$

a fatoração de $\overline{f}(X)$ em potências de fatores irredutíveis sobre $\overline{A} = A/\mathfrak{p}$, com coeficiente dominante 1. Então

$$\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r} \tag{2.12}$$

é a fatoração de $\mathfrak{p}$ em $\mathbb{A}_{\mathbb{L}}$, de modo e_i é o índice de ramificação de

$\mathfrak{B}_i$ *sobre* $\mathfrak{p}$, *e temos que*

$$\mathfrak{B}_i = \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_i(\alpha)\mathbb{A}_{\mathbb{L}}, \tag{2.13}$$

se $\mu_i(X) \in A[X]$ *é um polinômio com coeficiente dominante 1 cuja redução módulo* $\mathfrak{p}$ *é* $\overline{\mu}_i(X)$.

Demonstração: Sejam $\overline{\mu}(X)$ um fator irredutível de $\overline{f}(X)$, $\overline{\alpha}$ uma raiz de $\overline{\mu}(X)$, e $\mathfrak{B}$ o ideal primo de $\mathbb{A}_{\mathbb{L}}$ que é o kernel da função

$$A[\alpha] \longrightarrow \overline{A}[\overline{\alpha}].$$

Temos que $\mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu(\alpha)\mathbb{A}_{\mathbb{L}}$ está contido em $\mathfrak{B}$. Por outro lado, seja $g(\alpha) \in \mathfrak{B}$ onde $g(X) \in A[X]$. Então $\overline{g}(X) = \overline{\mu(X)h(X)}$ para algum $\overline{h}(X) \in \overline{A}[X]$, e portanto $g(X) - \mu(X)h(X)$, que é um polinômio com coeficientes em A, uma vez que tem coeficientes em $\mathfrak{p}$. Isto prova a inclusão contrária, provando (2.13). Para provar (2.12), seja $e_i^{'}$ o índice de ramificação de $\mathfrak{B}_i$, tal que

$$\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1^{'}} \cdots \mathfrak{B}_r^{e_r^{'}},$$

e seja d_i o grau de $\overline{\mu}_i$. Como $f(\alpha) = 0$, e como

$$f(X) - \mu_1(X)^{e_1} \cdots \mu_r(X)^{e_r} \in \mathfrak{p}A[X],$$

segue que

$$\mu_1(\alpha)^{e_1} \cdots \mu_r(\alpha)^{e_r} \in \mathfrak{p}\mathbb{A}_{\mathbb{L}}. \tag{2.14}$$

Por outro lado, temos que

$$\mathfrak{B}_i^{e_i} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_i(\alpha)^{e_i}\mathbb{A}_{\mathbb{L}},$$

consequentemente usando a Equação (2.14) temos que

$$\mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_1(\alpha)^{e_1} \cdots \mu_r(\alpha)^{e_r}\mathbb{A}_{\mathbb{L}} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1^{'}} \cdots \mathfrak{B}_r^{e_r^{'}}.$$

Isto prova que $e_i \geq e_i^{'}$ para todo i. Mas sabemos que

$$\sum e_i d_i = \partial f = [\mathbb{L} : \mathbb{K}] = \sum e_i^{'} d_i.$$

Assim $e_i = e_i^{'}$ para todo i, o que prova (2.12). ■

Teorema 2.4.2. *(*Samuel, 1967, p.74, Teo.1*) Se $\mathbb{K}$ é um corpo de números, então um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathbb{K}$ se, e somente se, p divide $D_{\mathbb{K}}$.* ■

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

Lema 2.4.1. *(*Marcus, 1977, p.78, Corol.*) Sejam ζ_m uma raiz m-ésima da unidade, $n = \varphi(m)$, p um número primo e $O_m(p)$ a ordem de p módulo m. Se p não divide m, então $p\mathbb{Z}[\zeta_m]$ se decompõe em $\frac{n}{O_m(p)}$ ideais primos distintos de $\mathbb{Z}[\zeta_m]$.* ■

Exemplo 2.4.1. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-17})$, então $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-17}]$ e $f(X) = X^2 + 17$ é o polinômio minimal de $\sqrt{-17}$ sobre $\mathbb{Q}$. Vamos obter a fatoração dos ideais $2\mathbb{A}_{\mathbb{K}}$, $3\mathbb{A}_{\mathbb{K}}$ e $5\mathbb{A}_{\mathbb{K}}$ em produto de ideais primos de $\mathbb{A}_{\mathbb{K}}$ usando o Lema de Kummer. Como*

$$X^2 + 17 \equiv (X+1)^2 (mod\ (\mathbb{Z}/2\mathbb{Z})[X]),$$

segue que

$$g = 1, \quad \overline{\mu_1}(X) = X + 1, \quad e_1 = 2 \quad e \quad f_1 = \partial \overline{\mu_1}(X) = 1$$
$$\mathfrak{p}_1 = 2\mathbb{A}_{\mathbb{K}} + (1 + \sqrt{-17})\mathbb{A}_{\mathbb{K}}.$$

Portanto, $2\mathbb{A}_{\mathbb{K}} = \mathfrak{p}_1^2$, onde $\mathfrak{p}_1$ é o ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $N(\mathfrak{p}_1) = p^{f_1} = 2$. Pela Proposição 2.4.1 segue que $\mathfrak{p}_1$ é o único ideal de $\mathbb{A}_{\mathbb{K}}$ acima do ideal $2\mathbb{Z}$ e é totalmente ramificado em $\mathbb{K}$. Para o ideal $3\mathbb{A}_{\mathbb{K}}$ como

$$X^2 + 17 \equiv (X+1)(X-1) (mod\ (\mathbb{Z}/3\mathbb{Z})[X]),$$

Segue que:

$$g = 2,\ \overline{\mu_1}(X) = X + 1,\ \overline{\mu_2}(X) = X - 1,\ e_1 = e_2 = 1\, e\, f_1 = f_2 = 1.$$
$$\mathfrak{q}_1 = 3\mathbb{A}_{\mathbb{K}} + (1 + \sqrt{-17})\mathbb{A}_{\mathbb{K}} \quad e \quad \mathfrak{q}_2 = 3\mathbb{A}_{\mathbb{K}} + (1 - \sqrt{-17})\mathbb{A}_{\mathbb{K}}.$$

Portanto, $3\mathbb{A}_{\mathbb{K}} = \mathfrak{q}_1\mathfrak{q}_2$ *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são os únicos ideais primos de* $\mathbb{A}_{\mathbb{K}}$ *acima de* $3\mathbb{Z}$ *com norma 3 e o ideal* $3\mathbb{Z}$ *é totalmente decomposto em* $\mathbb{K}$. *Finalmente, para o ideal* $5\mathbb{A}_{\mathbb{K}}$, *temos que* $X^2 + 17 \equiv X^2 + 2(mod\ (\mathbb{Z}/5\mathbb{Z})[X])$ *e* $X^2 + 2$ *é irredutível sobre* $\mathbb{Z}/5\mathbb{Z}$. *Logo* $5\mathbb{A}_{\mathbb{K}}$ *é um ideal primo de* $\mathbb{A}_{\mathbb{K}}$ *com norma 25 e o ideal* $5\mathbb{Z}$ *é inerte em* $\mathbb{K}$.

Exemplo 2.4.2. *Sejam* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{15}]$ *o anel de inteiros algébricos de* $\mathbb{K} = \mathbb{Q}(\zeta_{15})$ *e* $f(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ *o polinômio minimal de* ζ_{15} *sobre* $\mathbb{Q}$. *Vamos obter a fatoração de* $3\mathbb{A}_{\mathbb{K}}$. *Como*

$$f(X) \equiv (X^4 + X^3 + X^2 + X + 1)^2 (mod\ \mathbb{Z}/3\mathbb{Z})[X]),$$

segue que

$$g = 1,\ \overline{\mu_1}(X) = X^4 + X^3 + X^2 + X + 1,\ e_1 = 2\, e\, f_1 = \partial\overline{\mu_1}(X) = 4.$$
$$\mathfrak{p}_1 = 3\mathbb{A}_{\mathbb{K}} + (\zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1)\mathbb{A}_{\mathbb{K}}.$$

Portanto, $3\mathbb{A}_{\mathbb{K}} = \mathfrak{p}_1^2$, *onde* $\mathfrak{p}_1$ *é o único ideal primo de* $\mathbb{A}_{\mathbb{K}}$ *acima de* $3\mathbb{Z}$ *com norma* 3^4. *Note que neste caso* $3\mathbb{Z}$ *se ramifica em* $\mathbb{K}$, *mas não é totalmente ramificado em* $\mathbb{K}$.

Tendo em vista o Lema 2.4.1 e considerando $\frac{n}{O_m(p)} > 1$, temos que a menor decomposição possível do ideal $p\mathbb{Z}[\zeta_m]$ em produto de ideais primos distintos de $\mathbb{Z}[\zeta_m]$ ocorre primeiramente em $m = 3$ e $p \equiv 1(mod\ 3)$, pois $p\mathbb{Z}[\zeta_3]$ se decompõe em 2 ideais primos distintos de $\mathbb{Z}[\zeta_3]$. Usando o Lema de Kummer vejamos, por exemplo, como se dá a fatoração do ideal $13\mathbb{Z}[\zeta_3]$. Note que $13 \equiv 1(mod\ 3)$ e o

polinômio minimal de ζ_3 sobre $\mathbb{Q}$ é $X^2 + X + 1$. Logo

$$X^2 + X + 1 \equiv (X + 4)(X + 10)(mod\ (\mathbb{Z}/13\mathbb{Z})[X]).$$
$$g = 2,\ \overline{\mu_1}(X) = X + 4,\ \overline{\mu_2}(X) = X + 10,\ e_1 = e_2 = 1,\ f_1 = f_2 = 1.$$

Assim, $13\mathbb{Z}[\zeta_3] = \mathfrak{p}_1\mathfrak{p}_2$, onde $\mathfrak{p}_1 = 13\mathbb{Z}[\zeta_3] + (\zeta_3 + 4)\mathbb{Z}[\zeta_3]$ *e* $\mathfrak{p}_2 = 13\mathbb{Z}[\zeta_3] + (\zeta_3 + 10)\mathbb{Z}[\zeta_3]$.

Agora, sejam $\mathbb{K} \subset \mathbb{L}$ corpos de números com $\mathbb{L}$ uma extensão Galoisiana de $\mathbb{K}$ de grau n. Veremos que em uma extensão Galoisiana a decomposição de um ideal em $\mathbb{A}_{\mathbb{L}}$, dado como no Teorema 2.4.1, assume certas características particulares. Seja G o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Se G for um grupo abeliano diremos que $\mathbb{L}$ é uma extensão abeliana de $\mathbb{K}$.

Observação 2.4.1. *Seja $\mathbb{K}$ um corpo de números. Se $\mathbb{L} = \mathbb{K}(\zeta_m)$, então $\mathbb{L}$ é uma extensão galoisiana de $\mathbb{K}$ e o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é isomorfo a um subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$.*

Decorre da Observação 2.4.1 que toda extensão ciclotômica de $\mathbb{K}$ é abeliana e, em particular, todo subcorpo de um corpo ciclotômico é uma extensão abeliana de $\mathbb{Q}$. Reciprocamente, se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$, então existe um inteiro m tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$. Este resultado é conhecido como Teorema de Kronecker-Weber.

Lema 2.4.2. *(*Samuel, 1967, p.89, Lema 1*) Sejam A um anel e $\mathfrak{b}, \mathfrak{p}_1, \cdots, \mathfrak{p}_r$ ideais primos de A tais que $\mathfrak{b}$ não esteja contido em $\mathfrak{p}_i$, para $i = 1, \cdots, r$. Então existe b em $\mathfrak{b}$ tal que b não está em $\mathfrak{p}_i$, para todo $i = 1, \cdots, r$.*

Demonstração. Sem perda de generalidade, podemos considerar o caso em que $\mathfrak{p}_j$ não está contido em $\mathfrak{p}_i$, para $j \neq i$. Tomemos

elementos $x_{ij} \in \mathfrak{p}_j - \mathfrak{p}_i$ (para $j \neq i$, $1 \leq i \; e \; j \leq r$) e elementos $a_i \in \mathfrak{b} - \mathfrak{p}_i$. Se $b_i = a_i \prod_{j \neq i} x_{ij}$, então $b_i \in \mathfrak{b}$, $b_i \in A - \mathfrak{p}_i \, e \, b_i \in \mathfrak{p}_j$, para $j \neq i$. Colocando $b = b_1 + \cdots + b_r$, tem-se que $b \in \mathfrak{b}$ e $b \equiv b_i (mod \; \mathfrak{p}_i)$, isto é, $b \in \mathfrak{b} - \bigcup_{i=1}^{r} \mathfrak{p}_i$ é o elemento procurado. ■

Seja α um elemento de $\mathbb{A}_{\mathbb{L}}$. Aplicando $\sigma \in G$ na equação de dependência inteira de α sobre $\mathbb{A}_{\mathbb{K}}$ temos que $\sigma(\alpha) \in \mathbb{A}_{\mathbb{L}}$, ou seja, $\sigma(\mathbb{A}_{\mathbb{L}}) = \mathbb{A}_{\mathbb{L}}$ para todo $\sigma \in G$. Por outro lado, se $\mathfrak{p}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{q}$ é um ideal primo de $\mathbb{A}_{\mathbb{L}}$ tal que $\mathfrak{q}$ contém $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ como na Proposição 2.4.1, ou seja, $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, então $\sigma(\mathfrak{q}) \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$ para todo $\sigma \in G$, ou seja, $\sigma(\mathfrak{q})$ contém $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ e tem o mesmo expoente que $\mathfrak{q}$. Neste caso dizemos que $\mathfrak{q}$ e $\mathfrak{q}' = \sigma(\mathfrak{q})$ são ideais primos conjugados contidos em $\mathbb{A}_{\mathbb{L}}$.

Proposição 2.4.2. *(*Samuel, 1967, p.89, Prop.1*) Se $\mathfrak{p}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$, então os ideais primos $\mathfrak{p}_i$ de $\mathbb{A}_{\mathbb{L}}$ acima de $\mathfrak{p}$ são dois a dois conjugados, têm o mesmo grau residual f e o mesmo índice de ramificação e. Portanto, $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \left(\prod_{i=1}^{g} \mathfrak{p}_i \right)^e$ e $n = efg$.*

Demonstração: Suponhamos, por absurdo, que existam ideais primos $\mathfrak{q}$ e $\mathfrak{q}'$ acima de $\mathfrak{p}$ tais que $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$, para todo $\sigma \in G$. Como $\mathfrak{q}$ e $\mathfrak{q}'$ são ideais maximais, podemos supor que $\mathfrak{q}$ não esteja contido em $\sigma(\mathfrak{q}')$, para $\sigma \in G$. Pelo Lema 2.4.2, existe um elemento $\alpha \in \mathfrak{q} - \bigcup_{\sigma \in G} \sigma(\mathfrak{q}')$. Sendo α inteiro sobre $\mathbb{A}_{\mathbb{K}}$, segue que $\sigma(\alpha)$ também é inteiro sobre $\mathbb{A}_{\mathbb{K}}$, de onde $\prod_{\sigma \in G} \sigma(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha)$ é um elemento de $\mathfrak{q}$, e portanto um elemento de $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}}$.

Por outro lado, $\sigma(\alpha)$ não está em $\mathfrak{q}'$, pois caso contrário teríamos $\sigma^{-1}(\sigma(\alpha)) = \alpha \in \sigma^{-1}(\mathfrak{q}')$, contrariando a hipótese feita sobre α. Dessa forma, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$ não pertence a $\mathfrak{q}'$ (pois $\mathfrak{q}'$ é ideal

primo) e assim $\mathfrak{p}$ não está contido em $\mathfrak{q}$, o que é um absurdo. ■

Exemplo 2.4.3. *Se p é um número primo e $\mathbb{A}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, então o ideal $p\mathbb{A}_{\mathbb{K}}$ é da forma $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$. De fato: Se $1 \leq k, j \leq p-1$, então existe um inteiro t, onde $1 \leq t \leq p-1$ tal que $j \equiv kt (mod\ p)$. Assim,*

$$1-\zeta_p^j = 1-(\zeta_p^k)^t = (1-\zeta_p^k)(1+\zeta_p^k+\cdots+(\zeta_p^k)^{t-1}),$$

e portanto, $(1-\zeta_p^k)|(1-\zeta_p^j)$. Analogamente $(1-\zeta_p^j)|(1-\zeta_p^k)$. Assim $1-\zeta_p^j$ e $1-\zeta_p^k$ são associados em $\mathbb{A}_{\mathbb{K}}$. Como $p = \prod_{j=1}^{p-1}(1-\zeta_p^j)$, segue que existe um elemento inversível β em $\mathbb{A}_{\mathbb{K}}$ tal que $p = (1-\zeta_p)^{p-1}.\beta$. Assim, $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$ e $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ e da igualdade fundamental, segue que o grau residual de $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ sobre $\mathbb{Z}$ é 1.

Exemplo 2.4.4. *De modo análogo ao Exemplo* 2.4.3*, temos que se p é um número primo, r um número maior que 1 e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ então $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{(p-1)p^{r-1}}\mathbb{A}_{\mathbb{K}}$. Em síntese podemos classificar o ideal primo $p\mathbb{Z}$ como totalmente ramificado em $\mathbb{Q}(\zeta_{p^r})$, com $r \geq 1$.*

Definição 2.4.1. *Seja $\mathfrak{p}$ um ideal primo de $\mathbb{A}_{\mathbb{K}}$. Para cada ideal primo $\mathfrak{q}$ de $\mathbb{A}_{\mathbb{L}}$ satisfazendo $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, os conjuntos*

$$D(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

e

$$E(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x (mod\ \mathfrak{q}),\ para\ todo\ x \in \mathbb{A}_{\mathbb{L}}\}$$

são subgrupos de G, chamados de **grupo de decomposição** *e* **grupo de inércia** *de $\mathfrak{q}$ com relação a $\mathfrak{p}$, respectivamente.*

Quando $\mathbb{L}$ é uma extensão abeliana de $\mathbb{K}$, os grupos $D(\mathfrak{q}_i, \mathfrak{p})$, para $i = 1, \cdots, g$, onde os $\mathfrak{q}_i's$ são os ideais de $\mathbb{A}_{\mathbb{L}}$ acima de $\mathfrak{p}$, são todos iguais, dependendo somente do ideal $\mathfrak{p}$ de $\mathbb{A}_{\mathbb{K}}$. O mesmo acontece com os grupos $E(\mathfrak{q}_i, \mathfrak{p})$, para $i = 1, \cdots, g$. Em não havendo possibilidade de confusão denotamos tais grupos simplesmente por $D(\mathfrak{p})$ e $E(\mathfrak{p})$.

Se g denota o número de conjugados de $\mathfrak{q}$, então

$$card(G)card(D(\mathfrak{p}))^{-1} = g \text{ ou } card(D(\mathfrak{p})) = \frac{n}{g} = ef$$

Cada $\sigma \in D(\mathfrak{p})$ induz um automorfismo $\widetilde{\sigma}$ de $\mathbb{A}_{\mathbb{L}/\mathfrak{q}}$ tal que $\widetilde{\sigma}(x + \mathfrak{q}) = \sigma(x) + \mathfrak{q}$ (uma vez que o homomorfismo $x \longrightarrow \sigma(x) + \mathfrak{q}$ de $\mathbb{A}_{\mathbb{L}}$ em $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ é sobrejetivo e tem núcleo $\mathfrak{q}$). Como $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ é uma extensão Galoisiana de grau f de $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ ([6], *p.*90, *Prop.*2) e $\widetilde{\sigma}$ fixa o subcorpo $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$, pois σ fixa $\mathbb{K} \supset \mathbb{A}_{\mathbb{K}}$, concluímos que $\widetilde{\sigma} \in \widetilde{G}$, onde $\widetilde{G}$ denota o grupo de Galois de $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ sobre $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ e tal grupo é cíclico de ordem f. Além disso, temos que $\sigma \longrightarrow \widetilde{\sigma}$ é um homomorfismo sobrejetor de $D(\mathfrak{p})$ em $\widetilde{G}$ com núcleo $E(\mathfrak{p})$. Com isso, temos a seguinte proposição.

Proposição 2.4.3. *(*Marcus, 1977, p.99*)* $E(\mathfrak{p})$ *é um subgrupo normal de* $D(\mathfrak{p})$ *e* $D(\mathfrak{p})/E(\mathfrak{p}) \longrightarrow \widetilde{G}$ *é um isomorfismo de grupos.*

Como consequência da Proposição 2.4.3 temos que

$$card(\widetilde{G}) = card(D(\mathfrak{p}))card(E(\mathfrak{p}))^{-1}, \text{ ou seja, } card(E(\mathfrak{p})) = e.$$

Exemplo 2.4.5. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$ *e* $f(X) = X^8 - X^6 + X^4 - X^2 + 1$ *o polinômio minimal de* ζ_{20} *sobre* $\mathbb{Q}$. *A decomposição do ideal* $5\mathbb{A}_{\mathbb{K}}$ *em ideais primos de* $\mathbb{A}_{\mathbb{K}}$ *satisfaz:*

$$f(X) \equiv (X+3)^4(X+2)^4 (mod\ (\mathbb{Z}/5\mathbb{Z})[X]).$$

$$g = 2,\ \overline{\mu_1}(X) = X + 3,\ \overline{\mu_2}(X) = X + 2,\ e_1 = e_2 = 4\, e\, f_1 = f_2 = 1.$$

$$\mathfrak{p}_1 = 5\mathbb{A}_{\mathbb{K}} + (\zeta_{20} + 3)\mathbb{A}_{\mathbb{K}} \quad e \quad \mathfrak{p}_2 = 5\mathbb{A}_{\mathbb{K}} + (\zeta_{20} + 2)\mathbb{A}_{\mathbb{K}}.$$

Portanto, $5\mathbb{A}_{\mathbb{K}} = (\mathfrak{p}_1\mathfrak{p}_2)^4$. *O grupo* G *dos automorfismos de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $G = \{\sigma_i : mdc(i, 20) = 1$ *de forma que* $\sigma_i(\zeta_{20}) = \zeta_{20}^i\} = \{\sigma_1, \sigma_3, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{17}, \sigma_{19}\}$. *Além disso, temos que* $\mathfrak{p}_1$ *e* $\mathfrak{p}_2$ *são conjugados, uma vez que* $\sigma_3(\mathfrak{p}_1) = \mathfrak{p}_2$ *e* $\sigma_3(\mathfrak{p}_2) = \mathfrak{p}_1$. *Logo,* $\mathfrak{p}_1$ *e* $\mathfrak{p}_2$ *são ideais primos conjugados que têm o mesmo índice de ramificação (e=4) e o mesmo grau residual (f=1), conforme a Proposição* 2.4.2. *Visto que* $\mathbb{K}$ *é uma extensão abeliana de* $\mathbb{Q}$, *o grupo de decomposição* $D(5\mathbb{Z})$, *é dado por:*

$$D(5\mathbb{Z}) = \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\sigma_1, \sigma_9, \sigma_{13}, \sigma_{17}\}.$$

Da mesma forma, o grupo de inércia $E(5\mathbb{Z})$ *é dado por:*

$$E(5\mathbb{Z}) = \{\sigma \in G : \sigma(x) \equiv x(mod\ \mathfrak{p}_1), \text{ para todo } x \in \mathbb{A}_{\mathbb{K}}\} = \{\sigma \in D : \sigma(\zeta_{20}) \equiv \zeta_{20}(mod\ \mathfrak{p}_1)\}.$$

Como $card(E(5\mathbb{Z})) = 4$ *e como* $E(5\mathbb{Z})$ *é um subgrupo de* $D(5\mathbb{Z})$ *segue que* $E(5\mathbb{Z}) = D(5\mathbb{Z})$.

Quando tratamos de ideais no anel dos inteiros algébricos do corpo de números $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ com p e q números primos distintos, a fatoração dos ideais $p\mathbb{A}_{\mathbb{K}}$ ou $q\mathbb{A}_{\mathbb{K}}$ em produto de ideais primos de $\mathbb{A}_{\mathbb{K}}$ assume algumas particularidades interessantes que serão essenciais no próximo capítulo. Sejam $D_{\mathbb{L}}(p)$ o grupo de decomposição de um ideal de $\mathbb{A}_{\mathbb{L}}$ acima de $p\mathbb{Z}$ e $D_{\mathbb{K}}(p)$ o grupo de decomposição de um ideal de $A_{\mathbb{K}}$ acima de $p\mathbb{Z}$ em $\mathbb{K} = \mathbb{Q}(\zeta_q)$.

Observação 2.4.2. *Sejam* $\mathbb{A}_{\mathbb{L}}$ *o anel dos inteiros algébricos de* $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$, $\overline{\sigma}$ *a conjugação complexa de* $\mathbb{Q}(\zeta_{pq})$ *e* $p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g)^e$ *como na Proposição* 2.4.2. *Se* $\overline{\sigma}$ *não pertence ao grupo* $D_{\mathbb{L}}(p)$, *então para cada* $i = 1, \cdots, g$, *existe um único índice* k, $k \neq i$, *tal que* $\overline{\sigma}(\mathfrak{p}_i) = \overline{\mathfrak{p}_i} = \mathfrak{p}_k$ *(note que* $\overline{\sigma}(\overline{\mathfrak{p}_i}) = \mathfrak{p}_i$). *Aplicando* $\overline{\sigma}$ *no ideal* $p\mathbb{A}_{\mathbb{L}}$ *temos que*

$$p\mathbb{A}_{\mathbb{L}} = (\overline{\mathfrak{p}_1}\,\overline{\mathfrak{p}_2}\cdots\overline{\mathfrak{p}_g})^e.$$

Podemos supor $\overline{\mathfrak{p}_g} = \mathfrak{p}_1$, $\overline{\mathfrak{p}_{g-1}} = \mathfrak{p}_2, \cdots$ *e assim sucessivamente. Reordenando os ideais de maneira conveniente, obtemos que*

$$p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{g/2}\overline{\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{g/2}})^e.$$

Para saber em que situações teremos a fatoração acima, precisamos caracterizar quando $\overline{\sigma}$ pertence ao grupo de decomposição.

Proposição 2.4.4. *(*Flores, 2000, p.69, Teo.3.5.4*) Com as notações acima, temos que* $\overline{\sigma}$ *pertence a* $D_{\mathbb{L}}(p)$ *se, e somente se,* $\overline{\sigma}$ *pertence a* $D_{\mathbb{K}}(p)$.

Demonstração: Seja $\sigma_s \in D_{\mathbb{K}}(p)$ dado por $\sigma_s(\zeta_q) = \zeta_q^s$. Para cada $\sigma_s \in D_{\mathbb{K}}(p)$, existem $p-1$ automorfismos $\sigma_{s,i}$ de $D_{\mathbb{L}}(p)$ tais que $\sigma_{s,i}(x) = \sigma_s(x)$ para qualquer $x \in \mathbb{Q}(\zeta_q)$. Consideremos u e v tais que $pu + qv = 1$. Como cada $\sigma_{s,i}$ é definido por seu valor em ζ_{pq}, temos:

$$\sigma_{s,i}(\zeta_{pq}) = \sigma_{s,i}(\zeta_{pq}^{pu+qv}) = \sigma_{s,i}(\zeta_{pq}^{pu})\sigma_{s,i}(\zeta_{pq}^{qv}) = \sigma_{s,i}(\zeta_q^u)\sigma_{s,i}(\zeta_p^v) = \zeta_q^{us}\zeta_p^{vi} = \zeta_{pq}^{pus+qvi}.$$

Deste modo, $\overline{\sigma} \in D_{\mathbb{L}}(p)$ se, e somente se, existirem s, i tais que $pus + qvi \equiv -1(mod\ pq)$ e isto é o mesmo que

$$\begin{cases} pus + qvi \equiv -1(mod\ p) \\ pus + qvi \equiv -1(mod\ q). \end{cases}$$

A primeira condição vale sempre pois s pode assumir qualquer valor não nulo módulo p e a segunda condição equivale a $\overline{\sigma} \in D_{\mathbb{K}}(p)$, e isso conclui a demonstração. ■

Corolário 2.4.1. *(*Flores, 2000, p.70, Corol.3.5.5*) A conjugação complexa* $\overline{\sigma}$ *pertence a* $D_{\mathbb{L}}(p)$ *se, e somente se,* $O_q(p) \equiv 0(mod\ 2)$.

Demonstração: Pelo Lema 2.4.1 e pela Proposição 2.4.2 temos que o número g de conjugados de um ideal primo $\mathfrak{q}$ em $\mathbb{Q}(\zeta_q)$, acima de $p\mathbb{Z}$ é $\dfrac{q-1}{O_q(p)}$. Temos que $card(D(\mathfrak{p})) = \dfrac{n}{g}$ e assim, $g = \dfrac{n}{card(D(\mathfrak{p}))}$. Comparando com $g = \dfrac{q-1}{O_q(p)}$, temos que $card(D_{\mathbb{K}}(p)) = O_q(p)$, e assim 2 divide $O_q(p)$. Portanto $O_q(p) \equiv 0(mod\ 2)$. Reciprocamente, suponhamos que $O_q(p) \equiv 0(mod\ 2)$. Como o grupo $D_{\mathbb{K}}(p)$ é cíclico de ordem par, decorre que $\{-1, 1\}$ é o único subgrupo de ordem 2 deste grupo. ■

Exemplo 2.4.6. *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{15})$, $p = 3$ *e* $q = 5$. *Como* $O_5(3) = 4$, *pelo Corolário* 2.4.1, *segue que* $\overline{\sigma}$ *está em* $D_{\mathbb{L}}(3)$ *e, portanto, o ideal* $3\mathbb{A}_{\mathbb{L}}$ *não se decompõe segundo a Observação* 2.4.2. *Visto que* $O_3(5) = 2$, *o mesmo ocorre com o ideal* $5\mathbb{A}_{\mathbb{L}}$.

Exemplo 2.4.7. *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{57})$, $p = 19$ *e* $q = 3$. *Como* $O_3(19) = 1$, *segue pelo Corolário* 2.4.1, *que* $\overline{\sigma}$ *não pertence a* $D_{\mathbb{L}}(19)$. *Portanto o ideal* $19\mathbb{A}_{\mathbb{L}}$ *se decompõe segundo a Observação* 2.4.2.

3
Reticulados

3.1 Introdução

Os reticulados têm se mostrado bastante úteis em aplicações na Teoria das Comunicações. Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular.

Neste capítulo apresentamos as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e homomorfismo canônico. Através do homomorfismo canônico obtemos um método de gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números. O grande desafio é encontrar o anel dos inteiros de qualquer corpo de números, uma vez que são conhecidos apenas o anel dos inteiros dos corpos quadráticos e dos corpos ciclotômicos.

Deste modo, no presente capítulo apresentamos um estudo sobre reticulados no $\mathbb{R}^n$, explicitando alguns reticulados construtivos

conhecidos na literatura via o homomorfismo canônico. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

3.2 Reticulados

Nesta seção apresentamos o conceito de reticulados enfocando suas principais propriedades.

Definição 3.2.1. *Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subseteq \mathbb{K}$ um anel e $v_1, \cdots, v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$, com $m \leq n$. Chama-se* **reticulado** *com base $\beta = \{v_1, \cdots, v_m\}$ ao conjunto dos elementos de V da forma*

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \ \ com\ a_i \in A \right\},$$

que será denotado por H_β.

Nosso interesse maior será nos casos em que $\mathbb{K} = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $m = n$.

Definição 3.2.2. *Seja $H_\beta \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = \{v_1, \cdots, v_n\}$. O conjunto*

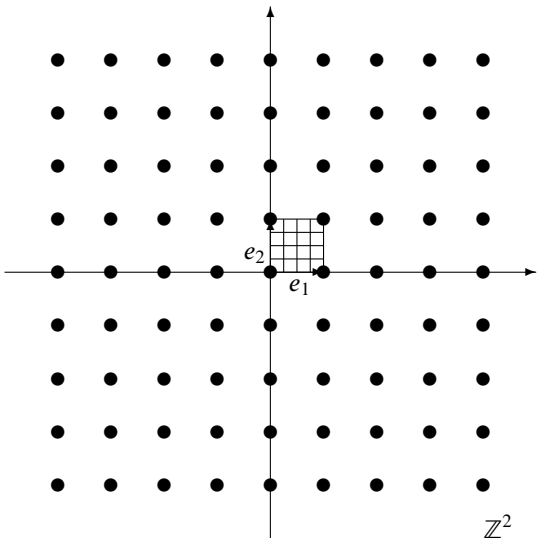
$$P_\beta = \left\{ x \in \mathbb{R}^n \ : \ x = \sum_{i=1}^{n} \lambda_i v_i, \ 0 \leq \lambda_i < 1 \right\},$$

é chamado de **região fundamental** *de H_β com relação a base $\{v_1, \cdots, v_n\}$.*

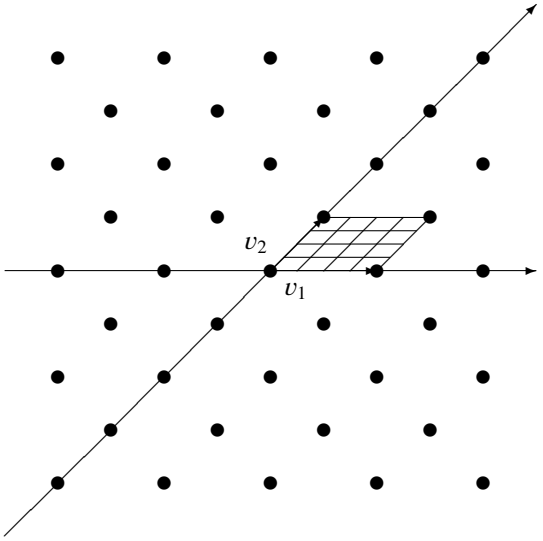
Se H_β é um reticulado com base $\beta = \{v_1, \cdots, v_n\}$ e se $c_1, \cdots, c_n$ são elementos quaisquer de H_β, então $c_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$.

Temos que uma condição necessária e suficiente para que $\{c_1, \cdots, c_n\}$ seja uma base de H_β é que $\det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Exemplo 3.2.1. *$H_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.*



Exemplo 3.2.2. *$H_\beta = \{(a, b) \in \mathbb{Z}^2; a + b \equiv 0 (mod\ 2)\}$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$ com região fundamental descrita pela figura abaixo.*



Definição 3.2.3. *Um subgrupo H do $\mathbb{R}^n$ é* **discreto** *se para qualquer subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, tivermos $H \cap \mathbb{K}$ finito.*

Exemplo 3.2.3. *Um típico exemplo de subconjunto discreto do $\mathbb{R}^n$ é $\mathbb{Z}^n$.*

O próximo teorema nos diz que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, a qual é então, uma $\mathbb{Z}$-base do reticulado dado.

Teorema 3.2.1. *(*Samuel, 1967, p.53, Teo.1*) Se H é um subgrupo discreto do $\mathbb{R}^n$, então H é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

Demonstração. Seja $\beta = \{e_1, \cdots, e_r\}$ um conjunto de vetores de H que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível com $r \leq n$. Seja o paralelepípedo

$$P_\beta = \left\{ x \in \mathbb{R}^n \,:\, x = \sum_{i=1}^{r} \alpha_i e_i,\ 0 \leq \alpha_i \leq 1 \right\}$$

construído a partir destes vetores. Como P_β é fechado e limitado, segue que P_β é compacto. Assim, $P_\beta \cap H$ é finito pois H é discreto. Se $x \in H$ então pela maximalidade de r, segue que $\{x, e_1, \cdots, e_r\}$ é linearmente dependente. Logo existem $\lambda_i \in \mathbb{R}$, $i = 1, \cdots, r$, não todos nulos, tal que $x = \sum_{i=1}^{r} \lambda_i e_i$. Para cada $j \in \mathbb{N}$, seja

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \in H, \tag{3.1}$$

onde [k] denota o maior inteiro menor ou igual a k. Assim,

$$x_j = j \sum_{i=1}^{r} \lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i \in P_e \cap H.$$

Dessa forma, se tomarmos $j = 1$ na Equação 3.1 temos que $x_1 = x - \sum_{i=1}^{r} [\lambda_i] e_i$, ou seja, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$. Assim, como $x_1 \in P_e \cap H$ e este é finito, segue que H é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, do fato de $P_e \cap H$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros j e k, tais que $x_j = x_k$. Da Equação (3.1), segue que $x_j = x_k \Longrightarrow jx - \sum_{i=1}^{r} [j\lambda_i] e_i = kx - \sum_{i=1}^{r} [k\lambda_i] e_i \Longrightarrow (j-k)x = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i \Longrightarrow (j-k) \sum_{i=1}^{r} \lambda_i e_i = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i \Longrightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \Longrightarrow \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{(j-k)}$, ou seja, $\lambda_i \in \mathbb{Q}$. Assim, H é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $e_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto dH. Temos que $dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Daí, pelo Teorema 1.2.1, segue que existe uma base $\{f_1, \cdots, f_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z} e_i$ e inteiros α_i, tal que $\{\alpha_1 f_1, \cdots, \alpha_r f_r\}$ gera dH sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo dH tem o mesmo posto de H e como $\sum_{i=1}^{r} \mathbb{Z} e_i \subset H$,

segue que o posto de $dH \geq r$. Pela maximalidade de r decorre que o posto de dH é r e os $\alpha_i's$ são não nulos, pois caso contrário dH não teria posto r. Assim os $f_i's$ são linearmente independentes sobre $\mathbb{R}$, uma vez que $\{e_1, \cdots, e_r\}$ é linearmente independente sobre $\mathbb{R}$. Portanto, dH é gerado por r vetores linearmente independentes sobre $\mathbb{R}$ e consequentemente H também é gerado por r vetores linearmente independentes sobre $\mathbb{R}$. ■

Observação 3.2.1. *Segue do Teorema* 3.2.1 *que um subgrupo discreto do* $\mathbb{R}^n$ *é um reticulado.*

3.3 Empacotamento esférico

A Teoria dos Códigos Corretores de Erros nasceu em 1948, com o famoso trabalho de Shannon (1948), onde foi demonstrado o Teorema da Capacidade do Canal. Em linhas gerais, este resultado diz que para a transmissão de dados abaixo de uma certa taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter a probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco (AWGN), limitado em faixa, consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico δ satisfazendo

$$\delta \geq \frac{\zeta(n)}{2^{n-1}},$$

onde ζ é a função zeta de Riemann. Como consequência, obtém-se

$$\frac{1}{n} log_2 \delta \geq -1. \tag{3.2}$$

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$, Conway e Sloane (1999) provaram que reticulados satisfazendo a cota de Minkowski, dada pela Equação (3.2) são equivalentes a códigos atingindo a capacidade do canal.

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18º Problema de Hilbert, proposto em 1900.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando Teoria Algébrica dos Números, Craig (1978) reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal no anel de inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis.

Para que possamos prosseguir no estudo de reticulados, precisamos da noção de **volume**. O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$-espaço V através do isomorfismo natural entre $\mathbb{R}^n$ e V, e definido por meio de uma base $\{v_1, \ldots, v_n\}$. Além disso, é possível restringir a subconjuntos C de

V que são reuniões finitas da região fundamental, usando apenas as seguintes propriedades de volume:

a) $Vol(x + C) = Vol(C)$, para todo $x \in V$.
b) $Vol(\gamma C) = \gamma^n Vol(C)$, para todo $\gamma \in \mathbb{R},\ \gamma > 0$.
c) Se $C \cap C' = \emptyset$, então $Vol(C \cup C') = Vol(C) + Vol(C')$.

Definição 3.3.1. *Sejam $H \subseteq \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \cdots, v_n\}$ uma base de H e P_β a região fundamental. Se $v_i = (v_{i1}, v_{i2}, \cdots, v_{in})$, para $i = 1, 2, \cdots, n$, definimos o volume da região fundamental P_β, como o módulo do determinante da matriz*

$$B = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

Proposição 3.3.1. *(*SAMUEL, 1967, p.55, Lema.1*) O volume da região fundamental $Vol(P_\beta)$ é independente da base β de H.*

Demonstração. Se $f = \{f_1, \ldots, f_n\}$ é uma outra base de H, então, $f_i = \sum_{j=1}^{n} \alpha_{ij} v_j$, com $\alpha_{ij} \in \mathbb{Z}$. Assim, $Vol(P_f) = |\det(\alpha_{ij})| Vol(P_v)$. Como a matriz de mudança de base (α_{ij}) é inversível, segue que $\det(\alpha_{ij}) = \pm 1$. Portanto, $Vol(P_f) = Vol(P_v)$. ■

Definição 3.3.2. *Seja $H_\beta \subseteq \mathbb{R}^n$ um reticulado com base $\beta = \{v_1, v_2, \cdots,$*
$v_n\}$. Definimos o volume do reticulado H_β como $Vol(H_\beta) = Vol(P_\beta)$.

Observamos que, sendo β' uma outra base para H_β, segue que $Vol(H_\beta) = Vol(H_{\beta'})$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido

definir o volume de H_β como sendo o volume de uma região fundamental.

Definição 3.3.3. **a)** *Um* **empacotamento esférico**, *ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*
b) *Um* **empacotamento reticulado** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* H_β *de* $\mathbb{R}^n$.
c) *Dado um empacotamento no* $\mathbb{R}^n$, *associado a um reticulado* H_β, *com* $\beta = \{v_1, \cdots, v_n\}$ *uma* $\mathbb{Z}$*-base, definimos a sua* **densidade de empacotamento** *como sendo a proporção do espaço* $\mathbb{R}^n$ *coberta pela união das esferas.*

Estamos interessados no empacotamento associado a um reticulado H_β em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado H_β é um conjunto finito, de onde segue que o número $H_{\beta_{min}} = min\{|\lambda|; \lambda \in H_\beta, \lambda \neq 0\}$ está bem definido e $(H_{\beta_{min}})^2$ é chamado de **norma mínima**. Observamos que $\rho = H_{\beta_{min}}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de H_β e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Denotando por $B(\rho)$ a esfera com centro na origem e raio ρ, temos que a **densidade de empacotamento** de H_β é igual a

$$\Delta(H_\beta) = \frac{\text{Volume da região coberta pelas esferas}}{\text{Volume da região fundamental}} = \frac{Vol(B(\rho))}{Vol(H_\beta)} =$$

$$\frac{Vol(B(1))\rho^n}{Vol(H_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(H_\beta) = \frac{\rho^n}{Vol(H_\beta)}.$$

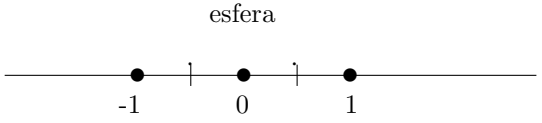
Exemplo 3.3.1. *Se* $H_\beta = \mathbb{Z}^2$ *com base* $(1,0)$ *e* $(0,2)$, *temos que* $\rho = 1/2$, $Vol(B(1)) = \pi.1 = \pi$, *o volume do reticulado é* $Vol(H_\beta) = 1.2 = 2$, *a densidade de empacotamento é*

$$\Delta(H_\beta) = Vol(B(1)).\frac{\rho^2}{Vol(H_\beta)} = \pi\frac{1}{4}.\frac{1}{2} = \frac{\pi}{8}$$

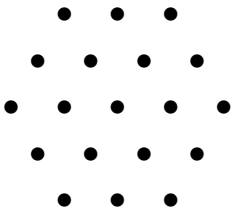
e a densidade de centro é $\delta(H_\beta) = 1/8$.

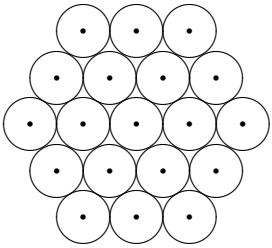
Exemplo 3.3.2. *Seja* $H_\beta = \mathbb{Z}^n$ *um reticulado do* $\mathbb{R}^n$, *gerado pelos vetores* $v_1 = (1,0,\dots,0), v_2 = (0,1,\dots,0), \dots, v_n = (0,0,\dots,1)$. *A forma quadrática* $|v|^2 = x_1^2 + \cdots + x_n^2$ *assume o valor mínimo quando um dos* $x_i = 1$, *para* $i = 1, \cdots, n$ *e os demais nulos. Assim* $|v|^2 = 1$ *e* $\rho = \frac{1}{2}$. *Visto que* $v(H_\beta) = |\det B|$, *e* B *neste caso é a matriz identidade, temos que o* $Vol(H_\beta) = 1$, *e portanto,* $\delta(H_\beta) = \frac{1}{2^n}$.

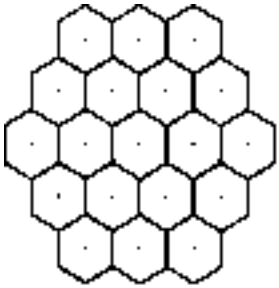
Um dos problemas de empacotamento esférico de um reticulado H_β do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso, as "esferas" são intervalos como podemos ver na figura abaixo.



Para dimensão dois o reticulado hexagonal é o de maior densidade, dada por $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado com base $\beta = \left\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$ é dado por







Em dimensão três Gauss mostrou em 1831 que o reticulado fcc, é o empacotamento com maior densidade (pirâmides de laranjas), sendo essa $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7405$.

Já para dimensões $n \geq 4$ conhece-se apenas algumas densidades de determinados empacotamentos, mais ainda não se sabe qual a maior densidade.

3.4 Reticulados importantes e suas propriedades

Nesta seção descreveremos as propriedades de alguns reticulados construtivos importantes conhecidos na literatura.

Definição 3.4.1. *Dizemos que um reticulado é equivalente a outro se este pode ser obtido do outro por rotação ou translação.*

1. **Reticulado cúbico n-dimensional $\mathbb{Z}^n$:** Temos que $\mathbb{Z}^n = \{(x_1, x_2, \ldots, x_n);\ x_i \in \mathbb{Z}\}$ é um reticulado chamado de cúbico. A sua matriz geradora $\boldsymbol{B}$ é a matriz identidade. Assim, $det\mathbb{Z}^n = 1$ e a norma mínima igual a 1, o raio de empacotamento é $\rho = \frac{1}{2}$, sua densidade de empacotamento é $\Delta = V_n 2^{-n}$ e sua densidade de centro é $\delta = 2^{-n}$. Desta forma $\mathbb{Z}$ tem densidade de empacotamento $\Delta = 1$, e as densidades de $\mathbb{Z}^2$, $\mathbb{Z}^3$, $\mathbb{Z}^4$ são $\Delta = \frac{\pi}{4} \approx 0.785$, $\Delta = \frac{\pi}{6} \approx 0.524$ e $\Delta = \frac{\pi^2}{32} \approx 0.308$, respectivamente.

2. **Reticulado n-dimensional A_n:** Para todo $n \geq 1$, $A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1};\ x_0 + x_1 + \cdots + x_n = 0\}$ é um reticulado. Por definição, temos que A_n está contido no hiperplano $\sum_i x_i = 0$ no $\mathbb{R}^{n+1}$, possui uma matriz geradora B,

dada por:

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix},$$

onde $det A_n = det(BB^t) = n + 1$, norma mínima igual a 2, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$ e densidade de centro $\delta = 2^{-n/2}(n+1)^{-1/2}$.

3. **Reticulado hexagonal:** Temos que $A_1 \simeq \mathbb{Z}$ e que A_2 é equivalente ao reticulado hexagonal. O reticulado hexagonal é gerado pelos vetores $(1, 0)$ e $\left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$, e assim sua matriz geradora é $B = \begin{bmatrix} 1 & 0 \\ \frac{-1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$. Desta forma $det A_2 = \frac{3}{4}$, norma mínima igual a 1, raio de empacotamento $\rho = \frac{1}{2}$, densidade de empacotamento $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$ e densidade de centro $\delta = \frac{1}{\sqrt{12}}$.

4. **Reticulado D_n, para $n \geq 3$:** Temos que $D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n$ é par$\}$ é um reticulado. Sua matriz geradora é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ . & . & . & \cdots & . & . \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix}$$

onde $det D_n = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$ e densidade de centro $\delta = 2^{-(n+2)/2}$.

5. **Reticulado face-centered cubic:** Temos que os reticulados A_3 e D_3 são equivalentes ao reticulado fcc. Assim, o fcc consiste de todos os pontos (x, y, z), onde x, y, z são inteiros com soma par. Um matriz geradora de D_3 é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix},$$

onde $det D_3 = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$, densidade $\Delta = \dfrac{\pi}{\sqrt{18}} \approx 0,7305$ e densidade de centro $\delta = 2^{-5/2}$.

• Para D_4, temos $\Delta \approx 0,61685$ e densidade de centro $\delta \approx 0,125$.

• Para D_5, temos $\Delta \approx 0,46526$ e densidade de centro $\delta \approx 0,08839$.

6. **Reticulado 8-dimensional E_8:** Temos que o sistema de coordenadas pares de E_8 consiste dos pontos $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z}$ ou $\forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 0(mod 2)\}$. O sistema de coordenadas ímpares é obtido mudando o sinal de qualquer

coordenada: os pontos são $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z}$ ou $\forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 2x_8(mod2)\}$. A matriz geradora de E_8 é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

detB=1, norma mínima=2, número de vizinhos τ=240, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^4}{384} \approx 0.2537$ e densidade de centro $\delta = \frac{1}{16}$.

7. **Reticulado 7-dimensional E_7:** Os vetores em E_8 perpendiculares a qualquer vetor minimal $v \in E_8$ formam o reticulado E_7, isto é, $E_7 = \{x \in E_8 : x \cdot v = 0\}$. A matriz geradora de E_7 é dada por

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{bmatrix},$$

detB=2, norma mínima=2, número de vizinhos τ=126, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^3}{105} \approx 0.2953$ e

densidade de centro $\delta = \frac{1}{16}$.

8. **Reticulado 6-dimensional E_6:** Os vetores em E_8 perpendiculares a qualquer A_2 subreticulado V em E_8 formam o reticulado E_6, isto é, $E_6 = \{x \in E_8 : x \cdot v = 0, \forall v \in V\}$. A matriz geradora de E_6 é dada por

$$B = \begin{bmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

detB=3, norma mínima=2, número de vizinhos τ=72, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$, densidade $\Delta = \frac{\pi^3}{48\sqrt{3}} \approx 0.3729$ e densidade de centro $\delta = \frac{1}{8\sqrt{3}}$.

9. **Reticulado 12-dimensional K_{12}:** Temos que K_{12} é gerado pelos vetores $\frac{1}{\sqrt{2}}(\pm\theta, \pm 1^5)$, onde $\theta = \omega - \overline{\omega} = \sqrt{-3}$ e $\omega = \frac{-1+\sqrt{-3}}{2}$. A matriz geradora de K_{12} é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & \omega & \omega & 1 & 0 & 0 \\ \omega & 1 & \omega & 0 & 1 & 0 \\ \omega & \omega & 1 & 0 & 0 & 1 \end{bmatrix},$$

detB=729, norma mínima=4, número de vizinhos τ=756, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^6}{19440} \approx 0.04945$ e densidade de centro $\delta = \frac{1}{27}$.

10. **Reticulado 16-dimensional Λ_{16}:** A matriz geradora de Λ_{16} é dada por B=

$$\frac{1}{\sqrt{2}}\begin{bmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix},$$

detB=256, norma mínima=4, número de vizinhos τ=4320, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^8}{16.8!} \approx 0.01471$ e densidade de centro $\delta = \frac{1}{16}$.

11. **Reticulado 24-dimensional Λ_{24}:** Temos que Λ_{24} é gerado pelos vetores da forma $\frac{1}{\sqrt{8}}(\pm 3, \pm 1^{23})$. A matriz geradora de

Λ_{24} é dada por

$$B = \frac{1}{\sqrt{8}}$$

8000	0000	0000	0000	0000	0000
4400	0000	0000	0000	0000	0000
4040	0000	0000	0000	0000	0000
4004	0000	0000	0000	0000	0000
4000	4000	0000	0000	0000	0000
4000	0400	0000	0000	0000	0000
4000	0040	0000	0000	0000	0000
2222	2222	0000	0000	0000	0000
4000	0000	4000	0000	0000	0000
4000	0000	0400	0000	0000	0000
4000	0000	0040	0000	0000	0000
2222	0000	2222	0000	0000	0000
4000	0000	0000	4000	0000	0000
2200	2200	2200	2200	0000	0000
2020	2020	2020	2020	0000	0000
2002	2002	2002	2002	0000	0000
4000	0000	0000	0000	4000	0000
2020	2002	2200	0000	2200	0000
2002	2200	2020	0000	2020	0000
2200	2020	2002	0000	2002	0000
0222	2000	2000	2000	2000	2000
0000	0000	2200	2200	2200	2200
0000	0000	2020	2020	2020	2020
-3111	1111	1111	1111	1111	1111

,

detB=1, norma mínima=2, número de vizinhos τ=196560, raio de empacotamento $\rho = 1$, densidade $\Delta = \frac{\pi^{12}}{12!} \approx 0.001930$ e densidade de centro $\delta = 1$.

3.5 Reticulados via corpos de números

Nesta seção apresentamos o método de Minkowiski, para a geração de reticulados via ideais do anel de inteiros de um corpos de números.

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{K} \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_j é **real**, caso contrário, σ_j é dito **imaginário**. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um **corpo totalmente real** e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um **corpo totalmente imaginário**. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2},$$

é um homomorfismo injetivo de anéis, chamado de **homomorfismo canônico** de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, e este homomorfismo pode também ser visto como

$$\begin{aligned} \sigma_{\mathbb{K}}(x) \quad = \quad & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathfrak{R}\sigma_{r_1+1}(x), \mathfrak{I}\sigma_{r_1+1}(x), \ldots, \mathfrak{R}\sigma_{r_1+r_2}(x), \\ & \mathfrak{I}\sigma_{r_1+r_2}(x)), \end{aligned}$$

onde as notações $\mathfrak{R}(x)$ e $\mathfrak{I}(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Exemplo 3.5.1. *Sejam o corpo quadrático* $\mathbb{K} = \mathbb{Q}(i)$, *onde* $i = \sqrt{-1}$, *e* $\{\sigma_1, \sigma_2\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$, *onde* σ_1 *é a aplicação identidade e* $\sigma_2(a + bi) = a - bi$, *com* $a, b \in \mathbb{Q}$. *Neste caso,* $r_1 = 0$ *e* $r_2 = 1$. *Para* $x = a + b_i \in \mathbb{K}$, *com* $a, b \in \mathbb{Q}$, *temos* $\sigma_{\mathbb{K}}(x) = (\mathfrak{R}\sigma_1(x), \mathfrak{I}\sigma_1(x)) = (a, b)$.

Exemplo 3.5.2. *Sejam o corpo ciclotômico* $\mathbb{K} = \mathbb{Q}(\zeta_5)$, *onde* $\zeta_5 = e^{\frac{2\pi i}{5}}$ *e* $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$. *Como* $\mathbb{K}$ *é um corpo totalmente complexo, temos que* $r_1 = 0$ *e* $r_2 = 2$. *Os 4 monomorfismos são dados por* $\sigma_1(\zeta_5) = \zeta_5$, $\sigma_2(\zeta_5) = \zeta_5^2$, $\sigma_3(\zeta_5) = \zeta_5^3$, $\sigma_4(\zeta_5) = \zeta_5^4$. *Se* $x = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 \in \mathbb{K}$, *com* $a, b, c, d, e \in \mathbb{Q}$, *temos que* $\sigma_{\mathbb{K}}(x) = (\mathfrak{R}\sigma_1(x), \mathfrak{I}\sigma_1(x), \mathfrak{R}\sigma_2(x), \mathfrak{I}\sigma_2(x))$.

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal nos resultados que seguem.

Proposição 3.5.1. *(*Samuel, 1967, p.56, Prop.1*) Seja* $\mathbb{K}$ *um corpo de números de grau* n. *Se* $M \subseteq \mathbb{K}$ *é um* $\mathbb{Z}$*-módulo livre de posto* n *e se* $(x_j)_{1 \leq j \leq n}$ *é uma* $\mathbb{Z}$*-base de M, então* $\sigma_{\mathbb{K}}(M)$ *é um reticulado no* $\mathbb{R}^n$, *com volume*

$$Vol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} |\det_{1 \leq j,\, k \leq n}(\sigma_j(x_k))|,$$

onde r_2 *é o número de monomorfismos imaginários.*

Demonstração. Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$ com

respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \tag{3.3}$$

Agora calculemos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (3.3) fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z+\overline{z})$, $\Im(z) = \frac{1}{2i}(z-\overline{z})$ para z em $\mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)$-ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)$-ésima coluna da sua posterior, para $l = 1, \ldots, r_2$. Assim,

$$D = \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \Re(\sigma_{r_1+1}(x_1)) & \ldots & \Re(\sigma_{r_1+1}(x_j)) & \ldots & \Re(\sigma_{r_1+1}(x_n)) \\ \Im(\sigma_{r_1+1}(x_1)) & \ldots & \Im(\sigma_{r_1+1}(x_j)) & \ldots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(x_1)) & \ldots & \Re(\sigma_{r_1+r_2}(x_j)) & \ldots & \Re(\sigma_{r_1+r_2}(x_n)) \\ \Im(\sigma_{r_1+r_2}(x_1)) & \ldots & \Im(\sigma_{r_1+r_2}(x_j)) & \ldots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^{r_2} \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1)+\overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n)+\overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1)-\overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_n)-\overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1)+\overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n)+\overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1)-\overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_n)-\overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$(-1)^{r_2}\left(\frac{1}{2}\right)^{\frac{r_2}{2}}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix} = (2i)^{-r_2}\det(\sigma_j(x_k)).$$

Portanto, $D = (2i)^{-r_2}\det(\sigma_j(x_k))$, $j, k = 1, \ldots, n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue da Proposição 1.6.3, que $\det(\sigma_j(x_k)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$, ou seja, $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$.

Como $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, segue que $m = \sum_{j=1}^{n} a_j x_j$, $a_j \in \mathbb{Z}$, e portanto, $m \in M$. Assim,

$$\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j),$$

$a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}$. Logo,

$$Vol(\sigma_{\mathbb{K}}(M)) = |D| = 2^{-r_2} \left| \det_{1\leq j,\, k\leq n} (\sigma_j(x_k)) \right|.$$

■

Exemplo 3.5.3. *Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ seu anel dos inteiros com $\mathbb{Z}$-base $\{1, \sqrt{3}\}$. Como $\mathbb{K}$ é totalmente real, segue que $r_2 = 0$, e portanto*

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) &= \left| \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{pmatrix} \right| = \left| \det \begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix} \right| \\ &= 2\sqrt{3}. \end{aligned}$$

Assim, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{3}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 do $\mathbb{R}^2$, cujo volume é $2\sqrt{3}$.

Exemplo 3.5.4. *Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ seu anel dos inteiros com $\mathbb{Z}$-base $\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$. Como $\mathbb{K}$ é*

totalmente imaginário, então $r_2 = 1$*, e portanto*

$$Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2}\left|\det\begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix}\right| = \frac{1}{2}\sqrt{7}.$$

Assim, $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}) \subseteq \mathbb{R}^2$ *é um reticulado de posto 2 de* $\mathbb{R}^2$ *com volume* $\frac{1}{2}\sqrt{7}$*.*

Exemplo 3.5.5. *Tomemos* $\mathbb{K} = \mathbb{Q}(\zeta_3)$*, onde* $\zeta_3 = e^{\frac{2\pi i}{3}}$ *e* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ *seu anel dos inteiros com* $\mathbb{Z}$*-base* $\{1, \zeta_3\}$*. Como* $\mathbb{K}$ *é totalmente imaginário, segue que* $r_2 = 1$*, e portanto*

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) &= \frac{1}{2}\left|\det\begin{pmatrix} 1 & \zeta_3 \\ 1 & \overline{\zeta_3} \end{pmatrix}\right| = \frac{1}{2}\left|-\frac{1}{2} - \frac{i\sqrt{3}}{2} - \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right| \\ &= \frac{1}{2}\sqrt{3}. \end{aligned}$$

A imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{3}])$ *é um reticulado de posto* 2 *no* $\mathbb{R}^2$*, cujo volume é* $\frac{\sqrt{3}}{2}$*.*

Proposição 3.5.2. *(*Samuel, 1967, p.57, Prop.2*) Seja* $\mathbb{K}$ *um corpo de números de grau* n*. Sejam* $D_{\mathbb{K}}$ *o discriminante absoluto de* $\mathbb{K}$*,* $\mathbb{A}_{\mathbb{K}}$ *o anel dos inteiros de* $\mathbb{K}$ *e* $\mathfrak{a}$ *um ideal não nulo de* $\mathbb{A}_{\mathbb{K}}$*. Então,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *e* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *são reticulados, com respectivos volumes,*

$$Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} \quad e \quad Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a}),$$

onde r_2 *é o número de monomorfismos imaginários.*

Demonstração. Como $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n, segue da Proposição 3.5.1, que $\sigma_{\mathbb{K}}(\mathfrak{a})$ e $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|\det(\sigma_i(x_k))|$, onde $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathbb{A}_{\mathbb{K}}$ e pela Proposição 1.6.3 temos que $D_{\mathbb{K}} = \det(\sigma_i(x_k))^2$.

Assim, $|D_{\mathbb{K}}|^{\frac{1}{2}} = |\det(\sigma_i(x_k))|$ e portanto $Vol(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$. Para a segunda fórmula, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ de índice $N(\mathfrak{a})$ uma vez que $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$ é isomorfo a $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})/\sigma_{\mathbb{K}}(\mathfrak{a})$. Além disso, como um domínio fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de $N(\mathfrak{a})$ cópias de um domínio fundamental de $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$, segue que

$$Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a}).$$

■

Chamamos de realização geométrica de um ideal $\mathfrak{a}$ ao reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$. Em consequência das Proposições 3.5.1 e 3.5.2, temos que a densidade de centro destes reticulados é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{a})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})}, \tag{3.4}$$

onde $\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2}min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$.

Proposição 3.5.3. *(*Conway; Sloane, 1999, p.225*) Sejam* $\mathbb{K}$ *um corpo de números e* $x \in \mathbb{K}$. *Então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}}.Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, & \text{se } \mathbb{K} \text{ for totalmente real} \\ \frac{1}{2}, & \text{se } \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Demonstração: Suponhamos que $\mathbb{K}$ seja um corpo de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_{\mathbb{K}}(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned} |\sigma_{\mathbb{K}}(x)|^2 &= (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2 + \\ &\quad \cdots + \Re(\sigma_{r_1+r_2}(x))^2 + \Im(\sigma_{r_1+r_2}(x))^2. \end{aligned}$$

Observe que $\Re(\sigma_k(x))^2 + \Im(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x})$, para $r_1 + 1 \leq k \leq r_1 + r_2$. Assim,

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \sigma_{r_1+1}(x\overline{x}) + \cdots + \sigma_{r_1+r_2}(x\overline{x}).$$

Se $r_1 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) = \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}),$$

pois sendo $\overline{\sigma}$ a conjugação complexa, temos que $\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, \cdots, r_2$. Logo,

$$2|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

e como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Se $r_2 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2$$

e como $\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$ segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$ e assim, $|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_1}(x\overline{x})$. Portanto,

$$|\sigma_{\mathbb{K}}(x)|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

e isto conclui a demonstração. ■

Observação 3.5.1. *Se $\mathbb{K}$ é um corpo de números e $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, podemos reescrever o raio de empacotamento do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ da seguinte forma:*

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2} min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\} = \frac{1}{2} min\left\{ \sqrt{c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0 \right\}.$$

Fazendo $t_{\mathfrak{a}} = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$ temos que:

1. *se $\mathbb{K}$ é totalmente real então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{\sqrt{t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\sqrt{\frac{t_{\mathfrak{a}}}{4}}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.$$

2. *se* $\mathbb{K}$ *é totalmente imaginário então*

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{2^{\frac{n}{2}}\left(\frac{\sqrt{\frac{1}{2}t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{2^{\frac{n}{2}} t_{\mathfrak{a}}^{\frac{n}{2}}}{2^{\frac{3n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{2^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} \\ &= \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{(\sqrt{4})^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{4^{\frac{n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.\end{aligned}$$

Portanto, a densidade de centro é a mesma para ambos os casos.

Exemplo 3.5.6. *Se* $\mathbb{K} = \mathbb{Q}(i)$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$ *e* $D_{\mathbb{K}} = -4$. *Se* $x = a + bi \in \mathbb{A}_{\mathbb{K}}$, *então* $x\overline{x} = (a+bi)(a-bi) = a^2 - abi + abi + b^2 = a^2 + b^2$, $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 2(a^2+b^2)$ *e* $t_{\mathbb{A}} = 2$, *para* $a = 1$ *e* $b = 0$. *Assim*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{\left(\frac{2}{4}\right)}{\sqrt{4}} = \frac{\left(\frac{1}{2}\right)}{2} = \frac{1}{4} = 0,25.$$

4

Reticulados via corpos quadráticos e ciclotômicos

4.1 Introdução

Neste capítulo apresentamos aplicações dos resultados apresentados nos capítulos anteriores, mais precisamente, calculamos a densidade de centro dos reticulados obtidos via o homomorfismo canônico. Visto que a representação geométrica de um ideal é um reticulado, nosso maior desafio no cálculo da densidade de centro é minimizar uma forma quadrática, caracterizada em função do traço. No caso dos corpos quadráticos, caracterizamos a forma quadrática e calculamos a densidade de centro da realização geométrica do anel dos inteiros algébricos e de ideais principais. No caso dos corpos ciclotômicos, apresentamos um estudo da representação geométrica de ideais do anel de inteiros dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$, onde p e q são números primos distintos e r é um inteiro positivo não nulo, e seguindo esta

linha nos direcionamos ao estudo de reticulados obtidos via estes corpos.

Visto que, pelo Teorema de Kronecker-Weber, todo corpo de números abeliano está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para algum n, estudamos também reticulados via corpos abelianos o que equivale ao estudo da representação geométrica de ideais via subcorpos de corpos ciclotômicos.

4.2 Reticulados via corpos quadráticos

Nesta seção, apresentamos o cálculo da densidade de centro de reticulados de posto 2 no $\mathbb{R}^2$. Pela Proposição 2.2.1, temos que todo corpo quadrático tem a forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um número inteiro livre de quadrados e que seu anel de inteiros algébricos é $\mathbb{A}_\mathbb{K} = \mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $3(mod\,4)$, com $D_\mathbb{K} = 4d$ ou $\mathbb{A}_\mathbb{K} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ se $d \equiv 1(mod\,4)$ com $D_\mathbb{K} = d$.

De acordo com a Observação 3.5.1, temos que

$$\delta(\sigma_\mathbb{K}(\mathbb{A}_\mathbb{K})) = \frac{\left(\frac{t_{\mathbb{A}_\mathbb{K}}}{4}\right)}{|D_\mathbb{K}|^{\frac{1}{2}}}. \tag{4.1}$$

A seguir exemplificamos o cálculo da densidade de centro de alguns reticulados via corpos quadráticos.

Exemplo 4.2.1. *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ *então* $\mathbb{A}_\mathbb{K} = \mathbb{Z}[\sqrt{7}]$ *e* $D_\mathbb{K} = 28$. *Se* $\alpha = a + b\sqrt{7} \in \mathbb{A}_\mathbb{K}$, *temos que* $\alpha\overline{\alpha} = (a + b\sqrt{7})(a + b\sqrt{7}) = a^2 + 2ab\sqrt{7} + 7b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = Tr(a^2 + 2ab\sqrt{7} + 7b^2) = Tr(a^2) + Tr(2ab\sqrt{7}) + Tr(7b^2) = 2a^2 + 14b^2 = 2(a^2 + 7b^2)$, *e portanto temos que* $t_{\mathbb{A}_\mathbb{K}} = min\{Tr(\alpha\overline{\alpha}); \alpha \neq 0,\ \alpha \in \mathbb{A}_\mathbb{K}\} = 2$, *para* $a = 1$ *e* $b = 0$. *Assim,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2\sqrt{28}} \simeq 0,09449.$$

Exemplo 4.2.2. *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *e* $D_{\mathbb{K}} = 5$. *Se* $\alpha = a + b\sqrt{5} \in \mathbb{A}_{\mathbb{K}}$, *temos que* $\alpha\overline{\alpha} = (a + b\sqrt{5})(a + b\sqrt{5}) = a^2 + 2ab\sqrt{5} + 5b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = Tr(a^2 + 2ab\sqrt{5} + 5b^2) = Tr(a^2) + Tr(2ab\sqrt{5}) + Tr(5b^2) = 2a^2 + 10b^2 = 2(a^2 + 5b^2)$, *e daí* $t_{\mathbb{A}_{\mathbb{K}}} = 2$, *para* $a = 1$ *e* $b = 0$. *Portanto,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2\sqrt{5}} \simeq 0,2236.$$

Consideremos, agora ideais principais do anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de um corpo quadrático $\mathbb{K}$. Seja $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, tal que $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$, onde $\gamma \in \mathbb{A}_{\mathbb{K}}$. Então, pela Proposição 3.5.2, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um reticulado de posto 2 no $\mathbb{R}^2$ e sua densidade de centro, pela Observação 3.5.1, é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)}{|D_{\mathbb{K}}|^{\frac{1}{2}}|N(\gamma)|}.$$

Exemplo 4.2.3. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{11})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{11}]$ *e* $\mathfrak{a}$ *o ideal principal de* $\mathbb{A}_{\mathbb{K}}$, *gerado por* $\gamma = 1 + 2\sqrt{11}$. *Se* $\alpha \in \gamma\mathbb{A}_{\mathbb{K}}$, *então existem* $a, b \in \mathbb{Z}$ *tais que* $\alpha = (1 + 2\sqrt{11})(a + b\sqrt{11}) = (a + 22b) + (2a+b)\sqrt{11}$. *Assim* $\alpha\overline{\alpha} = (a+22b)^2+11(2a+b^2)+2(a+22b)(2a+b)\sqrt{11}$ *e* $Tr(\alpha\overline{\alpha}) = 2[(a + 22b)^2 + 11(2a + b)^2]$. *Logo* $t_{\mathfrak{a}} = 90$, *para* $a = 1$ *e* $b = 0$. *Como* $D_{\mathbb{K}} = 44$ *e* $N(< 1 + 2\sqrt{11} >) = |N(1 + 2\sqrt{11})| = |(1 + 2\sqrt{11})(1 - 2\sqrt{11})| = |1 - 2\sqrt{11} + 2\sqrt{11} - 44| = |-43| = 43$, *segue que*

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{\frac{90}{4}}{\sqrt{44}\cdot 43} = \frac{\frac{90}{4}}{2\cdot\sqrt{11}\cdot 43} = \frac{\frac{90}{4}}{86\cdot\sqrt{11}} = \\ &= \frac{90}{4\cdot\sqrt{11}\cdot 86} = \frac{45}{2\cdot\sqrt{11}\cdot 86} = \frac{45}{172\cdot\sqrt{11}} \simeq 0,0788.\end{aligned}$$

Exemplo 4.2.4. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *e* $\mathfrak{a}$ *o ideal principal de* $\mathbb{A}_{\mathbb{K}}$, *gerado por* $\gamma = 3-2\sqrt{5}$. *Se* $\alpha \in \gamma\mathbb{A}_{\mathbb{K}}$, *então existem* $a, b \in \mathbb{Z}$ *tais que* $\alpha = \left(3a - \frac{7}{2}b\right) + \sqrt{5}\left(-2a + \frac{1}{2}b\right)$. *Assim* $\alpha\overline{\alpha} = \left(3a - \frac{7}{2}b\right)^2 + 5\left(-2a + \frac{1}{2}b\right)^2 + 2\sqrt{5}\left(3a - \frac{7}{2}b\right)\left(-2a + \frac{1}{2}b\right)$ *e portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = 2\left[\left(3a - \frac{7}{2}b\right)^2 + 5\left(-2a + \frac{1}{2}b\right)^2\right]$. *Logo* $t_{\mathfrak{a}} = 27$, *para* $a = 0$ *e* $b = 1$. *Como* $D_{\mathbb{K}} = 5$ *e* $|N_{\mathbb{K}/\mathbb{Q}}(\gamma)| = 11$ *segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{27}{44\sqrt{5}} \simeq 0,2744.$$

Proposição 4.2.1. *(*Vicente, 2000, p.72*) Se* $\mathbb{K}$ *é um corpo quadrático totalmente imaginário e* $\mathfrak{a}$ *é um ideal principal do anel dos inteiros algébricos de* $\mathbb{K}$, *então os reticulados* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *e* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *tem a mesma densidade de centro.*

Demonstração. Sejam $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$ um ideal principal de $\mathbb{A}_{\mathbb{K}}$ e $x \in \mathfrak{a}$, onde $x = \gamma l$, com $l \in \mathbb{A}_{\mathbb{K}}$. Assim, $x\overline{x} = \gamma\overline{\gamma}l\overline{l}$ e $Tr_{\mathbb{K}/\mathbb{Q}}(\gamma\overline{\gamma}) = 2(\gamma\overline{\gamma}l\overline{l})$, pois $\gamma\overline{\gamma}l\overline{l} \in \mathbb{Q}$. Como

$$\frac{\sqrt{\frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(\gamma\overline{\gamma}l\overline{l})}}{2} = \sqrt{\gamma\overline{\gamma}}\cdot\frac{\sqrt{l\overline{l}}}{2},$$

segue que, $\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})) = |N(\gamma)|\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))$ e sendo $\mathbb{K}$ um corpo qua-

drático totalmente imaginário segue que $r_2 = 1$. Portanto,

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}|N(\gamma)|} = \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^2}{|D_{\mathbb{K}}|^{\frac{1}{2}}\dfrac{\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}}))}{\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}} = \\ &= \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^2\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}{|D_{\mathbb{K}}|^{\frac{1}{2}}\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}}))} = \\ &= \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}{|D_{\mathbb{K}}|^{\frac{1}{2}}} = \\ &= \frac{2\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))^2}{|D_{\mathbb{K}}|^{\frac{1}{2}}} = \delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})).\end{aligned}$$

■

Exemplo 4.2.5. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[w]$, $\alpha = a + bw \in \mathbb{A}_{\mathbb{K}}$, *com* $w = \dfrac{11+\sqrt{-7}}{2}$ *e* $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$ *um ideal principal de* $\mathbb{A}_{\mathbb{K}}$. *Então* $\alpha\overline{\alpha} = \left[a + b\left(\frac{11}{2} + \frac{\sqrt{-7}}{2}\right)\right]\left[a + b\left(\frac{11}{2} - \frac{\sqrt{-7}}{2}\right)\right] = a^2 + ab\left(\frac{11}{2} - \frac{\sqrt{-7}}{2}\right) + ab\left(\frac{11}{2} + \frac{\sqrt{-7}}{2}\right) + b^2\left(\frac{121}{4} + \frac{7}{4}\right) = a^2 + ab\overline{w} + ab\omega + 32b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = 2(a^2 + 11ab + 32b^2)$ *e deste modo* $t_{\mathbb{A}_{\mathbb{K}}} = 2$, *para* $a = 1$ *e* $b = 0$. *Visto que* $D_{\mathbb{K}} = -7$, *temos que a densidade de centro é* $\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \dfrac{\frac{2}{4}}{\sqrt{7}} = \dfrac{\frac{1}{2}}{\sqrt{7}} = \dfrac{1}{2\sqrt{7}} \simeq 0,1889$.

4.3 Reticulados via corpos ciclotômicos

Nesta seção, apresentamos um estudo de como encontrar a maior densidade de centro para os reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$ onde p e q são números primos distintos e r é um inteiro positivo. Para isso, faremos uso das aplicações das formas quadráticas aos corpos ciclotômicos e desta forma calculamos a densidade de centro dos reticulados obtidos. Além disso, para alguns corpos ciclotômicos calculamos explicitamente a densidade de centro de algumas famílias de reticulados.

1 Reticulados via $\mathbb{Q}(\zeta_p)$.

Nesta seção apresentamos alguns resultados sobre os reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p)$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ o anel dos inteiros de $\mathbb{K}$ e $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i \in \mathbb{Z}[\zeta_p]$. Como $\overline{\zeta_p} = \zeta_p^{-1}$ segue que $\overline{\alpha} = \sum_{i=0}^{p-2} a_i\zeta_p^{-i}$ e assim,

$$\begin{aligned}\alpha\overline{\alpha} &= \left(\sum_{i=0}^{p-2} a_i\zeta_p^i\right)\left(\sum_{i=0}^{p-2} a_i\zeta_p^{-i}\right) = (a_0^2 + \cdots + a_{p-2}^2) + \\ &+ (a_0a_1 + \cdots + a_{p-3}a_{p-2})(\zeta_p + \zeta_p^{-1}) + \cdots + \\ &+ (a_0a_{p-3} + a_1a_{p-2})(\zeta_p^{p-3} + \zeta_p^{-(p-3)}) + \\ &+ a_0a_{p-2}(\zeta_p^{p-2} + \zeta_p^{-(p-2)}).\end{aligned}$$

Por outro lado, fazendo $\alpha_i = \zeta_p^i + \zeta_p^{-i}$ e $A_i = a_0a_i + a_1a_{i+1} + \cdots + a_{p-2-i}a_{p-2}$, temos que $\alpha\overline{\alpha} = A_0 + A_1\alpha_1 + \cdots + A_{p-2}\alpha_{p-2}$. Como $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = -2$ segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = (p-1)A_0 - 2(A_1 + A_2 + \cdots + A_{p-2}) = (p-1)A_0 - 2(a_0a_1 + \cdots + a_{p-3}a_{p-2} + a_0a_2 + \cdots + a_{p-4}a_{p-2} + \cdots + a_0a_{p-3} + a_1a_{p-2} + a_0a_{p-2})$. Assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i^2 + 2\sum_{0\le i<j\le p-2} a_ia_j\right]$$

e, portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i\right]^2. \tag{4.2}$$

Fazendo algumas operações no segundo membro da Equação (4.2), temos que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0\le i<j\le p-2} (a_i - a_j)^2, \tag{4.3}$$

que é a forma quadrática $Q_{p-1}(\underline{X})$ calculada em $(a_0, \cdots, a_{p-2})$.

Quando não houver possibilidade de confusão usaremos Q no lugar de Q_{p-1}.

Proposição 4.3.1. *(*Flores, 2000, p.41, Prop.3.1.1*) Sejam* $\mathfrak{p}$ *o ideal de* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ *gerado por* $1-\zeta_p$, $\alpha \in \mathbb{Z}[\zeta_p]$ *e* $f(X) \in \mathbb{Z}[X]$ *tal que* $\alpha = f(\zeta_p)$. *Então*

$$\alpha \in \mathfrak{p} \Longleftrightarrow f(1) \equiv 0 (mod\ p).$$

Demonstração: Sendo o polinômio minimal de ζ_p sobre $\mathbb{Q}$ dado por

$$h(X) = \frac{X^p - 1}{X - 1},$$

temos que $\mathbb{A}_{\mathbb{K}} \simeq \dfrac{\mathbb{Z}[X]}{< h(X) >}$. Se $\overline{u(X)}$ representa a classe de equivalência, módulo $h(X)$, do polinômio $u(X)$ em $\mathbb{A}_{\mathbb{K}}$, segue que $\alpha \in \mathfrak{p}$ é equivalente à existência de $u(X) \in \mathbb{Z}[X]$ tal que $f(X) \equiv (1 - X)u(X)(mod\ h(X))$ e isto é equivalente à existência de $v(X) \in \mathbb{Z}[X]$ tal que $f(X) = (1 - X)u(X) + v(X)h(X)$. Como

$$h(X) = \frac{X^p - 1}{X - 1} \equiv \frac{(X-1)^p}{X-1} \equiv (X-1)^{p-1} (mod\ p\mathbb{Z}[X]),$$

segue que

$$f(X) \equiv (1 - X)u(X) + v(X)(X-1)^{p-1} (mod\ p\mathbb{Z}[X]).$$

Colocando $1 - X$ em evidência, encontramos $t(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1 - X)t(X) (mod\ p\mathbb{Z}[X]),$$

ou seja, existe $g(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1 - X)t(X) + p.g(X),$$

e esta igualdade é equivalente à $f(1) \equiv 0 (mod\ p)$. ■

Proposição 4.3.2. *(*Flores, 1996, p.72, Prop.3.4.8*) Se $p > 2$ e $r = 1$ então $Q(\underline{x}) \geq 2p$, onde $x \in \mathfrak{p} = (1 - \zeta_p)\mathbb{A}_{\mathbb{K}}$ e $x \neq 0$. Além disso, $Q(\underline{x}) = 2p$ para $x = 1 - \zeta_p$.*

Demonstração: Seja $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ um elemento de $\mathfrak{p}$ e suponhamos que $(a_0, \cdots, a_{p-2}) \in I_1 = \{(b_1, \cdots, b_n) \in \mathbb{Z}^n, |b_i| \leq 1\}$. Sejam r e s o número de $a_i's$ iguais a 1 e -1, respectivamente. Assim, o número de $a_i's$ nulos será $p - r - s - 1$. Como a forma quadrática $Q(X)$ é totalmente simétrica, segue que

$$\begin{aligned} Q(a_0, \cdots, a_{p-2}) &= Q(1, \cdots, 1, -1, \cdots, -1, 0, \cdots, 0) = \\ &= r + s + 4rs + r(p - 1 - r - s) + s(p - 1 - r - s) = \\ &= r + s + 4rs + rp - r - r^2 - rs + sp - s - sr - s^2 = \\ &= 2rs + rp + sp - r^2 - s^2 = -(r - s)^2 + p(r + s). \end{aligned}$$

Sabemos que quando $x \in \mathfrak{p}$, pela Proposição 4.3.1, $f(1) \equiv 0(mod\ p)$, ou seja, sendo $f(x) = a_0 + a_1x + \cdots + a_{p-2}x^{p-2}$ segue que $f(1) = a_0 + \cdots + a_{p-2} = \sum_{i=0}^{p-2} a_i = r - s \equiv 0(mod\ p)$, e consequentemente $r = s$, tendo em vista o intervalo de variação de r e s. Portanto $Q(\underline{x}) = 2pr$ e para $r = 1$ temos que $Q(\underline{x}) = 2p$ é o valor mínimo. Se $(b_0, \cdots, b_{p-2})$ é uma $(p-1)$-upla de $I_2 - I_1$, então pelo Teorema 1.9.1, tomando $a_1 = 2$ e $r = 1$ teremos que $y = \frac{2}{2} = 1$ e assim

$$Q(b_0, \cdots, b_{p-2}) \geq Q(2, 1, \cdots, 1) = 4 + p - 2 + p - 2 = 4 + 2p - 4 = 2p.$$

Pelo Teorema 1.9.2, se $(b_0, \cdots, b_{p-2}) \in I_d - I_{d-1}$, com $d > 1$, segue que

$$Q(b_0, \cdots, b_{p-2}) \geq 2p,$$

o que demonstra a primeira parte da demonstração. Para a segunda parte, se $x = 1 - \zeta_p \in \mathfrak{p}$, então

$$\begin{aligned} Q(\underline{x}) &= Q_{p-1}(1, -1, 0, \cdots, 0) = 1^2 + (-1)^2 + 4 + (p - 3).1 + \\ &+ (p - 3).1 = 6 + p - 3 + p - 3 = 2p - 6 + 6 = 2p, \end{aligned}$$

e isto conclui a demonstração. ■

Nosso objetivo agora é considerar ideais principais não nulos do anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e calcular a densidade de centro da realização geométrica destes ideais. Deste modo, seja $\mathfrak{p} = \lambda\mathbb{A}_{\mathbb{K}}$ o ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $\lambda = 1 - \zeta_p$. Se $\alpha \in \mathfrak{p}$, com $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i$ temos que $\alpha \equiv \sum_{i=0}^{p-2} a_i (mod\ \mathfrak{p})$, uma vez que $\zeta_p \equiv 1 (mod\ \mathfrak{p})$. Assim, $\alpha \in \mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-2} a_i \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Como $1 - \zeta_p \in \mathfrak{p}$, pela Proposição 4.3.2, temos que $Q(1, -1, 0, \cdots, 0) = 2p$, e assim

$$t_{\mathfrak{p}} = min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}); \alpha \in \mathfrak{p},\ \alpha \neq 0\} = 2p.$$

Como $N(\mathfrak{p}) = N(\lambda) = p$ e $D_{\mathbb{K}} = \pm p^{p-2}$ segue que

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p})) = \frac{\left(\frac{2p}{4}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}.p} = \frac{p^{\frac{p-1}{2}}}{2^{\frac{p-1}{2}}.p^{\frac{p}{2}}} = \frac{1}{p^{\frac{1}{2}}.2^{\frac{p-1}{2}}}, \tag{4.4}$$

e como $t_{\mathbb{A}_{\mathbb{K}}} = p - 1$ segue, da Proposição 1.9.1, que

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{(p-1)^{\frac{p-1}{2}}}{2^{p-1}.p^{\frac{p-2}{2}}}. \tag{4.5}$$

Exemplo 4.3.1. *O quadro abaixo apresenta o valor aproximado da densidade de centro, $\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))$, da realização geométrica do ideal principal $\mathfrak{p}$ de $\mathbb{Z}[\zeta_p]$ gerado por $1-\zeta_p$, onde p é um número primo:*

p	*dimensão*	*densidade de centro*
3	*2*	$\frac{1}{2\sqrt{3}} \approx 0,288675$
5	*4*	$\frac{1}{4\sqrt{5}} \approx 0,111803$
7	*6*	$\frac{1}{8\sqrt{7}} \approx 0,047245$
11	*10*	$\frac{1}{32\sqrt{11}} \approx 0,009422$
13	*12*	$\frac{1}{64\sqrt{13}} \approx 0,004333$
17	*16*	$\frac{1}{2^8\sqrt{17}} \approx 0,000947404$
19	*18*	$\frac{1}{2^9\sqrt{19}} \approx 0,000448077$
23	*22*	$\frac{1}{2^{11}\sqrt{23}} \approx 0,000101813$
29	*28*	$\frac{1}{2^{14}\sqrt{29}} \approx 0,000011333$
97	*96*	$\frac{1}{2^{48}\sqrt{97}} \approx 3,6072342 \cdot 10^{-16}$
6619	*6618*	$\frac{1}{2^{3309}\sqrt{6619}} \approx 9,57961725 \cdot 10^{-999}$

Tabela (4.3.1)

Observamos que a densidade de centro $0,288675$ *é a maior conhecida em dimensão 2 e corresponde a densidade de centro do reticulados conhecido na literatura* A_2, *(Conway; Sloane, 1999, p.15).*

Passamos agora ao cálculo da densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, para $i \geq 1$. Assim, pelas condições para que um elemento de $\mathbb{A}_{\mathbb{K}}$ pertença ao ideal $\mathfrak{p}^i$, precisamos encontrar o mínimo que a forma quadrática assume nos elementos de $\mathfrak{p}^i$ para então calcular a densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$.

Proposição 4.3.3. *(*Flores, 2000, p.48, Lema.3.2.5*) Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *e* $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$. *Se* $x \in \mathfrak{p}^i$, *com* $i = 1, \cdots, (p-1)/2$, *então* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 2.p.i.$ ■

Pela Proposição 4.3.3 e pelo fato da norma ser multiplicativa, temos que

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) \geq \frac{\left(\frac{p.i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}.p^i} = \frac{p^{\frac{p-1}{2}}.\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}}.p^{\frac{1-p}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{i-\frac{1}{2}}}.$$

Esta expressão admite um limitante mínimo quando $i = \dfrac{p-1}{2\ln p}$. Deste modo, devemos tomar i como sendo um número inteiro próximo de $\dfrac{p-1}{2\ln p}$.

Exemplo 4.3.2. *O quadro abaixo apresenta o valor aproximado da densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, $i \geq 1$, onde $\mathfrak{p}^i$ é o ideal principal de $\mathbb{Z}[\zeta_p]$ gerado por $(1-\zeta_p)^i$, onde p é um número primo.*

p	*dimensão*	$\dfrac{p-1}{2\ln p}$	i	$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i))$
3	*2*	*0,91*	*1*	*0,288675*
5	*4*	*1,24*	*1*	*0,111803*
7	*6*	*1,54*	*2*	*0,054*
11	*10*	*2,08*	*2*	*0,027*
13	*12*	*2,33*	*3*	*0,021*
17	*16*	*2,82*	*3*	*0,022*
19	*18*	*3,07*	*3*	*0,02443*
23	*22*	*3,5*	*4*	*0,0351*
97	*96*	*10,49*	*10*	*474491823048089,9652*
6619	*6618*	*376,178*	*376*	$3,0254 \cdot 10^{6090}$

Tabela (4.3.2)

Agora veremos uma família de reticulados A_n, para cada dimensão n, a partir de subcorpos de $\mathbb{Q}(\zeta_p)$. Para isto precisamos dos seguintes resultados:

Teorema 4.3.1. *(*Flores; Nóbrega, 1999, p.45, Teo.1*) Sejam p um número primo e $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[\mathbb{K}:\mathbb{Q}] = up^j$ e tal que p não divide u. Então*

$$|D_{\mathbb{K}}| = p^{u\left((j+2)p^j - \frac{p^{j+1}-1}{p-1}\right)-1}.$$

Corolário 4.3.1. *(*Flores, 2000, p.22, Corol.2.1.18*) Se $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, então*

$$|D_{\mathbb{K}}| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Teorema 4.3.2. *(*Flores, 2000, p.50, Teo.3.3.1*) Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p)$, $\mathbb{K}$ um subcorpo de $\mathbb{L}$ de grau $(p-1)/t$ sobre $\mathbb{Q}$, $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ e $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p} \cap \mathbb{K}$. Então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^i)) \geq \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \tag{4.6}$$

Demonstração: Como $\mathfrak{p}_{\mathbb{K}}$ ramifica totalmente em $\mathbb{L}$, segue que $\mathfrak{p}_{\mathbb{K}}^i\mathbb{Z}[\zeta_p] = \mathfrak{p}^{t.i}$. Pela Proposição 4.3.3, temos que se $x \in \mathfrak{p}_{\mathbb{K}}^i$, para $i = 1, \cdots, (p-1)/2$, então $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 2.p.t.i$. Assim, como $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(Tr_{\mathbb{L}/\mathbb{K}}(x\overline{x})) = Tr_{\mathbb{K}/\mathbb{Q}}(t(x\overline{x})) = tTr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{t}Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq \frac{1}{t}2.p.t.i = 2.p.i$. Assim, o raio de empacotamento satisfaz

$$\rho \geq \frac{\sqrt{c_{\mathbb{K}}2pi}}{2},$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, \text{ se } \mathbb{K} \text{ for real;} \\ \frac{1}{2}, \text{ caso contrário.} \end{cases}$$

Pelo Corolário 4.3.1, temos que o discriminante de $\mathbb{K}$ é

$$D_{\mathbb{K}} = \pm p^{\frac{p-1}{t}-1},$$

e como a norma de $\mathfrak{p}_{\mathbb{K}}^i$ é p^i, segue que, a densidade de centro satisfaz

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i})) = \frac{2^{r_2}\rho(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i}))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{p}_{\mathbb{K}}^{i})} \geq \frac{2^{r_2}.(\frac{\sqrt{c_{\mathbb{K}}2pi}}{2})^{\frac{p-1}{t}}}{p^{\frac{p-1-t}{2t}}.p^{i}} = \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \quad \blacksquare$$

Usando o software Maple, Flores mostrou que quando p e t são fixados, o maior valor para o limitante inferior na Equação (4.6) é obtido quando i é igual ao inteiro mais próximo de $\dfrac{p-1}{2t\ln p}$.

Se $n \in \mathbb{N} - \{0\}$, então existem infinitos primos p tais que $p \equiv 1(mod\ n)$. Sejam

$$p_n = min\{p \mid p \text{ é } primo \text{ e } p \equiv 1(mod\ n)\}$$

e i_0 o inteiro mais próximo de $\dfrac{p_n - 1}{2t\ln p_n}$, onde $t = \dfrac{p_n - 1}{n}$. Denotamos por A_n a representação geométrica do ideal $\mathfrak{p}_{\mathbb{K}}^{i_0} = \mathfrak{p}^{i_0} \cap \mathbb{K} \subseteq \mathbb{A}_{\mathbb{K}}$, isto é, $A_n = \sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i_0})$ onde $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{p_n})$ de grau n sobre $\mathbb{Q}$.

Exemplo 4.3.3. *Como exemplo, mostramos na Tabela 4.3.3, para alguns valores de n, a densidade de centro e o ganho fundamental de codificação, $\gamma_n = \dfrac{d_{E\,min}^2}{Vol(A_n)^{2/n}}$, onde $d_{E,\,min}$ é a distância mínima Euclidiana de A_n.*

n	p_n	$t = \frac{p_n-1}{n}$	$\frac{p_n-1}{2t\ln p_n}$	i_0	$\delta(A_n)$	γ_n
2	*3*	*1*	*0,9*	*1*	*0,288675*	*0.624*
3	*7*	*2*	*0,771*	*1*	*0,133631*	*0.193*
4	*5*	*1*	*1,243*	*1*	*0,111803*	*1.263*
5	*11*	*2*	*1,04*	*1*	*0,0533002*	*0.927*
6	*7*	*1*	*1,5417*	*2*	*0,053994924*	*1.795*
7	*29*	*4*	*1,0394*	*1*	*0,0164133*	*0.921*
8	*41*	*5*	*1,077*	*1*	*0,00976086*	*1.472*
9	*19*	*2*	*1,528*	*2*	*0,0120745*	*1.758*
10	*11*	*1*	*2,085*	*2*	*0,027410122*	*2.896*

Tabela (4.3.3)

Uma das diferenças entre esta família e as demais da literatura, é que as constelações desta família são obtidas para qualquer dimensão.

2 Reticulados via $\mathbb{Q}(\zeta_{p^r})$

Nesta seção apresentamos alguns resultados sobre reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e $r \geq 1$, $r \in \mathbb{Z}$.

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ o anel dos inteiros de $\mathbb{K}$. Se $x = \sum_{i=0}^{m-1} a_i \zeta_{p^r}^i \in \mathbb{Z}[\zeta_{p^r}]$, onde $m = \varphi(p^r)$, existe uma única representação da forma

$$x = \sum_{j=0}^{t} x_j \zeta_{p^r}^j,$$

onde $t = p^{r-1} - 1$ e

$$x_j = \sum_{i=0,\, i \equiv j (mod\ p^{r-1})}^{m-1} a_i \zeta_{p^r}^i, \text{ para } j = 0, \cdots, t.$$

Observação 4.3.1. *Se* $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, *usamos a expressão*

$$x\overline{x} = A_0 + \sum_{i=1}^{m-1} A_i \alpha_i,$$

onde

$$\alpha_i = \zeta_{p^r}^i + \zeta_{p^r}^{-i} \text{ e } A_j = \sum_{i=0}^{m-(j+1)} a_i a_{j+i}, \text{ para } j = 0, \cdots, m-1.$$

Lema 4.3.1. *(*Flores, 2000, p.43, Teo.3.1.2*) Se p é um número primo e r é um número inteiro positivo, então*

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = \begin{cases} 0, \text{ se } mdc(k, p^r) < p^{r-1}; \\ -p^{r-1}, \text{ se } mdc(k, p^r) = p^{r-1}; \\ p^{r-1}(p-1), \text{ se } mdc(k, p^r) > p^{r-1}. \end{cases}$$

Demonstração: Temos que $(\zeta_{p^r})^{p^s} = e^{\frac{2\pi i p^s}{p^r}} = \zeta_{p^{r-s}}$, e que o polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é dado por

$$X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1.$$

Assim se $r \geq 1$ então $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = 0$. Se $mdc(k, p^r) = 1$, então $\zeta_{p^r}^k$ é um conjugado de ζ_{p^r}, ou seja, $\zeta_{p^r}^k$ é raiz do mesmo polinômio minimal e deste modo tem o mesmo traço que ζ_{p^r}. Portanto $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = 0$. Se $mdc(k, p^r) > 1$, temos três casos a considerar:
1º caso: Se $mdc(k, p^r) = p^s < p^{r-1}$, onde $s \leq r-2$, temos que $p^s | k$ e assim $k = p^s k'$, com $k' \in \mathbb{Z}$. Logo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^s k'} = \zeta_{p^{r-s}}^{k'}$, onde $mdc(p^{r-s}, k') = 1$, e assim

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) &= Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}^{k'}) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}) = \\ &= Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_{p^{r-s}})}(\zeta_{p^{r-s}})) = \\ &= p^s Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(\zeta_{p^{r-s}}) = p^s.0 = 0. \end{aligned}$$

2º caso: Se $mdc(k, p^r) = p^{r-1}$, temos que $p^{r-1} | k$ e assim $k = p^{r-1}k'$, com $k' \in \mathbb{Z}$. Logo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^{r-1}k'} = \zeta_p^{k'}$, onde $mdc(p, k') = 1$. Como o polinômio minimal de ζ_p sobre $\mathbb{Q}$ é $X^{p-1} + X^{p-2} + \cdots + X + 1$, segue que $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$. Assim,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_p) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_p)}(\zeta_p)) = p^{r-1} Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = \\ p^{r-1}(-1) = -p^{r-1}. \end{aligned}$$

3º caso: Se $mdc(k, p^r) > p^{r-1}$, temos que $mdc(k, p^r) = p^r$ e assim $p^r | k$ o que implica que $k = p^r k'$, com $k' \in \mathbb{Z}$. Deste modo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^r k'} = 1$. Portanto, $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = (p-1)p^{r-1}$. ■

O próximo teorema nos fornece uma relação entre uma forma quadrática com o cálculo de distâncias dos reticulados $\sigma_{\mathbb{K}}(\mathbb{Z}[\zeta_{p^r}])$.

Teorema 4.3.3. *(*Flores, 1996, p.67, Teo.3.4.3*) Sejam p um número primo, r um número inteiro positivo, $n = \varphi(p^r)$ e $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{n-1}\zeta_{p^r}^{n-1}$ um inteiro algébrico de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$. Então*

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\widetilde{Q}_r(\underline{x}),$$

onde $\underline{x} = (a_0, a_1, \cdots, a_{n-1})$, $\widetilde{Q}_r(\underline{x}) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t})$, com $t = p^{r-1} - 1$ e $\underline{x_k} = (a_k, a_{p^{r-1}+k}, \cdots, a_{(p-2)p^{r-1}+k})$.

Demonstração: Pelo Lema 3.5.3, temos que

$$|\sigma_{\mathbb{K}}(x)|^2 = \tfrac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Pelo Lema 4.3.1, temos que os elementos $\zeta_{p^r}^k$, com $mdc(k, p^r) < p^{r-1}$, tem traço nulo. Se $mdc(k, p^r) > p^{r-1}$ temos que $mdc(k, p^r) = p^r$. Assim, $k = 0$ ou $k \geq p^r > (p-1)p^{r-1}$, o que não ocorre pois $1 \leq k \leq n-1 = (p-1)p^{r-1} - 1$. Deste modo, podemos considerar apenas os índices k tais que $mdc(k, p^r) = p^{r-1}$. Tais k são: $p^{r-1}, 2p^{r-1}, \cdots, (p-2)p^{r-1}$. Tomando $x\overline{x}$ como na Observação 4.3.1 temos que

$$\begin{aligned}
|\sigma_{\mathbb{K}}(x)|^2 &= \frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{2}\left(Tr_{\mathbb{K}/\mathbb{Q}}(A_0) + \sum_{i=1}^{n-1} Tr_{\mathbb{K}/\mathbb{Q}}(A_i\alpha_i)\right) \\
&= \frac{1}{2}((p-1)p^{r-1}A_0 + Tr_{\mathbb{K}/\mathbb{Q}}(A_1\alpha_1) + \cdots + Tr_{\mathbb{K}/\mathbb{Q}}(A_{n-1}\alpha_{n-1})) \\
&= \frac{1}{2}\left((p-1)p^{r-1}\sum_{i=0}^{n-1} a_i^2 + \cdots + A_{n-1}Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_{n-1})\right) \\
&= \frac{(p-1)}{2}p^{r-1}\left(\sum_{i=0}^{n-1} a_i^2\right) - p^{r-1}\left(\sum_{j=1}^{p-2} A_{jp^{r-1}}\right) \\
&= \frac{p^{r-1}}{2}\left((p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right).
\end{aligned}$$

Fazendo

$$(p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) = (p-1)b_0 + \cdots + (p-1)b_t,$$

onde $t = p^{r-1} - 1$ e

$$\begin{cases} b_0 = a_0^2 + a_{p^{r-1}}^2 + \cdots + a_{(p-2)p^{r-1}}^2; \\ b_1 = a_1^2 + a_{p^{r-1}+1}^2 + \cdots + a_{(p-2)p^{r-1}+1}^2; \\ \vdots \\ b_t = a_t^2 + a_{p^{r-1}+t}^2 + \cdots + a_{(p-2)p^{r-1}+t}^2, \end{cases}$$

segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\left((p-1)b_0 + \cdots + (p-1)b_t - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right).$$

Temos que $\displaystyle\sum_{j=1}^{p-2} A_{jp^{r-1}} = \sum a_i a_j$, onde a última soma é tomada sobre todos os $a_i s$, para $i = 0, \cdots, n-1$, satisfazendo $i < j$ e $i \equiv j (mod\ p^{r-1})$, uma vez tomando $a_i a_j$ tal que $i < j$ e $i \equiv j (mod\ p^{r-1})$, temos que $p^{r-1} | (i-j)$ o que implica que existe $u \in \{1, \cdots, p-2\}$ tal que $i - j = up^{r-1}$, ou seja, $j = i + up^{r-1}$. Logo $a_i a_j = a_i a_{i+up^{r-1}}$. Como no primeiro somatório, um produto $a_i a_j$ aparece uma única vez, segue a igualdade. Podemos agora reescrever

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}((p-1)b_0 - 2d_0 + \cdots + (p-1)b_t - 2d_t),$$

onde $d_k = \sum a_i a_j$, onde $i < j,\ j \equiv k (mod\ p^{r-1})$, e $k = 0, \cdots, t$. Assim

$$(p-1)b_k - 2d_k = Q_{p-1}(a_k, a_{k+p^{r-1}}, \cdots, a_{k+(p-2)p^{r-1}}),$$

para $k = 0, \cdots, t$, o que completa a demonstração. ∎

Exemplo 4.3.4. *Sejam $p = 7, r = 1$ e $x = 1 - \zeta_7$ um elemento de $\mathbb{Z}[\zeta_7]$. Se $\underline{x} = (1, -1, 0, 0, 0, 0)$, então $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}\widetilde{Q_6}(\underline{x}) =$*

$\frac{1}{2}Q_6(1,-1,0,0,0,$
$0) = \frac{1}{2}(1^2+(-1)^2+4.1^2+4.(-1)^2+2^2) = \frac{1}{2}(1+1+4+4+4) = \frac{14}{2} = 7,$
ou seja, $|\sigma_{\mathbb{K}}(x)| = \sqrt{7}$.

Exemplo 4.3.5. *Sejam* $p = 3, r = 2$ *e* $x = 1-\zeta_9$ *um elemento de* $\mathbb{Z}[\zeta_9]$. *Se* $\underline{x} = (1,-1,0,0,0,0)$, *então* $|\sigma_{\mathbb{K}}(x)|^2 = \frac{3}{2}\widetilde{Q_2}(\underline{x}) = \frac{3}{2}(Q_2(1,0)+Q_2(-1,0)+Q_2(0,0)) = \frac{3}{2}(2+2+0) = \frac{12}{2} = 6$, *ou seja,* $|\sigma(x)| = \sqrt{6}$.

Nosso objetivo agora é calcular a densidade de centro de alguns reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$. Primeiramente calculamos a densidade de centro dos reticulados $\sigma(\mathfrak{p}^i)$, $i \geq 1$, onde $\mathfrak{p}$ é um ideal principal de $\mathbb{Z}[\zeta_{p^r}]$ gerado pelo elemento $1-\zeta_{p^r}$. Se $\mathbb{K}$ é um corpo ciclotômico, de grau n, então investigar os reticulados $\sigma_{\mathbb{K}}(\mathfrak{p})$, onde $\mathfrak{p} \subset \mathbb{A}_{\mathbb{K}}$ é um ideal, com densidade de centro máxima equivale a maximizar o quociente $\dfrac{\rho^n}{N(\mathfrak{p})}$, uma vez que a densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p})$ é dada por $\dfrac{2^{r_2}\rho^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{p})}$ e os valores 2^{r_2} e $|D_{\mathbb{K}}|^{\frac{1}{2}}$ são determinados.

Proposição 4.3.4. *(*Flores, 1996, p.69, Prop.3.4.4*) Se* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ *e* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$, *a densidade de centro dos reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^j)$, *para* $j \in \mathbb{N}$, *é periódica, ou seja,*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^n)) = \delta(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})),$$

onde $m = \varphi(p^r)$ *e* $n \in \mathbb{N}$.

Demonstração: Pelo Exemplo 2.4.3, temos que $\mathfrak{p}^m = p\mathbb{A}_{\mathbb{K}}$, uma vez que p ramifica completamente. Logo, $\mathfrak{p}^{n+m} = \mathfrak{p}^n.\mathfrak{p}^m = p.\mathfrak{p}^n$, o que implica que $N(\mathfrak{p}^{n+m}) = p^{n+m}$. Como $\mathfrak{p}^{n+m} = p.(\mathfrak{p}^n)$ segue que $x \in \mathfrak{p}^{n+m}$ se, e somente se, $x = py$, onde $y \in \mathfrak{p}^n$. Assim

$$\begin{aligned}\widetilde{Q}_r(\underline{x}) &= \frac{2|\sigma(x)|^2}{p^{r-1}} = \frac{2|\sigma(py)|^2}{p^{r-1}} = \frac{2Tr_{\mathbb{K}/\mathbb{Q}}(py\overline{py})}{p^{r-1}} = \frac{2}{p^{r-1}}Tr_{\mathbb{K}/\mathbb{Q}}(p^2y\overline{y}) \\ &= \frac{2}{p^{r-1}}p^2Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = p^2\frac{2}{p^{r-1}}Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) \\ &= p^2\frac{2}{p^{r-1}}|\sigma(y)|^2 = p^2\widetilde{Q}_r(\underline{y}),\end{aligned}$$

e

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)) = min\left\{\frac{|\sigma(x)|}{2};\ x \in \mathfrak{p}^n\right\}$$

$$\begin{aligned}\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})) &= min\left\{\frac{|\sigma(x)|}{2};\ x \in \mathfrak{p}^{n+m}\right\} = min\left\{\frac{|\sigma(x)|}{2};\ x \in p.\mathfrak{p}^n\right\} \\ &= p.\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)).\end{aligned}$$

Para a densidade de centro, temos que

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})) &= \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^{n+m}} = \frac{2^{r_2}(p.\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^{n+m}} = \\ &= \frac{2^{r_2}p^m(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^n.p^m} = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^n} = \delta(\sigma_{\mathbb{K}}(\mathfrak{p}^n)).\blacksquare\end{aligned}$$

A próxima proposição é uma generalização da Proposição 4.3.1

Proposição 4.3.5. *(*Flores, 2000, p.41, Prop.3.1.1*) Sejam* $\mathfrak{p}$ *o ideal de* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ *gerado por* $1-\zeta_{p^r}$, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$ *e* $f(X) \in \mathbb{Z}[X]$ *tal que* $\alpha = f(\zeta_{p^r})$. *Então*

$$\alpha \in \mathfrak{p}^{i+1} \Longleftrightarrow f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 (mod\ p),$$

onde $f^{(i)}(X)$ *denota a i-ésima derivada formal de* f, $0 \leq i < m$, *e* $m = \varphi(p^r)$.

Demonstração: Sendo o polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ dado por

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1},$$

temos que $\mathbb{A}_{\mathbb{K}} \simeq \dfrac{\mathbb{Z}[X]}{< h(X) >}$. Se $\overline{u(X)}$ representa a classe de equivalência, módulo $h(X)$, do polinômio $u(X)$ em $\mathbb{A}_{\mathbb{K}}$, segue que $\alpha \in \mathfrak{p}^{i+1}$ é equivalente à existência de $u(X) \in \mathbb{Z}[X]$ tal que $f(X) \equiv (1 - X)^{i+1}u(X)$
$(mod\ h(X))$ e isto é equivalente à existência de $v(X) \in \mathbb{Z}[X]$ tal que $f(X) = (1 - X)^{i+1}u(X) + v(X)h(X)$. Como

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \equiv \frac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} \equiv (X-1)^{p^r - p^{r-1}} \equiv (X-1)^{(p-1)p^{r-1}} (mod\ p\mathbb{Z}[X]),$$

segue que

$$f(X) \equiv (1 - X)^{i+1}u(X) + v(X)(X-1)^{(p-1)p^{r-1}} (mod\ p\mathbb{Z}[X]).$$

Colocando $(1 - X)^{i+1}$ em evidência, encontramos $t(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1 - X)^{i+1}t(X) (mod\ p\mathbb{Z}[X]),$$

ou seja, existe $g(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1 - X)^{i+1}t(X) + p.g(X),$$

e esta igualdade é equivalente à

$$f(1) \equiv f^{'}(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 (mod\ p). \qquad \blacksquare$$

Proposição 4.3.6. *(*Flores, 1996, p.72, Prop.3.4.8*) Se* $r > 1$ *então* $\widetilde{Q}_r(\underline{x}) \geq 2(p-1)$, *para* $x \in \mathfrak{p} = (1 - \zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *e* $x \neq 0$. *Além disso,* $\widetilde{Q}_r(\underline{x}) = 2(p-1)$ *para* $x = 1 - \zeta_{p^r}$.

Demonstração: Se $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, onde $m = \varphi(p^r)$ e então podemos escrevê-lo de uma única maneira como $x = x_0 + x_1\zeta_{p^r} + \cdots + x_t\zeta_{p^r}^t$, onde $t = p^{r-1} - 1$ e

$$\begin{cases} x_0 = a_0 + a_{p^{r-1}}.\zeta_{p^r}^{p^{r-1}} + \cdots + a_{(p-2)p^{r-1}}.\zeta_{p^r}^{(p-2)p^{r-1}}; \\ x_1 = a_1 + a_{p^{r-1}+1}.\zeta_{p^r}^{p^{r-1}+1} + \cdots + a_{(p-2)p^{r-1}+1}.\zeta_{p^r}^{(p-2)p^{r-1}+1}; \\ \vdots \\ x_t = a_t + a_{p^{r-1}+t}.\zeta_{p^r}^{p^{r-1}+t} + \cdots + a_{(p-2)p^{r-1}+t}.\zeta_{p^r}^{(p-2)p^{r-1}+t}. \end{cases}$$

Assim pelo Teorema 4.3.3, temos que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}.\widetilde{Q}_r(\underline{x}) = \frac{p^{r-1}}{2}\left(Q(\underline{x_1}) + \cdots + Q(\underline{x_t})\right).$$

Se $x \in \mathfrak{p}$ e se existir um único x_j não nulo na decomposição acima, então $Q(\underline{x_j}) \geq 2p$, e portanto $\widetilde{Q}_r(\underline{x}) \geq 2p > 2(p-1)$. Visto que $p-1$ é o menor valor que $Q(\underline{a})$ assume, com $\underline{a} \in \mathbb{Z}^{p-1}$, segue que se o número dos $a_i's$ não nulos for maior que 1, então

$$\widetilde{Q}_r(\underline{x}) \geq 2(p-1).$$

Finalmente, temos que o elemento $x = 1 - \zeta_{p^r} \in \mathfrak{p}$ satisfaz $\widetilde{Q}_r(\underline{x}) = 2(p-1)$ e isto conclui a demonstração. ■

Lema 4.3.2. *(*Flores, 1996, p.75, Lema.3.4.11*) O elemento* $1-\zeta_{p^r}^{p^{r-2}}$ *pertence a* $\mathfrak{p}^{p^{r-2}}$.

Demonstração: Sendo $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$, vimos que

$$p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{(p-1)p^{r-1}}\mathbb{A}_{\mathbb{K}},$$

uma vez que p se ramifica totalmente em $\mathbb{A}_{\mathbb{K}}$. Sejam $c_i = \begin{pmatrix} p^{r-2} \\ i \end{pmatrix}$, com $0 \leq i \leq p^{r-2}$, os coeficientes do desenvolvimento binomial de $(1-\zeta_{p^r})^{p^{r-2}}$. Pela Proposição 1.9.3, para $i = 1, \cdots, p^{r-2}-1$, temos que $v_p(c_i) \geq 1$, ou seja, p é um divisor de $(1-\zeta_{p^r})^{p^{r-2}} - (1-\zeta_{p^r}^{p^{r-2}})$. Consequentemente,

$$1-\zeta_{p^r}^{p^{r-2}} \equiv (1-\zeta_{p^r})^{p^{r-2}} (mod\ \mathfrak{p}^{(p-1)p^{r-1}}),$$

o que implica que

$$1-\zeta_{p^r}^{p^{r-2}} \equiv (1-\zeta_{p^r})^{p^{r-2}} (mod\ \mathfrak{p}^{p^{r-2}}).$$

Como $\mathfrak{p}^{p^{r-2}} = p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{p^{r-2}}\mathbb{A}_{\mathbb{K}}$ então $(1-\zeta_{p^r})^{p^{r-2}} \in \mathfrak{p}^{p^{r-2}}$. Assim $1-\zeta_{p^r}^{p^{r-2}} \equiv 0\, mod\ \mathfrak{p}^{p^{r-2}}$ e portanto $1-\zeta_{p^r}^{p^{r-2}} \in \mathfrak{p}^{p^{r-2}}$. ■

Teorema 4.3.4. *(Flores, p.47, Teo.3.2.3) Se $r > 2$ e $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ então a maior densidade de centro entre os reticulados $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, para $i = 1, \cdots, p^{r-2}$, ocorre com $i = 1$.*

Demonstração: Pelo Lema 4.3.2 temos que o elemento $x = 1-\zeta_{p^r}^{p^{r-2}}$ pertence a $\mathfrak{p}^{p^{r-2}}$ e além disso temos que $\widetilde{Q}_r(\underline{x}) = 2(p-1)$. Assim, para $i = 1, \cdots, p^{r-2}$, temos que

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{\sqrt{(p-1)p^{r-1}}}{2},$$

e as densidades de centro são dadas por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{((p-1)p^{r-1})^{n/2}}{2^{n/2}.|D_{\mathbb{K}}|^{\frac{1}{2}}.p^i},$$

onde $n = \varphi(p^r)$ e $|D_{\mathbb{K}}| = p^{p^{r-1}(pr-r-1)}$. Isto mostra que $\sigma_{\mathbb{K}}(\mathfrak{p})$ tem a maior densidade de centro dentre os reticulados considerados. ■

Exemplo 4.3.6. *O quadro abaixo apresenta o valor aproximado para a densidade de centro $\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))$, onde $\mathfrak{p}$ é um ideal principal de $\mathbb{Z}[\zeta_{p^r}]$ gerado por $1-\zeta_{p^r}$, p é um número primo e $r > 2$.*

p	r	*dimensão*	*densidade de centro*
2	3	4	$\frac{1}{8} = 0,125$
2	4	8	$\frac{1}{32} = 0,03125$
3	3	18	$\frac{1}{3^{28}} \approx 4,37.10^{-14}$

O valor $0,125$ *obtido para a densidade de centro em dimensão 4 é o maior encontrado para esta dimensão, e corresponde a densidade de centro do reticulado conhecido na literatura* $\boldsymbol{D}_4$, *(Conway; Sloane, 1999, p.15).*

Teorema 4.3.5. *(Flores, p.47, Teo.3.2.4) Se* $r = 2$, $p > 2$ *e* $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *então a maior densidade de centro entre os reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, *para* $i = 1, \cdots, p$, *ocorre com* $i = 2$.

Demonstração: Mostramos que para $i = 2, \cdots, p$, o menor valor assumido por $\widetilde{Q_r}(\underline{x})$ para $x \in \mathfrak{p}^i$ é 2p. Consideramos primeiramente o caso $i = 2$ e sejam x um elemento de $\mathfrak{p}^2$ e os $x_i's$ como na Proposição 4.3.6. Se apenas um dos $x_i's$ não se anula, então, pela Proposição 4.3.2, temos que $\widetilde{Q_r}(\underline{x}) \geq 2p$, para $x \in \mathfrak{p}$. Para $\underline{a} \in \mathbb{Z}^{p-1}$ temos que o menor valor que $Q(\underline{a})$ assume é $p-1$. Assim, se o número dos $x_i's$ não nulos for maior do que 2, então $\widetilde{Q_r}(\underline{x}) \geq 3(p-1) \geq 2p$, uma vez que, $\widetilde{Q_r}(\underline{x}) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t})$, com $t = p^{r-1} - 1$, e portanto $\widetilde{Q_r}(\underline{x}) = Q_{p-1}(a_0, a_{p^{r-1}}, \cdots, a_{(p-2)p^{r-1}}) + \cdots + Q_{p-1}(a_t, a_{p^{r-1}+t}, \cdots, a_{(p-2)p^{r-1}+t}) \geq p-1+p-1+p-1 = 3(p-1) \geq 2p$. Deste modo, falta considerar o caso em que apenas dois dos $x_i's$ não se anulam, digamos x_i e x_j. Mostraremos, primeiramente, que neste caso $\widetilde{Q_r}(\underline{x})$ não atinge o valor $2(p-1)$. Se isto ocorre, temos que $Q(\underline{x_i}) = Q(\underline{x_j}) = p-1$ e isto ocorre apenas nos casos seguintes:
1°*caso* : Se $\underline{x_i} = \pm e_l$ e $\underline{x_j} = \pm e_s$, podemos supor, sem perda de generalidade, que $\underline{x_i} = e_l$ e $\underline{x_j} = -e_s$. Logo existem $a, b \in \mathbb{N}$ tais que

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^a - \zeta_{p^r}^b = f(\zeta_{p^r}),$$

onde $f(X) = X^a - X^b$. Como $x \in \mathfrak{p}^2$, segue que, pela Proposição 4.3.5, *que*

$$f'(1) \equiv a - b \equiv 0 (mod\ p).$$

Observe que $x = \zeta_{p^r}^a(1-\zeta_{p^r}^{b-a})$. Como estamos considerando apenas dois dos $x_i's$ não nulos, segue que $a-b \equiv 0(mod\ p)$ não ocorre, o que é uma contradição.

$2^{\underline{o}}$ *caso* : Se $\underline{x_i} = (1,1,\cdots,1)$ e $\underline{x_j} = \pm e_s$, temos que se $x \in \mathfrak{p}$ então $\underline{x_j} = e_s$. Logo x é da forma

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} + \zeta_{p^r}^{j+s} = f(\zeta_{p^r}),$$

onde $f(X) = X^i + \cdots + X^{j+s}$. Se $x \in \mathfrak{p}^2$, pela Proposição 4.3.5, temos que

$$f'(1) \equiv i + \cdots + (p-2)p + i + j + s \equiv i - j \equiv 0(mod\ p),$$

o que não ocorre, pois $i, j \in \{0,\cdots,p-1\}$.

$3^{\underline{o}}$ *caso* : Se $\underline{x_i} = (1,1,\cdots,1)$ e $\underline{x_j} = \pm(-1,-1,\cdots,-1)$, temos que $\underline{x_j} = (-1,-1,\cdots,-1)$ e

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} - \zeta_{p^r}^j - \cdots - \zeta_{p^r}^{(p-2)p+j} = f(\zeta_{p^r}),$$

onde $f(X) = X^i + \cdots + X^{(p-2)p+i} - X^j + \cdots + X^{(p-2)p+j}$. Se $x \in \mathfrak{p}^2$, então

$$f'(1) \equiv i - j \equiv 0(mod\ p),$$

o que novamente não ocorre.

Mostramos, assim, que para $x \in \mathfrak{p}^2$ e dois $x_i's$ não nulos, o valor $2(p-1)$ não é atingido por $\widetilde{Q}_r(\underline{x})$. Mas, pelo Lema 1.9.2, o valor $2p-1$ também não é atingido e portanto para $x \in \mathfrak{p}^2$ temos que $\widetilde{Q}_r(x) \geq 2p$. Observe que o elemento $x = 1-\zeta_{p^r}^p$ pertence a $\mathfrak{p}^i$, para $i = 1,\cdots,p$, e $\widetilde{Q}_r(\underline{x}) = 2p$. Como $|\sigma_{\mathbb{K}}(x)|^2 = \dfrac{p^{r-1}}{2}.\widetilde{Q}_r(\underline{x})$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}.2p = p^r,$$

o que implica que $\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{1}{2} min\{|\sigma(x)|,\ x \neq 0,\ x \in \mathfrak{p}^i\} = \frac{\sqrt{p^r}}{2}$, para $i = 1, 2, \cdots, p$. Como o ideal de menor norma é $\mathfrak{p}^2$, segue que $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$ tem a maior densidade de centro. Assim, para $i = 1, \cdots, p$, a maior densidade de centro é obtida em $\sigma_{\mathbb{K}}(\mathfrak{p})$ ou $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$. Para $r = 2$, temos que

$$\frac{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2))}{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))} = \left(\frac{p}{p-1}\right)^{\frac{(p-1)p}{2}-1} > 1.$$

Logo, $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$ é o mais denso dentre os reticulados considerados, e sua densidade de centro é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2)) = \frac{p^{(p-1)p}}{2^{\frac{(p-1)p}{2}}.|D_{\mathbb{K}}|^{\frac{1}{2}}.p^2}.$$ ■

Exemplo 4.3.7. *Se* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{3^2}]$ *e* $\mathfrak{p} = (1 - \zeta_{3^2})\mathbb{A}_{\mathbb{K}}$, *então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2)) = \frac{1}{8\sqrt{3}} \approx 0,072168.$$

Note que $\mathbb{A}_{\mathbb{K}}$ *tem dimensão 6 e que o reticulado* $\sigma_{\mathbb{K}}((1-\zeta_{3^2})^2\mathbb{Z}[\zeta_{3^2}])$ *apresenta maior densidade de centro que o reticulado* $\sigma_{\mathbb{K}}((1-\zeta_7)\mathbb{Z}[\zeta_7])$, *(Exemplo* 4.3.1*) e o reticulado* $\sigma_{\mathbb{K}}((1-\zeta_7)^2\mathbb{Z}[\zeta_7])$, *(Exemplo* 4.3.2*). Para esta dimensão temos que* $0,072168$ *é o maior valor conhecido para a densidade de centro e corresponde a densidade de centro do reticulado conhecido na literatura* E_6,*(Conway; Sloane, p.15).*

3 Reticulados via $\mathbb{Q}(\zeta_{pq})$

Nesta seção apresentamos alguns resultados sobre reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{pq})$, onde p e q são primos distintos.

Lema 4.3.3. *(Flores, p.64, Lema.3.5.1) Se p e q são números distintos então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = \begin{cases} 1, & se\ mdc(k,pq)=1; \\ 1-p, & se\ mdc(k,pq)=p; \\ 1-q, & se\ mdc(k,pq)=q; \\ (1-p)(1-q), & se\ mdc(k,pq)=pq. \end{cases}$$

Demonstração: Suponhamos que $mdc(k,pq)=1$. Como $mdc(p,q)=1$, segue que existem inteiros r, s tais que que $pr+qs=1$. Deste modo,

$$\zeta_{pq}^k = \zeta_{pq}^{k(pr+qs)} = \zeta_{pq}^{kpr+kps} = \zeta_{pq}^{kpr}.\zeta_{pq}^{kqs} = \zeta_q^{kr}.\zeta_p^{ks},$$

onde $mdc(kr,q)=mdc(ks,p)=1$. Então

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{kr}.\zeta_p^{ks}) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr}.\zeta_p^{ks})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}.Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q^{kr})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-\zeta_p^{kr}) = 1. \end{aligned}$$

Se $mdc(k,pq)=p$, então existe $i\in\mathbb{Z}$, com $mdc(i,q)=1$, tal que

$$\zeta_{pq}^k = \zeta_{pq}^{pi} = \zeta_q^i.$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^i)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-1) = 1-p.$$

Se $mdc(k,pq)=q$, então existe $i\in\mathbb{Z}$, com $mdc(i,p)=1$, tal que

$$\zeta_{pq}^k = \zeta_{pq}^{qi} = \zeta_p^i.$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_p^i)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^i(q-1)) = (q-1)Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^i) = (q-1)(-1) = 1-q.$$

Se $mdc(k, pq) = pq$, então existe $i \in \mathbb{Z}$, tal que $\zeta_{pq}^k = \zeta_{pq}^{pqi} = 1$. Logo,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(1)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(q-1) = (q-1)(p-1).$$

■

Corolário 4.3.2. *(Flores, p.65, Corol.3.5.2) Se* $0 \leq i \leq pq$ *então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i) = \begin{cases} pq, \text{ se } i = 0 \text{ ou } i = pq-p-q; \\ -pq \text{ se } i = pq-p \text{ ou } i = pq-q; \\ 0, \text{ caso contrário.} \end{cases}$$

Demonstração: Se $mdc(i, pq) = 1$, então

$$(1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i = \zeta_{pq}^i - \zeta_{pq}^{p+i} - \zeta_{pq}^{q+i} + \zeta_{pq}^{p+q+i},$$

sendo que o expoente de cada parcela é primo com pq. Logo, o traço de cada uma dessas parcelas é 1. Assim

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^i) - Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+i}) - Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{q+i}) + Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+q+i}) = 1-1-1+1 = 0.$$

Para $i = 0$, aplicando o Lema 4.3.3 temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q})) = (p-1)(q-1)+p-1+q-1+1 = pq.$$

Para $i = pq-p$, temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^{pq-p}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p} - 1 - \zeta_{pq}^{pq-p+q} - \zeta_{pq}^{q+pq}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p(q-1)} - 1 - \zeta_{pq}^{-p+q} + \zeta_{pq}^{q(1+p)}) = 1-p-(1-p)(1-q)-1+1-q = 1-p-pq+p+q-1-1+1-q = -pq.$$

Analogamente para $i = pq - q$, temos que $Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^{p} - \zeta_{pq}^{q} + \zeta_{pq}^{p+q}).\zeta_{pq}^{pq-q}) = -pq$. Para $i = pq - p - q$ temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^{p} - \zeta_{pq}^{q} + \zeta_{pq}^{p+q}).\zeta_{pq}^{pq-p-q}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p-q} - \zeta_{pq}^{pq-q} - \zeta_{pq}^{pq-p} + \zeta_{pq}^{pq}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{-p-q} - \zeta_{pq}^{q(p-1)} - \zeta_{pq}^{p(q-1)} + 1) = 1 - (1 - q) - (1 - p) + (1 - p)(1 - q) = pq,$$

e isto conclui a demonstração. ∎

Proposição 4.3.7. *(*Simonato, 2000, p.47, Prop.3.3.8*) Se p e q são números primos distintos, $n = \varphi(pq)$ e x é um elemento de $\mathbb{Z}[\zeta_{pq}]$, com $x = a_0 + a_1\zeta_{pq} + \cdots + a_{n-1}\zeta_{pq}^{n-1}$, então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)A_0 + 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k,$$

onde $A_k = \sum_{i=0}^{n-(k+1)} a_i a_{k+i}$, *para* $k = 0, 1, \cdots, n-1$.

Demonstração: Pela Observação 4.3.1 e da linearidade da função traço temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(A_0) + \sum_{k=1}^{n-1} A_k Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_k),$$

onde $\alpha_k = \zeta_{pq}^{k} + \zeta_{pq}^{-k}$. Pelo Lema 4.3.3 temos que

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) &= A_0(p-1)(q-1) + A_1 Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{1} + \zeta_{pq}^{-1}) + \cdots + \\ &+ A_{n-1} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{n-1} + \zeta_{pq}^{-n+1}) = (p-1)(q-1)A_0 + \\ &+ 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k, \end{aligned}$$

e isto conclui a demonstração. ∎

Exemplo 4.3.8. *Se $p = 3$, $q = 7$ e $x = 1 + \zeta_{21}^{3} + \zeta_{21}^{6} + \zeta_{21}^{9}$ é um elemento de $\mathbb{Z}[\zeta_{21}]$, então $\underline{x} = (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$ e os A_{k}'s*

são dados por $A_0 = 4$, $A_3 = 3$, $A_6 = 2$, $A_9 = 1$ *e* $A_1 = A_2 = A_4 = A_5 = A_7 = A_8 = A_{10} = A_{11} = 0$. *Logo,* $Tr_{\mathbb{Q}(\zeta_{21})\mathbb{Q}}(x\overline{x}) = 48-24 = 24$ *e portanto* $|\sigma_{\mathbb{K}}(x)| = \sqrt{12}$. *Agora, se* $x = 1-\zeta_{21}^3$ *em* $\mathbb{Z}[\zeta_{21}]$ *então* $\underline{x} = (1,0,0,-1,0,0,0,0,0,0,0,0)$, *e os* $A_{k}'s$ *são dados por* $A_0 = 2$, $A_3 = -1$ *e* $A_1 = A_2 = A_4 = A_5 = A_6 = A_7 = A_8 = A_9 = A_{10} = A_{11} = 0$. *Logo,* $Tr_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}}(x\overline{x}) = 24+4 = 28$ *e portanto* $|\sigma_{\mathbb{K}}(x)| = \sqrt{14}$.

Se $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{pq}]$, pela Seção 2.4, temos que se p e q são números primos distintos tais que $O_q(p) \equiv O_p(q) \equiv 1(mod\ 2)$ então

$$p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r\overline{\mathfrak{p}_1 \cdots \mathfrak{p}_r})^{p-1} \quad \text{e} \quad q\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1 \cdots \mathfrak{q}_s\overline{\mathfrak{q}_1 \cdots \mathfrak{q}_s})^{q-1}. \quad (4.7)$$

Tomando o ideal $\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s$ temos que x pertence a $\mathfrak{p}$ se, e somente se, $x\overline{x}$ pertence a $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$. De fato, se x pertence a $\mathfrak{p}$, então $x\overline{x}$ é um elemento de $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$, uma vez que $p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r\overline{\mathfrak{p}_1 \cdots \mathfrak{p}_r})^{p-1} = (1-\zeta_{pq}^p)^{p-1}\mathbb{A}_{\mathbb{L}} = ((1-\zeta_{pq}^p)\mathbb{A}_{\mathbb{L}})^{p-1}$. Por outro lado, se x não é um elemento de $\mathfrak{p}$, então pelo menos um dos $\mathfrak{p}_{i}'s$ ou $\mathfrak{q}_{i}'s$ não aparecerá na fatoração do ideal $x\mathbb{A}_{\mathbb{L}}$ e portanto na fatoração de $x\overline{x}\mathbb{A}_{\mathbb{L}}$ não aparecerão todos os fatores de $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$, contradizendo a hipótese. Visto que o corpo $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ é totalmente complexo, segue que a densidade de centro do reticulado $\sigma_{\mathbb{L}}(\mathfrak{p})$, é dada por

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{\frac{n}{2}}\rho^n}{|D_{\mathbb{L}}|^{\frac{1}{2}}N(\mathfrak{p})},$$

onde $n = [\mathbb{L} : \mathbb{Q}]$ e

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{1}{2}min\left\{\sqrt{\frac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ : \ x \in \mathfrak{p},\ x \neq 0\right\}.$$

Exemplo 4.3.9. *Veremos a construção algébrica de* K_{12} *via a representação geométrica de um ideal primo acima de* $7\mathbb{A}_{\mathbb{L}}$ *em* $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{21}]$ *com* $\mathbb{L} = \mathbb{Q}(\zeta_{21})$. *Seja* $f(X)$ *o polinômio minimal de*

ζ_{21} *sobre* $\mathbb{Q}$. *Vamos fatorar os ideais* $3\mathbb{A}_{\mathbb{L}}$ *e* $7\mathbb{A}_{\mathbb{L}}$ *em um produto de ideais primos utilizando o Lema de Kummer. Temos que* $f(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$, *e portanto* $f(X) \equiv (X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^2 (mod\ (\mathbb{Z}/3\mathbb{Z})[X])$. *Assim*

$$g = 1,\ \overline{\mu_1}(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\ e_1 = 2\, e\, f_1 = 6.$$
$$\mathfrak{p}_1 = 3\mathbb{A}_{\mathbb{L}} + (\zeta_{21}^6 + \zeta_{21}^5 + \zeta_{21}^4 + \zeta_{21}^3 + \zeta_{21}^2 + 1)\mathbb{A}_{\mathbb{L}}.$$

Portanto, $3\mathbb{A}_{\mathbb{L}} = \mathfrak{p}_1^2$ *com* $N(\mathfrak{p}_1) = 3^6$. *Note que o ideal* $3\mathbb{A}_{\mathbb{L}}$ *não se fatora conforme a Equação (4.7), o que já era possível concluir pois* $O_7(3) = 6 \equiv 0(mod\ 2)$ *ou simplesmente observando que* $card(D_{\mathbb{L}}(3)) = e_1 f_1 = 12$. *Portanto* $D_{\mathbb{L}}(3) = G$, *onde* G *é o grupo de Galois de* $\mathbb{L}$ *sobre* $\mathbb{Q}$. *Para o caso* $7\mathbb{A}_{\mathbb{L}}$, *temos que*

$$f(X) \equiv (X+3)^6 (X+5)^6 (mod\ (\mathbb{Z}/7\mathbb{Z})[X])$$

Assim

$$g = 2,\ \overline{\mu_1}(X) = X + 3,\ \overline{\mu_2}(X) = X + 5,\ e_1 = e_2 = 6\, e\, f_1 = f_2 = 1.$$
$$\mathfrak{q}_1 = 7\mathbb{A}_{\mathbb{L}} + (\zeta_{21} + 3)\mathbb{A}_{\mathbb{L}} \quad e \quad \mathfrak{q}_2 = 7\mathbb{A}_{\mathbb{L}} + (\zeta_{21} + 5)\mathbb{A}_{\mathbb{L}}.$$

Portanto, $7\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2)^6$, *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são ideais com norma 7 e* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$. *Observamos que* $O_3(7) = 1 \equiv 1(mod\ 2)$ *e que* $\overline{\sigma} = \sigma_{20}$ *não pertence a* $D_{\mathbb{L}}(7) = \{\sigma_1, \sigma_4, \sigma_{10}, \sigma_{13}, \sigma_{16}, \sigma_{19}\}$. *Dado que o discriminante absoluto de* $\mathbb{L}$ *é* $3^6 7^{10}$ *(Teorema* 2.3.7*), segue que a densidade de centro de* $\sigma_{\mathbb{L}}(\mathfrak{q}_1)$ *é dada por* $\delta(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \dfrac{2^6 \rho^{12}}{3^3 7^6}$. *Calculamos então o raio de empacotamento*

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \tfrac{1}{2} min\left\{ \sqrt{\tfrac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ :\ x \in \mathfrak{q}_1,\ x \neq 0 \right\}.$$

Temos que $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *é par, ou seja,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 2l$, $l \in \mathbb{Z}$ *e para* x *em* $\mathfrak{q}_1$ *temos que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \in 7\mathbb{Z}$, *o que implica que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *é múltiplo de 14. Como* $mdc(p, q) = 1$, *segue que para* x *em* $\mathfrak{q}_1$, $x = \alpha_0 + \alpha_1\zeta_3$ *com* $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_7]$, *segue que*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_7)}(x\overline{x}) = \alpha_0\overline{\alpha_0} + \alpha_1\overline{\alpha_1} + (\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1}).$$

Aplicando o traço novamente temos:

$$Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(Tr_{\mathbb{L}/\mathbb{Q}(\zeta_7)}(x\overline{x})) =$$
$$Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) + Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_1\overline{\alpha_1}) + Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}[(\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1})].$$

Temos duas possibilidades para $x = \alpha_0 + \alpha_1\zeta_3$.

1^o *caso* : *Se* $\alpha_0 = \alpha_1$, *então* $x = \alpha_0(1+\zeta_3) \in \mathfrak{q}_1$. *Como* $1+\zeta_3$ *não pertence ao ideal primo* $\mathfrak{q}_1$, *segue que* $\alpha_0 \in \mathfrak{q}_1$. *Logo,* $Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) \geq 14$. *Portanto*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 2Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) \geq 28.$$

2^o *caso* : *Se* $\alpha_0 \neq \alpha_1$, *para* $y = \sum_{i=0}^{5} a_i\zeta_7^i \in \mathbb{Z}[\zeta_7]$, *segue do Teorema 4.3.3, que* $Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(y\overline{y})$ *é uma forma quadrática* $Q_6(a_0, a_1, a_2, a_3, a_4, a_5)$ *cujo valor mínimo é 6, (Proposição 1.9.1). Então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 6 + 6 + 6 = 18 \quad e \quad Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \equiv 0(mod\ 14),$$

e portanto $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 28$. *Vamos caracterizar um elemento de* $\mathfrak{q}_1$. *Em* $\mathfrak{q}_1$ *temos que* $\zeta_{21} \equiv -3(mod\ \mathfrak{q}_1)$ *e então para* x *em* $\mathfrak{q}_1$ *temos que*

$$x = \sum_{i=0}^{11} a_i\zeta_{21}^i \equiv \sum_{i=0}^{11} a_i(-3)^i(mod\ \mathfrak{q}_1).$$

Como $\mathfrak{q}_1 \cap \mathbb{Z} = 7\mathbb{Z}$, *segue que*

$$x \in \mathfrak{q}_1 \Longleftrightarrow \sum_{i=0}^{11} a_i(-3)^i \equiv 0(mod\ 7).$$

O elemento $x = 1-\zeta_{21}^3 \in \mathbb{A}_{\mathbb{L}}$. *Como* $\underline{x} = (1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0)$, *segue que* $\sum_{i=0}^{11} a_i(-3)^i = 1 - (-3)^3 = 28 \equiv 0(mod\ 7)$ *e portanto* x *pertence a* $\mathfrak{q}_1$. *Pelo Exemplo* 4.3.8, *temos que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 28$. *Logo o menor valor de* $\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in \mathfrak{q}_1, x \neq 0\}$ *é de fato 28. Portanto,* $\rho = \frac{\sqrt{14}}{2} = \sqrt{\frac{7}{2}}$, *e a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \frac{2^6\left(\sqrt{\frac{7}{2}}\right)^{12}}{3^3.7^6} = \frac{1}{3^3} \approx 0,037037.$$

Para esta dimensão temos que esta é a maior densidade de centro já obtida, e corresponde a densidade de centro do reticulado conhecido na literatura $\boldsymbol{K}_{12}$, *(Conway; Sloane, 1999, p.15).*

Exemplo 4.3.10. *Veremos a construção do reticulado* Λ_{24}. *Dados* $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{39}]$ *o anel dos inteiros algébricos de* $\mathbb{L} = \mathbb{Q}(\zeta_{39})$ *e* $f(X)$ *o polinômio minimal de* ζ_{39} *sobre* $\mathbb{Q}$, *vejamos as fatorações dos ideais* $3\mathbb{A}_{\mathbb{L}}$ *e* $13\mathbb{A}_{\mathbb{L}}$ *como um produto de ideais primos de* $\mathbb{A}_{\mathbb{L}}$. *Como*

$$\begin{aligned} f(X) \quad &= X^{24} - X^{23} + X^{21} - X^{20} + X^{18} - X^{17} + X^{15} - X^{14} + \\ &+ X^{12} - X^{10} + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1, \end{aligned}$$

segue que

$$f(X) \equiv (X^3 + 2X + 2)^2(X^3 + X^2 + X + 2)^2(X^3 + 2X^2 + 2X + 2)^2(X^3 + X^2 + 2)^2 (mod\ (\mathbb{Z}/3\mathbb{Z})[X]).$$

Assim

$$\begin{aligned} &g = 4, \qquad e_1 = e_2 = e_3 = e_4 = 2, \qquad f_1 = f_2 = f_3 = f_4 = 3 \\ &\overline{\mu_1}(X) = X^3 + 2X + 2, \qquad \overline{\mu_2}(X) = X^3 + X^2 + X + 2, \\ &\overline{\mu_3}(X) = X^3 + 2X^2 + 2X + 2, \qquad \overline{\mu_4}(X) = X^3 + X^2 + 2, \end{aligned}$$

Logo,

$$\begin{aligned} \mathfrak{p}_1 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + 2\zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_2 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + \zeta_{39}^2 + \zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_3 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + 2\zeta_{39}^2 + 2\zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_4 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + \zeta_{39}^2 + 2)\mathbb{A}_{\mathbb{L}} \end{aligned}$$

Portanto $3\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^2$, *com* $N(\mathfrak{p}_i) = 3^3$, *para* $i = 1, 2, 3, 4$. *Como* $O_{13}(3) = 3 \equiv 1 (mod\ 2)$, *segue que* $\overline{\sigma} = \sigma_{38} \notin D_{\mathbb{L}}(3) = \{\sigma_1, \sigma_{14}, \sigma_{16}, \sigma_{22}, \sigma_{29}, \sigma_{35}\}$. *Neste caso, temos que* $\mathfrak{p}_4 = \overline{\mathfrak{p}_1}$ *e* $\mathfrak{p}_3 = \overline{\mathfrak{p}_2}$. *Para o ideal* $13\mathbb{A}_{\mathbb{L}}$ *temos que*

$$f(X) \equiv (X+4)^{12}(X+10)^{12}(mod\ (\mathbb{Z}/13\mathbb{Z})[X]).$$

$$g = 2, \quad \overline{\mu_1} = X+4, \quad \overline{\mu_2} = X+10, \quad e_1 = e_2 = 12, \quad f_1 = f_2 = 1.$$

$$\mathfrak{q}_1 = 13\mathbb{A}_{\mathbb{L}} + (\zeta_{39}+4)\mathbb{A}_{\mathbb{L}} \quad e \quad \mathfrak{q}_2 = 13\mathbb{A}_{\mathbb{L}} + (\zeta_{39}+10)\mathbb{A}_{\mathbb{L}}.$$

Logo, $13\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2)^{12}$, *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são ideais primos com norma 13. Observe novamente que* $\overline{\sigma} \notin D_{\mathbb{L}}(13) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{10}, \sigma_{16}, \sigma_{19}, \sigma_{22}, \sigma_{25}, \sigma_{28}, \sigma_{31}, \sigma_{34}, \sigma_{37}\}$, *pois* $O_3(13) = 1 \equiv 1(mod\ 2)$. *Neste caso, temos que* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$. *Considerando o ideal* $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_1$, *vamos calcular a densidade de centro de* $\sigma_{\mathbb{L}}(\mathfrak{p})$. *Como* $D_{\mathbb{L}} = 3^{12}13^{22}$ *e* $N(\mathfrak{p}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{q}_1) = 3^6.13$, *segue que*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{12}\rho^{24}}{3^{12}13^{12}}.$$

Precisamos agora determinar

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{1}{2} min\left\{ \sqrt{\frac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ : \ x \in \mathfrak{p},\ x \neq 0 \right\}.$$

Veremos agora que se $x \in \mathfrak{p}$, *então* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 4.39$. *Visto que* $mdc(p,q) = 1$, *para* $x \in \mathfrak{p}$, *podemos escrever* $x = \alpha_0 + \alpha_1\zeta_3$, *com* $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_{13}]$. *Temos também que se* x *pertence a* $\mathfrak{p}$, *então* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \equiv 0(mod\ 2.39)$. *Pelo Exemplo* 4.3.9, *temos que*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) =$$
$$Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha}_0) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha}_1) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0-\alpha_1)(\overline{\alpha_0-\alpha_1})].$$

Nesta soma, para que o valor 2.39 *seja atingido, as únicas possibilidades são, a menos de ordem,* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha}_0) = 12$, $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha}_1) = 30$ *e* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0-\alpha_1)(\overline{\alpha_0-\alpha_1})] = 36$. *As possibilidades para* α_0 *e* α_1 *são:*

$$\alpha_0 = \pm\zeta_{13}^{i_0}, \ i_0 = 0, \cdots, 12;$$
$$\alpha_1 = \pm(\zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}),$$

onde i_1, i_2, i_3, *são dois a dois distintos. Sejam* $\alpha_0 = -\zeta_{13}^{i_0}$ *e* $\alpha_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$. *Se* $i_0 \neq i_k$, *com* $k = 1, 2, 3$, *então* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1})] = 36$. *Sendo* x *um elemento de* $\mathfrak{p}$, *segue que*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(\alpha_0\overline{\alpha}_0 + \alpha_1\overline{\alpha}_1) - (\alpha_0 + \alpha_1)\overline{(\alpha_0 + \alpha_1)} \in 3\mathbb{Z}[\zeta_{13}],$$

e portanto, se $y = (\alpha_0+\alpha_1)\overline{(\alpha_0 + \alpha_1)}$. *Assim* $y \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}])$. *Seja* $\gamma : \mathbb{Z}[\zeta_{13}] \longrightarrow \mathbb{Z}$ *o homomorfismo de anéis dado por* $\gamma\left(\sum_{i=0}^{11} a_i\zeta_{13}^i\right) = \sum_{i=0}^{11} a_i$. *Como* y *está em* $3\mathbb{Z}[\zeta_{13}]$ *segue que* $\gamma(y) \equiv 0 (mod\ 3)$. *Reescrevendo* y *substituindo* α_0 *e* α_1 *pelos valores fixados acima temos que*

$$y = (-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) = 4 - A + B \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}]),$$

onde $A = \sum_{s=1}^{3}(\zeta_{13}^{i_0-i_s} + \zeta_{13}^{i_s-i_0})$ *e* $B = \sum_{r,s=1}^{3} \zeta_{13}^{i_r-i_s}$. *Sendo* n_A *o número de expoentes tais que* $i_0 - i_s = -1$ *ou* $i_s - i_0 = -1$ *e* n_B *o número de expoentes tais que* $i_r - i_s = -1$, *segue que as possibilidades para* n_A *são* 0 *ou* 1, *uma vez que* i_1, i_2, i_3 *são dois a dois distintos. Por outro lado, para* n_B *as possibilidades são* 0, 1 *ou* 2. *Observe que* $\gamma(\zeta_{13}^{-1}) = \gamma(-1 - \zeta_{13} - \cdots - \zeta_{13}^{11}) = -12 \equiv 0 (mod\ 3)$. *Assim,*

$$\gamma(A) = 6 - n_A \text{ e } \gamma(B) = 6 - n_B.$$

Logo, $\gamma(y) = 4 - \gamma(A) + \gamma(B) \equiv 1 + n_A - n_B \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}])$ *e as únicas soluções possíveis são*

$$n_A = 0 \text{ e } n_B = 1$$

ou

$$n_A = 1 \text{ e } n_B = 2.$$

Suponhamos $n_A = 0$ *e* $n_B = 1$. *Dado* $0 < a \leq 11$, *por hipótese, o coeficiente de* ζ_{13}^a *é múltiplo de 3. Temos*

$$B = \zeta_{13}^{-1} + \sum_{r,s=1}^{3} \zeta_{13}^{i_r - i_s}, \text{ com } i_r - i_s \neq -1.$$

Se existem r *e* s *tais que* $i_r - i_s = a$, *então o coeficiente de* ζ_{13}^a *na equação acima é nulo, pois* $\zeta_{13}^{-1} = -1 - \zeta_{13} - \cdots - \zeta_{13}^{11}$. *Assim,* ζ_{13}^a *aparece também com coeficiente nulo na expansão de* A *na base integral* $\{1, \cdots, \zeta_{13}^{11}\}$. *Se não existem* r *e* s *tais que* $i_r - i_s = a$, *novamente* ζ_{13}^a *aparece com coeficiente nulo na decomposição de* y. *Deste modo, a única possibilidade portanto é* $a = 0$ *e* $y = 3$. *Então como*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(\alpha_0\overline{\alpha}_0 + \alpha_1\overline{\alpha}_1) - (\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1}),$$

temos

$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(3(\alpha_0\overline{\alpha_0} + \alpha_1\overline{\alpha_1}) - (\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1})) =$
$3Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) + 3Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha_1}) - Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1})) =$
$3 \cdot 12 + 3 \cdot 30 - 36 = 90$, *e isto não ocorre pois 90 não é múltiplo de* $2 \cdot 39$. *Quando* $n_A = 1$ *e* $n_B = 2$ *a verificação é análoga. Portanto* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 4.39 = 156$. *O elemento* $x = 1 - \zeta_{39}^3 - \zeta_{39}^{13} + \zeta_{39}^{16}$ *pertence ao ideal* $\mathfrak{p}$ *e observando que* $\underline{x} = (1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, *pela Proposição* 4.3.7, *temos que* $Tr(x\overline{x}) = 156$. *Portanto,* $\rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \dfrac{\sqrt{78}}{2} = \sqrt{\dfrac{39}{2}}$ *e a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{12}\left(\sqrt{\frac{39}{2}}\right)^{24}}{3^{12}13^{12}} = 1.$$

Para dimensão 24 a densidade de centro obtida neste exemplo é a maior conhecida, e corresponde a densidade de centro do reticulado conhecido na literatura Λ_{24}. (Conway; Sloane, 1999, p.15).

5

Os canais Gaussiano e com desvanecimento do tipo Rayleigh

5.1 Introdução

Neste capítulo, apresentamos através do trabalho de Boutros; Viterbo; Rastello; Belfiori (1996), constelações de reticulados que são eficientes para ambos os canais Gaussianos e com desvanecimento do tipo Rayleigh, enfocando a construção das versões rotacionadas dos reticulados já conhecidos na literatura: D_4, K_{12} e Λ_{16}, através da matriz mudança de base de um ideal contido no anel dos inteiros de um corpo de números.

5.2 Breve histórico

O rápido crescimento da comunicação sem fio requer um aumento na capacidade e melhoria no desempenho dos sistemas de transmissão. Os canais de comunicação móvel são agrupados em

dois tipos: canal via satélite e canal terrestre. O canal de comunicação terrestre é caracterizado pelo efeito de múltiplos percursos de propagação. Tal efeito pode alterar de maneira significativa a amplitude do sinal, mesmo para uma pequena variação na distância ou orientação entre o transmissor e o receptor, comportamento que é comumente rotulado como desvanecimento. Limitações nas perdas de propagação, variação no tempo, ruído, inferência e desvanecimento fazem com que, nestes sistemas, a transmissão de dados com altas taxas de transmissão não seja uma tarefa fácil.

Para se alcançar essas altas taxas de transmissão de dados é necessário aumentar a capacidade do canal de comunicações móveis. Quando o desvanecimento compromete substancialmente a qualidade da transmissão, o aumento da capacidade do canal ou equivalentemente, a diminuição da taxa de erro é extremamente difícil.

Uma alternativa mais simples para aumentar a capacidade do canal com desvanecimento é utilizar técnicas de diversidade. Estas técnicas geralmente fornecem ao receptor réplicas da informação transmitida que experimentam desvanecimentos descorrelacionados. Neste caso, se uma componente do sinal estiver sobre um desvanecimento profundo, algumas das outras componentes terão uma grande probabilidade de sofrer uma atenuação mais leve.

A função densidade de probabilidade de Rayleigh caracteriza o desvanecimento percebido em uma comunicação móvel onde não há predominância direta entre a antena transmissora e a receptora. Esse desvanecimento indica que existe uma maior probabilidade da amplitude da envoltória do sinal recebido estar abaixo de um valor médio.

Os códigos projetados para canais com desvanecimento Ray-

leigh levam em conta dois parâmetros fundamentais: o ganho de diversidade, que descreve a diminuição exponencial da taxa de erro na decodificação em função da relação sinal-ruído na curva de desempenho e o ganho de codificação que resulta em deslocamentos à esquerda dessa curva. Os melhores valores para estes parâmetros foram obtidos maximizando-se, respectivamente, o posto mínimo e a média geométrica mínima dos autovalores, de um conjunto de matrizes complexas formadas pelas diferenças entre palavras-código tomadas duas a duas.

A principal desvantagem destes códigos é que são extremamente difíceis de se projetar, pois os critérios utilizados na sua construção baseiam-se em operações no domínio complexo das modulações em banda básica e não no domínio binário ou discreto no qual os códigos de canal são tradicionalmente projetados. Uma grande capacidade computacional é necessária para acompanhar a busca, codificação e decodificação destes códigos.

O canal de comunicação via satélite é um canal AWGN (Additive White Gaussian Noise) onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal. O termo AWGN é utilizado em modulamentos matemáticos para caracterizar aqueles canais onde o tipo de ruído responsável por degradar a comunicação é um ruído branco adicionado ao sinal. Este tipo de ruído é um dos mais "bem comportados" e a teoria acerca do desenvolvimento de receptores ótimos para a utilização em canais AWGN já se tornou clássica.

O ruído branco é um sinal aleatório e tem um modelamento matemático que o considera como possuindo largura de faixa infinita, média nula e correlação nula entre suas amplitudes tomadas a instantes de tempo distintos, ou seja, o valor da amplitude do

ruído em um determinado instante independe daquele observado em outro instante de tempo qualquer. O termo gaussiano se deve ao fato desse tipo de ruído possuir uma função densidade de probabilidade gaussiana com média nula, com desvio padrão igual à sua tensão rms e variância igual à potência dissipada de um resistor de 1W. No canal gaussiano, usando esquemas convencionais de modulação e codificação de canal apropriada, pode-se reduzir a probabilidade de erro e bit de 10^{-2} a 10^{-3} por meio de um aumento da relação sinal-ruído de somente 1 ou 2 dB.

5.3 Boas constelações para ambos os canais Gaussianos e com desvanecimento do tipo Rayleigh

Nesta seção estabelecemos condições sobre os reticulados construídos para que tenhamos boas constelações para ambos os canais Gaussianos e Rayleigh com desvanecimento.

1. **Canal Gaussiano**

   - A probabilidade de erro de símbolo é limitada superiormente por

$$P_e(\Lambda) \leq \frac{\tau}{2}\, erfc\left(\frac{d_{E\,min}/2}{\sqrt{2N_0}}\right), \tag{5.1}$$

   onde τ é o número de vizinhos, $erfc$ é a função erro, N_0 é a variância gaussiana e $d_{E\,min}$ é a distância mínima Euclidiana do reticulado Λ. O ganho de codificação do reticulado Λ é dado por

$$\gamma = \frac{d_{E\,min}^2}{Vol(\Lambda)^{2/n}}.$$

- Constelações eficientes podem ser obtidas através de reticulados com alta densidade de empacotamento. Assim, constelações com boas propriedades de simetria podem ser obtidas.
- Usando corpos de números totalmente reais e com discriminante absoluto mínimo a grande desvantagem é que a densidade de empacotamento esférico é baixa.
- Usando corpos de números totalmente complexos e com discriminante absoluto mínimo a grande vantagem é que é possível obter reticulados com alta densidade de empacotamento.

2. **Canal Rayleigh com Desvanecimento**

- A probabilidade de erro de símbolo com alta relação sinal-ruído satisfaz,

$$P_e(\Lambda) \leq \frac{1}{2} \sum_{l=L}^{n} \frac{1}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^l d_p^{(l)}(x,y)^2}, \tag{5.2}$$

onde onde E_b é a energia média por bit, $\eta = \dfrac{2m}{n}$ é a eficiência espectral e $d_p^{(l)}(x,y)^2$ é a distância l-produto normalizada de x a y, quando esses pontos diferem em l componentes e é dada por

$$d_p^{(l)}(x,y)^2 = \frac{\prod_{x_i \neq y_i} (x_i - y_i)^2}{\left(\dfrac{E}{n}\right)^l}, \tag{5.3}$$

onde $E = E(\|x\|^2)$ é a energia média por ponto da constelação S.

- Constelações eficientes, ou seja, aquelas em que a probabilidade de erro é mínima, podem ser obtidas através de reticulados com diversidade máxima $L = min(l)$, menor energia média da constelação E e maior distância produto mínima $d_{p,min} = min(d_p^{(L)}(x, y))$.

- Usando corpos de números totalmente reais e com discriminante absoluto mínimo, a grande vantagem é que eles apresentam diversidade máxima.

- Usando corpos de números totalmente complexos e com discriminante absoluto mínimo a grande vantagem é que obtemos uma menor energia média da constelação.

Assim, concluímos que para obter boas constelações de reticulados para ambos os canais, procura-se construir reticulados com alta densidade de empacotamento e com diversidade máxima.

Através da família de reticulados A_n que vimos a partir de subcorpos de $\mathbb{Q}(\zeta_p)$ é possível obter constelações que têm máxima diversidade e boa densidade de empacotamento, que fazem estes reticulados úteis para uso nos canais Gaussiano e Rayleigh com desvanecimento.

Corpos de números algébricos totalmente reais com discriminante absoluto mínimo são conhecidos até a dimensão 8 e são dados na 1ª coluna da Tabela (5.3.1).

Discriminantes absolutos mínimos
(Valores com * são os melhores valores conhecidos)

n	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$	$r_2 = 3$	$r_2 = 4$
2	5	-3	-	-	-
3	49	-23	-	-	-
4	725	-275	117	-	-
5	14641	-4511	1609	-	-
6	300125	-92779^*	28037^*	-9747	-
7	20134393	?	?	?	-
8	282300416	?	?	?	125778^*

Tabela (5.3.1)

Pela Tabela (5.3.1) notamos que os discriminantes absolutos dos corpos totalmente complexos são menores do que dos corpos totalmente reais. Os corpos da Tabela (5.3.1) (especialmente em dimensão acima de 4) tem sido objeto de estudos na teoria dos números algébricos computacionais.

Definição 5.3.1. *A diversidade de um reticulado Λ é a distância mínima de Hamming entre quaisquer dois vetores de Λ.*

Teorema 5.3.1. *(*BoutrosS; Viterbo; Rastello; Belfiori, 1996*) Sejam $\mathbb{K}$ um corpo de números, $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ os $\mathbb{Q}$-homomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $\{w_1, w_2, \cdots, w_n\}$ uma base integral de $\mathbb{K}$. Os reticulados obtidos a partir da matriz geradora $\boldsymbol{G} =$*

$$\begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \Im\sigma_{r_1+1}(w_1) & \cdots & \Re\sigma_{r_1+r_2}(w_1) & \Im\sigma_{r_1+r_2}(w_1) \\ \sigma_1(w_2) & \cdots & \sigma_{r_1}(w_2) & \Re\sigma_{r_1+1}(w_2) & \Im\sigma_{r_1+1}(w_2) & \cdots & \Re\sigma_{r_1+r_2}(w_2) & \Im\sigma_{r_1+r_2}(w_2) \\ \vdots & \ddots & & \vdots & & \ddots & & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \Im\sigma_{r_1+1}(w_n) & \cdots & \Re\sigma_{r_1+r_2}(w_n) & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}$$

possuem diversidade $\boldsymbol{L = r_1 + r_2}$.

Demonstração. Seja $z \neq 0$ um ponto arbitrário de $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$. Assim $z = (z_1, z_2, \cdots, z_n) = \sum_{i=1}^{n} \lambda_i v_i$, com $\lambda_i \in \mathbb{Z}$ e $v_i = (v_{ij}) = \sigma(w_i)$ são as linhas do reticulado da matriz geradora $\boldsymbol{G}$. Logo,

$$d^n(0,z) = \prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| =$$

$$= \prod_{j=1}^{r_1} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \times \prod_{j=r_1+1}^{r_1+r_2} \left| \Re\sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \times \prod_{j=r_1+1}^{r_1+r_2} \left| \Im\sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right|.$$

Os inteiros algébricos $\sum_{i=1}^{n} \lambda_i w_i$ são não nulos pois todos os $\lambda_i's$ são não nulos ($z \neq 0$). Isto implica que $\sigma_j(\sum_{i=1}^{n} \lambda_i w_i) \neq 0$ e assim o primeiro produto do lado direito da última igualdade contém exatamente r_1 fatores não nulos. O número mínimo de fatores não nulos no segundo e no terceiro produtos é r_2 pois as partes real e imaginária de qualquer um dos monomorfismos complexos não são ambos nulos. Assim concluímos que para tal reticulado temos uma diversidade $L \geq r_1 + r_2$. Agora, se $\alpha = 1$ em $\mathbb{A}_{\mathbb{K}}$, então $\sigma_j(1) = 1$ para $j = 1, 2, \cdots, r_1 + r_2$ e portanto $\sigma(1)$ fornece $r_1 + r_2$ componentes não nulos. Assim $L = r_1 + r_2$. ■

No caso de um corpo de números algébricos totalmente real temos que a matriz geradora $\boldsymbol{G}$ é da forma

$$\boldsymbol{G} = \begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1) & \cdots & \sigma_n(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2) & \cdots & \sigma_n(w_2) \\ \vdots & & \ddots & \vdots \\ \sigma_1(w_n) & \sigma_2(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}.$$

Neste caso, o reticulado $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$ construído atinge o grau máximo de diversidade $L = n$.

Para corpos totalmente complexos $\mathbb{K}$ temos que $r_2 = n/2$ é par e a matriz geradora do reticulado $\sigma(\mathbb{A}_{\mathbb{K}})$ é dada por

$$G = \begin{pmatrix} \Re\sigma_1(w_1) & \Im\sigma_1(w_1) & \cdots & \Re\sigma_{r_2}(w_1) & \Im\sigma_{r_2}(w_1) \\ \Re\sigma_1(w_2) & \Im\sigma_1(w_2) & \cdots & \Re\sigma_{r_2}(w_2) & \Im\sigma_{r_2}(w_2) \\ \vdots & & \ddots & & \vdots \\ \Re\sigma_1(w_n) & \Im\sigma_1(w_n) & \cdots & \Re\sigma_{r_2}(w_n) & \Im\sigma_{r_2}(w_n) \end{pmatrix}.$$

Definição 5.3.2. *Um polinômio minimal é chamado* **reduzido** *se as potências de uma de suas raízes (o elemento primitivo) é uma base integral do corpo de números.*

A Tabela (5.3.2) apresenta os polinômios minimais reduzidos dos corpos da Tabela (5.3.1) com o volume fundamental do reticulado correspondente obtido via o homomorfismo canônico, indicados por $\Lambda_{n,L}$.

$\Lambda_{n,L}$	$\mu_\theta(x)$	$redVol(\Lambda_{n,L})$
$\Lambda_{2,1}$	$X^2 - X + 1$	0.8660
$\Lambda_{2,2}$	$X^2 - X - 1$	2.2361
$\Lambda_{3,2}$	$X^3 - X - 1$	2.3979
$\Lambda_{3,3}$	$X^3 + X^2 - 2X - 1$	7
$\Lambda_{4,2}$	$X^4 - X^3 - X^2 + X + 1$	2.7042
$\Lambda_{4,3}$	$X^4 - X^3 + 2X - 1$	8.2916
$\Lambda_{4,4}$	$X^4 - X^3 - 3X^2 + X + 1$	26.9258
$\Lambda_{5,3}$	$X^5 - X^3 + X^2 + X - 1$	10.0281
$\Lambda_{5,4}$	$X^5 - 2X^3 + X^2 - 1$	33.5820
$\Lambda_{5,5}$	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	121
$\Lambda_{6,3}$	$X^6 - 3X^5 + 4X^4 - 4X^3 + 4X^2 - 2X + 1$	12.3409
$\Lambda_{6,4}$	$X^6 - 2X^5 + 3X^3 - 2X - 1$	41.8606
$\Lambda_{6,5}$	$X^6 + X^5 - 2X^4 - 3X^3 - X^2 + 2X + 1$	152.2982
$\Lambda_{6,6}$	$X^6 - X^5 - 7X^4 + 2X^3 + 7X^2 - 2X - 1$	547.8367
$\Lambda_{7,7}$	$X^7 + X^6 - 6X^5 - 5X^4 + 8X^3 + 5X^2 - 2X - 1$	4487.1364
$\Lambda_{8,4}$	$X^8 - 2X^7 + 4X^5 - 4X^4 + 3X^2 - 2X + 1$	70.0928
$\Lambda_{8,8}$	$X^8 + 2X^7 - 7X^6 - 8X^5 + 15X^4 + 8X^3 - 9X^2 - 2X + 1$	16801.7980

Tabela (5.3.2)

Os passos para a construção de um reticulado a partir de um corpo de números algébricos $K = \mathbb{Q}(\theta)$ pode ser resumido do seguinte modo:

- Encontre uma base integral de $\mathbb{K}$, que identifica $\mathbb{A}_{\mathbb{K}}$.
- Encontre as n raízes de $g_\theta(X)$, que identifica os n monomorfismos $\sigma_1, \sigma_2, \cdots, \sigma_n$.
- Construa a matriz geradora aplicando o homomorfismo canônico.

Exemplo 5.3.1. *Seja* $\mathbb{K} = \mathbb{Q}(i\sqrt{3})$. *Como* $-3 \equiv 1 (mod\, 4)$ *segue que a base integral de* $\mathbb{K}$ *é* $\{1, (1+i\sqrt{3})/2\}$. *Os dois monomorfismos são* $\sigma_1(i\sqrt{3}) = i\sqrt{3}$, $\sigma_2(i\sqrt{3}) = -i\sqrt{3}$ *e a matriz geradora é dada por*

$$G = \begin{pmatrix} \mathfrak{R}\sigma_1(1) & \mathfrak{I}\sigma_1(1) \\ \mathfrak{R}\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right) & \mathfrak{I}\sigma_1\left(\frac{1+i\sqrt{3}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

O volume fundamental do reticulado é dado por

$$|\det(G)| = \frac{\sqrt{3}}{2} = 0,8660254.$$

A diversidade é $L = 1$ *pois* $r_1 = 0$ *e* $r_2 = 1$. *Portanto,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *corresponde ao reticulado* $\Lambda_{2,1}$.

Exemplo 5.3.2. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{7+2\sqrt{5}})$. *As raízes do polinômio minimal* X^4-14X^2+29 *são* $\theta_1 = \sqrt{7+2\sqrt{5}}$, $\theta_2 = -\sqrt{7+2\sqrt{5}}$, $\theta_3 = \sqrt{7-2\sqrt{5}}$, $\theta_4 = -\sqrt{7-2\sqrt{5}}$. *O elemento primitivo é* $\theta = \theta_1$ *e os 4 monomorfismos são* $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, $\sigma_3(\theta) = \theta_3$, *e* $\sigma_4(\theta) = \theta_4$. *Mas* $\{1, \theta, \theta^2, \theta^3\}$ *não é base integral pois* X^4-14X^2+29 *não é*

reduzido. Uma base integral é $\{1, \frac{1}{2}(1+\theta), \frac{1}{4}(3+\theta^2), \frac{1}{8}(1+\theta)(3+\theta^2)\}$. *A matriz geradora é dada por*

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 1.000 \\ -1.193 & -0.294 & 1.294 & 2.193 \\ 3.618 & 1.381 & 1.381 & 8.618 \\ -4.318 & -0.407 & 1.789 & 7.936 \end{pmatrix}.$$

O volume fundamental do reticulado é $|\det(G)| = 26.92$. *A diversidade é* $L = 4$ *pois* $r_1 = 4$ *e* $r_2 = 0$. *Portanto,* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *corresponde ao reticulado* $\Lambda_{4,4}$.

5.4 Construção das versões rotacionadas dos reticulados D_4, K_{12}, e Λ_{16}

Craig (1978) como construir os reticulados E_6, E_8, Λ_{24} a partir dos corpos ciclotômicos totalmente complexos $\mathbb{K} = \mathbb{Q}(e^{i2\pi/n})$, para $n = 9, 20, 39$. Via este procedimento Boutros; Viterbo; Rastello; Belfiori (1996) encontrou D_4, K_{12} e Λ_{16} a partir das 8-ésima, 21-ésima e 40-ésima raízes da unidade. Estes reticulados são obtidos aplicando o homomorfismo canônico em ideais destes corpos ciclotômicos. Os ideais são dados na Tabela (5.3.3). Os reticulados obtidos são subreticulados de $\sigma(\mathbb{A}_{\mathbb{K}})$, mas com um ganho fundamental muito maior comparado com os reticulados presentes na Tabela (5.3.2).

Sejam $\mathbb{K}$ um corpo de números de grau n, $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$, $\mathfrak{a} \subseteq \mathbb{A}_{\mathbb{K}}$ um ideal e $\{\gamma_1, \cdots, \gamma_n\}$ uma $\mathbb{Z}$-base de $\mathfrak{a}$. Aplicando o homomorfismo canônico $\sigma_{\mathbb{K}}$ ao ideal $\mathfrak{a}$ de $\mathbb{A}_{\mathbb{K}}$, pela Proposição 3.5.2 obtemos o reticulado $\Lambda_{\mathfrak{a}} = \sigma(\mathfrak{a})$ de posto n contido em $\Lambda = \sigma(\mathbb{A}_{\mathbb{K}})$. A matriz geradora $G_{\mathfrak{a}}$ de $\Lambda_{\mathfrak{a}}$ é dada por

$$G_{\mathfrak{a}} = \begin{pmatrix} \sigma_1(\gamma_1) & \cdots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \cdots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & \ddots & & \vdots & & \ddots & & \vdots \\ \sigma_1(\gamma_n) & \cdots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix}.$$

Comparando $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{a}$ como $\mathbb{Z}$-módulo, vemos que existe uma relação entre as matrizes $\boldsymbol{G}$ de $\sigma(\mathbb{A}_{\mathbb{K}})$ e a matriz $\boldsymbol{G}_{\mathfrak{a}}$ de $\sigma(\mathfrak{a})$. Seja $\boldsymbol{T}$ a matriz mudança de base $n \times n$ da primeira base para a segunda base, isto é,

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = T \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}.$$

Como, os $\gamma_i^{'}s$ são inteiros algébricos segue que são escritos como combinação linear dos $w_i^{'}s$, ou seja, $\gamma_i = \sum_{k=1}^{n} t_{ik} w_k$, onde $t_{ik} \in \mathbb{Z}$. Assim que $\boldsymbol{T} = [t_{ij}]$ é uma matriz inteira. A matriz $\boldsymbol{T}$ é conhecida como **matriz da representação integral** de $\mathfrak{a}$. Com isso temos a seguinte proposição.

Proposição 5.4.1. *(*Boutros; Viterbo; Rastello; Belfiori, 1996*) A matriz geradora $\boldsymbol{G}_{\mathfrak{a}}$ do reticulado $\Lambda_{\mathfrak{a}}$ é obtida a partir da matriz geradora $\boldsymbol{G}$ do reticulado Λ pela aplicação da matriz mudança de base T entre as $\mathbb{Z}$-bases de $\mathfrak{a}$ e $\mathbb{A}_{\mathbb{K}}$, isto é, $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$.*

Demonstração. O resultado segue diretamente da fórmula $\gamma_i = \sum_{k=1}^{n} t_{ik} w_k$, que também é válido tomando as partes real e imaginária de ambos os lados $\sigma_j(\gamma_i) = \sum_{k=1}^{n} \sigma_j(t_{ik} w_k) = \sum_{k=1}^{n} t_{ik} \sigma_j(w_k)$, e isto conclui a demonstração. ∎

Da igualdade $G_{\mathfrak{a}} = TG$ temos que $\det G_{\mathfrak{a}} = \det T \cdot \det G$, o que significa que

$$Vol(\Lambda_{\mathfrak{a}}) = |\det T| \cdot Vol(\Lambda).$$

Se $\mathfrak{a}$ é um ideal principal, isto é, $\mathfrak{a} = \alpha\mathbb{A}_{\mathbb{K}}$ então a matriz mudança de base é dada por $T = R(\alpha)$. A $\mathbb{Z}$-base do ideal principal $\mathfrak{a} = \alpha\mathbb{A}_{\mathbb{K}}$ é o conjunto $\{\alpha w_i,\ i = 1, \cdots, n\}$. Assim podemos escrever

$$\alpha \cdot \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = R(\alpha) \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}.$$

A procura de reticulados rotacionados da Tabela (5.3.3) com dimensão n e diversidade $n/2$ segue os seguintes passos:

1. Calcule o polinômio minimal de ζ_n sobre $\mathbb{Q}$ que tem grau $\phi(n)$.

2. Encontre todos os ideais $\mathfrak{a}$ de $\mathbb{A}_{\mathbb{K}}$ com norma inteira.

3. Usando a matriz mudança de base T, calcule a matriz geradora $G_{\mathfrak{a}} = TG$ e avalie os parâmetros dos reticulados, por exemplo, a densidade de centro e o número de vizinhos. Se eles são iguais aos parâmetros de D_4, E_6, E_8, Λ_{12}, Λ_{16} ou Λ_{24}, então obtemos uma versão rotacionada destes reticulados pois tais reticulados são os únicos com tais parâmetros.

   Este procedimento é aplicado sucessivamente para obter uma matriz geradora para cada um dos reticulados presentes na Tabela (5.3.3).

   Alguns reticulados conhecidos dos corpos ciclotômicos:

	$\mathbb{Q}(\theta)$	n	Ideais
$D_{4,2}$	θ^4+1	8	$(2,\theta+1)$
$E_{6,3}$	$\theta^6-\theta^3+1$	9	$(3,(\theta+1)^2)$
$E_{8,4}$	$\theta^8-\theta^6+\theta^4-\theta^2+1$	20	$(5,\theta-2)$
$K_{12,6}$	$\theta^{12}-\theta^{11}+\theta^9-\theta^8+\theta^6-\theta^4+\theta^3-\theta+1$	21	$(7,\theta+3)$
$\Lambda_{16,8}$	$\theta^{16}-\theta^{12}+\theta^8-\theta^4+1$	40	$(2,\theta^4+\theta^3+\theta^2+\theta+1)$ $(5,\theta^2+2)$
$\Lambda_{24,12}$	$\theta^{24}-\theta^{23}+\theta^{21}-\theta^{20}+\theta^{18}-\theta^{17}+\theta^{15}-\theta^{14}+$ $+\theta^{12}-\theta^{10}+\theta^9-\theta^7+\theta^6-\theta^4+\theta^3-\theta+1$	39	$(3,\theta^3+\theta^2-1)$ $(3,\theta^3+\theta^2+\theta+1)$ $(13,\theta-3)$

Tabela (5.3.3)

Exemplo 5.4.1. *(Construção de $D_{4,2}$). Note que $\phi(8)=4$ e que para outros valores de n tal que $\phi(n)=4$ não resultam na versão rotacionada de D_4, cuja densidade de centro é 1/8. O polinômio minimal de $\theta=\zeta_8$ sobre $\mathbb{Q}$ é dado na Tabela (5.3.2), o discriminante absoluto do corpo $\mathbb{K}=\mathbb{Q}(\zeta_8)$ é $D_{\mathbb{K}}=2^8$, $r_1=0$ e $r_2=2$. Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a})=\frac{2^{4/2}}{\sqrt{2^8}}\frac{\rho^4}{\frac{1}{8}}=2^3\rho^4,$$

e para $N(\mathfrak{a})=2$ devemos tomar $\rho=\dfrac{1}{\sqrt{2}}$. O ideal $\mathfrak{a}$ com norma 2 pode ser obtido da fatoração do ideal primo (2), *que tem norma 2^4 do seguinte modo*

$$(2)=(2,\theta+1)^4=\mathfrak{a}^4.$$

Assim $\mathfrak{a}$ tem a norma desejada 2. A matriz geradora do reticulado é $G_{\mathfrak{a}}=TG$, onde T é a matriz da representação integral de $\mathfrak{a}$

$$T=\begin{pmatrix}2&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}$$

e $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $0.125 = \dfrac{1}{8}$ *e o número de vizinhos é* 24, *sendo exatamente como* $\boldsymbol{D}_4$. *Como* $\boldsymbol{D}_4$ *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 2.*

Exemplo 5.4.2. *(Construção de* $\boldsymbol{K}_{12,6}$*). Note que* $\phi(21) = 12$ *e que para outros valores de* n *tal que* $\phi(n) = 21$ *não resultam na versão rotacionada de* $\boldsymbol{K}_{12}$, *cuja densidade de centro é* 1/27. *O polinômio minimal de* $\theta = \zeta_{21}$ *sobre* $\mathbb{Q}$ *é dado na Tabela (5.3.2), o discriminante absoluto do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{21})$ *é* $D_{\mathbb{K}} = 3^6.7^{10}$, $r_1 = 0$ *e* $r_2 = 6$. *Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a}) = \frac{2^{12/2}}{\sqrt{3^6.7^{10}}} \frac{\rho^{12}}{\frac{1}{27}} = \frac{2^6\rho^{12}}{7^5},$$

e para $N(\mathfrak{a}) = 7$ *devemos tomar* $\rho = \dfrac{\sqrt{7}}{\sqrt{2}}$. *O ideal* $\mathfrak{a}$ *com norma 7 pode ser obtido da fatoração do ideal primo* (7), *que tem norma* 7^{12}, *ou seja,*

$$(7) = (7, \theta + 3)^6(7, \theta + 5)^6 = \mathfrak{a}_1^6\mathfrak{a}_2^6.$$

Como $N(\mathfrak{a}_1) = N(\mathfrak{a}_2) = 7$, *podemos escolher* $\mathfrak{a} = \mathfrak{a}_1$, *que tem a norma desejada. A matriz geradora do reticulado é* $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$, *onde* $\boldsymbol{T}$ *é a matriz da representação integral de* $\mathfrak{a}$

$$T = \begin{pmatrix} 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

e $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $\frac{1}{27}$ *e o número de vizinhos é* 756, *sendo exatamente como* $\boldsymbol{K}_{12}$. *Como* $\boldsymbol{K}_{12}$ *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 6.*

Exemplo 5.4.3. *(Construção de* $\Lambda_{16,8}$*). Note que* $\phi(40) = 16$ *e que para outros valores de* n *tal que* $\phi(n) = 16$ *não resultam na versão rotacionada de* Λ_{16}, *cuja densidade de centro é* 1/16. *O polinômio minimal de* $\theta = \zeta_{40}$ *sobre* $\mathbb{Q}$ *é dado na Tabela (5.3.2), o discriminante absoluto do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{40})$ *é* $D_{\mathbb{K}} = 2^{32}.5^{12}$, $r_1 = 0$ *e* $r_2 = 8$. *Pela Equação* (3.4) *temos que*

$$N(\mathfrak{a}) = \frac{2^{16/2}}{\sqrt{2^{32}.5^{12}}} \frac{\rho^{16}}{\frac{1}{16}} = \frac{\rho^{16}}{5^6.2^4},$$

e para $N(\mathfrak{a}) = 2^4.5^2$ *devemos tomar* $\rho = \sqrt{2.5}$. *O ideal* $\mathfrak{a}$ *com tal norma pode ser obtido da fatoração dos ideais* (2) *e* (5) *que tem*

norma 2^{16} *e* 5^{16}, *respectivamente. Assim*

$$(2) = (2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)^4 = \mathfrak{a}_1^4$$
$$(5) = (5, \theta^2 + 2)^4 (5, \theta^2 + 3)^4 = \mathfrak{a}_2^4 \mathfrak{a}_3^4.$$

Como, $N(\mathfrak{a}_1) = 2^4$, $N(\mathfrak{a}_2) = 5^2$, $N(\mathfrak{a}_3) = 5^2$, *podemos escolher* $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ *que tem a norma desejada* $N(\mathfrak{a}) = N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2) = 2^4 5^2$. *A matriz geradora do reticulado é* $\boldsymbol{G}_{\mathfrak{a}} = \boldsymbol{TG}$, *onde* $\boldsymbol{T}$ *é a matriz da representação integral de* $\mathfrak{a}$ *e* $\boldsymbol{G}$ *é a matriz geradora de* $\sigma(\mathbb{A}_{\mathbb{K}})$. *O reticulado gerado por* $\boldsymbol{G}_{\mathfrak{a}}$ *tem densidade de centro* $0,0625$ *e o número de vizinhos é* 4320, *sendo exatamente como* Λ_{16}. *Como* Λ_{16} *é o único reticulado com estes parâmetros, obtemos sua versão rotacionada com diversidade igual a 8.*

5.5 Conclusão

Duas diferentes aproximações tem sido usadas para estudar duas famílias de reticulados com o objetivo de atingir bom desempenho sobre ambos os canais Gaussianos e Rayleigh com desvanecimento.

A primeira família é gerada pelo homomorfismo canônico sobre o anel dos inteiros de um corpo de números. Entre os reticulados desta família, demos importância aos reticulados obtidos a partir de corpos totalmente reais e totalmente complexos. Vimos que os reticulados obtidos a partir de corpos totalmente reais tem bom desempenho sobre o canal Rayleigh com desvanecimento com uma diversidade máxima n. Mas eles tem um ganho negativo sobre o canal Gaussiano causado pela sua baixa densidade de empacotamento. Os reticulados obtidos a partir de corpos totalmente complexos tem um acordo entre diversidade e densidade de empacotamento. Eles mostram um ganho positivo sobre o canal Gaussiano

e bom desempenho sobre o canal Rayleigh com desvanecimento com uma diversidade $\frac{n}{2}$.

A segunda família de reticulados é gerada pelo homomorfismo canônico sobre determinados ideais nos anéis dos inteiros dos corpos ciclotômicos que são corpos totalmente complexos. Esta família inclui versões dos famosos reticulados conhecidos na literatura; $\boldsymbol{D}_4$, $\boldsymbol{E}_6$, $\boldsymbol{E}_8$, $\boldsymbol{K}_{12}$, Λ_{16} e Λ_{24}. Estes reticulados atuam de modo análogo aos reticulados de diversidade $\frac{n}{2}$ sobre o canal Rayleigh e então podem atingir a diversidade de 2 até 12. Além disso, estes são os melhores reticulados para o canal Gaussiano.

O ponto importante nesta conclusão é o fato de que corpos de números com discriminante absoluto mínimos são conhecidos somente em graus menores ou iguais a 8. Assim, a diversidade de reticulados obtidos a partir de corpos totalmente reais não podem exceder 8, a menos que encontremos corpos ótimos com alto grau. Ao contrário, os reticulados da segunda família são menos limitados na diversidade, $\Lambda_{24,12}$ atinge uma diversidade 12. Naturalmente, podemos pensar em construir $\Lambda_{32,16}$ e $\Lambda_{64,32}$ que tem diversidades 16 e 32, respectivamente. Mas somos limitados pela proporção da complexidade de um sistema sobre o ganho prático. Não podemos nos esquecer também que o estudo da primeira família possibilita-nos construir e entender a segunda família.

Referências bibliográficas

ALENCAR FILHO, E. de. *Teoria elementar dos números*. 3.ed. São Paulo: Livraria Nobel, 1992.

BERTOLDI, T. C. *Constelações e códigos sobre corpos numéricos quadráticos*. São José do Rio Preto, 2003. Dissertação (Mestrado) – Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

BOUTROS, J.; VITERBO, E.; RASTELLO, C.; BELFIORI, J. C. Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels. *IEEE Trans. Inform. Theory*, v.42, n.2, March, 1996.

CONWAY, J. H.; N. J. A. *Sphere Packings, Lattices and Groups*. New York: Springer, 1999.

CRAIG, M. Extreme Forms and Cyclotomy. *Mathematika*, v.25, p.44-56, 1978a.

_____. A Cyclotomic Construction for Leech's Lattice. *Mathematika*, v.25, p.236-41, 1978b. ENDLER, O. *Teoria dos números algébricos*. IMPA: Rio de Janeiro, 1986.

FLORES, A. L. *Representação geométrica de ideais de corpos de números*. Campinas, 1996. Dissertação (Mestrado) – Instituto de Matemática, Estatística e Computação Científica (IMECC), Universidade de Campinas.

_____. *Reticulados em corpos abelianos*. Campinas, 2000. Tese (Doutorado) – Faculdade de Engenharia Elétrica e de Computação (FEEC), Universidade de Campinas.

FLORES, A. L.; NÓBREGA, T. P. Lattices in Abelian Fields. In: VII ENCONTRO EM ÁLGEBRA (ENAL) USP-UNICAMP. *Atas...*, jul. 1999, p.43-52.

GIRAUD, X.; BELFIORI, J. C. Constellations Matched to the Rayleigh Fading Channel. *IEEE Trans. Inform. Theory*, v.42, n.1, p.106-15, January 1996.

HERSTEIN, I. N. *Tópicos de álgebra*. São Paulo: Editora Polígono, 1970.

LANG, S. *Algebraic Number Theory*. Boston: Addison-Wesley Publishing Company, 1970.

_____. *Álgebra*. Boston: Addison-Wesley Publishing Company, 1972.

MARCUS, D. A. *Number Fields*. Berlin: Springer-Verlag, 1977.

RIBEIRO, A. C. *Reticulados sobre corpos de números*. São José do Rio Preto, 2003. Dissertação (Mestrado) – Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

RIBENBOIM, P. *Algebraic Numbers*. New Jersey: Wiley-Interscience, 1972.

RODRIGUES, T. M. Cúbicas Galoisianas. São José do Rio Preto, 2003. Dissertação (Mestrado) – Instituto de Biociências,

Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

SAMUEL, P. *Algebraic Theory of Numbers*. Paris: Hermana, 1967.

SHANNON, C. E. A Mathematical Theory of Communications. *BSTJ*, v.27, p.379-423 e 623-56, 1948.

SILVA, C. V. *Reticulados de Posto 4 em corpos de números*. São José do Rio Preto, 2001. Dissertação (Mestrado) – Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

SIMONATO, A. L. *Reticulados em corpos ciclotômicos*. São José do Rio Preto, 2000. Dissertação (Mestrado) – Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

STEWART, I.; TALL, D. *Algebraic Number Theory*. New York: Chapman & Hall, 1987.

VICENTE, J. P. G. *Reticulados de Posto 3 em corpos de números*. São José do Rio Preto, 2000. Dissertação (Mestrado) – Instituto de Biociências, Letras e Ciências Exatas (Ibilce), Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp).

WASHINGTON, L. C. *Introduction to Ciclotomic Fields*. Berlin: Springer-Verlag, 1982.

SOBRE O LIVRO

Formato: 14 x 21 cm
Mancha: 23,7 x 42,5 paicas
Tipologia: Horley Old Style 10,5/14
Papel: Off-set 75 g/m^2 (miolo)
Cartão Supremo 250 g/m^2 (capa)
1ª edição: 2014

EQUIPE DE REALIZAÇÃO

Coordenação Geral
Marcos Keith Takahashi

No presente livro, Carina Alves e Antonio Aparecido de Andrade apresentam um estudo sobre resultados envolvendo corpos de números, com ênfase nos corpos ciclotômicos.

Inicialmente os autores introduzem os resultados básicos de teoria algébrica dos números, tais como módulo, inteiro algébrico, anel dos inteiros algébricos, norma e traço de um elemento, discriminante, base integral, formas quadráticas, decomposição de ideais primos em uma extensão, anel oetheriano e de Dedekind.

Em uma segunda etapa, apresentam um estudo sobre reticulados, empacotamento esférico, volume, densidade de centro e o homomorfismo canônico (ou de Minkowski) para a obtenção de reticulados via representação geométrica de ideais dos anéis de inteiros algébricos.

Finalmente, fazendo uso desse homomorfismo, os autores constróem, via anel dos inteiros dos corpos ciclotômicos, reticulados rotacionados nas dimensões 4, 12, 16 e 24 com densidade de centro ótima e que são eficientes para ambos os canais Gaussianos e com desvanecimento do tipo Rayleigh.

Carina Alves é graduada (2002) e mestre em Matemática (2005) pela Universidade Estadual Paulista (Unesp), *campus* de São José do Rio Preto. Possui doutorado em Matemática (2008) pelo Instituto de Matemática e Computação Científica (Imecc) da Universidade Estadual de Campinas (Unicamp) e pós-doutorado (2012) pela Telecom ParisTech (Paris). Trabalha desde 2009 na Unesp, *campus* de Rio Claro. Tem experiência na área de Álgebra, atuando principalmente em teoria algébrica dos números e reticulados.

Antonio Aparecido de Andrade é graduado em Matemática (1984) pelo Instituto de Biociências, Letras e Ciências Exatas (Ibilce) da Unesp, *campus* de São José do Rio Preto, mestre em Matemática (1988) pelo Imecc da Unicamp, doutor em Engenharia Elétrica (1996) pela Faculdade de Engenharia Elétrica e de Computação (Feec) da Unicamp e livre-docente em Matemática (2008) pela Unesp. Trabalha na área de Álgebra com, aplicações em códigos e reticulados.

editora unesp DIGITAL