UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de São José do Rio Preto

Reticulados Algébricos via Corpos Abelianos

Agnaldo José Ferrari

Orientador: Prof. Dr. Antonio Aparecido de Andrade

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

São José do Rio Preto - SP

Fevereiro - 2008

Prof. Dr. Aide

Reticulados Algébricos via Corpos Abelianos

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

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
dooP-Se
IBILCE-UNESP-S

dooP-Se

aareAtoadsProf. Dr.

À meu pai Ambrósio Ferrari (in memoriam),
dedico.

Agradecimentos

Ao concluir este trabalho agradeço:

À Deus.

À minha esposa Renata, pela paciência, pelo amor, apoio e incentivo durante o curso de graduação e pós-graduação, e por me ajudar a superar os momentos de dificuldades nestes 10 anos de união conjugal.

Ao Prof. Dr. Antonio Aparecido de Andrade, pela amizade, paciência e dedicação durante a orientação e principalmente pela confiança e liberdade, que foram primordiais para o desenvolvimento deste trabalho.

À minha mãe Evanira e a meu irmão Vilmosnei, pelo apoio durante toda essa caminhada.

À meu tio Orizanir, pelo apoio, incentivo e por estar sempre torcendo por mim.

Aos meus colegas do curso de Pós-Graduação, pelo agradável convívio, pelos risos sempre presentes que me ajudaram a superar os momentos difíceis.

À banca examinadora.

À FAPESP, pelo apoio financeiro.

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

Valeu a pena? Tudo vale a pena
Se a alma não é pequena.

Trecho do poema *Mar Português* - Fernando Pessoa.

Sumário

Índices 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

$\mathbb{L}, \mathbb{K}, \mathbb{M}, \mathbb{F}, \mathbb{T}, ¢¢¢$: corpos

$\mathbb{L}/\mathbb{K}$: $\mathbb{L}$ é uma extensão de $\mathbb{K}$

$dim_{\mathbb{K}}\mathbb{L}$: dimensão de $\mathbb{L}$ como espaço vetorial sobre $\mathbb{K}$

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

R_f: raízes do polinômio f

$\mathbb{K}(\alpha_1, ¢¢¢\ , \alpha_n)$: corpo obtido pela adjunção de $\alpha_1, ¢¢¢\ , \alpha_n$ a $\mathbb{K}$

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

$Aut(\mathbb{L})$: conjunto dos automorfismos de $\mathbb{L}$

$ker(f)$: núcleo do homomorfismo f

$\mathbb{Z}_n^*$: grupo multiplicativo das classes de restos módulo n

$\pm(x)$: ordem do elemento x

$min(X)$: minímo do conjunto X

$a \mid b$: a divide b

$\pm(X)$: cardinalidade do conjunto X

Df: derivada do polinômio f

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

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

∂f: grau do polinômio f

$\underline{x} = (x_1, \cdots, x_n) \in \mathbb{R}^n$

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

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

$\mathfrak{B}$: anel dos inteiros algébricos

$O_{\mathbb{L}}$: anel dos inteiros algébricos do corpo de números $\mathbb{L}$

(a_{ij}): matriz

$detA$: determinante da matriz A.

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

$\mathfrak{D}_{\mathbb{L}}$: discriminante do corpo $\mathbb{L}$

$\mathsf{A}, \mathsf{B}, \mathsf{P}, ¢¢¢$: ideais

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

$\zeta_n : e^{\frac{2 \downarrow i}{n}} = cos\frac{2\Pi}{n} + isen\frac{2\Pi}{n}$, raiz n-ésima da unidade

$\sum$: somatório

$\prod$: produtório

H: reticulado

$Disc(\mathsf{H})$: discriminante do reticulado H

$\Delta(\mathsf{H})$: densidade de empacotamento do reticulado H

$\delta(\mathsf{H})$: densidade de centro do reticulado H

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

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

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

$\mu(n)$: função de Möbius para o inteiro n

$[x]$: inteiro mais próximo de x

$\mathsf{d}x\mathsf{e}$: inteiro mais próximo de x, maior do que ou igual a x

$\mathsf{b}x\mathsf{c}$: inteiro mais próximo de x, menor do que ou igual a x

Resumo

Dado um ideal A do anel dos inteiros algébricos de um corpo de números, tem-se que a imagem deste ideal via o homomorfismo de Minkowski é um reticulado no $\mathbb{R}^n$, chamado de reticulado algébrico. Deste modo, o principal objetivo do presente trabalho é a construção de reticulados algébricos no $\mathbb{R}^n$ que sejam versões rotacionadas de reticulados conhecidos na literatura, e trabalhamos de modo particular até a dimensão 8. Além disso, vimos também reticulados obtidos via perturbações do homomorfismo de Minkowski.

Palavras-chave: reticulados, reticulados algébricos, empacotamento esférico, densidade de empacotamento e densidade de centro.

Abstract

We stablished that the image of an ideal A of the algebraic integer ring of a number field by the Minkowski homomorphism is a lattice in $\mathbb{R}^n$, named algebraic lattice. In this way, the main goal of this work is the construction of algebraic lattices in $\mathbb{R}^n$ that be rotated versions of known lattices in the literature, and particularly we worked in dimensions up to 8. We also studied lattices obtained by perturbations of Minkowski homomorphism.

Keywords: lattices, algebraic lattices, sphere packing, density of packing and center density.

Introdução

Entendemos por empacotamente esférico a disposição de esferas de mesmo raio no espaço euclidiano n-dimensional de tal modo que a intersecção de duas delas tenha no máximo um ponto.

Um problema associado ao empacotamento esférico é o de dispor essas esferas no espaço, de modo que elas ocupem a maior fração desse espaço, ou seja, que esta distribuição tenha alta densidade.

Devido à importância dessa questão, durante o *Congresso Internacional de Matemática* em Paris no ano de 1900, David Hilbert citou-a como sendo o 18º Problema de uma seleta lista de desafios que viriam ocupar destaque no desenvolvimento da ciência moderna.

Dentre os empacotamentos esféricos, aqueles cujo conjunto de centros das esferas constituía um subgrupo discreto do $\mathbb{R}^n$, despertaram particular interesse e passaram a se chamar empacotamentos reticulados.

Em 1948 com a publicação do artigo de Claude E. Shannon, ficou estabelecido que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes. A partir daí, passaram-se a associar o estudo dos códigos ao dos reticulados. Com isso, o interesse pelo 18º Problema de David Hilbert aumentou consideravelmente, surgiram várias famílias de reticulados, cada uma delas visando dar uma melhor contribuição no que diz respeito à densidade de empacotamento.

Dentre tais modelos, destaca-se o descrito por Hermann Minkowski, chamado método algébrico baseado na Teoria Algébrica dos Números, o qual utilizaremos neste trabalho.

Tal modelo consiste de um corpo de números $\mathbb{L}$ de grau n e o seu anel de inteiros algébricos $\mathcal{O}_{\mathbb{L}}$, de onde obtém-se um homomorfismo de $\mathbb{L}$ em $\mathbb{R}^n$, com o auxílio dos n monomorfismos de $\mathbb{L}$ em $\mathbb{C}$, de modo que a imagem de um ideal $\mathcal{A}$ não nulo de $\mathcal{O}_{\mathbb{L}}$ é um reticulado de posto n no $\mathbb{R}^n$, chamado realização geométrica do ideal $\mathcal{A}$.

O cálculo da densidade de centro de tal reticulado é feito a partir do discriminante do corpo, da norma do ideal e da minimização de uma forma quadrática com entradas inteiras oriunda de uma função traço. Assim, utilizamos ferramentas da Teoria Algébrica dos Números para calcular a densidade de centro de reticulados gerados pelo homomorfismo de Minkowski.

O presente trabalho tem por objetivo estudar os reticulados do $\mathbb{R}^n$ obtidos via o

homomorfismo de Minkowski, enfocando os seus principais parâmetros: região fundamental, empacotamento esférico, densidade de empacotamento e densidade de centro. Para tanto o trabalho se divide da seguinte maneira.

No Capítulo 1, fazendo uso das referências [1] a [5], apresentamos conceitos básicos, juntamente com alguns resultados, de tópicos importantes para o desenvolvimento do nosso trabalho. Fizemos um estudo sobre módulos, resultados básicos sobre teoria de Galois, o grupo $\mathbb{Z}_n^*$ e formas quadráticas sobre o $\mathbb{R}^n$.

No Capítulo 2, fazendo uso das referências [1], [2] e [7] a [11], destinado aos leitores com menos conhecimentos em Teoria Algébrica dos Números, apresentamos conceitos e notações que foram usados no desenvolvimento dos demais capítulos. Fizemos um estudo de norma e traço, inteiros algébricos, discriminante, norma de um ideal, corpos quadráticos, corpos ciclotômicos e apresentamos também a decomposição de um ideal em uma extensão.

No Capítulo 3, fazendo uso da referência [12], apresentamos as definições de reticulado, empacotamento esférico e algumas famílias de reticulados conhecidos na literatura.

No Capítulo 4, fazendo uso das referências [1] e [20], apresentamos o homomorfismo de Minkowski, que é um método de gerar reticulados no $\mathbb{R}^n$, com a vantagem de serem reticulados manipuláveis, ao contrário dos reticulados apresentados no Capítulo 3 - Seção 4.

No Capítulo 5, fazendo uso das referências [5] e [13], apresentamos um estudo das formas quadráticas via o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ e seu subcorpo maximal, e via $\mathbb{Q}(\zeta_p)$, onde p é primo, e seus subcorpos. Essas formas quadráticas são essenciais para o cálculo do raio de empacotamento de reticulados gerados a partir desses corpos e subcorpos. Destacamos ainda que, a forma quadrática sobre o subcorpo maximal de $\mathbb{Q}(\zeta_n)$, deu origem a [16].

No Capítulo 6, apresentamos um estudo dos reticulados gerados a partir de duas perturbações do homomorfismo de Minkowski, e das relações entre elas, sempre com o intuito de construir reticulados de alta densidade. Destacamos que, o estudo das perturbações do homomorfismo de Minkowski com relação ao parâmetro densidade de centro, que é apresentado neste capítulo, é um estudo original.

No Capítulo 7p(p(p2 4675TD[(fo23(c66)-445(defi)1(n)1ra)1(d)14675-524(67)-485(Cap)110(´)380(ı)

Capítulo

1

Conceitos básicos

1.1 Introdução

O objetivo deste capítulo é apresentar alguns conceitos que serão indispensáveis ao desenvolvimento do nosso trabalho. Desse modo, na Seção 1.2, apresentamos os conceitos e propriedades de módulos. Na Seção 1.3, apresentamos algumas definições referentes à teoria de Galois e um resultado importante sobre extensões galoisianas. Na Seção 1.4, o objetivo é encontrar os valores de n para os quais o grupo $\mathbb{Z}_n^*$ é cíclico, e na Seção 1.5, apresentamos as formas quadráticas sobre o $\mathbb{R}^n$, cuja aplicação se faz quando tentamos determinar o raio de empacotamento de reticulados algébricos.

1.2 Módulos

O objetivo desta seção é apresentar o conceito de módulo, juntamente com suas principais propriedades.

Definição 1.2.1 *Seja A um anel comutativo com unidade. Um A-módulo é um grupo abeliano M, juntamente com uma aplicação $\varphi : A \pounds M \ ¡ ! \ M$, denotada por $(a, m) \ ¡ ! \ am$, tal que, quaisquer que sejam os elementos $a, b \ 2 \ A$ e $m, n \ 2 \ M$, tem-se:*

1. $(a + b)m = am + bm$,
2. $a(m + n) = am + an$,
3. $(ab)m = a(bm)$,
4. $1m = m$.

Definição 1.2.2 *Dizemos que um A-módulo M é um A-módulo livre quando existe uma família $(x_i)_{i \in I}$ de elementos de M, satisfazendo as seguintes condições:*

1. *A família* $(x_i)_{i \in I}$ *é linearmente independente.*

2. *Todo elemento* $x \in M$ *é uma combinação linear da família* $(x_i)_{i \in I}$.

Uma família satisfazendo as condições da Definição 1.2.2 é chamada uma base do A-módulo livre, onde o número de elementos da base é chamado o posto de M. Se I é um conjunto finito, dizemos que o A-módulo M é finitamente gerado, ou do tipo finito.

Definição 1.2.3 *Sejam* A *um anel,* M *um* A*-módulo e* $N \subseteq M$, $N \neq \emptyset$, *um subconjunto. Dizemos que* N *é um submódulo do* A*-módulo* M*, se:*

1. N *é um subgrupo de* M.

2. $(\forall a \in A)\,(\forall n \in N) \;\Rightarrow\; an \in N$.

Teorema 1.2.1 ([1]) *Se* A *é um anel principal,* M *um* A*-módulo livre de posto* n*, e* N *um* A*-submódulo de* M*, então*

1. N *é livre de posto* q, $0 \leq q \leq n$.

2. *Se* $N \neq \{0\}$, *então existe uma base* $\{e_1, \ldots, e_n\}$ *de* M *e elementos não nulos* $a_1, \ldots, a_q \in A$ *tais que* $\{a_1 e_1, \ldots, a_q e_q\}$ *é uma base de* N*, e que* a_i *divide* a_{i+1}*, para todo* $1 \leq i \leq q - 1$.

1.3 Teoria de Galois

Nesta seção apresentamos alguns conceitos importantes da teoria de Galois.

Definição 1.3.1 *Se* $\mathbb{K} \subseteq \mathbb{L}$ *são corpos, tal que* $dim_{\mathbb{K}}\mathbb{L} = n$*, então* $\mathbb{L}$ *é chamado uma extensão do corpo* $\mathbb{K}$*, denotamos* $\mathbb{L}/\mathbb{K}$*, e* n *é chamado o grau de* $\mathbb{L}$ *sobre* $\mathbb{K}$.

Definição 1.3.2 *Sejam* $\mathbb{L}$ *uma extensão de* $\mathbb{K}$ *e* $\alpha \in \mathbb{L}$. *Dizemos que* α *é algébrico sobre* $\mathbb{K}$*, se existe um polinômio não nulo* $f(x) \in \mathbb{K}[X]$ *tal que* $f(\alpha) = 0$.

Definição 1.3.3 *Um número complexo* α *é chamado número algébrico se for algébrico sobre* $\mathbb{Q}$*, isto é, se existe um polinômio não nulo* $f(x)$ *com coeficientes racionais tal que* $f(\alpha) = 0$.

Definição 1.3.4 *Seja* $\mathbb{L}$ *um corpo, tal que* $\mathbb{Q} \subseteq \mathbb{L}$. *Dizemos que* $\mathbb{L}$ *é um corpo de números se* $dim_{\mathbb{Q}}\mathbb{L} = n$*, e* n *é chamado o grau de* $\mathbb{L}$ *sobre* $\mathbb{Q}$.

Teorema 1.3.1 ([2]) *Se* $\mathbb{L}$ *é um corpo de números, então* $\mathbb{L} = \mathbb{Q}(\theta)$ *para algum número algébrico* $\theta \in \mathbb{L}$.

Teorema 1.3.2 ([2]) *Se $\mathbb{L} = \mathbb{Q}(\theta)$ é um corpo de números de grau n sobre $\mathbb{Q}$, então existem exatamente n monomorfismos distintos $\sigma_i : \mathbb{L} \to \mathbb{C}$, $i = 1, 2, \ldots, n$. Os elementos $\sigma_i(\theta) = \theta_i$ são os zeros em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.*

Definição 1.3.5 *Sejam $\mathbb{L}$ uma extensão de $\mathbb{K}$ e $f \in \mathbb{K}[X]$. Dizemos que $\mathbb{L}$ é um corpo de raízes de f se $\mathbb{L}$ é o menor corpo contendo $\mathbb{K}$ e todas as raízes de f. Denotamos $\mathbb{L}$ por $\mathbb{L} = \mathbb{K}(R_f)$.*

Definição 1.3.6 *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma extensão galoisiana sobre $\mathbb{K}$ se $\mathbb{L} = \mathbb{K}(R_f)$, para algum $f \in \mathbb{K}[X]$ separável.*

Definição 1.3.7 *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é dado por*

$$Gal(\mathbb{L}/\mathbb{K}) = \{\sigma \in Aut(\mathbb{L});\ \sigma(x) = x,\ \forall x \in \mathbb{K}\}.$$

Definição 1.3.8 *Sejam $\mathbb{L}$ uma extensão finita sobre $\mathbb{K}$ e $H \subset Aut(\mathbb{L})$. O corpo*

$$\mathbb{L}^H = \{\alpha \in \mathbb{L} :\ \sigma(\alpha) = \alpha,\ \forall \sigma \in H\},$$

é chamado de corpo fixo pelo conjunto H.

Proposição 1.3.1 ([3]) *Se $\mathbb{M}$ e $\mathbb{F}$ são extensões Galoisianas sobre $\mathbb{K}$ tais que $\mathbb{M}$ e $\mathbb{F}$ são subcorpos de algum outro corpo, então:*

1. *$\mathbb{MF}/\mathbb{F}$ é uma extensão galoisiana.*
2. *$\mathbb{M}/\mathbb{M} \cap \mathbb{F}$ é uma extensão galoisiana.*
3. *Se H é o grupo de Galois de $\mathbb{MF}$ sobre $\mathbb{F}$, G é o grupo de Galois de $\mathbb{M}$ sobre $\mathbb{K}$ e $\sigma \in H$, então a restrição de σ a $\mathbb{M}$ pertence a G, e a aplicação $\sigma \mapsto \sigma|_{\mathbb{M}}$ nos dá um isomorfismo de H no grupo de Galois de $\mathbb{M}$ sobre $\mathbb{M} \cap \mathbb{F}$.*

Demonstração:
(**1**) Se $\mathbb{M}/\mathbb{K}$ e $\mathbb{F}/\mathbb{K}$ são extensões Galoisianas, então por definição $\mathbb{M} = \mathbb{K}(R_f)$ para algum $f(x) \in \mathbb{K}[X]$ separável e $\mathbb{F} = \mathbb{K}(R_g)$ para algum $g(x) \in \mathbb{K}[X]$ separável. Assim, $\mathbb{MF} = \{mn;\ m \in \mathbb{K}(R_f) \text{ e } n \in \mathbb{K}(R_g)\}$. Se $h(x) = f(x)g(x)$, então $R_h = R_f \cup R_g$. Agora, temos os seguintes fatos:
(**a**) $R_f \cap R_g = \emptyset$. Como f e g são separáveis, segue que f e g possuem raízes distintas. Logo h possui raízes distintas, ou seja, h é separável. Além disso, temos que

$$\mathbb{K}(R_h) = \mathbb{K}(R_f \cup R_g) = \mathbb{K}(R_f, R_g) = \mathbb{K}(R_f)(R_g),$$

$\mathbb{K}(R_f) \subset \mathbb{K}(R_f)(R_g)$ e $R_g \in \mathbb{K}(R_f)(R_g)$. Como $1 \in \mathbb{K}(R_f)$ segue que $\mathbb{K}(R_f) = \{m.1;\ m \in \mathbb{K}(R_f) \text{ e } 1 \in \mathbb{K}(R_g)\} \subset \mathbb{MF}$. Como $R_g = 1.R_g$, onde $1 \in \mathbb{K}(R_f)$ e $R_g \in \mathbb{K}(R_g)$, segue que $R_g \subset \mathbb{MF}$. Mas $\mathbb{K}(R_f)(R_g)$ é o menor corpo contendo R_g e $\mathbb{K}(R_f)$, e como $\mathbb{MF}$ contém R_g e $\mathbb{K}(R_f)$, segue que

$$\mathbb{K}(R_f)(R_g) \subset \mathbb{MF}. \tag{1.3.1}$$

Agora, se $x \in \mathbb{MF}$, então $x = mn$, onde $m \in \mathbb{K}(R_f)$ e $n \in \mathbb{K}(R_g)$. Mas como $\mathbb{K}(R_f) \subset \mathbb{K}(R_f)(R_g)$ e $\mathbb{K}(R_g) \subset \mathbb{K}(R_f)(R_g)$, segue que $m, n \in \mathbb{K}(R_f)(R_g)$. Logo $x = mn \in \mathbb{K}(R_f)(R_g)$, e portanto

$$\mathbb{MF} \subset \mathbb{K}(R_f)(R_g). \tag{1.3.2}$$

Das Equações (1.3.1) e (1.3.2) concluímos que $\mathbb{MF} = \mathbb{K}(R_f)(R_g) = \mathbb{K}(R_h)$, onde $h(x) \in \mathbb{K}[X]$ é separável. Logo $\mathbb{MF}/\mathbb{K}$ é uma extensão galoisiana, e como $\mathbb{K} \subset \mathbb{F} \subset \mathbb{MF}$, segue que $\mathbb{MF}/\mathbb{F}$ é uma extensão galoisiana.

(**b**) $R_f \setminus R_g \neq \emptyset$. Se $R_f \setminus R_g = \{\alpha_1, \alpha_2 \ldots, \alpha_t\}$, então $R_f = \{\alpha_1, \alpha_2 \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_m\}$ e $R_g = \{\alpha_1, \alpha_2 \ldots, \alpha_t, \gamma_1, \gamma_2, \ldots, \gamma_n\}$, onde $\beta_i \neq \gamma_j$ para $i = 1, 2, \ldots, m$ e $j = 1, 2, \ldots, n$. Temos que

$$\mathbb{M} = \mathbb{K}(R_f) = \mathbb{K}(\alpha_1, \alpha_2 \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_m) = \mathbb{T}(\beta_1, \beta_2, \ldots, \beta_m),$$

$$\mathbb{F} = \mathbb{K}(R_g) = \mathbb{K}(\alpha_1, \alpha_2 \ldots, \alpha_t, \gamma_1, \gamma_2, \ldots, \gamma_n) = \mathbb{T}(\gamma_1, \gamma_2, \ldots, \gamma_n),$$

onde $\mathbb{T} = \mathbb{K}(\alpha_1, \alpha_2 \ldots, \alpha_t)$. Como $\mathbb{M}/\mathbb{K}$ e $\mathbb{F}/\mathbb{K}$ são extensões galoisianas e $\mathbb{K} \subset \mathbb{T} \subset \mathbb{M}$, $\mathbb{K} \subset \mathbb{T} \subset \mathbb{F}$, segue que $\mathbb{M}/\mathbb{T}$ e $\mathbb{F}/\mathbb{T}$ são extensões galoisianas, ou seja, existem $\tilde{f}(x), \tilde{g}(x) \in \mathbb{T}[X]$ separáveis, tais que $\mathbb{M} = \mathbb{T}(R_{\tilde{f}})$ e $\mathbb{F} = \mathbb{T}(R_{\tilde{g}})$, assim, $\mathbb{T}(R_{\tilde{f}}) = \mathbb{T}(\beta_1, \beta_2, \ldots, \beta_m)$ e $\mathbb{T}(R_{\tilde{g}}) = \mathbb{T}(\gamma_1, \gamma_2, \ldots, \gamma_n)$. Neste caso, temos que $R_{\tilde{f}} \setminus R_{\tilde{g}} = \emptyset$, pois caso contrário teríamos $\beta_i = \gamma_j$, para algum $i =, 2, \ldots, m$ e $j = 1, 2, \ldots, n$, o que seria um absurdo. Tomando $\tilde{h}(x) = \tilde{f}(x)\tilde{g}(x) \in \mathbb{T}[X]$ temos que $\mathbb{T}(R_{\tilde{h}}) = \mathbb{T}(R_{\tilde{f}})(R_{\tilde{g}})$, onde $\tilde{h}(x)$ é separável em seu corpo de raízes. Usando raciocínio análogo ao ítem (**a**), concluímos que $\mathbb{MF}/\mathbb{T}$ é uma extensão galoisiana e como $\mathbb{T} \subset \mathbb{F} \subset \mathbb{MF}$, segue que $\mathbb{MF}/\mathbb{F}$ é uma extensão galoisiana.

(**2**) Temos por hipótese que $\mathbb{M}/\mathbb{K}$ é uma extensão galoisiana, e como $\mathbb{K} \subset \mathbb{M} \setminus \mathbb{F} \subset \mathbb{M}$, segue que $\mathbb{M}/\mathbb{M} \setminus \mathbb{F}$ é uma extensão galoisiana.

(**3**) Temos que $H = \{\sigma \in Aut(\mathbb{MF});\ \sigma(x) = x,\ \forall x \in \mathbb{F}\}$. Assim dado $\sigma \in H$, a restrição de σ a $\mathbb{M}$, fixa os elementos de $\mathbb{F}$ que estão em $\mathbb{M}$, ou seja, fixa $\mathbb{K} \subset \mathbb{M} \setminus \mathbb{F}$. Logo $\sigma\jmath_{\mathbb{M}}$ pertence a $G = \{\sigma \in Aut(\mathbb{M});\ \sigma(x) = x,\ \forall x \in \mathbb{K}\}$. Agora, definimos

$$\begin{aligned} \rho : H &\to Gal(\mathbb{M}/\mathbb{M} \setminus \mathbb{F}) \\ \sigma &\mapsto \sigma\jmath_{\mathbb{M}} \end{aligned}$$

Se $\sigma, \psi \in H$, então $\sigma \pm \psi$ é um homomorfismo, pois σ e ψ são homomorfismos. Logo $(\sigma \pm \psi)\jmath_{\mathbb{M}}$ é um homomorfismo, e portanto ρ é homomorfismo. Além disso, temos que

$$Ker(\rho) = \{\sigma \in H;\ \rho(\sigma) = id_{Gal(\mathbb{M}/\mathbb{M}\cap\mathbb{F})}\} = \{\sigma \in H;\ \sigma\jmath_{\mathbb{M}} = id_{Gal(\mathbb{M}/\mathbb{M}\cap\mathbb{F})}\} = id_H,$$

pois id_H é o único isomorfismo de H que restrito a $\mathbb{M}$ nos dá a identidade de $Gal(\mathbb{M}/\mathbb{M} \setminus \mathbb{F})$. Portanto, ρ é injetora. Para a sobrejetora, se $H' = Im(\rho)$, então H' deixa $\mathbb{M}/\mathbb{F}$ fixo, ou seja, $\mathbb{M}/\mathbb{F} \subset \mathbb{M}^{H'}$. Reciprocamente, se $\alpha \in \mathbb{M}^{H'}$, então $\alpha \in \mathbb{M}$ é fixo por H', e portanto $\psi(\alpha) = \alpha$, $\forall \psi \in H'$. Como $H' \subset Gal(\mathbb{M}/\mathbb{M} \setminus \mathbb{F})$, segue que $\alpha \in \mathbb{M} \setminus \mathbb{F}$. Assim, $\mathbb{M}^{H'} \subset \mathbb{M} \setminus \mathbb{F}$, e daí concluímos que $\mathbb{M}^{H'} = \mathbb{M} \setminus \mathbb{F}$. Logo pela Teoria de Galois temos que $H' = Gal(\mathbb{M}/\mathbb{M} \setminus \mathbb{F})$, e portanto ρ é sobrejetora. Assim, concluímos que $\sigma \mapsto \sigma\jmath_{\mathbb{M}}$ é um isomorfismo de H em $Gal(\mathbb{M}/\mathbb{M} \setminus \mathbb{F})$. ∎

1.4 O grupo $\mathbb{Z}_n^{¤}$

O objetivo desta seção é mostrarmos para quais valores de n, o grupo $\mathbb{Z}_n^*$ é cíclico. Este resultado será muito útil na caracterização das extensões ciclotômicas cíclicas. O conteúdo desta seção está em ([3]), mas fizemos algumas adaptações nas demonstrações, assim, alguns lemas são de nossa autoria. Iniciamos com alguns resultados de grupos.

Proposição 1.4.1 ([3]) *Se x e y são dois elementos de ordens finitas de um grupo abeliano G e se $mdc(\pm(x), \pm(y)) = 1$, então $\pm(xy) = \pm(x) \pm (y)$.*

Demonstração: Tomamos $\pm(x) = a$ e $\pm(y) = b$. Como G é abeliano segue que $(xy)^{ab} = (x^a)^b(y^b)^a = e$, logo xy tem ordem finita e $\pm(xy)$ **j** ab. Por outro lado, se $(xy)^t = e$, temos:

$$e = [(xy)^t]^a = (x^a y^a)^t = y^{at},$$
$$e = [(xy)^t]^b = (x^b y^b)^t = x^{bt}.$$

Logo b **j** at e a **j** bt, e como $mdc(a, b) = 1$, segue que b **j** t e a **j** t. Assim ab **j** t, e portanto, $\pm(xy) = ab = \pm(x) \pm (y)$. ∎

Proposição 1.4.2 ([3]) *Se x é um elemento de ordem finita n de um grupo abeliano G e se d é um divisor positivo de n, então existe em G um elemento de ordem d.*

Demonstração: Se d é um divisor positivo de n, então existe m **2** $\mathbb{N}$ tal que $n = md$. Tomando $y = x^m$ temos $y^d = (x^m)^d = x^{md} = x^n = e$. Se $\pm(y) = t$, então t **·** d. Se $t < d$, e como m **2** $\mathbb{N}$, então $mt < md = n$. Logo $x^{mt} = (x^m)^t = y^t = e$, com $mt < n$, o que é um absurdo, pois $\pm(x) = n$. Portanto, $t = d$, ou seja, $\pm(y) = d$. ∎

Proposição 1.4.3 ([3]) *Se x e y são dois elementos de ordens finitas a e b respectivamente, de um grupo abeliano G, então existe em G um elemento de ordem igual a $mmc(a, b)$.*

Demonstração: Sejam $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$ e $b = {p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_r}^{\beta_r}$ as decomposições de a e b em fatores primos positivos $p_1, \dots p_r$, onde α_i, β_i **2** $\mathbb{N}$ para $i = 1, 2, \dots, r$, e

$$\gamma_i = max\{\alpha_i, \beta_i\}, \quad i = 1, 2 \dots r.$$

Logo $p_i^{\gamma_i}$ **j** a ou $p_i^{\gamma_i}$ **j** b, para $i = 1, 2, ¢¢¢ , n$. Assim, em virturde da Proposição 1.4.2, existe x_i **2** G tal que $\pm(x_i) = p_i^{\gamma_i}$, para $i = 1, 2, ¢¢¢ , n$. Portanto, de acordo com uma generalização imediata da Proposição 1.4.1, temos:

$$\pm(x_i x_2 \dots x_n) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} = mmc(a, b),$$

o que prova a proposição. ∎

Proposição 1.4.4 ([3]) *Seja G um grupo abeliano e suponhamos que todo elemento de G tenha ordem finita. Se n é a ordem máxima dos elementos de G, então a ordem de qualquer elemento de G é um divisor de n.*

Demonstração: Por hipótese, existe $a \in G$ tal que $\pm(a) = max\{\pm(x);\ x \in G\} = n$. Seja $x \in G$ um elemento qualquer e suponhamos, por absurdo, que $\pm(x)$ não divide n. Assim, pela Proposição 1.4.3, existe $y \in G$ tal que $\pm(y) = mmc(n, \pm(x)) > n$, o que é um absurdo, pois $n = max\{\pm(x);\ x \in G\}$, e portanto $\pm(x) \mid n$. ∎

Proposição 1.4.5 ([3]) *Se G é um subgrupo finito de um grupo abeliano multiplicativo K^* de um corpo K, então G é um grupo cíclico.*

Demonstração: Sejam $\pm(G) = n$ e $a \in G$ um elemento de ordem máxima r. Como $\langle a \rangle$ é um subgrupo de G, segue pelo Teorema de Lagrange que, $r \mid n$, e assim $r \leq n$. Pela Proposição 1.4.4, dado $x \in G$ temos que $\pm(x) \mid r$, ou seja, existe $q \in \mathbb{N}$ tal que $r = \pm(x)q$. Logo $x^r = x^{\circ(x)q} = (x^{\circ(x)})^q = 1$ para todo $x \in G$. Consideremos o polinômio $f(x) = x^r - 1 \in \mathbb{K}[X]$. Assim $f(x) = 0$, para todo $x \in G$ e como $|G| = n$, segue que o polinômio f possui no mínimo n raízes distintas. Logo $r = \partial f \geq n$, e como tínhamos $r \leq n$, segue que $r = n$. Portanto, $G = \langle a \rangle$, ou seja, G é cíclico. ∎

Proposição 1.4.6 ([3]) *Se K é um corpo finito, então o grupo abeliano multiplicativo K^*, do corpo K, é cíclico.*

Demonstração: Basta aplicar a Proposição 1.4.5 para $G = K^*$. ∎

Lema 1.4.1 ([3]) *Se $A_1, A_2, \ldots, A_s$ $(s > 1)$ são grupos finitos, então o grupo produto $A_1 \times A_2 \times \ldots \times A_s$ é cíclico se, e somente se, cada A_i é cíclico e as ordens de A_i e A_j $(i \neq j,\ 1 < i, j < s)$ são primos entre si.*

Lema 1.4.2 ([3]) *Se r e s são dois números naturais não nulos com $mdc(r, s) = 1$ então*

$$\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s.$$

Demonstração: Sejam $\sigma_r : \mathbb{Z} \to \mathbb{Z}_r$ e $\sigma_s : \mathbb{Z} \to \mathbb{Z}_s$ os homomorfismos canônicos de $\mathbb{Z}$ em $\mathbb{Z}_r$ e $\mathbb{Z}$ em $\mathbb{Z}_s$ respectivamente. Considerando a aplicação

$$\begin{aligned} \rho :\ & \mathbb{Z} \to \mathbb{Z}_r \times \mathbb{Z}_s \\ & x \mapsto (\sigma_r(x), \sigma_s(x)), \end{aligned}$$

temos os seguintes fatos

1. ρ é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_r \times \mathbb{Z}_s$.
   De fato, dados $x, y \in \mathbb{Z}$ temos

   $$\begin{aligned} \rho(x+y) &= (\sigma_r(x+y), \sigma_s(x+y)) = ((x+y)+r\mathbb{Z}, (x+y)+s\mathbb{Z}) = \\ &= ((x+r\mathbb{Z})+(y+r\mathbb{Z}), (x+s\mathbb{Z})+(y+s\mathbb{Z})) = (x+r\mathbb{Z}, x+s\mathbb{Z})+(y+r\mathbb{Z}, y+s\mathbb{Z}) = \\ &= (\sigma_r(x), \sigma_s(x)) + (\sigma_r(y), \sigma_s(y)) = \rho(x) + \rho(y). \end{aligned}$$

   $$\begin{aligned} \rho(xy) &= (\sigma_r(xy), \sigma_s(xy)) = ((xy)+r\mathbb{Z}, (xy)+s\mathbb{Z}) = ((x+r\mathbb{Z})(y+r\mathbb{Z}), (x+s\mathbb{Z})(y+s\mathbb{Z})) = \\ &= (x+r\mathbb{Z}, x+s\mathbb{Z})(y+r\mathbb{Z}, y+s\mathbb{Z}) = (\sigma_r(x), \sigma_s(x))(\sigma_r(y), \sigma_s(y)) = \rho(x)\rho(y). \end{aligned}$$

2. $Ker(\rho) = rs\mathbb{Z}$.
   De fato, $Ker(\rho) = \{x \in \mathbb{Z};\ \rho(x) = (\overline{0}, \overline{0})\} = \{x \in \mathbb{Z};\ (\sigma_r(x), \sigma_s(x)) = (\overline{0}, \overline{0})\}$. Como $mdc(r, s) = 1$, segue que $Ker(\rho) = rs\mathbb{Z}$ e também $\pm(\mathbb{Z}_r \times \mathbb{Z}_s) = rs$.

3. ρ é sobrejetora.
   De fato, se $\alpha = (1 + r\mathbb{Z}, 1 + s\mathbb{Z}) \in \mathbb{Z}_r \times \mathbb{Z}_s$, então

   $\alpha^{rs} = (rs)\alpha = rs(1 + r\mathbb{Z}, 1 + s\mathbb{Z}) = (rs(1 + r\mathbb{Z}), rs(1 + s\mathbb{Z})) =$
   $= ((r(1 + r\mathbb{Z}))(s(1 + r\mathbb{Z})), (r(1 + s\mathbb{Z}))(s(1 + s\mathbb{Z}))) = (\overline{0}, \overline{0}).$

   Se $o(\alpha) = t$ então $(\overline{0}, \overline{0}) = \alpha^t = t\alpha = t(1 + r\mathbb{Z}, 1 + s\mathbb{Z}) = (t + r\mathbb{Z}, t + s\mathbb{Z})$. Assim, $t \in r\mathbb{Z}$ e $t \in s\mathbb{Z}$, ou seja, existem $k_1, k_2 \in \mathbb{Z}$ tal que $t = rk_1$ e $t = sk_2$. Como $mdc(r, s) = 1$, segue pela identidade de Bezout que, existem $p, q \in \mathbb{Z}$ tal que $1 = pr + qs$. Assim

   $$t = prt + qst = pr(sk_2) + qs(rk_1) = rs(pk_2) + rs(qk_1) = rs(pk_2 + qk_1),$$

   ou seja, $rs \mid t$. Deste modo $rs \cdot t$, e como $\alpha^{rs} = (\overline{0}, \overline{0})$, segue que $t \cdot rs$. Logo $t = rs$, ou seja, $o(\alpha) = rs$, e portanto $\mathbb{Z}_r \times \mathbb{Z}_s = \langle(1+r\mathbb{Z}, 1+s\mathbb{Z})\rangle$. Assim, se $(x+r\mathbb{Z}, y+s\mathbb{Z}) \in \mathbb{Z}_r \times \mathbb{Z}_s$, então existe $z \in \mathbb{Z}$ tal que

   $$(x + r\mathbb{Z}, y + s\mathbb{Z}) = z.(1 + r\mathbb{Z}, 1 + s\mathbb{Z}) = (z + r\mathbb{Z}, z + s\mathbb{Z}) = \rho(z).$$

Portanto ρ é sobrejetora. De **(1), (2) e (3)** e usando o Teorema do Homomorfismo segue que

$$\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s,$$

o que prova o lema. ■

Lema 1.4.3 ([3]) *Se r e s são dois números naturais tais que $r, s > 1$ e $mdc(r, s) = 1$, então*

$$\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*.$$

Demonstração: Considerando os homomorfismos canônicos $\sigma_{rs} : \mathbb{Z} \to \mathbb{Z}_{rs}$, $\sigma_r : \mathbb{Z} \to \mathbb{Z}_r$, $\sigma_s : \mathbb{Z} \to \mathbb{Z}_s$ e a aplicação

$$\begin{aligned} \rho : \ & \mathbb{Z}_{rs}^* \to \mathbb{Z}_r^* \times \mathbb{Z}_s^* \\ & \sigma_{rs}(x) \mapsto (\sigma_r(x), \sigma_s(x)), \end{aligned}$$

temos os seguintes fatos

1. ρ está bem definida e é injetora.
   De fato, se $d = mdc(x, r)$ e $d' = mdc(x, s)$, então $d \mid r$ e $d' \mid s$. Assim $d \mid rs$ e $d' \mid rs$ e como $d \mid x$ e $d' \mid x$, segue que d e d' são divisores comuns de x e rs. Agora, como $mdc(x, rs) = 1$, segue que $d = d' = 1$ e portanto $\sigma_r(x) \in \mathbb{Z}_r^*$ e $\sigma_s(x) \in \mathbb{Z}_s^*$. Agora, dado $x, y \in \mathbb{Z}$, temos que

   $$\begin{array}{lll} \rho(\sigma_{rs}(x)) = \rho(\sigma_{rs}(y)) & \Leftrightarrow (\sigma_r(x), \sigma_s(x)) = (\sigma_r(y), \sigma_s(y)) & \Leftrightarrow \sigma_r(x) = \sigma_r(y) \ \ e \ \ \sigma_s(x) = \sigma_s(y) \\ & \Leftrightarrow x \equiv y (mod\ r) \ \ e \ \ x \equiv y (mod\ s) & \Leftrightarrow r \mid x - y \ \ e \ \ s \mid x - y \\ & \Leftrightarrow rs \mid x - y \quad \Leftrightarrow \quad x \equiv y (mod\ rs) & \Leftrightarrow \sigma_{rs}(x) = \sigma_{rs}(y). \end{array}$$

2. ρ é sobrejetora.
   De fato, dado $(m, n) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, temos que $m = x + r\mathbb{Z}$ e $n = y + s\mathbb{Z}$, onde $x, y \in \mathbb{Z}$, $mdc(x, r) = 1$ e $mdc(y, s) = 1$. Como $\mathbb{Z}_r^* \times \mathbb{Z}_s^* \subseteq \mathbb{Z}_r \times \mathbb{Z}_s$, pelo Lema 1.4.2, segue que existe $z \in \mathbb{Z}$ tal que $(x + r\mathbb{Z}, y + s\mathbb{Z}) = (z + r\mathbb{Z}, z + s\mathbb{Z})$, ou seja

   $$z \equiv x (mod\ r) \ \ e \ \ z \equiv y (mod\ s)$$

Se $d = mdc(z, r)$, então $d \mid z$ e $d \mid r$. Como $z \equiv x (mod\ r)$, segue que $r \mid m - x$, e assim $d \mid z - x$. Como $d \mid z$ segue que $d \mid x$, e assim $d \mid r$ e $d \mid x$. Mas como $mdc(x, r) = 1$, segue que $d = 1$, ou seja, $mdc(z, r) = 1$. Analogamente, $mdc(z, s) = 1$. Agora, se $d' = mdc(z, rs)$, então $d' \mid z$ e $d' \mid rs$, e como $mdc(r, s) = 1$ segue que $d' \mid r$ ou $d' \mid s$. Assim,
- se $d' \mid r$, então como $d' \mid z$ e $mdc(z, r) = 1$, segue que $d' = 1$, e
- se $d' \mid s$, então como $d' \mid z$ e $mdc(z, s) = 1$, segue que $d' = 1$.
Logo, $mdc(z, rs) = 1$, e portanto $\sigma_{rs}(z) \in \mathbb{Z}_{rs}{}^*$. Assim, se $(m, n,) = (\sigma_r(x), \sigma_s(y)) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, então existe $\sigma_{rs}(z) \in \mathbb{Z}_{rs}^*$ tal que

$$\rho(\sigma_{rs}(z)) = (\sigma_r(z), \sigma_s(z)) = (\sigma_r(x), \sigma_s(y)) = (m, n)$$

Portanto, ρ é sobrejetora.

3. ρ é homomorfismo.
De fato, se $\sigma_{rs}(x), \sigma_{rs}(y) \in \mathbb{Z}_{rs}^*$, então

$$\begin{aligned}\rho(\sigma_{rs}(x)+\sigma_{rs}(y)) &= \rho(\sigma_{rs}(x+y)) = (\sigma_r(x+y), \sigma_s(x+y)) = (\sigma_r(x)+\sigma_r(y), \sigma_s(x)+\sigma_s(y)) = \\ &= (\sigma_r(x), \sigma_s(x)) + (\sigma_r(y), \sigma_s(y)) = \rho(\sigma_{rs}(x)) + \rho(\sigma_{rs}(y)).\end{aligned}$$

$$\begin{aligned}\rho(\sigma_{rs}(x)\sigma_{rs}(y)) &= \rho(\sigma_{rs}(xy)) = (\sigma_r(xy), \sigma_s(xy)) = (\sigma_r(x)\sigma_r(y), \sigma_s(x)\sigma_s(y)) = \\ &= (\sigma_r(x), \sigma_s(x))(\sigma_r(y), \sigma_s(y)) = \rho(\sigma_{rs}(x))\rho(\sigma_{rs}(y)).\end{aligned}$$

De (**1**), (**2**) e (**3**), concluímos que $\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. ∎

Lema 1.4.4 ([3]) *Se $n > 1$ é um número natural e se $n = {p_1}^{r_1}{p_2}^{r_2} \dots {p_t}^{r_t}$ é a decomposição de n em fatores primos positivos, então*

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{r_1}}^* \times \mathbb{Z}_{p_2^{r_2}}^* \times \dots \times \mathbb{Z}_{p_t^{r_t}}^*.$$

Demonstração: Faremos a prova por indução. Como $mdc(p_1^{r_1}, p_2^{r_2}) = 1$, segue pelo Lema 1.4.3, que

$$\mathbb{Z}_{p_1^{r_1}p_2^{r_2}}^* \simeq \mathbb{Z}_{p_1^{r_1}}^* \times \mathbb{Z}_{p_2^{r_2}}^*.$$

Suponhamos o resultado válido para ${p_1}^{r_1}{p_2}^{r_2} \dots {p_{t-1}}^{r_{t-1}}$, ou seja,

$$\mathbb{Z}_{{p_1}^{r_1}{p_2}^{r_2}\dots{p_{t-1}}^{r_{t-1}}}^* \simeq \mathbb{Z}_{p_1^{r_1}}^* \times \mathbb{Z}_{p_2^{r_2}}^* \times \dots \times \mathbb{Z}_{p_{t-1}^{r_{t-1}}}^*.$$

Assim,

$$\mathbb{Z}_n^* = \mathbb{Z}_{{p_1}^{r_1}{p_2}^{r_2}\dots{p_t}^{r_t}}^* \simeq \mathbb{Z}_{{p_1}^{r_1}{p_2}^{r_2}\dots{p_{t-1}}^{r_{t-1}}}^* \times \mathbb{Z}_{p_t^{r_t}}^*,$$

pois $mdc({p_1}^{r_1}{p_2}^{r_2} \dots {p_{t-1}}^{r_{t-1}}, p_t^{r_t}) = 1$, e portanto usando a hipótese de indução temos que

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{r_1}}^* \times \mathbb{Z}_{p_2^{r_2}}^* \times \dots \times \mathbb{Z}_{{p_{t-1}}^{r_{t-1}}}^* \times \mathbb{Z}_{p_t^{r_t}}^*,$$

o que prova o lema. ∎

Definição 1.4.1 *Seja n um inteiro positivo. A função ϕ de Euler, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Como consequência dos Lemas 1.4.3 e 1.4.4 temos o seguinte resultado

Lema 1.4.5 ([3]) *Se r e s são dois números naturais não nulos com $mdc(r,s)=1$, então*

$$\phi(rs)=\phi(r)\phi(s),$$

onde ϕ é a função de Euler.

Demonstração: Pelo Lema 1.4.3 temos que $\mathbb{Z}_{rs}^* \simeq \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. Assim $\pm(\mathbb{Z}_{rs}^*)=\pm(\mathbb{Z}_r^*)\pm(\mathbb{Z}_s^*)$, pois $mdc(r,s)=1$, e portanto $\phi(rs)=\phi(r)\phi(s)$. ∎

Lema 1.4.6 ([3]) *Se $n>1$ é um número natural e se $n=p_1{}^{r_1}p_2{}^{r_2}\dots p_t{}^{r_t}$ é a decomposição de n em fatores primos positivos, então*

$$\phi(n)=\phi(p_1^{r_1})\phi(p_2^{r_2})\dots\phi(p_t^{r_t}).$$

Demonstração: Segue por indução aplicando o Lema 1.4.5. ∎

Lema 1.4.7 ([3]) *Se $p>2$ é um número primo e t é um número natural, então*

$$(1+p)^{p^t} \equiv 1+p^{t+1}(mod\ p^{t+2}).$$

Demonstração: Faremos por indução sobre t. Para $t=0$ o resultado é imediato. Agora, suponhamos que o resultado seja válido para t, $t>0$, e mostremos que é válido para $t+1$. Assim, por hipótese de indução

$$(1+p)^{p^t}=(1+p^{t+1})+\lambda\, p^{t+2},\ \text{para algum } \lambda \in \mathbb{Z}.$$

Logo

$$\begin{aligned}(1+p)^{p^{t+1}} &= [(1+p)^{p^t}]^p=[1+p^{t+1}(1+\lambda p)]^p= \\ &= 1+\binom{p}{1}p^{t+1}(1+\lambda p)+\binom{p}{2}p^{2t+2}(1+\lambda p)^2+\ldots+p^{pt+p}(1+\lambda p)^p= \\ &= 1+p^{t+2}+\lambda p^{t+3}+\tfrac{1}{2}(p-1)p^{2t+3}(1+\lambda p)^2+\ldots+p^{pt+p}(1+\lambda p)^p= \\ &= 1+p^{t+2}+\mu p^{t+3},\ \text{com } \mu \in \mathbb{Z}.\end{aligned}$$

Assim, $(1+p)^{p^{t+1}} \equiv 1+p^{t+2}(mod\ p^{t+3})$, o que prova o lema. ∎

Lema 1.4.8 ([3]) *Se $p>2$ é um número primo e r é um inteiro positivo, então o grupo $\mathbb{Z}_{p^r}^*$ é cíclico.*

Demonstração: Sejam o homomorfismo canônico $\sigma_{p^r}:\mathbb{Z}\to\mathbb{Z}_{p^r}$ e $\sigma_{p^r}=\tau_r$. Pela Proposição 1.4.6, temos que $\mathbb{Z}_p{}^*$ é um grupo cíclico, e deste modo existe $b \in \mathbb{Z}$ tal que p não divide b e $\pm(\tau_1(b))=p-1$. Se $a=b^{p^{r-1}}$ e $d=mdc(a,p^r)$, então $d \mid p^r$ e $d \mid b^{p^{r-1}}$. Se $d \mid p^r$, como p é primo, segue que $d=1,p,p^2,\dots,p^r$. Se $d \neq 1$, então $d=p^i$ para algum $i \in \{1,2,\dots,r\}$. Temos que p não divide b, ou seja, p não aparece na decomposição por fatores primos de b. Conseqüentemente p^i também não aparece, e assim p^i não divide b. Se $b=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, então

$p_j \neq p$ para todo $j = 1, 2, \ldots s$, e assim $a = b^{p^{r-1}} = p_1^{\alpha_1 p^{r-1}} p_2^{\alpha_2 p^{r-1}} \cdots p_s^{\alpha_s p^{r-1}}$. Logo p^i não divide a, para todo $i = 1, 2, \ldots, r$, o que é um absurdo. Portanto $d = 1$, ou seja, $mdc(a, p^r) = 1$, e deste modo $\alpha = \tau_r(a) \in \mathbb{Z}_{p^r}^*$. Assim

$$\alpha^{p-1} = [\tau_r(a)]^{p-1} = [b^{p^{r-1}}]^{p-1} = b^{p^{r-1}(p-1)} = 1,$$

pois $\pm(\mathbb{Z}_{p^r}^*) = \phi(p^r) = p^r - p^{r-1}$, e como p^i não divide b, para todo $i = 1, 2, \ldots, r$, segue que $mdc(b, p^r) = 1$, e portanto $b \in \mathbb{Z}_{p^r}^*$, ou seja, $\pm(\alpha) = p - 1$.
No que se segue, vamos supor que $r > 1$. Mostremos que o elemento $\beta = \tau_r(1 + p) \in \mathbb{Z}_{p^r}^*$ tem ordem p^{r-1}. Com efeito, tomando $t = r - 1$, pelo Lema 1.4.7 temos que $(1 + p)^{p^{r-1}} \equiv 1 + p^r (mod\ p^{r+1})$, e assim

$$(1 + p)^{p^{r-1}} = 1 + p^r + \lambda p^{r+1} = 1 + p^r + \lambda p p^r = 1 + (1 + \lambda p)p^r,$$

para algum $\lambda \in \mathbb{Z}$. Tomando $\mu = 1 + \lambda p$, obtemos que $(1 + p)^{p^{r-1}} = 1 + \mu p^r$, ou seja, $(1+p)^{p^{r-1}} \equiv 1 (mod\ p^r)$. Logo $\beta^{p^{r-1}} = \tau_r(1)$, e deste modo $\pm(\beta) \mid p^{r-1}$. Portanto, $\pm(\beta) = p^j$, com $0 \leq j \leq r - 1$. Agora, se $j < r - 1$, então $(\tau_r(1+p))^{p^j} = \tau_r(1)$, ou seja, $(1+p)^{p^j} \equiv 1 (mod\ p^r)$. Pelo Lema 1.4.7 temos que $(1+p)^{p^j} \equiv 1+p^{j+1} (mod\ p^{j+2})$, e assim existem $u, v \in \mathbb{Z}$ tais que $(1+p)^{p^j} = 1 + up^r$ e $(1 + p)^{p^j} = 1 + p^{j+1} + vp^r$. Logo, $up^r = p^{j+1} + vp^{j+2}$ e $p^{j+1} = up^r - vp^{j+2} = up^{j+2}p^k - vp^{j+2} = p^{j+2}(up^k - v)$, pois $j+2 \leq r$. Assim $p^{j+1} \equiv 0 (mod\ p^{j+2})$, o que é um absurdo. Portanto, $\pm(\beta) = p^{r-1}$. Como $mdc(\pm(\alpha), \pm(\beta)) = mdc(p - 1, p^{r-1}) = 1$, pela Proposição 1.4.1, segue que $\pm(\alpha\beta) = \pm(\alpha) \pm (\beta) = (p - 1)p^{r-1} = \pm(\mathbb{Z}_{p^r}^*)$. Portanto $\mathbb{Z}_{p^r}^*$ é gerado pelo elemento $\alpha\beta$, ou seja, $\mathbb{Z}_{p^r}^*$ é cíclico. ∎

Lema 1.4.9 ([3]) *Se b é um inteiro ímpar e t é um número natural, então*

$$b^{2^{t+1}} \equiv 1 (mod\ 2^{t+3})$$

Demonstração: Faremos a prova por indução sobre t. Como b é ímpar, existe $k \in \mathbb{Z}$ tal que $b = 2k + 1$. Para $t = 0$ temos que $b^2 = 4k(k + 1) + 1$, e assim $b^2 \equiv 1 (mod\ 2^3)$. Suponhamos a congruência verdadeira para t, $t > 0$, ou seja

$$b^{2^{t+1}} = 1 + \lambda 2^{t+3}, \text{ com } \lambda \in \mathbb{Z},$$

e mostremos que é válida para $t+1$. Assim, $b^{2^{t+2}} = (b^{2^{t+1}})^2 = (1+\lambda 2^{t+3})^2 = 1+\lambda 2^{t+4}+\lambda^2 2^{2t+6} = 1 + 2^{t+4}(\lambda + \lambda^2 2^{t+2})$. Logo $b^{2^{t+2}} \equiv 1 (mod\ 2^{t+4})$, ou seja, a congruência é válida para $t + 1$, e portanto, é válida para todo $t \in \mathbb{N}$. ∎

Lema 1.4.10 ([3]) *Os grupos $\mathbb{Z}_2^*$ e $\mathbb{Z}_4^*$ são cíclicos, e para $r \geq 3$ o grupo $\mathbb{Z}_{2^r}^*$ não é cíclico.*

Demonstração: Temos que $\mathbb{Z}_2^* = \{\overline{1}\}$, logo $\mathbb{Z}_2^*$ é gerado pelo elemento $\overline{1}$, e portanto é cíclico. Temos que $\mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}$, mas o elemento $\overline{3}$ é um gerador de $\mathbb{Z}_4^*$, e portanto $\mathbb{Z}_4^*$ é cíclico. Agora suponhamos $r \geq 3$ e tomamos o homomorfismo canônico $\tau_r : \mathbb{Z} \to \mathbb{Z}_{2^r}$. Notemos que, dado $b \in \mathbb{Z}$, temos que $\tau_r(b) \in \mathbb{Z}_{2^r}^*$ se, e somente se, b é ímpar. Agora, dado $x \in \mathbb{Z}_{2^r}^*$, existe um inteiro ímpar b tal que $x = \tau_r(b)$. Pelo Lema 1.4.9, tomando $t = r - 3$, obtemos $b^{2^{r-2}} \equiv 1 (mod\ 2^r)$. Logo $x^{2^{r-2}} = \tau_r(1)$, e assim $\pm(x) \mid 2^{r-2}$. Como $\pm(\mathbb{Z}_{2^r}^*) = 2^{r-1}$, concluímos que $\mathbb{Z}_{2^r}^*$ não é cíclico. ∎

Teorema 1.4.1 ([3]) *O grupo $\mathbb{Z}_n^*$ $(n > 1)$ é cíclico se, e somente se, $n = 2, 4, p^r$ ou $2p^r$, onde $p > 2$ é um número primo e $r \geq 1$ é um número natural.*

Demonstração: Suponhamos que $\mathbb{Z}_n^*$ $(n > 1)$ seja cíclico. Se n for uma potência de 2, então pelo Lema 1.4.10, n somente pode assumir os valores 2 ou 4. Agora, temos os seguintes fatos

1. Se n for par e não for uma potência de 2, então n possui uma decomposição em fatores primos dada por $n = 2^a {p_1}^{r_1} {p_2}^{r_2} \cdots {p_t}^{r_t}$, onde $a \geq 1$, $t \geq 1$, $p_i \neq 2$, *e* $p_i \neq p_j$, *se* $i \neq j$. Pelo Lema 1.4.4 temos que

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{2^a}^* \times \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{r_t}}^*$$

   e pelo Lema 1.4.1, segue que $a = 1$ ou $a = 2$, mas não podemos ter $a = 2$, pois $mdc(4, {p_1}^{r_1} - {p_1}^{r_1-1}) = 2$. Também não podemos ter $t > 1$, pois ${p_1}^{r_1} - {p_1}^{r_1-1}$ e ${p_2}^{r_2} - {p_2}^{r_2-1}$ são números pares. Logo $mdc({p_1}^{r_1} - {p_1}^{r_1-1}, {p_2}^{r_2} - {p_2}^{r_2-1}) \neq 1$. Portanto, temos que $a = 1$ e $t = 1$, ou seja, $n = 2{p_1}^{r_1}$.

2. Se n for ímpar, então n tem uma decomposição em fatores primos dada por $n = {p_1}^{r_1} {p_2}^{r_2} \ldots {p_t}^{r_t}$ onde $r_i \geq 1$, $t \geq 1$, $p_i \neq 2$, *e* $p_i \neq p_j$, *se* $i \neq j$. Temos que $t = 1$, pois se $t > 1$, pelo Lema 1.4.4, temos que $\mathbb{Z}_n^* \simeq \mathbb{Z}_{{p_1}^{r_1}}^* \times \mathbb{Z}_{{p_2}^{r_2}}^* \times \ldots \times \mathbb{Z}_{{p_t}^{r_t}}^*$, e pelo Lema 1.4.1, segue que o grupo do segundo membro é cíclico, o que é um absurdo, pois $mdc({p_i}^{r_i} - {p_i}^{r_i-1}, {p_j}^{r_j} - {p_j}^{r_j-1}) \neq 1$, para qualquer i, j. Logo $n = {p_1}^{r_1}$.

Portanto, se $\mathbb{Z}_n^*$ é cíclico, então $n = 2, 4, p^r$ *ou* $2p^r$, com $p > 2$ um número primo e $r \geq 1$ um número natural. Reciprocamente, se $n = 2$ ou $n = 4$, pelo Lema 1.4.10 segue que $\mathbb{Z}_n^*$ é cíclico. Se $n = p^r$, pelo Lema 1.4.8, segue que $\mathbb{Z}_n^*$ é cíclico. Se $n = 2p^r$, como $mdc(2, p^r) = 1$, então pelo Lema 1.4.4 temos que $\mathbb{Z}_{2p^r}^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{p^r}^* \simeq \mathbb{Z}_{p^r}^*$ que é cíclico, portanto $\mathbb{Z}_{2p^r}^*$ é cíclico. ∎

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

Nesta seção apresentamos as formas quadráticas sobre o $\mathbb{R}^n$, que serão muito úteis no estudo das aplicações das formas quadráticas aos corpos ciclotômicos.

Definição 1.5.1 *Para cada inteiro n, definimos a forma quadrática sobre o $\mathbb{R}^n$ por*

$$Q_n(\underline{x}) = Q_n(x_1, \cdots, x_n) = \sum_{i=1}^{n} x_i^2 + \sum_{1 \leq i < j \leq n} (x_i - x_j)^2,$$

onde $\underline{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$.

Da igualdade

$$\sum_{1 \leq i < j \leq n} (x_i - x_j)^2 = (n - 1) \sum_{i=1}^{n} x_i^2 - 2 \sum_{1 \leq i < j \leq n} x_i x_j,$$

obtem-se que

$$Q_n(x_1, \cdots, x_n) = n\sum_{i=1}^{n} x_i^2 - 2\sum_{1\le i<j\le n} x_i x_j.$$

Para cada r, s inteiros, também podemos escrever

$$Q_{r,s}(x_1, \cdots, x_r) = \sum_{i=1}^{r} x_i^2 + s\sum_{1\le i<j\le r} (x_i - x_j)^2.$$

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 $\{1, \cdots, n\}$.

Proposição 1.5.1 ([4]) *Seja $Q_n(\underline{x})$ uma forma quadrática.*
(**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 $\mathbb{Z}^n$.*

Lema 1.5.1 ([4]) *Se $Q_n(x_1, \cdots, x_n) = \sum_{i=1}^{n} x_1^2 + \sum_{i<j}(x_i - x_j)^2$, e $\underline{a} = (a_1, \cdots, a_n) \in \mathbb{R}^n$, então*

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

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

Teorema 1.5.1 ([4]) *Dados os números inteiros $a_1, \cdots, a_t$, com $t < n$. Se*

$$F(x_{t+1}, \cdots, x_n) = Q_{n,1}(a_1, \cdots, a_t, x_{t+1}, \cdots, x_n),$$

então F atinge seu mínimo com coordenadas inteiras no ponto

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

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

Corolário 1.5.1 ([5]) *Sejam os números inteiros $a_1, \cdots, a_t$, com $t < \dfrac{n}{r}$. Se*

$$F(x_{t+1}, \cdots, x_{n/r}) = Q_{n/r,r}(a_1, \cdots, a_t, x_{t+1}, \cdots, x_{n/r}),$$

então F atinge seu mínimo com entradas inteiras no ponto

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

Capítulo

2

Teoria algébrica dos números

2.1 Introdução

O objetivo deste capítulo é apresentar uma coleção de resultados básicos de Teoria Algébrica dos Números, fornecendo assim uma base teórica para o desenvolvimento dos demais capítulos. Com a intenção de tornar este trabalho prático e acessível, omitimos a maioria das demonstrações, no entanto, cada resultado enunciado será acompanhado de um número que representa a referência que o contém. Desse modo, na Seção 2.2, apresentamos os conceitos e propriedades de norma e traço, e um resultado importante sobre as extensões galoisianas. Na Seção 2.3, apresentamos os conceitos de inteiros algébricos e o anel dos inteiros algébricos. Na Seção 2.4, definimos discriminante de uma n-upla e discriminante de um corpo de números. Na Seção 2.5, introduzimos o conceito de norma de um ideal. Nas Seções 2.6 e 2.7, apresentamos os corpos quadráticos e os corpos ciclotômicos, respectivamente. Para finalizar, a Seção 2.8 é dedicada à decomposição de ideais primos em uma extensão, com destaque para o Lema de Kummer.

2.2 Norma e traço

Nesta seção apresentamos os conceitos de norma e traço, enfocando sua principais propriedades.

Definição 2.2.1 *Sejam $\mathbb{K} \subsetneq \mathbb{L}$ corpos de números, com $n = [\mathbb{L} : \mathbb{K}]$, e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Dado um elemento $\alpha \in \mathbb{L}$, define-se a norma e o traço de α relativamente a extensão $\mathbb{L}/\mathbb{K}$, como sendo respectivamente:*

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

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

Observação 2.2.1 *Quando não houver dúvida quanto a extensão que contém o elemento α, usaremos $N(\alpha)$ ao invés de $N_{\mathbb{L}/\mathbb{K}}(\alpha)$.*

Observação 2.2.2 *Se* $\mathbb{K} \subset \mathbb{L}$ *são corpos de números,* $[\mathbb{L} : \mathbb{K}] = n$, $x, y \in \mathbb{L}$ *e* $a \in \mathbb{K}$, *então valem as seguintes propriedades:*

(**1**) $Tr_{\mathbb{L}/\mathbb{K}}(x+y) = Tr_{\mathbb{L}/\mathbb{K}}(x) + Tr_{\mathbb{L}/\mathbb{K}}(y)$,
(**2**) $Tr_{\mathbb{L}/\mathbb{K}}(ax) = aTr_{\mathbb{L}/\mathbb{K}}(x)$,
(**3**) $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$,
(**4**) $N_{\mathbb{L}/\mathbb{K}}(xy) = N_{\mathbb{L}/\mathbb{K}}(x)\ N_{\mathbb{L}/\mathbb{K}}(y)$,
(**5**) $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$.

No caso $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, dado $x \in \mathbb{M}$, valem:
(**6**) $N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(x))$,
(**7**) $Tr_{\mathbb{M}/\mathbb{K}}(x) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(x))$.

Em particular, se $x \in \mathbb{L}$, então:
(**8**) $Tr_{\mathbb{M}/\mathbb{K}}(x) = [\mathbb{M} : \mathbb{L}]Tr_{\mathbb{L}/\mathbb{K}}(x)$,
(**9**) $N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}(x)^{[\mathbb{M}:\mathbb{L}]}$.

Proposição 2.2.1 ([3]) *Sejam* $\mathbb{M}$ *e* $\mathbb{F}$ *extensões galoisianas sobre* $\mathbb{K}$ *tais que* $\mathbb{M}$ *e* $\mathbb{F}$ *são subcorpos de algum outro corpo. Dado* $\alpha \in \mathbb{M}$, *se* $\mathbb{M} \cap \mathbb{F} = \mathbb{K}$ *então*

$$Tr_{\mathbb{MF}/\mathbb{F}}(\alpha) = Tr_{\mathbb{M}/\mathbb{K}}(\alpha).$$

Demonstração: Pela Proposição 1.3.1 temos que

$$\begin{aligned} \rho : Gal(\mathbb{MF}/\mathbb{F}) &\to Gal(\mathbb{M}/\mathbb{K}) \\ \sigma &\mapsto \sigma|_{\mathbb{M}} \end{aligned}$$

é um isomorfismo. Seja $\sigma|_{\mathbb{M}} \in Gal(\mathbb{M}/\mathbb{K})$. Como $\sigma : \mathbb{MF} \to \mathbb{MF}$ e $\mathbb{M} \subset \mathbb{MF}$, segue que $\sigma|_{\mathbb{M}} \in Gal(\mathbb{MF}/\mathbb{F})$. Logo $Gal(\mathbb{M}/\mathbb{K}) \subset Gal(\mathbb{MF}/\mathbb{F})$, e como são isomorfos, segue que

$$Gal(\mathbb{MF}/\mathbb{F}) = Gal(\mathbb{M}/\mathbb{K}),$$

e conseqüentemente dado $\alpha \in \mathbb{M}$ temos que

$$Tr_{\mathbb{MF}/\mathbb{F}}(\alpha) = Tr_{\mathbb{M}/\mathbb{K}}(\alpha),$$

o que prova a proposição. ∎

2.3 Inteiros algébricos

O objetivo desta seção é apresentar conceitos e resultados básicos envolvendo inteiros algébricos.

Definição 2.3.1 *Sejam* $A \subset B$ *anéis. Dizemos que um elemento* $\alpha \in B$ *é um inteiro sobre* A, *se existe um polinômio mônico não nulo* $f(x)$ *com coeficientes em* A *tal que* $f(\alpha) = 0$.

Definição 2.3.2 *Sejam* $A \subset B$ *anéis. Dizemos que* B *é inteiro sobre* A *se todo elemento de* B *é inteiro sobre* A. *Pode ser mostrado que o conjunto* $\mathcal{O}_B = \{\alpha \in B : \ \alpha \text{ é inteiro sobre } A\}$ *é um anel.*

Definição 2.3.3 *Sejam A μ B anéis.*

1. $O_B = f\alpha$ 2 B : α *é inteiro sobre* Ag *é chamado anel dos inteiros de* A *em* B.
2. *Se* A *é um domínio e* $B = \mathbb{K}$ *é o corpo de frações de* A, *dizemos que* O_B *é o anel dos inteiros de* A *em* $\mathbb{K}$. *Além disso, se* $A = O_B$ *dizemos que* A *é um anel integralmente fechado.*

Definição 2.3.4 *Um elemento* α 2 $\mathbb{C}$ *é chamado um inteiro algébrico se existe um polinômio mônico* $f(x)$ *com coeficientes inteiros tal que* $f(\alpha) = 0$. *Pode ser mostrado que o conjunto*

$$\mathfrak{B} = f\alpha \ 2 \ \mathbb{C}; \quad irr(\alpha, \mathbb{Q}) \ 2 \ \mathbb{Z}[X]g$$

formado pelos inteiros algébricos de $\mathbb{C}$ *é um anel, chamado anel dos inteiros algébricos.*

Exemplo 2.3.1 *O elemento* $\alpha = \sqrt{2} + \sqrt{3}$ *é um inteiro algébrico, pois é raiz do polinômio* $f(x) = x^4 - 10x^2 + 1$ 2 $\mathbb{Z}[X]$.

Definição 2.3.5 *Seja* $\mathbb{L}$ *um corpo de números de grau* n. *Um elemento* α 2 $\mathbb{L}$ *é chamado um inteiro algébrico do corpo* $\mathbb{L}$, *se existe um polinômio mônico* $f(x)$ *com coeficientes inteiros tal que* $f(\alpha) = 0$. *Pode ser mostrado que o conjunto* $O_{\mathbb{L}} = \mathfrak{B} \setminus \mathbb{L}$ *formado pelos inteiros algébricos de* $\mathbb{L}$ *é um anel, chamado anel dos inteiros algébricos do corpo* $\mathbb{L}$.

Teorema 2.3.1 ([2]) *Se* α 2 $\mathbb{L}$ *é um inteiro algébrico, então* $N_{\mathbb{L}/\mathbb{Q}}(\alpha)$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha)$ *são números inteiros.*

Lema 2.3.1 ([6]) *Sejam* $\mathbb{Q}$ μ $\mathbb{L}$ *uma extensão finita de grau* n, $O_{\mathbb{L}}$ *o anel dos inteiros algébricos de* $\mathbb{L}$, $f\alpha_1, \ldots, \alpha_n g$ *uma base de* $\mathbb{L}$ *sobre* $\mathbb{Q}$, *onde* $det(Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_i\alpha_j))$ 6= 0 *e* α 2 $\mathbb{L}$. *Se* $Tr_{\mathbb{L}|\mathbb{Q}}(\alpha\beta) = 0$, *para todo* β 2 $\mathbb{L}$, *então* $\alpha = 0$.

Demonstração: Se α 2 $\mathbb{L}$, então $\alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + \ldots + a_n\alpha_n$, onde a_i 2 $\mathbb{Q}$, para $i = 1, 2, ¢¢¢ , n$. Multiplicando por α_j, $j = 1, 2, \ldots, n$, obtemos:

$$\alpha\alpha_j = a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + ¢¢¢ + a_n\alpha_n\alpha_j.$$

Assim,

$$0 = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha\alpha_j) = a_1 Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_1\alpha_j) + a_2 Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_2\alpha_j) + ¢¢¢ + a_n Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_n\alpha_j).$$

Na forma matricial, temos que

$$\begin{bmatrix} Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_1\alpha_1) & Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_2\alpha_1) & ¢¢¢ & Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_n\alpha_1) \\ Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_1\alpha_2) & Tr_{\mathbb{L}\mathbb{Q}}(\alpha_2\alpha_2) & ¢¢¢ & Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_1\alpha_n) & Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_2\alpha_n) & ¢¢¢ & Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_i\alpha_j))$ 6= 0 segue que $a_1 = a_2 = ¢¢¢ = a_n = 0$. Portanto, $\alpha = 0$. ∎

Lema 2.3.2 ([6]) *Sejam* $\mathbb{Q} \subset \mathbb{L}$ *uma extensão finita de grau* n, *e* $\mathcal{O}_{\mathbb{L}}$ *o anel dos inteiros algébricos do corpo* $\mathbb{L}$. *Se* $B = \{\alpha_1, \ldots, \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{Q}$, *onde* $det(Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_i\alpha_j)) \neq 0$, *então a aplicação* $\rho : \mathbb{L} \to Hom_{\mathbb{Q}}(\mathbb{L}, \mathbb{Q})$ *definida por* $\rho(\alpha) = S_\alpha$, *onde* $S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha\beta)$, *com* $\beta \in \mathbb{L}$, *é um isomorfismo.*

Demonstração: Temos que ρ é homomorfismo, pois dado $\alpha_1, \alpha_2 \in \mathbb{L}$, temos

$$\begin{aligned}\rho(\alpha_1+\alpha_2)(\beta) &= S_{\alpha_1+\alpha_2}(\beta) = Tr_{\mathbb{L}|\mathbb{Q}}((\alpha_1+\alpha_2)\beta)\\ &= Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_1\beta) + Tr_{\mathbb{L}|\mathbb{Q}}(\alpha_2\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (\rho(\alpha_1)+\rho(\alpha_2))(\beta),\end{aligned}$$

e

$$\rho(a\alpha)(\beta) = S_{a\alpha}(\beta) = Tr_{\mathbb{L}|\mathbb{Q}}(a\alpha\beta) = aTr_{\mathbb{L}|\mathbb{Q}}(\alpha\beta) = aS_\alpha(\beta) = a\rho(\alpha)(\beta),$$

para todo $\beta \in \mathbb{L}$. Agora, seja $\alpha \in \mathbb{L}$ tal que $\rho(\alpha) = 0$. Assim, $\rho(\alpha)(\beta) = S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha\beta) = 0$, $\forall \beta \in \mathbb{L}$. Pela Lema 2.3.1, segue que $\alpha = 0$, provando assim que ρ é injetora. Dados $\alpha, x, y \in \mathbb{L}$, e $a \in \mathbb{Q}$, temos

$$S_\alpha(x+y) = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha(x+y)) = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha x) + Tr_{\mathbb{L}|\mathbb{Q}}(\alpha y) = S_\alpha(x) + S_\alpha(y), \text{ e}$$

$$S_\alpha(ax) = Tr_{\mathbb{L}|\mathbb{Q}}(\alpha a x) = aTr_{\mathbb{L}|\mathbb{Q}}(\alpha x) = aS_\alpha(x).$$

Portanto, $S_\alpha : \mathbb{L} \to \mathbb{Q}$ é uma forma linear. Assim, se tomarmos uma base $B = \{\beta_1, \beta_2, \ldots, \beta_n\}$ de $\mathbb{L}$ sobre $\mathbb{Q}$, podemos definir

$$S_{\alpha_i} : \mathbb{L} \to \mathbb{Q}$$
$$\beta_j \mapsto S_{\alpha_i}(\beta_j) = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

Logo, a base $B^* = \{S_{\alpha_1}, S_{\alpha_2}, \ldots, S_{\alpha_n}\}$ é a base dual de B, e deste modo $dim_{\mathbb{Q}}\mathbb{L} = dim_{\mathbb{Q}}(Hom_{\mathbb{Q}}(\mathbb{L}, \mathbb{Q})) = n$, ou seja, ρ é sobrejetora. Portanto, ρ é um isomorfismo. ∎

Proposição 2.3.1 ([6]) *Se* $\mathbb{Q} \subset \mathbb{L}$ *é uma extensão finita de grau* n, $\mathcal{O}_{\mathbb{L}}$ *o anel dos inteiros algébricos do corpo* $\mathbb{L}$ *e* $\mathcal{A}$ *um ideal não nulo de* $\mathcal{O}_{\mathbb{L}}$, *então* $\mathcal{A}$ *e* $\mathcal{O}_{\mathbb{L}}$ *são* $\mathbb{Z}$*-módulos livres de posto* n.

Demonstração: Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. Como toda extensão finita é algébrica, segue que todos os α_i's são algébricos sobre $\mathbb{L}$, ou seja, existem $b_i \in \mathbb{Q}$, $i = 1, 2, \ldots, n$, não todos nulos, tal que

$$b_n{\alpha_i}^n + b_{n-1}{\alpha_i}^{n-1} + \ldots + b_0 = 0.$$

Podemos multiplicar cada coeficiente pelo mínimo múltiplo comum dos denominadores de cada um (pois são números racionais), para que pertençam a $\mathbb{Z}$. Assim, podemos reescrever a igualdade da seguinte forma

$$a_n{\alpha_i}^n + a_{n-1}{\alpha_i}^{n-1} + \ldots + a_0 = 0, \ a_i \in \mathbb{Z}, \text{ para todo } i = 1, 2, \cdots, n. \tag{2.3.1}$$

Supondo que $a_n \neq 0$, e multiplicando a Equação 2.3.1 por a_n^{n-1}, temos

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

$$(a_n\alpha_i)^n + a_{n-1}(a_n\alpha_i)^{n-1} + \ldots + a_n^{n-1}a_0) = 0.$$

Assim, $a_n\alpha_i$ é um inteiro algébrico. Tomamos $a_n\alpha_i = z_i \in \mathcal{O}_{\mathbb{L}}$, para cada $i = 1, 2, \ldots, n$. Mostremos que $\{z_i, z_2, \ldots, z_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. Seja $b_1z_1 + b_2z_2 + \ldots + b_nz_n = 0$, onde $b_i \in \mathbb{Z}$, para todo $i = 1, 2, \ldots, n$. Assim

$$b_1a_n\alpha_1 + \ldots + b_na_n\alpha_n = 0.$$

Como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, segue que $b_ia_n = 0$. Mas $a_n \neq 0$, logo $b_i = 0$, para todo $i = 1, 2, \ldots, n$. Portanto, $\{z_1, z_2, \ldots, z_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, contida em $\mathcal{O}_{\mathbb{L}}$. Pelo Lema 2.3.2 existe uma base $\{\beta_1, \ldots, \beta_n\}$ de $\mathbb{L}$ sobre $\mathbb{Q}$ tal que

$$\rho(z_i)(\beta_j) = S_{z_i}(\beta_j) = Tr_{\mathbb{L}|\mathbb{Q}}(z_i\beta_j) = \delta_{ij}, \text{para todo } i, j = 1, 2, \ldots, n.$$

Se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $\alpha z_i \in \mathcal{O}_{\mathbb{L}}$, e assim pelo Teorema 2.3.1 segue que $Tr_{\mathbb{L}|\mathbb{Q}}(\alpha z_i) \in \mathbb{Z}$, para todo $i = 1, 2, \ldots, n$. Se $\alpha \in \mathcal{O}_{\mathbb{L}}$, podemos escrever

$$\alpha = c_1\beta_1 + \ldots + c_n\beta_n, \text{ onde } c_i \in \mathbb{Q}, \text{para } i = 1, 2, \ldots, n.$$

Assim,

$$Tr_{\mathbb{L}|\mathbb{Q}}(\alpha z_i) = Tr_{\mathbb{L}|\mathbb{Q}}((c_1\beta_1 + \ldots + c_n\beta_n)z_i) = c_1Tr_{\mathbb{L}|\mathbb{Q}}(\beta_1 z_i) + \ldots + c_nTr_{\mathbb{L}|\mathbb{Q}}(\beta_n z_i) = c_i \in \mathbb{Q},$$

para todo $i = 1, 2, \ldots, n$. Como $Tr_{\mathbb{L}|\mathbb{Q}}(\alpha z_i) \in \mathbb{Z}$, segue que $c_i \in \mathbb{Z}$, para todo $i = 1, 2, \ldots, n$. Logo, $\mathcal{O}_{\mathbb{L}} \subseteq \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$. Mas, por outro lado, segue que o conjunto $\mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$ é um $\mathbb{Z}$-módulo, pois é um grupo abeliano e podemos definir uma aplicação $\varphi : \mathbb{Z} \times \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n \to \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$, e dados $a, b \in \mathbb{Z}$ e $m, n \in \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$, os mesmos satisfazem as propriedades de módulo. Como $\{\beta_1, \ldots, \beta_n\}$ é linearmente independente e gera $\mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$, segue que $\mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$ é um $\mathbb{Z}$-módulo livre de posto n. Agora, como $\mathcal{O}_{\mathbb{L}}$ é um grupo, segue que $\mathcal{O}_{\mathbb{L}}$ é subgrupo de $\mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n$, e se tomarmos $\alpha \in \mathcal{O}_{\mathbb{L}}$, então α é raiz de um polinômio minimal com coeficientes em $\mathbb{Z}$, ou seja,

$$\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0 = 0, \text{ onde } b_i \in \mathbb{Z}, \text{ para todo } i = 1, 2, \ldots, n.$$

Assim, dado $a \in \mathbb{Z}$, temos que $a^n(\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0) = 0$, e deste modo

$$(a\alpha)^n + ab_{n-1}(a\alpha)^{n-1} + \ldots + a^{n-1}b_1(a\alpha) + a^nb_0 = 0, \text{ onde } a^ib_{n-i} \in \mathbb{Z}, \text{para todo } i = 1, 2, \ldots, n.$$

Portanto, $a\alpha \in \mathcal{O}_{\mathbb{L}}$, e deste modo $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um $\mathbb{Z}$-módulo livre de posto n. Como $\mathbb{Z}$ é um anel principal, segue pelo Teorema 1.2.1 que $\mathcal{O}_{\mathbb{L}}$ é livre de posto menor ou igual a n. Como $\mathcal{O}_{\mathbb{L}}$ contém a base $\{z_1, \ldots, z_n\}$, segue que $\mathcal{O}_{\mathbb{L}}$ é um $\mathbb{Z}$-módulo livre de posto n. Finalmente, se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$, então $\mathcal{A}$ é um submódulo de $\mathcal{O}_{\mathbb{L}}$, e pelo Teorema 1.2.1, é livre de posto menor ou igual a n. Se $\{z_1, \ldots, z_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ e a é um elemento não nulo de $\mathcal{A}$, então $az_i \in \mathcal{A}$, para todo $i = 1, 2, \ldots, n$. Tomemos a seguinte combinação

$$\alpha_1az_1 + \alpha_2az_2 + \ldots + \alpha_naz_n = 0.$$

Como $\{z_1, \ldots, z_n\}$ é base, segue que $\alpha_ia = 0$, para todo $i = 1, 2, \ldots, n$, e como $a \neq 0$, segue que $\alpha_i = 0$, para todo $i = 1, 2, \ldots, n$. Assim, $\{az_1, az_2, \ldots, az_n\}$ é um conjunto linearmente independente contido em $\mathcal{A}$. Portanto, $\mathcal{A}$ é um $\mathbb{Z}$-módulo livre de posto n. ∎

Definição 2.3.6 *Uma $\mathbb{Z}$-base para o grupo aditivo $O_{\mathbb{L}}$ é chamada de base integral de $\mathbb{L}$ ou de $O_{\mathbb{L}}$.*

Observação 2.3.1 *Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Z}$-base de $O_{\mathbb{L}}$, onde n é o grau de $\mathbb{L}$ sobre $\mathbb{Q}$, então todo elemento $\alpha \in O_{\mathbb{L}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, 2, \cdots, n$.*

2.4 Discriminante

Nesta seção apresentamos conceitos básicos de discriminante enfocando suas principais propriedades.

Definição 2.4.1 *Sejam $\mathbb{L}$ um corpo de números de grau n, $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$ e $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. Definimos o discriminante dessa base por*

$$D(\alpha_1, \cdots, \alpha_n) = det[\sigma_i(\alpha_j)]^2.$$

Teorema 2.4.1 ([2]) *O discriminante de qualquer base de $\mathbb{L} = \mathbb{Q}(\theta)$ é racional e não nulo. Se todos os $\mathbb{L}$-monomorfismos de θ são reais, então o discriminante de qualquer base é positivo.*

Teorema 2.4.2 ([2]) *Sejam $\alpha_1, \cdots, \alpha_n$ elementos de $O_{\mathbb{L}}$ formando uma $\mathbb{Q}$-base para $\mathbb{L}$. Se $D(\alpha_1, \cdots, \alpha_n)$ é livre de quadrados, então $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral.*

Teorema 2.4.3 ([2]) *Se $\mathbb{L}$ é um corpo de números de grau n, $\{\alpha_1, \cdots, \alpha_n\}$ e $\{\beta_1, \cdots, \beta_n\}$ são bases integrais de $\mathbb{L}$, então*

$$D(\alpha_1, \cdots, \alpha_n) = D(\beta_1, \cdots, \beta_n).$$

Proposição 2.4.1 ([2]) *Seja $\mathbb{L} = \mathbb{Q}(\theta)$ um corpo de números, onde θ tem polinômio minimal p de grau n. A $\mathbb{Q}$-base $\{1, \theta, \cdots, \theta^{n-1}\}$ de $\mathbb{L}$ tem discriminante dado por*

$$D(1, \theta, \cdots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{L}/\mathbb{Q}}(Dp(\theta))$$

onde Dp é a derivada formal de p.

Proposição 2.4.2 ([2]) *Seja $\mathbb{L}$ um corpo de números. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Q}$-base de $\mathbb{L}$, então*

$$D(\alpha_1, \cdots, \alpha_n) = det(Tr_{\mathbb{L}/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j=1}^{n}.$$

Definição 2.4.2 *Sejam $\mathbb{L}$ um corpo de números, $O_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$ e $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $O_{\mathbb{L}}$. Definimos o discriminante do corpo $\mathbb{L}$ como sendo o ideal principal de $\mathbb{Z}$ gerado por $D(\alpha_1, \cdots, \alpha_n)$, e denotamos por $\mathfrak{D}_{\mathbb{L}}$.*

Observação 2.4.1 *Pelo Teorema* 2.4.3 *temos que o discriminante do corpo $\mathbb{L}$ independe da base de $O_{\mathbb{L}}$.*

2.5 Norma de um ideal

Nesta seção introduzimos o conceito de norma de um ideal juntamente com suas principais propriedades.

Definição 2.5.1 *Sejam $\mathbb{L}$ um corpo de números de grau finito n, $O_{\mathbb{L}}$ o anel dos inteiros de $\mathbb{L}$ e A um ideal não nulo de $O_{\mathbb{L}}$. Definimos a norma do ideal A como sendo o número de elementos do anel quociente $O_{\mathbb{L}}/A$, isto é, $N_{\mathbb{L}/\mathbb{Q}}(A) = \pm(O_{\mathbb{L}}/A)$.*

Observação 2.5.1 *Quando não houver dúvida quanto ao anel que contém o ideal A, usaremos $N(A)$ ao invés de $N_{\mathbb{L}/\mathbb{Q}}(A)$.*

Teorema 2.5.1 ([2]) *Se $A = h\alpha i$ é um ideal principal de $O_{\mathbb{L}}$, então $N(A) = jN(\alpha)j$.*

Teorema 2.5.2 ([2]) *Se $\mathbb{L}$ é um corpo de números e A,B são ideais não nulos de $O_{\mathbb{L}}$, então*

$$N(AB) = N(A)N(B).$$

Para o próximo resultado é conveniente introduzirmos uma outra notação para a palavra divide. Se A é um ideal de $O_{\mathbb{L}}$ e $b \in O_{\mathbb{L}}$ tal que $A \mid hbi$, então escrevemos também $A \mid b$ e dizemos que A divide b.

Teorema 2.5.3 ([2]) *Sejam $\mathbb{L}$ um corpo de números e A um ideal de $O_{\mathbb{L}}$, $A \neq 0$.*
(a) Se $N(A)$ é um primo, então A é um ideal primo,
(b) $N(A)$ é um elemento de A, ou equivalentemente, $A \mid N(A)$,
(c) Se A é um ideal primo que divide um primo p, então $N(A) = p^m$, onde m é o grau de $\mathbb{L}$.

2.6 Corpos quadráticos

Nesta seção apresentamos os corpos quadráticos, enfocando suas principais propriedades.

Definição 2.6.1 *Um corpo quadrático é um corpo de números $\mathbb{L}$ de grau 2 sobre $\mathbb{Q}$. Mais especificamente, $\mathbb{L} = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, e θ é um zero de um polinômio*

$$x^2 + ax + b \qquad (a, b \in \mathbb{Z}).$$

Proposição 2.6.1 ([2]) *Os corpos quadráticos são precisamente aqueles da forma $\mathbb{Q}(\sqrt{d})$ para d um inteiro livre de quadrados.*

Exemplo 2.6.1 *O corpo $\mathbb{L} = \mathbb{Q}(\sqrt{13})$ é um corpo quadrático, pois $\theta = \sqrt{13}$ é um zero do polinômio $f(x) = x^2 - 13$.*

Teorema 2.6.1 ([2]) *Se $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, então o anel dos inteiros algébricos de $\mathbb{L}$ é dado por:*
(i) $\mathbb{Z}[\sqrt{d}]$, se $d \not\equiv 1 (mod\ 4)$,
(ii) $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$, se $d \equiv 1 (mod\ 4)$.

Teorema 2.6.2 ([2]) *Seja* $\mathbb{Q}(\sqrt{d})$ *um corpo quadrático, onde* d *é um inteiro livre de quadrados.*
(a) Se $d \equiv 1 \pmod 4$*, então o corpo* $\mathbb{Q}(\sqrt{d})$ *tem uma base integral da forma* $\{1, \sqrt{d}\}$ *e discriminante* $4d$*.*
(b) Se $d \not\equiv 1 \pmod 4$*, então* $\mathbb{Q}(\sqrt{d})$ *tem uma base integral da forma* $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ *e discriminante* d*.*

Observação 2.6.1 *Um corpo quadrático* $\mathbb{Q}(\sqrt{d})$ *é dito real, se* d *é positivo, e imaginário se* d *é negativo.*

2.7 Corpos ciclotômicos

Nesta seção apresentamos os corpos ciclotômicos juntamente com suas propriedades. É sobre esses corpos e também sobre seus subcorpos que nosso trabalho está inserido.

Definição 2.7.1 *Seja* n *um inteiro positivo. Dizemos que* ζ_n *é uma raiz* n*-ésima da unidade se* $\zeta_n^n = 1$*, e que* ζ_n *é uma raiz* n*-ésima primitiva da unidade se* $\zeta_n^n = 1$ *e* $\zeta_n^m \neq 1$*, para todo* $1 \leq m \leq n - 1$*. O corpo* $\mathbb{Q}(\zeta_n)$ *é chamado corpo ciclotômico.*

Teorema 2.7.1 ([7]) *Se* n *é um inteiro positivo,* ζ_n *uma raíz* n*-ésima primitiva da unidade e* $\mathbb{L} = \mathbb{Q}(\zeta_n)$ *o corpo ciclotômico correspondente, então*

1. $[\mathbb{L} : \mathbb{Q}] = \phi(n)$*, onde* ϕ *é a função de Euler.*
2. $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n]$ *e* $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}\}$ *é uma base integral de* $\mathbb{L}$*.*
3. $[\mathbb{L} : \mathbb{K}] = 2$*, onde* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *é o subcorpo maximal real.*
4. $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ *e* $\{\zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \ldots, \zeta_n^{\frac{\phi(n)}{2}} + \zeta_n^{\frac{i\,\phi(n)}{2}}\}$ *é uma base integral do subcorpo* $\mathbb{K}$*.*

Proposição 2.7.1 ([8]) *Se* n *e* m *são dois números inteiros tais que* $n, m \geq 1$ *e* $mdc(n, m) = 1$*, então*

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

Teorema 2.7.2 ([7]) *O discriminante do corpo* $\mathbb{L} = \mathbb{Q}(\zeta_n)$ *é dado por*

$$\mathfrak{D}_{\mathbb{L}} = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}},$$

onde p *é um número primo.*

Teorema 2.7.3 ([9]) *Se p é um número primo ímpar, r um inteiro positivo e $\mathbb{K} \subset \mathbb{Q}(\zeta_{p^r})$, onde $[\mathbb{K}:\mathbb{Q}] = up^j$, e p não divide u, então*

$$\mathfrak{D}_{\mathbb{K}} = \langle p^v \rangle,$$

onde $v = u((j+2)p^j - \frac{p^{j+1}-1}{p-1}) - 1$.

Exemplo 2.7.1 *Tomando o corpo ciclotômico $\mathbb{L} = \mathbb{Q}(\zeta_{25})$, pelo Teorema 2.7.1, segue que $[\mathbb{L}:\mathbb{Q}] = 20$, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{25}]$, $\{1, \zeta_{25}, \zeta_{25}^2, \ldots, \zeta_{25}^{19}\}$ é uma base integral de $\mathbb{L}$ e pelo Teorema 2.7.2 temos que $\mathfrak{D}_{\mathbb{L}} = \langle 5^{35} \rangle$. Temos também que $\mathbb{K} = \mathbb{Q}(\zeta_{25}+\zeta_{25}^{-1})$ é o subcorpo maximal real de $\mathbb{L}$ com base integral $\{\zeta_{25}+\zeta_{25}^{-1}, \zeta_{25}^2+\zeta_{25}^{-2}, \ldots, \zeta_{25}^{10}+\zeta_{25}^{-10}\}$, e pelo Teorema 2.7.3 temos que $\mathfrak{D}_{\mathbb{K}} = \langle 5^{17} \rangle$.*

Definição 2.7.2 *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma extensão cíclica, se o grupo $G = Gal(\mathbb{L}/\mathbb{K})$ é cíclico.*

Teorema 2.7.4 *A extensão ciclotômica $\mathbb{Q}(\zeta_n)$ é cíclica se, e somente se, $n = 2, 4, p^r$ ou $2p^r$, onde $p > 2$ é um número primo e $r \geq 1$ é um número natural.*

Demonstração: Como o grupo de Galois de $\mathbb{Q}(\zeta_n)$ é isomorfo a $\mathbb{Z}_n^*$, segue pelo Teorema 1.4.1 o resultado. ∎

2.8 Decomposição de ideais em uma extensão

Nesta seção apresentamos a decomposição de ideais em uma extensão juntamente com suas principais propriedades. O resultado mais importante desta seção é o Lema de Kummer que nos auxilia na fatoração de ideais em uma extensão.

Definição 2.8.1 *Um anel é dito um anel noetheriano quando seus ideais são finitamente gerados.*

As condições abaixo são equivalentes à Definição 2.8.1. Para isso, seja A um anel.

1. A condição de cadeia ascendente: Dada uma cadeia ascendente de ideais de A

   $$A_1 \subset A_2 \ldots \subset A_n \subset \ldots$$

   então existe algum n_0 tal que $A_n = A_{n_0}$, para todo $n \geq n_0$, ou seja, toda cadeia ascendente é estacionária.

2. A condição maximal: Todo conjunto não vazio de ideais do anel A tem um elemento maximal, isto é, um elemento que não está propriamente contido em qualquer outro elemento.

Definição 2.8.2 *Um anel é dito um anel de Dedekind se for integralmente fechado, noetheriano e se todo ideal primo não nulo for maximal.*

Teorema 2.8.1 ([2]) *O anel do inteiros algébricos $O_{\mathbb{L}}$ de um corpo de números $\mathbb{L}$ tem as seguintes propriedades:*
(**a**) *$O_{\mathbb{L}}$ é um domínio, com corpo de frações $\mathbb{L}$,*
(**b**) *$O_{\mathbb{L}}$ é Noetheriano,*
(**c**) *Se α 2 $\mathbb{L}$ satisfaz um polinômio mônico com coeficientes em $O_{\mathbb{L}}$, então α 2 $O_{\mathbb{L}}$,*
(**d**) *Todo ideal primo não nulo de $O_{\mathbb{L}}$ é maximal.*

Temos que um ideal pode ser descrito como um $O_{\mathbb{L}}$-submódulo de $O_{\mathbb{L}}$, dessa forma restringimos ao estudo de $O_{\mathbb{L}}$-submódulos de $O_{\mathbb{L}}$.

Definição 2.8.3 *Sejam $\mathbb{L}$ um corpo de números e $O_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$. Um $O_{\mathbb{L}}$-submódulo A de $\mathbb{L}$ é dito um ideal fracionário de $O_{\mathbb{L}}$ se existe algum c 2 $O_{\mathbb{L}}$, não nulo, tal que cA μ $O_{\mathbb{L}}$.*

Teorema 2.8.2 ([2]) *Sejam $\mathbb{L}$ um corpo de números e $O_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$. Os ideais fracionários não nulos de $O_{\mathbb{L}}$ formam um grupo abeliano multiplicativo.*

Teorema 2.8.3 ([2]) *Sejam $\mathbb{L}$ um corpo de números e $O_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$. Todo ideal não nulo de $O_{\mathbb{L}}$ pode ser escrito como o produto de ideais primos unicamente determinados a menos da ordem dos fatores.*

Proposição 2.8.1 ([1]) *Se $\mathbb{K}$ ½ $\mathbb{L}$ são corpos de números, com $[\mathbb{L} : \mathbb{K}] = n$, P um ideal primo não nulo de $O_{\mathbb{K}}$ e*

$$PO_{\mathbb{L}} = \prod_{i=1}^{g} P_i^{e_i}$$

a decomposição de $PO_{\mathbb{L}}$ em ideais primos P_i de $O_{\mathbb{L}}$, então os ideais P_i são precisamente os ideais primos Q de $O_{\mathbb{L}}$ tais que $Q \setminus O_{\mathbb{K}} = P$.

Definição 2.8.4 *Nas condições da Proposição* 2.8.1*, dizemos que os ideais P_i estão acima do ideal P, g é denominado número de decomposição de P na extensão $\mathbb{L}/\mathbb{K}$, e os expoentes e_i são chamados de índices de ramificação, que denotaremos por $e(Q|P)$. Dizemos que um ideal primo P de $O_{\mathbb{K}}$ é ramificado em $O_{\mathbb{L}}$(ou em $\mathbb{L}$) se, $e(Q|P) > 1$ para algum ideal primo Q de $O_{\mathbb{L}}$ acima de P.*

Teorema 2.8.4 ([10]) *Sejam $\mathbb{K}$ μ $\mathbb{L}$ corpos, $O_{\mathbb{K}}$ e $O_{\mathbb{L}}$ seus respectivos anéis dos inteiros algébricos. Se P é um ideal primo de $O_{\mathbb{K}}$ e Q um ideal primo de $O_{\mathbb{L}}$, então as seguintes condições são equivalentes:*
(*a*) *Q j $PO_{\mathbb{L}}$,*
(*b*) *Q ¾ $PO_{\mathbb{L}}$,*
(*c*) *Q ¾ P,*
(*d*) *$Q \setminus O_{\mathbb{K}} = P$,*
(*e*) *$Q \setminus \mathbb{K} = P$.*

Observação 2.8.1 *Na ocorrência de qualquer uma das condições acima, dizemos que Q está acima de P. Os anéis quocientes $O_{\mathbb{K}}/P$ e $O_{\mathbb{L}}/Q$ são corpos, pois todo ideal primo não nulo de $O_{\mathbb{K}}$ e $O_{\mathbb{L}}$ são ideais maximais. Como $O_{\mathbb{K}}$ ½ $O_{\mathbb{L}}$, se tomarmos o homomorfismo canônico $\rho : O_{\mathbb{K}}$! $O_{\mathbb{L}}/Q$, segue que $Ker(\rho) = Q \setminus O_{\mathbb{K}} = P$. Assim, pelo teorema do homomorfismo $O_{\mathbb{K}}/Ker(\rho)$ ' $Im(\rho)$ ½ $O_{\mathbb{L}}/Q$, ou seja, obtemos a imersão $O_{\mathbb{K}}/P$! $O_{\mathbb{L}}/Q$. Deste modo, podemos olhar $O_{\mathbb{K}}/P$ como um subcorpo de $O_{\mathbb{L}}/Q$. Esses corpos são chamados de corpos residuais associados a P e a Q. Além disso, são corpos finitos, e assim $[O_{\mathbb{L}}/Q : O_{\mathbb{K}}/P] = f$, onde f é chamado grau de inércia ou grau residual de Q sobre P, e denotamos por $f(Q|P)$.*

Teorema 2.8.5 ([10]) *(Igualdade fundamental) Sejam $\mathbb{K}$ µ $\mathbb{L}$ corpos tal que $[\mathbb{L} : \mathbb{K}] = n$, e $O_{\mathbb{K}}$ e $O_{\mathbb{L}}$ seus respectivos anéis dos inteiros algébricos. Se $Q_1, \ldots, Q_g$ são os ideais primos de $O_{\mathbb{L}}$ acima do ideal primo P de $O_{\mathbb{K}}$, então*

$$n = \sum_{i=1}^{g} e_i f_i = \left[\frac{O_{\mathbb{L}}}{PO_{\mathbb{L}}} : \frac{O_{\mathbb{K}}}{P} \right] = [O_{\mathbb{L}} : PO_{\mathbb{L}}],$$

onde $e_1, \ldots, e_g$ e $f_1, \ldots, f_g$ são os correspondentes índices de ramificação e graus residuais.

Definição 2.8.5 *Sejam $\mathbb{K}$ µ $\mathbb{L}$ corpos tal que $[\mathbb{L} : \mathbb{K}] = n$, e $O_{\mathbb{K}}$ e $O_{\mathbb{L}}$ seus respectivos anéis dos inteiros algébricos. Dizemos que o ideal P de $O_{\mathbb{K}}$ é:*
(i) totalmente decomposto em $\mathbb{L}$, se $g = n$ e assim $e_i = f_i = 1$ para todo $i = 1, 2, \ldots, g$,
(ii) inerte em $\mathbb{L}$, se $g = 1$, $e_1 = 1$ e assim $f_1 = n$,
(iii) totalmente ramificado em $\mathbb{L}$, se $g = 1$ e assim $f_1 = 1$ e $e_1 = n$.

Teorema 2.8.6 ([1]) *Seja $\mathbb{L}$ um corpo de números. Uma condição necessária e suficiente para que um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifique em $O_{\mathbb{L}}$ é que p divida $\mathfrak{D}_{\mathbb{L}}$.*

Lema 2.8.1 ([11]) *(Lema de Kummer) Sejam $\mathbb{L}$ um corpo de números, $O_{\mathbb{L}}$ o seu anel dos inteiros algébricos e θ 2 $O_{\mathbb{L}}$ tal que $\mathbb{L} = \mathbb{Q}(\theta)$. Se p é um número tal que p não divide $[O_{\mathbb{L}} : \mathbb{Z}[\theta]]$ e $f(x)$ é o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem polinômios irredutíveis $p_1(x), \ldots, p_g(x)$ 2 $\mathbb{Z}[X]$, $e_1, \ldots, e_g$ 2 $\mathbb{N}^*$, tais que*

$$f(x) \acute{} p_1(x)^{e_1} \ldots p_g(x)^{e_g} (mod\ p\mathbb{Z}[X]),$$

e além disso

1. *$P_i = (p, p_i(\theta)) = pO_{\mathbb{L}} + p_i(\theta)O_{\mathbb{L}}$ são ideais primos de $O_{\mathbb{L}}$ acima de $p\mathbb{Z}$, $i = 1, 2, \ldots, g$.*
2. *$pO_{\mathbb{L}} = \prod_{i=1}^{g} P_i^{e_i}$.*
3. *$[O_{\mathbb{L}}/P_i : \mathbb{Z}/p\mathbb{Z}] = \partial p_i(x) = f_i$, onde $\partial p_i(x)$ denota o grau de $p_i(x)$.*

Exemplo 2.8.1 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{11})$, $x^2 - 11$ *o polinômio irredutível de* $\sqrt{11}$ *sobre* $\mathbb{Q}$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{11}]$ *o seu anel dos inteiros algébricos. Considerando o ideal* $5\mathbb{Z} \subsetneq \mathbb{Z}$, *temos que o polinômio* $x^2 - 11$ *fatora-se como:*

$$x^2 - 11 \equiv (x+1)(x+4)(mod\ 5\mathbb{Z}[X]).$$

Assim, pelo Lema de Kummer, temos:
(**i**) $\mathcal{P}_1 = \langle 5, \theta + 1 \rangle$, *e* $\mathcal{P}_2 = \langle 5, \theta + 4 \rangle$ *são ideais de* $\mathcal{O}_{\mathbb{L}}$ *acima de* $5\mathbb{Z}$,
(**ii**) $5\mathbb{Z} = \mathcal{P}_1\mathcal{P}_2$,
(**iii**) $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}_1} : \dfrac{\mathbb{Z}}{5\mathbb{Z}}\right] = \left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}_2} : \dfrac{\mathbb{Z}}{5\mathbb{Z}}\right] = 1 = f_1 = f_2$.
E pelo Teorema da Igualdade Fundamental, temos que os graus residuais são $f_1 = f_2 = 1$ *e os índices de ramificação são* $e_1 = e_2 = 1$.

Exemplo 2.8.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{7})$, $x^2 - 7$ *o polinômio irredutível de* $\sqrt{7}$ *sobre* $\mathbb{Q}$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{7}]$ *o seu anel dos inteiros algébricos. Considerando o ideal* $2\mathbb{Z} \subsetneq \mathbb{Z}$, *temos que o polinômio* $x^2 - 7$ *fatora-se como:*

$$x^2 - 7 \equiv (x+1)^2(mod\ 2\mathbb{Z}[X]).$$

Assim, pelo Lema de Kummer, temos:
(**i**) $\mathcal{P}_1 = \langle 2, \theta + 1 \rangle$ *é o único ideal primo de* $\mathcal{O}_{\mathbb{L}}$ *acima de* $2\mathbb{Z}$,
(**ii**) $2\mathbb{Z} = \mathcal{P}_1\mathcal{P}_1$,
(**iii**) $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}_1} : \dfrac{\mathbb{Z}}{2\mathbb{Z}}\right] = 1 = f_1$.
E pelo Teorema da Igualdade Fundamental, temos que o grau residual é $f_1 = 1$ *e o índice de ramificação é* $e_1 = 2$.

Sejam $\mathbb{L}$ uma extensão galoisiana de $\mathbb{K}$, $\mathcal{O}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{K}}$ seus respectivos anéis dos inteiros algébricos e $\mathcal{Q}$,$\mathcal{Q}'$ ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de um ideal primo $\mathcal{P}$ de $\mathcal{O}_{\mathbb{K}}$.

Teorema 2.8.7 ([10]) *(Teorema da Evidência) Sejam* $\mathbb{K} \subset \mathbb{L}$ *corpos,* $\mathcal{O}_{\mathbb{K}}$ *e* $\mathcal{O}_{\mathbb{L}}$ *seus respectivos anéis dos inteiros algébricos. Se* $\mathbb{L}/\mathbb{K}$ *é uma extensão galoisiana com grupo de Galois* G *e,* $\mathcal{Q}$ *e* $\mathcal{Q}'$ *são ideais primos de* $\mathcal{O}_{\mathbb{L}}$ *tais que* $\mathcal{Q} \cap \mathcal{O}_{\mathbb{K}} = \mathcal{Q}' \cap \mathcal{O}_{\mathbb{K}}$, *então existe* $\sigma \in G$ *tal que* $\sigma(\mathcal{Q}) = \mathcal{Q}'$.

Capítulo

3

Reticulados

3.1 Introdução

Neste capítulo apresentamos as definições e as principais propriedades dos reticulados. Desse modo, na Seção 3.2, definimos reticulado e região fundamental. Na Seção 3.3, definimos empacotamento esférico, densidade de empacotamento, volume de um reticulado e densidade de centro. Para finalizar, na Seção 3.4, apresentamos também as propriedades de alguns reticulados construtivos importantes conhecidos na literatura, principalmente os reticulados até dimensão 8.

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 μ $\mathbb{K}$ um anel e $v_1, ¢¢¢ , v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$ com $m \cdot n$. Chama-se* **reticulado** *com base $\beta = fv_1, ¢¢¢ , v_mg$ ao conjunto dos elementos de V da forma*

$$H_\beta = \left\{ x = \sum_{i=1}^{m} a_i v_i, \quad com\ a_i\ 2\ A \right\}.$$

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_β ½ $\mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = fv_1, ¢¢¢ , v_ng$. O conjunto*

$$P_\beta = \left\{ x\ 2\ \mathbb{R}^n : x = \sum_{i=1}^{n} \lambda_i v_i,\ 0 \cdot \lambda_i < 1 \right\},$$

é chamado de região fundamental de H_β com relação a base $fv_1, ¢¢¢ , v_ng$.

Note que a região fundamental depende da escolha dos geradores. 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 $\mathbb{Z}$.

Observação 3.2.1 *Denotamos por H e P, respectivamente, o reticulado e a região fundamental com relação a base canônica.*

Lema 3.2.1 ([2]) *Cada elemento do $\mathbb{R}^n$ pertence a exatamente um dos conjuntos $P + l$, para $l \in H$.*

Demonstração: Primeiramente mostremos a existência do conjunto $P + l$. Se $\{e_1, \ldots, e_n\}$ é um conjunto de vetores linearmente independentes do $\mathbb{R}^n$, então todo elemento $x \in \mathbb{R}^n$ pode ser escrito da seguinte maneira:

$$x = \sum_{i=1}^{n} a_i e_i, \text{ onde } a_i \in \mathbb{R}, \text{ para } i = 1, 2, \ldots, n.$$

Mas podemos separar a parte inteira de cada coeficiente a_i, ou seja, podemos escrever

$$a_i = \alpha_i + \beta_i, \text{ onde } \alpha_i \in \mathbb{Z}, \ 0 \leq \beta_i < 1 \text{ e } \beta_i \in \mathbb{R}, \text{ para } i = 1, 2, \ldots, n.$$

Assim, podemos reescrever x da seguinte maneira:

$$x = \sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) e_i = \sum_{i=1}^{n} \alpha_i e_i + \sum_{i=1}^{n} \beta_i e_i,$$

Portanto $x \in P + l$. Para a unicidade, suponhamos que x pertença simultaneamente a $P + l_1$ e $P + l_2$, onde $l_1, l_2 \in H$, ou seja,

$$x = \sum_{i=1}^{n} \beta_i e_i + \sum_{i=1}^{n} \alpha_i e_i, \quad \text{com } \alpha_i \in \mathbb{Z}, \ 0 \leq \beta_i < 1 \text{ e } \beta_i \in \mathbb{R}, \text{ para } i = 1, 2, \ldots, n.$$

$$x = \sum_{i=1}^{n} \gamma_i e_i + \sum_{i=1}^{n} \delta_i e_i, \quad \text{com } \delta_i \in \mathbb{Z}, \ 0 \leq \gamma_i < 1 \text{ e } \gamma_i \in \mathbb{R}, \text{ para } i = 1, 2, \ldots, n.$$

onde a primeira parcela das equações pertence a H e a segunda parcela são l_1 e l_2, respectivamente. Igualando, obtemos $\sum_{i=1}^{n} (\beta_i + \alpha_i) e_i = \sum_{i=1}^{n} (\gamma_i + \delta_i) e_i$. Assim,

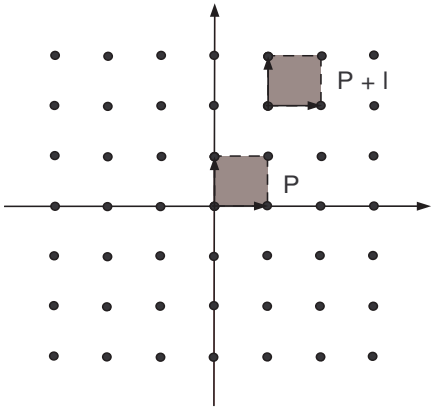
$$\sum_{i=1}^{n} (\beta_i + \alpha_i) e_i - \sum_{i=1}^{n} (\gamma_i + \delta_i) e_i = \sum_{i=1}^{n} (\beta_i + \alpha_i - \gamma_i - \delta_i) e_i = 0.$$

Como $\{e_1, \ldots, e_n\}$ é linearmente independente, segue que $\beta_i + \alpha_i - \gamma_i - \delta_i = 0$, para $i = 1, 2, \ldots, n$, e assim

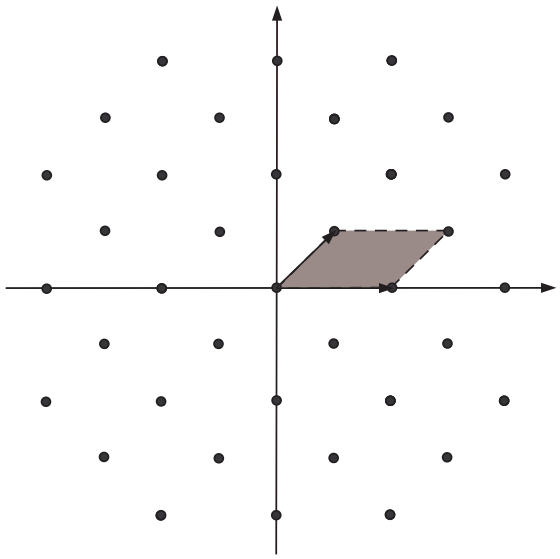
$$\beta_i - \gamma_i = \delta_i - \alpha_i. \tag{3.2.1}$$

Como $0 \leq \beta_i, \gamma_i < 1$, segue que $-1 < \beta_i - \gamma_i < 1$. Mas pela Equação (3.2.1), e pelo fato de que $\delta_i - \alpha_i \in \mathbb{Z}$, concluímos que $\delta_i = \alpha_i$, para $i = 1, 2, \ldots, n$. Assim, $l_1 = l_2$, e portanto x pertence a exatamente um dos conjuntos $P + l$, com $l \in H$. ∎

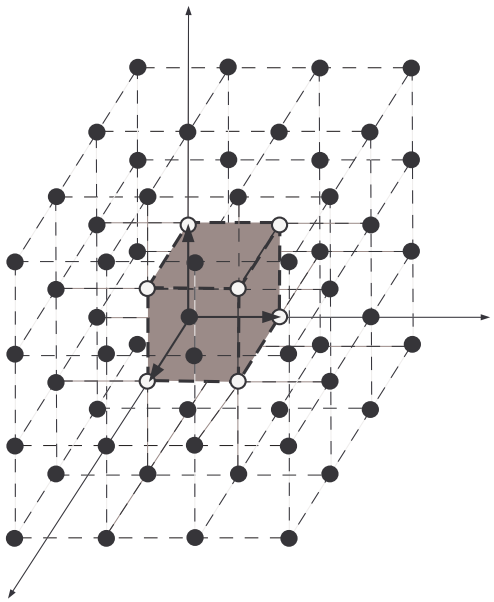
Exemplo 3.2.1 *$H = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$, com região fundamental P e uma translação $P + l$ descrita na figura abaixo.*



Exemplo 3.2.2 *Se $T : \mathbb{R}^2 \; ¡ \; ! \; \mathbb{R}^2$ é uma transformação linear definida por $T(x, y) = (x + y, x \; ¡ \; y)$, então $H_\beta = T(\mathbb{Z}^2)$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$, com região fundamental descrita na figura abaixo.*



Exemplo 3.2.3 *$H = \mathbb{Z}^3$ é um reticulado gerado pelos vetores $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ e $e_3 = (0, 0, 1)$, 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 K do $\mathbb{R}^n$, tivermos $H \setminus K$ finito.*

Exemplo 3.2.4 $\mathbb{Z}^3$ *é um subconjunto discreto do* $\mathbb{R}^3$.

3.3 Empacotamento esférico

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. 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 $C \setminus C' = \emptyset$, então $Vol(C \cup C') = Vol(C) + Vol(C')$.

Definição 3.3.1 *Sejam $H_\beta \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \ldots, v_n\}$ uma base de H_β e P_β a região fundamental. Se $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para $i = 1, 2, \ldots, n$, definimos o volume da*

região fundamental P_β, *como o módulo do determinante da matriz*

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

Definição 3.3.2 *Sejam* H_β *um reticulado e* $\beta = \{v_1, \cdots, v_n\}$ *uma base de* H_β, *onde* $v_i = (v_{i1}, v_{i2}, \cdots, v_{in})$, *para* $i = 1, 2, \cdots, n$. *Definimos o discriminante do reticulado* H_β *por*

$$Disc(H_\beta) = (det\ B)^2,$$

onde

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

Exemplo 3.3.1 *Seja* H_β *um reticulado,* $\beta = \{(1,1,2), (0,3,1), (i, 1, 3, 2)\}$ *uma base de* H_β *e* P_β *a região fundamental. Assim*

$$Vol(P_\beta) = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 3 & 1 \\ i & 1 & 3 & 2 \end{vmatrix} = |i\ i\ 4| = 4.$$

Proposição 3.3.1 ([1]) *O volume da região fundamental* $Vol(P_\beta)$ *é independente da base* β *de* H_β.

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

Definição 3.3.3 *Seja* H_β *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 α uma outra base para H_β, segue que $Vol(H_\beta) = Vol(H_\alpha)$, pois β e α 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 3.3.4

1. *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.*

2. *Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* H_β *de* $\mathbb{R}^n$.

3. *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.*

Observação 3.3.1 *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, assim* ρ *é chamado raio de empacotamento do reticulado. 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*

$$\Delta(H_\beta) = \frac{\textit{Volume da esfera}}{\textit{Volume da região fundamental}} = \frac{Vol(B(\rho))}{Vol(H_\beta)} = \frac{Vol(B(1))\rho^n}{Vol(H_\beta)}.$$

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

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

Logo, tiramos a seguinte relação

$$\Delta(H_\beta) = Vol(B(1))\delta(H_\beta)$$

ou seja, a densidade de empacotamente de H_β *é igual ao produto entre o volume da esfera com centro na origem e raio* 1 *e a densidade de centro* $\delta(H_\beta)$.

Exemplo 3.3.2 *Se* $H_\beta = \mathbb{Z}^2$ *com base* $\beta = \{(2,0),(1,1)\}$, *então* $\rho = \sqrt{2}/2$, $Vol(B(1)) = \pi$, *e o volume do reticulado é dado por*

$$Vol(H_\beta) = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} = 2.1 = 2,$$

e a densidade de centro é $\delta(H_\beta) = \dfrac{1}{4}$. *Logo, a densidade de empacotamento é dada por*

$$\Delta(H_\beta) = \frac{\pi}{4}.$$

Exemplo 3.3.3 *Se* $H_\beta = \mathbb{Z}^3$ *com base* $\beta = \{(4,0,0),(0,3,0),(0,2,1)\}$, *então* $\rho = \sqrt{5}/2$, $Vol(B(1)) = \dfrac{4\pi}{3}$, *e o volume do reticulado é dado por*

$$Vol(H_\beta) = \begin{vmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 2 & 1 \end{vmatrix} = 12,$$

e a densidade de centro é $\delta(H_\beta) = \dfrac{5\sqrt{5}}{96}$. *Logo, a densidade de empacotamente é dada por*

$$\Delta(H_\beta) = \frac{5\pi\sqrt{5}}{72}.$$

3.4 Reticulados importantes e suas propriedades

Nesta seção apresentamos as definições de reticulados conhecidos na literatura e que possuem densidade de centro recorde. Além disso, é provado que essas densidades são as melhores até a dimensão 8. Em dimensões maiores que 8, existem reticulados com densidades de centro ótimas (K_{12} e Λ_{24}), e existem reticulados com densidades de centro recordes, mas não se sabe se essas densidades são ótimas.

3.4.1 Reticulado n-dimensional A_n

Para todo $n \geq 1$, temos que

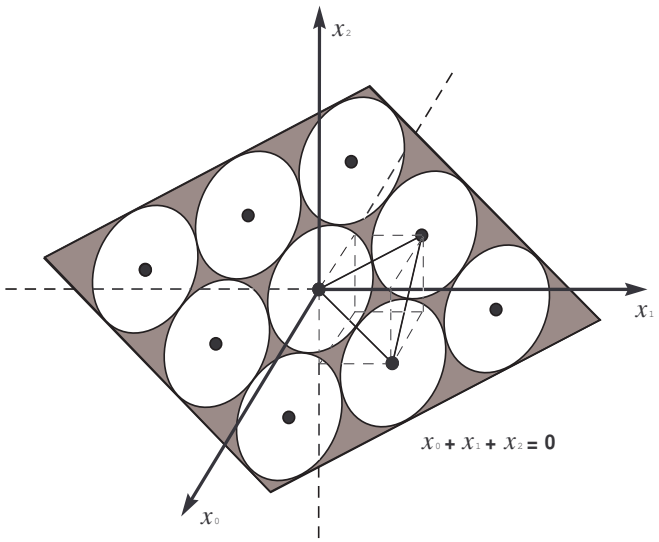
$$A_n = \{(x_0, x_1, \cdots, x_n) \in \mathbb{Z}^{n+1} : \ x_0 + x_1 + \cdots + x_n = 0\}$$

é um reticulado. Por definição, A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$, e possui uma matriz geradora M, dada por:

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

raio de empacotamento $\rho = \sqrt{2}/2$ e densidade de centro $\delta = 2^{-n/2}(n+1)^{-1/2}$.

Exemplo 3.4.1 *Reticulado 2-dimensional* A_2. *O reticulado* A_2 *é formado por todos os pontos* (x_0, x_1, x_2) *de* $\mathbb{Z}^3$ *que pertencem ao plano* $x_0+x_1+x_2 = 0$, *contido em* $\mathbb{R}^3$. *A figura abaixo mostra a disposição dos pontos do reticulado no espaço tridimensional, assim como o empacotamento associado.*



O raio de empacotamento é $\rho = \sqrt{2}/2$*, a densidade de centro é* $\delta = 1/2\sqrt{3} = 0,28868$*, que é a densidade de centro máxima para a dimensão 2.*

3.4.2 Reticulado n-dimensional D_n

Para todo $n \geq 3$, temos que

$$D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : \ x_1 + x_2 + \ldots + x_n \text{ é par}\}$$

é um reticulado. Em outras palavras, este reticulado pode ser obtido colorindo os pontos de $\mathbb{Z}^n$ alternadamente com vermelho e branco e tomando os pontos vermelhos. Possui matriz geradora M, dada por:

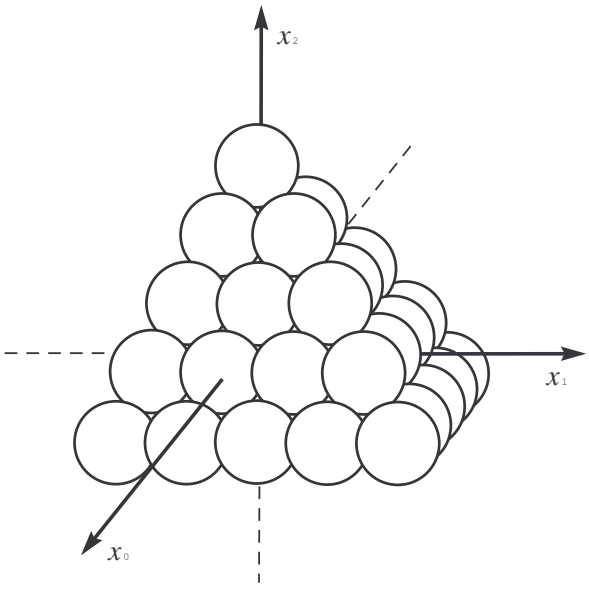
$$M = \begin{bmatrix} -1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 & 0 \\ . & . & . & . & \ddots & . & . \\ 0 & 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix},$$

raio de empacotamento $\rho = \sqrt{2}/2$ e densidade de centro $\delta = 2^{-(n+2)/2}$.

Exemplo 3.4.2 *Reticulado 3-dimensional* D_3*. O reticulado* D_3 *é formado por todos os pontos* $(x_1, x_2, x_3) \in \mathbb{Z}^3$ *tal que* $x_1 + x_2 + x_3$ *é um número par. Uma matriz geradora para* D_3 *é dada por*

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

A figura abaixo mostra o arranjo das esferas do empacotamento associado a D_3*.*



Este é o empacotamento normalmente encontrado em bancas de frutas (pirâmide de laranjas) ou empilhamento de balas de canhão, encontrado nos memoriais de guerra. O raio de empacotamento é $\rho = \sqrt{2}/2$*, a densidade de centro é* $\delta = 1/4\sqrt{3} = 0,17678$*, que é a densidade de centro máxima para a dimensão 3.*

Exemplo 3.4.3 *Reticulado 4-dimensional* D_4*. O reticulado* D_4 *é formado por todos os pontos* $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ *tal que* $x_1 + x_2 + x_3 + x_4$ *é um número par. Uma matriz geradora para* D_4 *é dada por*

$$M = \begin{bmatrix} i\,1 & i\,1 & 0 & 0 \\ 1 & i\,1 & 0 & 0 \\ 0 & 1 & i\,1 & 0 \\ 0 & 0 & 1 & i\,1 \end{bmatrix}.$$

O raio de empacotamento é $\rho = \sqrt{2}/2$*, a densidade de centro é* $\delta = 1/8 = 0,125$*, que é a densidade de centro máxima para a dimensão 4.*

Exemplo 3.4.4 *Reticulado 5-dimensional* D_5*. O reticulado* D_5 *é formado por todos os pontos* $(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$ *tal que* $x_1 + x_2 + x_3 + x_4 + x_5$ *é um número par. Uma matriz geradora para* D_5 *é dada por*

$$M = \begin{bmatrix} i\,1 & i\,1 & 0 & 0 & 0 \\ 1 & i\,1 & 0 & 0 & 0 \\ 0 & 1 & i\,1 & 0 & 0 \\ 0 & 0 & 1 & i\,1 & 0 \\ 0 & 0 & 0 & 1 & i\,1 \end{bmatrix}.$$

O raio de empacotamento é $\rho = \sqrt{2}/2$*, a densidade de centro é* $\delta = 1/8\sqrt{2} = 0,08839$*, que é a densidade de centro máxima para a dimensão 5.*

3.4.3 Reticulado 8-dimensional E_8

O reticulado E_8 é definido por

$$E_8 = \{(x_0, x_1, \cdots, x_8) \in \mathbb{R}^8 : \forall x_i,\ x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + 1/2,\ \sum x_i \equiv 0 (mod 2)\}.$$

Uma matriz geradora é dada por

$$M = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{bmatrix}.$$

O raio de empacotamento é $\rho = \sqrt{2}/2$, a densidade de centro é $\delta = 1/16 = 0,06250$, que é a densidade de centro máxima para a dimensão 8.

3.4.4 Reticulado 7-dimensional E_7

O reticulado E_7 é definido por

$$E_7 = \{x \in E_8 : xv = 0\},\ \textit{para algum vetor minimal } v \in E_8.$$

Uma matriz geradora é dada por

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 \\ 0 & 0 & 1/2 & 1/2 & 1/2 & 0 & 1/2 \end{bmatrix}.$$

O raio de empacotamento é $\rho = \sqrt{2}/2$, a densidade de centro é $\delta = 1/16 = 0,06250$, que é a densidade de centro máxima para a dimensão 7.

3.4.5 Reticulado 6-dimensional E_6

O reticulado E_6 é definido por

$$E_6 = \{x \in E_8 : xv = 0,\ \forall v \in V\},\ \textit{onde } V \textit{ é um } A_2 \textit{ subreticulado em } E_8.$$

Uma matriz geradora é dada por

$$M = \begin{bmatrix} 0 & i\,1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i\,1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i\,1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i\,1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & i\,1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & i\,1/2 & i\,1/2 & i\,1/2 & i\,1/2 \end{bmatrix}.$$

O raio de empacotamento é $\rho = \sqrt{2}/2$, a densidade de centro é $\delta = 1/8\sqrt{3} = 0,07217$, que é a densidade de centro máxima para a dimensão 6.

3.4.6 Reticulado laminado Λ_n

Seja $\Lambda_0 = \{A\}$, onde A é um ponto do $\mathbb{R}^n$. Para $n \geq 1$, tomemos todos os reticulados n-dimensionais com norma mínima igual a 4, que tenham no mínimo um subreticulado Λ_{n-1}, e selecione aqueles com discriminante mínimo. Este reticulado é chamado de reticulado laminado Λ_n.

Observação 3.4.1 *Até a dimensão* 8*, para as famílias de reticulados definidas acima, temos as seguintes equivalências:*

$$\begin{array}{ll} \Lambda_1 \cong \mathbb{Z} \cong A_1, & \Lambda_2 \cong A_2, \\ \Lambda_3 \cong A_3 \cong D_3, & \Lambda_4 \cong D_4, \\ \Lambda_5 \cong D_5, & \Lambda_6 \cong E_6, \\ \Lambda_7 \cong E_7, & \Lambda_8 \cong E_8. \end{array}$$

Observação 3.4.2 *Esses reticulados possuem densidades ótimas, no entanto no Capítulo* 7 *apresentamos reticulados algébricos de dimensões* 2*,* 4*,* 6 *e* 8 *que possuem a mesma densidade de centro destes reticulados. Além disso, esses reticulados algébricos possuem propriedades algébricas de melhor visualização dos mesmos.*

Capítulo

4

Reticulados via o homomorfismo de Minkowski

4.1 Introdução

Neste capítulo apresentamos o método de Minkowski, para a geração de reticulados no $\mathbb{R}^n$ via ideais do anel de inteiros de um corpo de números. Na Seçao 4.2, apresentamos a construção de reticulados pelo método de Minkowski, que neste trabalho chamaremos de reticulados algébricos.

4.2 Reticulados algébricos

Sejam $\mathbb{L}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_j : \mathbb{L} \to \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{L}) \subset \mathbb{R}$ diz-se que σ_j é real, caso contrário, σ_j é dito imaginário. Quando todos os monomorfismos são reais diz-se que $\mathbb{L}$ é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que $\mathbb{L}$ 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, $\sigma_j(\mathbb{L}) \subseteq \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_j(\mathbb{L}) \subseteq \mathbb{R}$, 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 $j = 1, \ldots, r_2$. Desse modo, $n - r_1$ é um número par, e assim podemos escrever $r_1 + 2r_2 = n$.

Definição 4.2.1 *Seja $x \in \mathbb{L}$ um elemento. O homomorfismo $\sigma_{\mathbb{L}} : \mathbb{L} \to \mathbb{R}^n$ definido por*

$$\sigma_{\mathbb{L}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

é um homomorfismo injetivo de anéis, chamado de homomorfismo canônico (ou Minkowski), onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Exemplo 4.2.1 *Sejam o corpo quadrático $\mathbb{L} = \mathbb{Q}(\sqrt{5})$ e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$,*

com $a, b \in \mathbb{Q}$. *Neste caso,* $r_1 = 2$ *e* $r_2 = 0$. *Para* $x = a + b\sqrt{5} \in \mathbb{L}$, *com* $a, b \in \mathbb{Q}$, *temos*

$$\sigma_{\mathbb{L}}(x) = (\sigma_1(x), \sigma_2(x)) = (a + b\sqrt{5}, a - b\sqrt{5}).$$

Exemplo 4.2.2 *Sejam o corpo ciclotômico* $\mathbb{L} = \mathbb{Q}(\zeta_3)$, *onde* $\zeta_3 = e^{\frac{2\pi i}{3}}$ *e* $\{\sigma_1, \sigma_2\}$ *o grupo dos* $\mathbb{Q}$*-monomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$. *Como* $\mathbb{L}$ *é um corpo totalmente complexo, temos que* $r_1 = 0$ *e* $r_2 = 1$. *Os 2 monomorfismos são dados por* $\sigma_1(\xi_3) = \xi_3$ *e* $\sigma_2(\xi_3) = \xi_3^2$. *Se* $x = a + b\xi_3 \in \mathbb{L}$, *com* a, $b \in \mathbb{Q}$, *temos que*

$$\sigma_{\mathbb{L}}(x) = (\Re\sigma_1(x),\ \Im\sigma_1(x)) = (\Re(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i), \Im(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i)) = (a - \frac{b}{2}, \frac{b\sqrt{3}}{2}).$$

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 $\mathbb{L}$. Isto pode ser visto de maneira formal nos resultados que seguem.

Proposição 4.2.1 ([1]) *Seja* $\mathbb{L}$ *um corpo de números de grau* n. *Se* $M \subset \mathbb{L}$ *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* $\sigma_{\mathbb{L}}(M)$ *é um reticulado no* $\mathbb{R}^n$, *com volume*

$$Vol(\sigma_{\mathbb{L}}(M)) = 2^{-r_2}\left|\det_{1\leq j,k\leq n}(\sigma_j(x_k))\right|.$$

Demonstração: Para cada j fixo, as coordenadas de $\sigma_{\mathbb{L}}(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \tag{4.2.1}$$

Agora calculemos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (4.2.1) 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 linha da sua posterior, para $l = 1, \ldots, r_2$. Assim,

$$D = \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \Re(\sigma_{r_1+1}(x_1)) & \ldots & \Re(\sigma_{r_1+1}(x_j)) & \ldots & \Re(\sigma_{r_1+1}(x_n)) \\ \Im(\sigma_{r_1+1}(x_1)) & \ldots & \Im(\sigma_{r_1+1}(x_j)) & \ldots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(x_1)) & \ldots & \Re(\sigma_{r_1+r_2}(x_j)) & \ldots & \Re(\sigma_{r_1+r_2}(x_n)) \\ \Im(\sigma_{r_1+r_2}(x_1)) & \ldots & \Im(\sigma_{r_1+r_2}(x_j)) & \ldots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix} =$$

$$= \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \frac{1}{2}[\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)}] & \dots & \frac{1}{2}[\sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)}] & \dots & \frac{1}{2}[\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)}] \\ \frac{1}{2i}[\sigma_{r_1+1}(x_1) \ i \ \overline{\sigma_{r_1+1}(x_1)}] & \dots & \frac{1}{2i}[\sigma_{r_1+1}(x_j) \ i \ \overline{\sigma_{r_1+1}(x_j)}] & \dots & \frac{1}{2i}[\sigma_{r_1+1}(x_n) \ i \ \overline{\sigma_{r_1+1}(x_n)}] \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{1}{2}[\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)}] & \dots & \frac{1}{2}[\sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)}] & \dots & \frac{1}{2}[\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)}] \\ \frac{1}{2i}[\sigma_{r_1+r_2}(x_1) \ i \ \overline{\sigma_{r_1+r_2}(x_1)}] & \dots & \frac{1}{2i}[\sigma_{r_1+r_2}(x_j) \ i \ \overline{\sigma_{r_1+r_2}(x_j)}] & \dots & \frac{1}{2i}[\sigma_{r_1+r_2}(x_n) \ i \ \overline{\sigma_{r_1+r_2}(x_n)}] \end{vmatrix}$$

$$= \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} 2^{r_2} D_1,$$

onde

$$D_1 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+1}(x_1) \ i \ \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) \ i \ \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) \ i \ \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \\ \sigma_{r_1+r_2}(x_1) \ i \ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) \ i \ \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) \ i \ \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

Assim,

$$D = \left(\frac{1}{2i}\right)^{r_2} D_1 = \left(\frac{1}{2i}\right)^{r_2} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_j)} & \dots & \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \end{vmatrix} =$$

$$= \left(\frac{1}{2i}\right)^{r_2} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix} = (2i)^{-r_2} \det(\sigma_j(x_k)).$$

Portanto, $D = (2i)^{-r_2}\det(\sigma_j(x_k))$, para $j,\ k = 1, \cdots, n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, pelo Teorema 2.4.1 segue que $\det(\sigma_j(x_k)) \neq 0$ e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{L}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{L}}(M)$. Do fato de $\{x_1, \ldots, x_n\}$ ser uma $\mathbb{Z}$-base de M, então dado $m \in M$, segue que $m = \sum_{j=1}^{n} a_j x_j$, com $a_j \in \mathbb{Z}$. Assim, $\sigma_{\mathbb{L}}(m) = \sum_{j=1}^{n} a_j \sigma_{\mathbb{L}}(x_j)$, com $a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{L}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{L}}(x_j);\ a_j \in \mathbb{Z} \right\}$ é um reticulado no $\mathbb{R}^n$, com volume

$$Vol(\sigma_{\mathbb{L}}(M)) = |D| = 2^{-r_2}\left|\det_{1\leq j,k\leq n}(\sigma_j(x_k))\right|,$$

o que prova a proposição. ∎

Proposição 4.2.2 ([1]) *Se $\mathbb{L}$ é um corpo de números de grau n, $\mathfrak{D}_{\mathbb{L}}$ o discriminante de $\mathbb{L}$, $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$, A um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$ e r_2 a metade do número de monomorfismos imaginários, então, $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$ e $\sigma_{\mathbb{L}}(A)$ são reticulados, com respectivos volumes,*

$$Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = 2^{-r_2}|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}},$$

$$Vol(\sigma_{\mathbb{L}}(A)) = Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}))N(A).$$

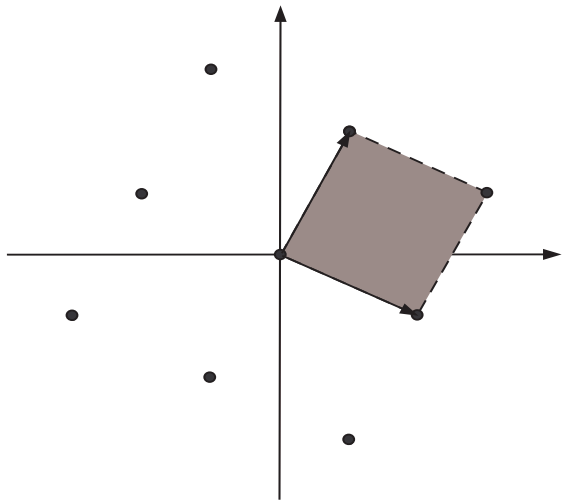
Demonstração: Pela Proposição 2.3.1 segue que A e $\mathcal{O}_{\mathbb{L}}$ são $\mathbb{Z}$-módulos livres de posto n. Logo pela Proposição 4.2.1 temos que $\sigma_{\mathbb{L}}(A)$ e $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = 2^{-r_2}|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}$, pois pela Definição 2.4.1 temos que $\mathfrak{D}_{\mathbb{L}} = \det(\sigma_i(x_k))^2$, onde $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}}$. Para a segunda fórmula, temos que $\sigma_{\mathbb{L}}(A)$ é um subgrupo de $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$ de índice $N(A)$ uma vez que $\mathcal{O}_{\mathbb{L}}/A$ é isomorfo a $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})/\sigma_{\mathbb{L}}(A)$. Além disso, como a região fundamental de $\sigma_{\mathbb{L}}(A)$ é a união disjunta de $N(A)$ cópias de uma região fundamental de $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$, segue que $Vol(\sigma_{\mathbb{L}}(A)) = 2^{-r_2}|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}N(A)$. Portanto $Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = 2^{-r_2}|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}$ e $Vol(\sigma_{\mathbb{L}}(A)) = Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}))N(A)$. ∎

Definição 4.2.2 *Sejam $\mathbb{L}$ um corpo de números, $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros algébricos de $\mathbb{L}$, $A \subsetneq \mathcal{O}_{\mathbb{L}}$ um ideal não nulo e $\sigma_{\mathbb{L}}$ o homomorfismo de Minkowski de $\mathbb{L}$. O reticulado $\sigma_{\mathbb{L}}(A)$ neste trabalho será chamado de reticulado algébrico.*

Exemplo 4.2.3 *Sejam $\mathbb{L} = \mathbb{Q}(i)$, onde $i^2 = -1$, e $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[i]$ seu anel dos inteiros algébricos com $\mathbb{Z}$-base $\{1, i\}$. Como $\mathbb{L}$ é totalmente imaginário, segue que $r_1 = 0$ e $r_2 = 1$. Seja A um ideal principal de $\mathbb{Z}[i]$ gerado por $2 - i$. Assim, dado $x \in A$ temos que $x = (2 - i)(a + bi)$, onde $a, b \in \mathbb{Z}$, ou seja, $x = (2a + b) + (2b - a)i$. Logo a imagem do homomorfismo canônico $\sigma_{\mathbb{L}}(A) \mu \mathbb{R}^2$ é dado por*

$$\begin{aligned}\sigma_{\mathbb{L}}(A) &= (<[\sigma_1((2a+b)+(2b-a)i)], =[\sigma_1((2a+b)+(2b-a)i)]) \\ &= (<[(2a+b)+(2b-a)i], =[(2a+b)+(2b-a)i]) \\ &= (2a+b, 2b-a).\end{aligned}$$

Portanto, $\sigma_{\mathbb{L}}(A)$ é um reticulado de posto 2 do $\mathbb{R}^2$, gerado pelos vetores $v_1 = (2, -1)$ e $v_2 = (1, 2)$, com região fundamental descrita na figura abaixo,



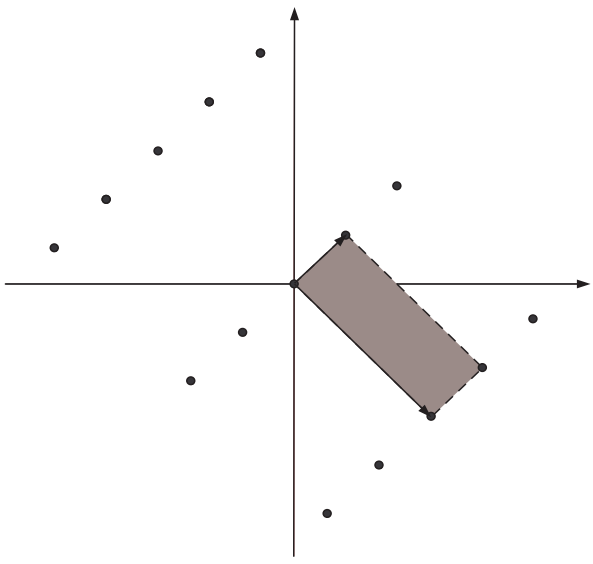
e volume dado por

$$Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = 2^{-1}\left|\left[\det\begin{pmatrix}\sigma_1(1) & \sigma_1(i)\\ \sigma_2(1) & \sigma_2(i)\end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \frac{1}{2}\left|\left[\det\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \frac{1}{2}2 = 1.$$

Pelo Teorema 2.5.1 *temos que* $N(A) = 5$*, logo*

$$Vol(\sigma_{\mathbb{L}}(A)) = Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}))N(A) = 1.5 = 5.$$

Exemplo 4.2.4 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{7})$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{7}]$ *seu anel dos inteiros algébricos com* $\mathbb{Z}$*-base* $\{1, \sqrt{7}\}$*. Como* $\mathbb{L}$ *é totalmente real, segue que* $r_1 = 2$ *e* $r_2 = 0$*. Assim, dado* $x = a_0 + a_1\sqrt{7} \in \mathcal{O}_{\mathbb{L}}$*, onde* $a_0, a_1 \in \mathbb{Z}$*, a imagem do homomorfismo canônico* $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}) \mu \mathbb{R}^2$ *que é dado por* $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}) = (a_0 + a_1\sqrt{7}, a_0 - a_1\sqrt{7})$*, é um reticulado de posto* 2 *do* $\mathbb{R}^2$*, gerado pelos vetores* $v_1 = (1, 1)$ *e* $v_2 = (\sqrt{7}, -\sqrt{7})$*, com região fundamental descrita na figura abaixo,*



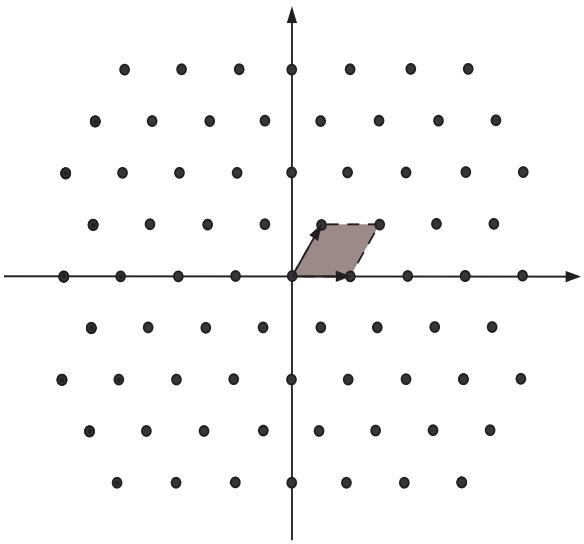
e volume dado por

$$Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = \left|\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{7}) \\ \sigma_2(1) & \sigma_2(\sqrt{7}) \end{pmatrix}\right| = \left|\det\begin{pmatrix} 1 & \sqrt{7} \\ 1 & i\sqrt{7} \end{pmatrix}\right| = 2\sqrt{7}.$$

Exemplo 4.2.5 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{i\,3})$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\frac{1+\sqrt{i\,3}}{2}]$ *o seu anel dos inteiros algébricos com* $\mathbb{Z}$*-base* $\{1, \frac{1+\sqrt{i\,3}}{2}\}$*. Como* $\mathbb{L}$ *é totalmente imaginário, segue que* $r_1 = 0$ *e* $r_2 = 1$*. Assim, dado* $x = a_0 + a_1(\frac{1+\sqrt{-3}}{2}) \in \mathcal{O}_{\mathbb{L}}$*, onde* $a_0, a_1 \in \mathbb{Z}$*, a imagem do homomorfismo canônico* $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}) \mu \mathbb{R}^2$ *é dado por*

$$\begin{aligned} \sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}) &= (<[\sigma_1(a_0 + a_1(\tfrac{1+\sqrt{-3}}{2}))], =[\sigma_1(a_0 + a_1(\tfrac{1+\sqrt{-3}}{2}))]) \\ &= (<[a_0 + \tfrac{a_1}{2} + \tfrac{\sqrt{3}a_1}{2}i], =[a_0 + \tfrac{a_1}{2} + \tfrac{\sqrt{3}a_1}{2}i]) \\ &= (a_0 + \tfrac{a_1}{2}, \tfrac{\sqrt{3}a_1}{2}). \end{aligned}$$

Portanto, $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$ *é um reticulado de posto* 2 *do* $\mathbb{R}^2$*, gerado pelos vetores* $v_1 = (1, 0)$ *e* $v_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$*, com região fundamental descrita na figura abaixo,*



e volume dado por

$$Vol(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = \frac{1}{2}\left|\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\frac{1+\sqrt{-3}}{2}) \\ \sigma_2(1) & \sigma_2(\frac{1+\sqrt{-3}}{2}) \end{pmatrix}\right| = \frac{1}{2}\left|\det\begin{pmatrix} 1 & \frac{1+\sqrt{-3}}{2} \\ 1 & \frac{1-\sqrt{-3}}{2} \end{pmatrix}\right| = \frac{1}{2}\sqrt{3}.$$

Proposição 4.2.3 ([1]) *Se* $\mathbb{L}$ *é um corpo de números de grau* n*,* $\mathfrak{D}_{\mathbb{L}}$ *o discriminante de* $\mathbb{L}$*,* $\mathcal{O}_{\mathbb{L}}$ *o anel dos inteiros algébricos de* $\mathbb{L}$*,* $\mathcal{A}$ *um ideal não nulo de* $\mathcal{O}_{\mathbb{L}}$ *e* r_2 *metade do número de monomorfismos imaginários, então a densidade de centro do reticulado* $\sigma_{\mathbb{L}}(\mathcal{A})$ *é dada por*

$$\delta(\sigma_{\mathbb{L}}(\mathcal{A})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{L}}(\mathcal{A})))^n}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}\mathcal{N}(\mathcal{A})}.$$

Demonstração: Segue diretamente da Observação 3.3.1. ∎

Proposição 4.2.4 ([12]) *Se* $\mathbb{L}$ *é um corpo de números e* $x \in \mathbb{L}$*, então*

$$|\sigma_{\mathbb{L}}(x)|^2 = c_{\mathbb{L}} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}),$$

onde

$$c_{\mathbb{L}} = \begin{cases} 1, & \text{se } \mathbb{L} \text{ for totalmente real.} \\ \dfrac{1}{2}, & \text{se } \mathbb{L} \text{ for totalmente imaginário.} \end{cases}$$

Demonstração: Suponhamos que $\mathbb{L}$ seja um corpo de números de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_{\mathbb{L}}(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned} |\sigma_{\mathbb{L}}(x)|^2 &= (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2 + \cdots + \Re(\sigma_{r_1+r_2}(x))^2 + \\ &+ \Im(\sigma_{r_1+r_2}(x))^2. \end{aligned}$$

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 $r_1 + 1 \cdot k \cdot r_1 + r_2$. Assim,

$$|\sigma_{\mathbb{L}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2 + \sigma_{r_1+1}(x\overline{x}) + \cdots + \sigma_{r_1+r_2}(x\overline{x}).$$

Se $r_1 = 0$, então

$$|\sigma_{\mathbb{L}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) = \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}),$$

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 $j = 1, \ldots, r_2$. Logo,

$$2|\sigma_{\mathbb{L}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \cdots + \sigma_{r_2+r_2}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

e como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, segue que

$$|\sigma_{\mathbb{L}}(x)|^2 = \frac{1}{2} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}).$$

Se $r_2 = 0$, então

$$|\sigma_{\mathbb{L}}(x)|^2 = (\sigma_1(x))^2 + \cdots + (\sigma_{r_1}(x))^2.$$

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, $|\sigma_{\mathbb{L}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_1}(x\overline{x})$. Portanto,

$$|\sigma_{\mathbb{L}}(x)|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}),$$

e isto conclui a demonstração. ∎

Observação 4.2.1 *Se $\mathbb{L}$ é um corpo de números de grau n, totalmente real ou totalmente imaginário, $O_{\mathbb{L}}$ é o anel dos inteiros algébricos de $\mathbb{L}$ e A é um ideal não nulo de $O_{\mathbb{L}}$, então podemos reescrever o raio de empacotamento do reticulado $\sigma_{\mathbb{L}}(A)$ da seguinte forma:*

$$\rho(\sigma_{\mathbb{L}}(A)) = \frac{1}{2} min\{|\sigma_{\mathbb{L}}(x)|,\ x \in A,\ x \neq 0\} = \frac{1}{2} min\left\{\sqrt{c_{\mathbb{L}} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})},\ x \in A,\ x \neq 0\right\},$$

onde

$$c_{\mathbb{L}} = \begin{cases} 1, & \text{se } \mathbb{L} \text{ for totalmente real.} \\ \dfrac{1}{2}, & \text{se } \mathbb{L} \text{ for totalmente imaginário.} \end{cases}$$

Proposição 4.2.5 *Se $\mathbb{L}$ é um corpo de números de grau n, totalmente real ou totalmente imaginãrio, $O_{\mathbb{L}}$ é o anel dos inteiros algébricos de $\mathbb{L}$ e A é um ideal não nulo de $O_{\mathbb{L}}$, então a densidade de centro do reticulado $\sigma_{\mathbb{L}}(A)$ é dada por:*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}} \frac{t^{\frac{n}{2}}}{N(A)},$$

onde $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}),\ x \in A,\ x \neq 0\}$

Demonstração: Seja $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}),\ x \in A,\ x \neq 0\}$. Pela Proposição 4.2.3 temos

1. se $\mathbb{L}$ é totalmente real então

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{\left(\frac{\sqrt{t}}{2}\right)^n}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\left(\sqrt{\frac{t}{4}}\right)^n}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}} \frac{t^{\frac{n}{2}}}{N(A)}.$$

2. se $\mathbb{L}$ é totalmente imaginário então

$$\begin{aligned} \delta(\sigma_{\mathbb{L}}(A)) &= \frac{2^{\frac{n}{2}} \left(\frac{\sqrt{\frac{1}{2}t}}{2}\right)^n}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\frac{2^{\frac{n}{2}} t^{\frac{n}{2}}}{2^{\frac{3n}{2}}}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\frac{t^{\frac{n}{2}}}{2^n}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\frac{t^{\frac{n}{2}}}{(\sqrt{4})^n}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{\frac{t^{\frac{n}{2}}}{4^{\frac{n}{2}}}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \\ &= \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}} N(A)} = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{\frac{1}{2}}} \frac{t^{\frac{n}{2}}}{N(A)}. \end{aligned}$$

Portanto, a densidade de centro é a mesma para ambos os casos. ∎

Exemplo 4.2.6 *Se $\mathbb{L} = \mathbb{Q}(\sqrt{-17})$ então $O_{\mathbb{L}} = \mathbb{Z}[\sqrt{-17}]$ e $\mathfrak{D}_{\mathbb{L}} = -68$. Se $x \in O_{\mathbb{L}}$, temos que $x = a + b\sqrt{-17} = a + b\sqrt{17}i$ e*

$$x\overline{x} = (a + b\sqrt{17}i)(a - b\sqrt{17}i) = a^2 - ab\sqrt{17}i + ab\sqrt{17}i + 17b^2 = a^2 + 17b^2.$$

Logo, $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 2(a^2 + 17b^2)$ e $t = 2$, para $a = 1$ e $b = 0$. Assim

$$\delta(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) = \frac{\left(\frac{2}{4}\right)}{\sqrt{68}} = \frac{\left(\frac{1}{2}\right)}{2\sqrt{17}} = \frac{1}{4\sqrt{17}} \approx 0,06.$$

Observação 4.2.2 *Pela Proposição* 4.2.5*, vimos que, se* $\mathbb{L}$ *é um corpo de números de grau* n*, totalmente real ou totalmente imaginário,* $\mathcal{O}_{\mathbb{L}}$ *é o anel dos inteiros algébricos de* $\mathbb{L}$ *e* $\mathcal{A}$ *é um ideal não nulo de* $\mathcal{O}_{\mathbb{L}}$*, então dado* $x \in \mathcal{A}$*,* $x \neq 0$*, para calcular a densidade de centro do reticulado* $\sigma_{\mathbb{L}}(\mathcal{A})$*, o grande desafio é obter a expressão* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$*, que é uma forma quadrática, e minimizá-la. Assim, o próximo capítulo será dedicado ao estudo dessas formas quadráticas obtidas via corpos ciclotômicos, pois é sobre esses corpos que o nosso trabalho está inserido.*

Capítulo

5

Formas quadráticas via corpos ciclotômicos

5.1 Introdução

O objetivo deste capítulo é fazer um estudo das formas quadráticas via corpos ciclotômicos oriundas de uma função traço, conforme Observação 4.2.2, que serão muito úteis no cálculo do raio de empacotamento e, conseqüentemente, na densidade de centro de reticulados algébricos. Dessa forma, dividimos o capítulo em duas seções. A Seção 5.2, é dedicada às formas quadráticas via o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ e ao seu subcorpo maximal $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$, onde o principal resultado obtido foi a forma quadrática sobre o subcorpo maximal [16]. A Seção 5.3, será dedicada às formas quadráticas via o corpo ciclotômico $\mathbb{Q}(\zeta_p)$, onde p é um primo, e seus subcorpos, pois sobre $\mathbb{Q}(\zeta_p)$ é possível fazer um amplo estudo.

5.2 Forma quadrática via o corpo ciclotômico $\mathbb{Q}(\zeta_n)$

Nesta seção apresentamos a forma quadrática via o corpo ciclotômico $\mathbb{Q}(\zeta_n)$, que será muito útil na determinação de reticulados algébricos com densidade de centro ótima. O conteúdo desta seção encontra-se em [13], mas fizemos adaptações em algumas demonstrações, assim alguns lemas e os corolários do Teorema 5.2.1 são de nossa autoria.

Lema 5.2.1 ([13]) *Sejam j, n números inteiros. Se $mdc(j,n) = d$ então*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\phi(n)}{\phi(n/d)}\, Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}).$$

Demonstração: Se $j \in \mathbb{Z}$, então $\zeta_n^j \in \mathbb{Q}(\zeta_n)$. Mas, como $\zeta_n^j = \zeta_{n/d}^{j/d}$, segue que $\mathbb{Q}(\zeta_{n/d}^{j/d}) \subseteq \mathbb{Q}(\zeta_n)$. Agora, consideremos as seguintes extensões $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n/d}^{j/d}) \subseteq \mathbb{Q}(\zeta_n)$. Como $mdc(j,n) = d$, segue que $mdc(j/d, n/d) = 1$, o que implica que $\zeta_{n/d}^{j/d}$ é um gerador do conjunto das raízes n/d-ésimas da unidade. Deste modo temos que $\mathbb{Q}(\zeta_{n/d}^{j/d}) = \mathbb{Q}(\zeta_{n/d})$ e da Observação 2.2.2 temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{n/d}^{j/d}) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/d}^{j/d})]\; Tr_{\mathbb{Q}(\zeta_{n/d}^{j/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}).$$

Do fato que $\zeta_{n/d}^{j/d} = \zeta_n^j$ e $\mathbb{Q}(\zeta_{n/d}^{j/d}) = \mathbb{Q}(\zeta_{n/d})$, temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/d}^{j/d})]\ Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}),$$

e como $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/d}^{j/d})] = \dfrac{\phi(n)}{\phi(n/d)}$, segue o resultado. ∎

Exemplo 5.2.1 *Na tabela abaixo damos exemplos, para alguns valores de n e j.*

n	j	d	$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = [\phi(n)/\phi(n/d)]\ Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d})$
18	12	6	$Tr_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}}(\zeta_{18}^{12}) = 3\ Tr_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\zeta_3^2)$
242	22	22	$Tr_{\mathbb{Q}(\zeta_{242})/\mathbb{Q}}(\zeta_{242}^{22}) = 11\ Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}(\zeta_{11})$
250	10	10	$Tr_{\mathbb{Q}(\zeta_{250})/\mathbb{Q}}(\zeta_{250}^{10}) = 5\ Tr_{\mathbb{Q}(\zeta_{25})/\mathbb{Q}}(\zeta_{25})$
338	52	26	$Tr_{\mathbb{Q}(\zeta_{338})/\mathbb{Q}}(\zeta_{338}^{52}) = 13\ Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\zeta_{13}^2)$
686	6	2	$Tr_{\mathbb{Q}(\zeta_{686})/\mathbb{Q}}(\zeta_{686}^6) = \ Tr_{\mathbb{Q}(\zeta_{343})/\mathbb{Q}}(\zeta_{343}^3)$

Lema 5.2.2 ([13]) *Se j, a_i são números inteiros, onde $a_i \geq 1$ e p_i é um número primo tal que $mdc(j, {p_i}^{a_i}) = 1$, então*

$$Tr_{\mathbb{Q}(\zeta_{{p_i}^{a_i}})/\mathbb{Q}}(\zeta_{{p_i}^{a_i}}^j) = \begin{cases} -1, & \text{se } a_i = 1. \\ 0, & \text{se } a_i > 1. \end{cases}$$

Demonstração: Se $a_i = 1$, então $irr_{\mathbb{Q}}(\zeta_{p_i}) = x^{p_i-1} + x^{p_i-2} + \ldots + x + 1$ e como $mdc(j, p_i) = 1$, segue que ζ_{p_i} e $\zeta_{p_i}^j$ são conjugados. Logo são raízes do mesmo polinômio minimal e conseqüentemente possuem o mesmo traço, ou seja,

$$Tr_{\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}}(\zeta_{p_i}^j) = Tr_{\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}}(\zeta_{p_i}) = -1.$$

Se $a_i > 1$, então $irr_{\mathbb{Q}}(\zeta_{{p_i}^{a_i}}) = x^{(p_i-1){p_i}^{a_i-1}} + x^{(p_i-2){p_i}^{a_i-1}} + \ldots + x^{{p_i}^{a_i-1}} + 1$, e assim $Tr_{\mathbb{Q}(\zeta_{{p_i}^{a_i}})/\mathbb{Q}}(\zeta_{{p_i}^{a_i}}) = 0$, pois o coeficiente de $x^{(p_i-1){p_i}^{a_i-1}-1}$ no polinômio $irr_{\mathbb{Q}}(\zeta_{{p_i}^{a_i}})$ é nulo. Agora, como $mdc(j, {p_i}^{a_i}) = 1$, segue que $\zeta_{{p_i}^{a_i}}$ e $\zeta_{{p_i}^{a_i}}^j$ são conjugados, e portanto possuem o mesmo traço, ou seja,

$$Tr_{\mathbb{Q}(\zeta_{{p_i}^{a_i}})/\mathbb{Q}}(\zeta_{{p_i}^{a_i}}^j) = Tr_{\mathbb{Q}(\zeta_{{p_i}^{a_i}})/\mathbb{Q}}(\zeta_{{p_i}^{a_i}}) = 0,$$

o que prova o lema. ∎

Definição 5.2.1 *Seja $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$, onde $a_k \geq 1$, para $k = 1, 2, \ldots, s$. A função*

$$\mu(n) = \begin{cases} (-1)^s, & \text{se } a_k = 1, \text{ para todo } k. \\ 1, & \text{se } n = 1. \\ 0, & \text{se } a_k > 1, \text{ para algum } k. \end{cases}$$

é chamada função de Möbius.

Observação 5.2.1 *Sejam $n = p_1p_2\dots p_{k+1}$, onde os $p_i's$, $i = 1,2\dots,k+1$, são primos distintos, $a = p_1p_2\dots p_k$ e $b = p_{k+1}$, $\mathbb{M} = \mathbb{Q}(\zeta_b)$ e $\mathbb{F} = \mathbb{Q}(\zeta_a)$. Temos que $\mathbb{M}$ e $\mathbb{F}$ são extensões galoisianas sobre $\mathbb{Q}$ e ζ_n 2 $\mathbb{Q}(\zeta_n)$. Logo $\zeta_b = {\zeta_n}^a$ 2 $\mathbb{Q}(\zeta_n)$ e assim $\mathbb{M} = \mathbb{Q}(\zeta_b)$ ½ $\mathbb{Q}(\zeta_n)$. Analogamente, $\zeta_a = {\zeta_n}^b$ 2 $\mathbb{Q}(\zeta_n)$, e assim $\mathbb{F} = \mathbb{Q}(\zeta_a)$ ½ $\mathbb{Q}(\zeta_n)$. Portanto $\mathbb{MF}$ ½ $\mathbb{Q}(\zeta_n)$. Reciprocamente, como $mdc(a,b) = 1$, segue que existem u, v 2 $\mathbb{Z}$ tais que $au + bv = 1$. Logo*

$$\zeta_n = {\zeta_n}^1 = {\zeta_n}^{au+bv} = {\zeta_n}^{au}{\zeta_n}^{bv} = {\zeta_b}^u{\zeta_a}^v.$$

Mas ${\zeta_b}^u{\zeta_a}^v$ 2 $\mathbb{MF}$, pois ${\zeta_b}^u$ 2 $\mathbb{M}$ e ${\zeta_a}^v$ 2 $\mathbb{F}$. Logo ζ_n 2 $\mathbb{MF}$, e assim $\mathbb{Q}(\zeta_n)$ ½ $\mathbb{MF}$. Portanto, $\mathbb{Q}(\zeta_n) = \mathbb{MF}$, e como $mdc(a,b) = 1$, pela Proposição 2.7.1*, segue que $\mathbb{M} \setminus \mathbb{F} = \mathbb{Q}$. Daí pela Proposição* 1.3.1*, temos os seguintes resultados:*

1. *$\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)$ é uma extensão galoisiana, pois $\mathbb{Q}$ ½ $\mathbb{Q}(\zeta_a)$ ½ $\mathbb{Q}(\zeta_n)$ e $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é uma extensão galoisiana.*

2. *$\mathbb{Q}(\zeta_b)/\mathbb{Q}$ é uma extensão galoisiana.*

3. *Se H é o grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}(\zeta_a)$, G é o grupo de Galois de $\mathbb{Q}(\zeta_b)$ sobre $\mathbb{Q}$ e σ 2 H, então a restrição de σ a $\mathbb{Q}(\zeta_b)$ pertence a G, e a aplicação σ 7! $\sigma|_{\mathbb{Q}(\zeta_b)}$ nos dá um isomorfismo de H no grupo de Galois de $\mathbb{Q}(\zeta_b)$ sobre $\mathbb{Q}$.*

Agora, dado α 2 $\mathbb{Q}(\zeta_b)$, pela Proposição 2.2.1*, temos que*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)}(\alpha) = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\alpha).$$

Lema 5.2.3 ([13]) *Se $n = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$, onde a_k ¸ 1, para todo $k = 1,2,\dots,s$, e j é um número inteiro com $mdc(j,n) = d$, então*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{\phi(n)}{\phi(n/d)}\ \mu(n/d),$$

onde μ é a função de Möbius.

Demonstração: Pelo Lema 5.2.1, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \dfrac{\phi(n)}{\phi(n/d)}\ Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d})$. Logo basta mostrarmos que

$$Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}) = \mu(n/d).$$

Temos por hipótese que $mdc(j,n) = d$, e assim $mdc(j/d, n/d) = 1$. Para simplificar, tomamos $n/d = m$ e $j/d = i$, e assim $mdc(i,m) = 1$. Como $n = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$ e d|n, segue que $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, onde $0 \cdot \alpha_i \cdot a_i$, para $i = 1,2,\dots,s$. Mas, sem perda de generalidade, podemos supor $\alpha_i > 0$. Se $m = 1$, então $Tr_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(\zeta_1^i) = Tr_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(1) = 1 = \mu(1)$, o que prova que o resultado vale. Se m 6= 1, então temos os seguintes casos:
(**a**) m é livre de quadrados. Neste caso a demonstração será feita por indução sobre a quantidade de números primos na decomposição de m. Se m é livre de quadrados, então $m = p_1p_2\dots p_s$. Se $s = 1$, e como $mdc(i,p_1) = 1$, pelo Lema 5.2.2 segue que $Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^i) =$ i $1 = \mu(p_1)$. Agora, suponhamos que a igualdade seja verdadeira para $s = k$, ou seja,

$$Tr_{\mathbb{Q}(\zeta_{p_1\dots p_k})/\mathbb{Q}}(\zeta_{p_1\dots p_k}^i) = \mu(p_1\dots p_k) = (\text{ i } 1)^k.$$

Dado $m = p_1 p_2 \dots p_{k+1}$, sejam $a = p_1 p_2 \dots p_k$ e $b = p_{k+1}$. Logo $mdc(a, b) = 1$, e assim existem $u, v \in \mathbb{Z}$ tais que $au + bv = 1$. Além disso

$$\zeta_m^i = \zeta_m^{i(au+bv)} = \zeta_{ab}^{iau} = \zeta_{ab}^{ibv} = \zeta_b^{iu}\zeta_a^{iv},$$

onde $mdc(iu, b) = mdc(iv, a) = 1$. De fato, se $mdc(iu, b) = t > 1$, então

mdc

onde $P = p_1 \dots p_s$, $t_j = mdc(j, P)$ *e* $j = 1, 2, \dots, \phi(P) - 1$.

Demonstração: Suponhamos $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) \neq 0$ com $d \neq (n/P)t_j$. Por hipótese temos que n/d não é livre de quadrados, logo, pela definição da função de Möbius temos que $\mu(n/d) = 0$, e portanto $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = 0$, o que é um absurdo. Reciprocamente, se $d = (n/P)t_j$ e $i = (n/P)j$, primeiramente mostremos que $mdc(i, n) = d$, com $j = 1, 2, \dots, \phi(P) - 1$. Com efeito, se $mdc(i, n) = d'$, então $mdc((n/P)j, n) = d'$. Logo $mdc(((n/P)j)/(n/P), n/(n/P)) = d'/(n/P)$, ou seja, $t_j = mdc(j, P) = (P/n)d'$, o que implica que $d' = (n/P)t_j = d$, e $j = 1, 2, \dots, \phi(P) - 1$, pois usando o Lema 1.4.6, temos

$$\frac{\phi(n)}{\phi(P)} = \frac{\phi(p_1^{a_1} \dots p_s^{a_s})}{\phi(p_1 \dots p_s)} = \frac{\phi(p_1^{a_1}) \dots \phi(p_s^{a_s})}{\phi(p_1) \dots \phi(p_s)} = \frac{[{p_1}^{a_1-1}(p_1 - 1)] \dots [{p_s}^{a_s-1}(p_s - 1)]}{(p_1 - 1) \dots (p_s - 1)} =$$
$$= p_1^{a_1-1} \dots p_s^{a_s-1} = \frac{n}{P}.$$

Logo, se $j > \phi(P)$, então $i = (n/P)j = ((\phi(n))/(\phi(P))j > ((\phi(n))/(\phi(P))(\phi(P) = \phi(n)$, o que é um absurdo, e portanto $j = 1, 2, \dots, \phi(P) - 1$. Agora, se $d = (n/P)t_j$, onde $t_j = mdc(j, P)$, para $j = 1, 2, \dots, \phi(P) - 1$, então os valores que t_j pode assumir são 1 e $p_{\alpha_1} \dots p_{\alpha_t}$, onde $1 \leq \alpha_k \leq s$ (para $k = 1, 2, \dots, t$ e $t = 1, 2, \cdots, s$) e $\alpha_k \neq \alpha_l$ se $k \neq l$. Logo, $d = p_1^{a_1-1} \dots p_s^{a_s-1}$ ou $d = p_1^{a_1-1} \dots p_{\alpha_1}^{a_{\alpha_1}} \dots p_{\alpha_t}^{a_{\alpha_t}} \dots p_s^{a_s-1}$, e assim $n/d = p_1 \dots p_s$ ou $n/d = p_1 \dots p_{\alpha_1-1} p_{\alpha_1+1} \dots p_{\alpha_t-1} p_{\alpha_t+1} \dots p_s$. Portanto, $\mu(n/d) = \pm 1 \neq 0$. Portanto, pelo Lema 5.2.3, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \dfrac{\phi(n)}{\phi(n/d)}\mu(n/d) \neq 0$. ∎

Teorema 5.2.1 ([13]) *Se* $n = p_1^{a_1} \dots p_s^{a_s}$, *com* $a_k \geq 1$, *para* $k = 1, 2, \dots s$, $n \neq 2^r$, $r \geq 2$, $m = \phi(n)$ *e* $x = a_0 + a_1\zeta_n + \dots + a_{m-1}\zeta_n^{m-1}$ *é um inteiro algébrico de* $\mathbb{L} = \mathbb{Q}(\zeta_n)$, *então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \frac{n}{P}\left\{ \phi(P)\sum_{i=0}^{m-1} a_i^2 + 2\sum_{j=1}^{\phi(P)-1} \mu(\frac{P}{t_j})\phi(t_j)A_{\frac{n}{P}j} \right\},$$

onde
$P = p_1 \dots p_s$;
$t_j = mdc(j, P)$, *para* $j = 1, 2, \dots, \phi(P) - 1$;
$A_i = a_o a_i + a_1 a_{i+1} + \dots + a_{m-1-i} a_{m-1}$, *para* $i = 1, 2, \dots, m - 1$.

Demonstração: Temos que

$$x\overline{x} = \sum_{i=0}^{m-1} a_i^2 + \sum_{i=0}^{m-1} A_i\beta_i,$$

onde $A_i = a_o a_i + a_1 a_{i+1} + \dots + a_{m-1-i} a_{m-1}$ e $\beta_i = \zeta_n^i + \zeta_n^{-i}$, para todo $i = 1, 2, \cdots, m - 1$. Assim,

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=0}^{m-1} a_i^2 + \sum_{i=0}^{m-1} A_i\beta_i \right) = Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=0}^{m-1} a_i^2 \right) + Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=0}^{m-1} A_i\beta_i \right) =$$
$$= m\sum_{i=0}^{m-1} a_i^2 + \sum_{i=0}^{m-1} A_i Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^i + \zeta_n^{-i}).$$

Como ζ_n^i e ζ_n^{-i} são conjugados, para todo $i = 0, 1, \ldots, m - 1$, segue que eles possuem o mesmo traço, e assim

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = m\sum_{i=0}^{m-1} a_i^2 + 2\sum_{i=0}^{m-1} A_i Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_n^i).$$

Pelo Lema 5.2.3, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \dfrac{\phi(n)}{\phi(n/d)}\ \mu(n/d)$, onde $d = mdc(i, n)$, e deste modo podemos escrever

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = m\sum_{i=0}^{m-1} a_i^2 + 2\sum_{i=0}^{m-1} A_i \frac{\mu(n/d)}{\phi(n/d)}\ m. \tag{5.2.1}$$

Pelo Lema 5.2.4, temos que o somatório $\displaystyle\sum_{i=0}^{m-1} A_i \frac{\mu(n/d)}{\phi(n/d)}\ m$ é não nulo quando $d = (n/P)t_j$, onde $t_j = mdc(j, P)$ e $i = (n/P)j$, para $j = 1, 2, \ldots, \phi(P) - 1$, e usando o Lema 1.4.6 temos também que $\phi(n) = (n/P)\phi(P)$. Temos que $mdc((P/t_j), t_j) = 1$, pois caso contrário, se $mdc((P/t_j), t_j) = t > 1$, então, $t \mid (P/t_j)$ e $t \mid t_j$. Logo existem $k_1, k_2 \in \mathbb{Z}$ tais que $P/t_j = tk_1$ e $t_j = tk_2$, e assim $P = t^2 k_1 k_2$, ou seja, $t^2 | P$. Agora, como $t > 1$ segue que $t^2 > 1$, e portanto, $t^2 = p_{\alpha_1} \ldots p_{\alpha_r}$, onde $p_{\alpha_k} \in \{p_1, \ldots p_s\}$, para $k = 1, 2, \ldots, r$, o que é um absurdo, pois os p_k's são distintos. Assim $\phi(P) = \phi((P/t_j).t_j) = \phi(P/t_j)\phi(t_j)$, ou seja, $\phi(P/t_j) = \phi(P)/\phi(t_j)$. Retomando a Equação (5.2.1) temos que

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) &= m\sum_{i=0}^{m-1} a_i^2 + 2\sum_{i=0}^{m-1} A_i \frac{\mu(\frac{n}{d})}{\phi(\frac{n}{d})}\ m = \phi(n)\sum_{i=0}^{m-1} a_i^2 + 2\sum_{j=1}^{\phi(P)-1} A_{\frac{n}{P}j}\ \mu(\frac{P}{t_j})\frac{1}{\phi(\frac{P}{t_j})}\ \phi(n) = \\ &= \frac{n}{P}\ \phi(P)\sum_{i=0}^{m-1} a_i^2 + 2\sum_{j=1}^{\phi(P)-1} A_{\frac{n}{P}j}\ \mu(\frac{P}{t_j})\frac{\phi(t_j)}{\phi(P)}\frac{n}{P}\ \phi(P) = \\ &= \frac{n}{P}\left\{\ \phi(P)\sum_{i=0}^{m-1} a_i^2 + 2\sum_{j=1}^{\phi(P)-1} \mu(\frac{P}{t_j})\phi(t_j)A_{\frac{n}{P}j}\ \right\}. \end{aligned}$$

o que prova o teorema. ∎

Corolário 5.2.1 *Se $n = 2^r$, $r \geq 2$ e $x = a_0 + a_1\zeta_{2^r} + \ldots + a_{2^{r-1}-1}\zeta_{2^r}^{2^{r-1}-1}$ é um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_{2^r})$, então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 2^{r-1}\sum_{i=0}^{2^{r-1}-1} a_i^2$$

Demonstração: Da demonstração do Teorema 5.2.1 e pelo Lema 5.2.3 temos que

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 2^{r-1}\sum_{i=0}^{2^{r-1}-1} a_i^2 + 2\sum_{i=0}^{2^{r-1}-1} A_i Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^i).$$

onde $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^i) = \dfrac{\phi(2^r)}{\phi(2^r/d)}\ \mu(2^r/d)$, e $d = mdc(i, 2^r)$. Agora, temos que $i \cdot 2^{r-1} - 1 < 2^{r-1}$, assim $d < 2^{r-1}$, pois $d \mid i$. Mas, $d = 1$ se o primo 2 não aparece

na decomposição de i, ou $d = 2^q$ se o primo 2 aparece na decomposição de i, onde $q < r$ ¡ 1, pois $d < 2^{r-1}$. Assim,

$$\mu(2^r/d) = \mu(2^r) = 0 \quad \text{ou} \quad \mu(2^r/d) = \mu(2^{r-q}) = 0$$

pois r ¸ 2 e r ¡ $q > 1$. Portanto, $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^i) = 0$, e segue o resultado. ■

Os dois próximos corolários caracterizam a forma quadrática obtida no Teorema 5.2.1 para extensões ciclotômicas cíclicas.

Corolário 5.2.2 *Se $n = p^r$, onde p é um primo, r um número natural maior do que ou igual a 1, $m = \phi(n)$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ é um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$, então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(p^r) \sum_{i=0}^{\phi(p^r)-1} a_i^2 \quad ¡ \quad 2p^{r-1}\left(\sum_{j=1}^{p-2} A_{p^r ¡ 1j} \right).$$

Demonstração: Tomando $m = \phi(p^r) = p^{r-1}(p ¡ 1)$, $P = p$, temos que $\phi(P) = p ¡ 1$, $\mu(P) = \mu(p) = ¡ 1$, e $t_j = mdc(j, P) = 1$, para $j = 1, 2, \ldots, p ¡ 2$. Assim, tomando $n = p^r$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ temos, pelo Teorema 5.2.1, que

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(p^r) \sum_{i=0}^{\phi(p^r)-1} a_i^2 \quad ¡ \quad 2p^{r-1}\left(\sum_{j=1}^{p-2} A_{p^r ¡ 1j} \right),$$

o que prova o corolário. ■

Corolário 5.2.3 *Se $n = 2p^r$, onde p é um primo ímpar, r um número natural maior do que ou igual a 1, $m = \phi(n)$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ é um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$, então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(2p^r) \sum_{i=0}^{\phi(2p^r)-1} a_i^2 \; + \; 2p^{r-1}\left(\sum_{\substack{j=1 \\ j:impar}}^{p-2} A_{p^r ¡ 1j} \quad ¡ \quad \sum_{\substack{j=1 \\ j:par}}^{p-2} A_{p^r ¡ 1j} \right).$$

Demonstração: Tomando $m = \phi(2p^r) = p^{r-1}(p ¡ 1)$, $P = 2p$, temos que $\phi(P) = \phi(2p) = \phi(2)\phi(p) = \phi(p) = p ¡ 1$, pois $mdc(2, p) = 1$, e ainda $\mu(P) = \mu(2p) = 1$, e $t_j = mdc(j, P)$ com $j = 1, 2, \ldots, p ¡ 2$. Logo

$$t_j = mdc(j, 2p) = \begin{cases} 1, & \textit{se } j \text{ é } \textit{impar}. \\ 2, & \textit{se } j \text{ é } \textit{par}. \end{cases}$$

Temos também que $\frac{n}{P}j = p^{r-1}j$. Assim, tomando $n = 2p^r$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ temos, pelo Teorema 5.2.1, que

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(2p^r) \sum_{i=0}^{\phi(2p^r)-1} a_i^2 \; + \; 2p^{r-1}\left(\sum_{\substack{j=1 \\ j:impar}}^{p-2} A_{p^r ¡ 1j} \quad ¡ \quad \sum_{\substack{j=1 \\ j:par}}^{p-2} A_{p^r ¡ 1j} \right),$$

o que prova o corolário. ■

Corolário 5.2.4 *Se $n = pq$, onde p e q são primos distintos, $m = \phi(n)$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ é um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$, então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(pq)\sum_{i=0}^{\phi(pq)-1} a_i^2 \;-\; 2(p-1)\sum_{\substack{j=1\\ j:\,multiplo\,de\,p}}^{\phi(pq)-1} A_j \;-\; 2(q-1)\sum_{\substack{j=1\\ j:\,multiplo\,de\,q}}^{\phi(pq)-1} A_j \;+\; 2\sum_{\substack{j=1\\ (j,pq)=1}}^{\phi(pq)-1} A_j.$$

Demonstração: Tomando $m = \phi(pq) = \phi(P)$, $\mu(P) = \mu(pq) = 1$ e $t_j = mdc(j, P)$ com $j = 1, 2, \ldots, \phi(pq) - 1$, temos que

$$t_j = mdc(j, pq) = \begin{cases} p, & \text{se } j \text{ é multiplo de } p.\\ q, & \text{se } j \text{ é multiplo de } q.\\ 1, & \text{se caso contrário.}\end{cases}$$

Temos também que $\frac{n}{P}j = j$. Assim, tomando $n = pq$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$ temos, pelo Teorema 5.2.1, que

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \phi(pq)\sum_{i=0}^{\phi(pq)-1} a_i^2 \;-\; 2(p-1)\sum_{\substack{j=1\\ j:\,multiplo\,de\,p}}^{\phi(pq)-1} A_j \;-\; 2(q-1)\sum_{\substack{j=1\\ j:\,multiplo\,de\,q}}^{\phi(pq)-1} A_j \;+\; 2\sum_{\substack{j=1\\ (j,pq)=1}}^{\phi(pq)-1} A_j,$$

o que prova o corolário. ∎

Corolário 5.2.5 *Se $n = p_1^{a_1}\ldots p_s^{a_s}$, com $a_k \neq 1$, para $k = 1, 2, \ldots s$, $n \neq 2^r$, $r \in \mathbb{N}$, $m = \phi(n)$ e $x = a_0 + a_1\zeta_n + \ldots + a_{m-1}\zeta_n^{m-1}$ é um inteiro algébrico de $\mathbb{L} = \mathbb{Q}(\zeta_n)$, então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \equiv 0 \;(mod\ \frac{2n}{P}).$$

Demonstração: Temos que $\phi(P) = \phi(p_1\ldots p_s) = \phi(p_1)\ldots\phi(p_s) = (p_1 - 1)\ldots(p_s - 1)$. Se $s = 1$, então $n = p_1^{a_1}$, com $p_1 \neq 2$. Logo $P = p_1$ e assim $\phi(P) = p_1 - 1$ é um número par, pois p_1 é ímpar. Portanto $\phi(P) = 2t$ com $t \in \mathbb{Z}$. Se $s > 1$, então em $n = p_1^{a_1}\ldots p_s^{a_s}$ existe pelo menos um p_j ímpar, pois os números primos na decomposição de n são distintos. Logo $\phi(P) = (p_1 - 1)\ldots(p_j - 1)\ldots(p_s - 1)$ é um número par, e portanto $\phi(P) = 2t$ com $t \in \mathbb{Z}$. Portanto, pelo Teorema 5.2.1, temos que

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \frac{2n}{P}\left\{\; t\sum_{i=0}^{m-1} a_i^2 + \sum_{j=1}^{\phi(P)-1}\mu(\frac{P}{t_j})\phi(t_j)A_{\frac{n}{P}j}\;\right\},$$

e segue o resultado. ∎

Observação 5.2.2 *Se $n = 2^r$, com $r \in \mathbb{N}$, então não podemos garantir o resultado do Corolário 5.2.5, pois se $P = 2$ então $\phi(P) = 1$. Assim*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \frac{n}{P}\left\{\; 1\sum_{i=0}^{2^{r-1}-1} a_i^2 + 0\;\right\} = \frac{n}{P}\left(\;\sum_{i=0}^{2^{r-1}-1} a_i^2\;\right).$$

Se tomarmos n

$\rho(t_i) = \mu(\frac{P}{t_i})\phi(t_i)$, *tal que* μ *(respec.* ϕ*) é a função de Möbius (respec. Euler);*
$A_j = a_1a_{j+1} + a_2a_{j+2} + \ldots + a_{\frac{m}{2}-j}a_{\frac{m}{2}}$;

$$B_j = \sum_{\substack{k=1 \\ k<j-k\leq \frac{m}{2}}} a_k a_{j-k}.$$

Demonstração: Dado $x \in \mathcal{O}_{\mathbb{K}}$, pelo Teorema 2.7.1, podemos escrever

$$x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}}),$$

com $a_i \in \mathbb{Z}$, para $i = 1, 2, \ldots \frac{\phi(n)}{2}$. Assim,

$$\begin{aligned} x\overline{x} &= (a_1\zeta_n + a_1\zeta_n^{-1} + \ldots + a_{\frac{m}{2}}\zeta_n^{\frac{m}{2}} + a_{\frac{m}{2}}\zeta_n^{-\frac{m}{2}})(a_1\zeta_n^{-1} + a_1\zeta_n + \ldots + a_{\frac{m}{2}}\zeta_n^{-\frac{m}{2}} + a_{\frac{m}{2}}\zeta_n^{\frac{m}{2}}) = \\ &= [(a_1\zeta_n + a_2\zeta_n^2 + \ldots a_{\frac{m}{2}}\zeta_n^{\frac{m}{2}}) + (a_1\zeta_n^{-1} + a_2\zeta_n^{-2} + \ldots a_{\frac{m}{2}}\zeta_n^{-\frac{m}{2}})]^2 = A^2 + \overline{A}^{\,2} + 2A\overline{A}, \end{aligned}$$

onde $A = a_1\zeta_n + a_2\zeta_n^2 + \ldots a_{\frac{m}{2}}\zeta_n^{\frac{m}{2}}$. Assim

$$x\overline{x} = \sum_{j=1}^{m/2} a_j^2(\zeta_n^{2j} + \zeta_n^{-2j}) + 2\left(\sum_{j=3}^{m-1} B_j\beta_j\right) + 2\left(\sum_{j=1}^{m/2} a_j^2 + \sum_{j=1}^{m/2-1} A_j\beta_j\right),$$

onde
$A_j = a_1a_{j+1} + a_2a_{j+2} + \ldots + a_{\frac{m}{2}-j}a_{\frac{m}{2}}$;

$$B_j = \sum_{\substack{k=1 \\ k<j-k\leq \frac{m}{2}}} a_k a_{j-k};$$

$\beta_j = \zeta_n^j + \zeta_n^{-j}$
Agora, pelas propriedades do traço (Observação 2.2.2), temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x\overline{x}) = [\mathbb{Q}(\zeta_n) : \mathbb{L}]\ Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Logo

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{2}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x\overline{x}),$$

e assim, podemos escrever

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= \frac{1}{2}\left[Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(2\sum_{j=1}^{m/2} a_j^2 + 2\sum_{j=1}^{m/2-1} A_j\beta_j + \sum_{j=1}^{m/2} a_j^2(\zeta_n^{2j} + \zeta_n^{-2j}) + 2\sum_{j=3}^{m-1} B_j\beta_j\right)\right] = \\ &= m\sum_{j=1}^{m/2} a_j^2 + \sum_{j=1}^{m/2} a_j^2 Tr_{\mathbb{Q}(\zeta_n)\mathbb{Q}}(\zeta_n^{2j}) + 2\left(\sum_{j=1}^{m/2-1} A_j Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) + \sum_{j=3}^{m-1} B_j Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j)\right). \end{aligned} \tag{5.2.2}$$

Mas, pelos Lemas 5.2.3 e 5.2.4, podemos escrever

$$\sum_{j=1}^{m/2} a_j^2 Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{2j}) = \frac{n}{P}\sum_{\substack{i=u \\ \frac{n}{P}i:par}}^{\phi(P)} \mu(\frac{P}{t_i})\phi(t_i)a^2_{\frac{n}{2P}i}, \tag{5.2.3}$$

$$\sum_{j=1}^{m/2-1} A_j Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \frac{n}{P}\sum_{i=1}^{s}\mu(\frac{P}{t_i})\phi(t_i)A_{\frac{n}{P}i}, \tag{5.2.4}$$

$$\sum_{j=3}^{m-1} B_j Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^j) = \sum_{i=v}^{\phi(P)-1}\mu(\frac{P}{t_i})\phi(t_i)B_{\frac{n}{P}i}, \tag{5.2.5}$$

onde $u = \left\lceil \frac{2P}{n} \right\rceil$, $s = \left\lfloor \frac{\phi(P)}{2} - 1 \right\rfloor$, $v = \left\lceil \frac{3P}{n} \right\rceil$. Finalmente, substituindo as Equações (5.2.3), (5.2.4) e (5.2.5) na Equação (5.2.2), obtemos o resultado. ∎

Observação 5.2.3 *No Teorema* 5.2.2*, quando* $n = 2^{a_1}3^{a_2}$, $n > 6$, *devemos tomar cuidado na aplicação da fórmula, uma vez que algum somatório pode não fazer sentido, neste caso tal somatório é nulo. Com esta precaução o resultado continua válido.*

Exemplo 5.2.3 *Se* $\mathbb{K} = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ *e* $x = a_1(\zeta_7 + \zeta_7^{-1}) + a_2(\zeta_7^2 + \zeta_7^{-2}) + a_3(\zeta_7^3 + \zeta_7^{-3})$ *é um inteiro algébrico de* $\mathbb{K}$*, então*

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= 6\sum_{i=1}^{3}a_i^2 + \sum_{\substack{i=2 \\ i:par}}^{6}\rho(t_i)a_{\frac{i}{2}}^2 + 2\sum_{i=1}^{2}\rho(t_i)A_i + 2\sum_{i=3}^{5}\rho(t_i)B_i = \\ &= 6\sum_{i=1}^{3}a_i^2 - a_1^2 - a_2^2 - a_3^2 - 2(A_1 + A_2 + B_3 + B_4 + B_5) = \\ &= 5\sum_{i=1}^{3}a_i^2 - 2(a_1a_2 + a_2a_3 + a_1a_3 + a_1a_2 + a_1a_3 + a_2a_3) = \\ &= 5\sum_{i=1}^{3}a_i^2 - 4(a_1a_2 + a_1a_3 + a_2a_3). \end{aligned}$$

Exemplo 5.2.4 *Se* $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ *e* $x = a_1(\zeta_{11} + \zeta_{11}^{-1}) + \ldots + a_5(\zeta_{11}^5 + \zeta_{11}^{-5})$ *é um inteiro algébrico de* $\mathbb{K}$*, então*

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= 10\sum_{i=1}^{5}a_i^2 + \sum_{\substack{i=2 \\ i:par}}^{10}\rho(t_i)a_{\frac{i}{2}}^2 + 2\sum_{i=1}^{4}\rho(t_i)A_i + 2\sum_{i=3}^{9}\rho(t_i)B_i = \\ &= 10\sum_{i=1}^{5}a_i^2 - a_1^2 - a_2^2 - a_3^2 - a_4^2 - a_5^2 - 2\sum_{i=1}^{4}A_i - 2\sum_{i=3}^{9}B_i = \\ &= 9\sum_{i=1}^{5}a_i^2 - 4(a_1a_2 + a_1a_3 + a_1a_4 + a_1a_5 + a_2a_3 + a_2a_4 + a_2a_5 + a_3a_4 + a_3a_5 + a_4a_5). \end{aligned}$$

Os dois próximos corolários caracterizam a forma quadrática obtida no Teorema 5.2.2 para extensões ciclotômicas cíclicas.

Corolário 5.2.6 *Se* $n = p^r$*, onde* p *é um primo,* r *um número natural maior do que ou igual a* 1*,* $m = \phi(n)$ *e* $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}})$ *é um inteiro algébrico*

de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \phi(p^r) \sum_{i=1}^{\frac{\phi(p^r)}{2}} a_i^2 \; - \; p^{r-1} \left(\sum_{\substack{i=u \\ \frac{n}{P}\, i:par}}^{p-1} a^2_{i\frac{p^r - 1}{2}} + 2\sum_{i=1}^{\frac{p-3}{2}} A_{ip^{r-1}} + 2\sum_{i=v}^{p-2} B_{ip^{r-1}} \right),$$

onde
$u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$; $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$,
$A_j = a_1 a_{j+1} + a_2 a_{j+2} + \ldots + a_{\frac{\phi(p^r)}{2}-j} a_{\frac{\phi(p^r)}{2}}$,
$B_j = \sum_{\substack{k=1 \\ k<j \; k \cdot \frac{\phi(p^r)}{2}}} a_k a_{j-k}$.

Demonstração: Tomando $m = \phi(p^r)$, $P = p$, temos que $\frac{n}{P} = p^{r-1}$ e $\phi(P) = p - 1$. Assim, usando as notações do Teorema 5.2.2 temos que $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $s = \frac{p-3}{2}$ e $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$. Além disso, $t_i = mdc(i, P) = mdc(i, p) = 1$, pois $1 \cdot i \cdot p - 1$. Assim $\rho(t_i) = \mu(\frac{P}{t_i})\phi(t_i) = \mu(p)\phi(1) = -1$. Finalmente substituindo esses valores na expressão obtida no Teorema 5.2.2, obtemos o resultado. ∎

Corolário 5.2.7 *Se* $n = 2p^r$, *onde* p *é um primo ímpar,* r *um número natural maior do que ou igual a* 1, $m = \phi(n)$ *e* $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}})$ *é um inteiro algébrico de* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \phi(2p^r) \sum_{i=1}^{\frac{\phi(2p^r)}{2}} a_i^2 \; - \; p^{r-1} \left(\sum_{\substack{i=u \\ i:par}}^{p-1} a^2_{i\frac{p^r - 1}{2}} \; - \; 2U + 2V \right),$$

onde
$U = \sum_{\substack{i=1 \\ i:\, impar}}^{\frac{p-3}{2}} A_{ip^{r-1}} + \sum_{\substack{i=v \\ i:\, impar}}^{p-2} B_{ip^{r-1}}$;
$V = \sum_{\substack{i=1 \\ i:\, par}}^{\frac{p-3}{2}} A_{ip^{r-1}} + \sum_{\substack{i=v \\ i:\, par}}^{p-2} B_{ip^{r-1}}$;
$u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$; $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$;
$A_j = a_1 a_{j+1} + a_2 a_{j+2} + \ldots + a_{\frac{\phi(2p^r)}{2}-j} a_{\frac{\phi(2p^r)}{2}}$;
$B_j = \sum_{\substack{k=1 \\ k<j \; k \cdot \frac{\phi(2p^r)}{2}}} a_k a_{j-k}$.

Demonstração: Tomando $m = \phi(2p^r)$ e $P = 2p$, temos que $\frac{n}{P} = p^{r-1}$ e $\phi(P) = p - 1$. Assim usando as notações do Teorema 5.2.2 temos que $u = \left\lceil \frac{2}{p^{r-1}} \right\rceil$, $s = \frac{p-3}{2}$ e $v = \left\lceil \frac{3}{p^{r-1}} \right\rceil$. Além disso,

temos que

$$t_i = mdc(i,P) = mdc(i,2p) = \begin{cases} 1, & \textit{se } i \textit{ é impar.} \\ 2, & \textit{se } i \textit{ é par.} \end{cases}$$

Portanto,

$$\rho(t_i) = \begin{cases} 1, & \textit{se } i \textit{ é impar.} \\ \phi(p-1), & \textit{se } i \textit{ é par.} \end{cases}$$

Agora, como p é ímpar, segue que $\frac{n}{P} = p^{r-1}$ é ímpar. Logo $\frac{n}{P}\ i$ é par se, e somente se, i é par. Finalmente, substituindo esses valores na expressão obtida no Teorema 5.2.2, obtemos o resultado. ∎

Corolário 5.2.8 *Se $n = pq$, onde p e q são primos distintos, $m = \phi(n)$ e $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}})$ é um inteiro algébrico de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \phi(pq)\sum_{i=1}^{\frac{\phi(pq)}{2}} a_i^2 + U + 2V + 2W,$$

onde

$$U = \phi(p-1)\sum_{\substack{i=2 \\ i:\ par\ e\ multiplo\ de\ p}}^{\phi(pq)} a_{\frac{i}{2}}^2 \ \phi(q-1)\sum_{\substack{i=2 \\ i:\ par\ e\ multiplo\ de\ q}}^{\phi(pq)} a_{\frac{i}{2}}^2 + \sum_{\substack{i=2 \\ i:\ par;\ (i,pq)=1}}^{\phi(pq)} a_{\frac{i}{2}}^2;$$

$$V = \phi(p-1)\sum_{\substack{i=1 \\ i:\ multiplo\ de\ p}}^{s} A_i \ \phi(q-1)\sum_{\substack{i=1 \\ i:\ multiplo\ de\ q}}^{s} A_i + \sum_{\substack{i=1 \\ (i,pq)=1}}^{s} A_i;$$

$$W = \phi(p-1)\sum_{\substack{i=3 \\ i:\ multiplo\ de\ p}}^{\phi(pq)-1} B_i \ \phi(q-1)\sum_{\substack{i=3 \\ i:\ multiplo\ de\ q}}^{\phi(pq)-1} B_i + \sum_{\substack{i=3 \\ (i,pq)=1}}^{\phi(pq)-1} B_i;$$

$$s = \left\lfloor \frac{\phi(pq)}{2} - 1 \right\rfloor;$$

$$A_j = a_1a_{j+1} + a_2a_{j+2} + \ldots + a_{\frac{\phi(pq)}{2}-j}a_{\frac{\phi(pq)}{2}};$$

$$B_j = \sum_{\substack{k=1 \\ k<j-k\cdot\frac{\phi(pq)}{2}}} a_k a_{j-k}.$$

Demonstração: Tomando $m = \phi(pq) = \phi(P)$, $\mu(P) = \mu(pq) = 1$ e $t_j = mdc(j,P)$ com $j = 1, 2, \ldots, \phi(pq) - 1$, temos que

$$t_j = mdc(j,pq) = \begin{cases} p, & \textit{se } j \textit{ é multiplo de } p. \\ q, & \textit{se } j \textit{ é multiplo de } q. \\ 1, & \textit{se caso contrário.} \end{cases}$$

$$\rho(t_i) = \begin{cases} \phi(p-1), & \textit{se } j \textit{ é multiplo de } p. \\ \phi(q-1), & \textit{se } j \textit{ é multiplo de } q. \\ 1, & \textit{se caso contrário.} \end{cases}$$

Temos também que $\frac{n}{P}j = j$. Assim, dado $n = pq$ e $x = a_1(\zeta_n+\zeta_n^{-1})+a_2(\zeta_n^2+\zeta_n^{-2})+\ldots+a_{\frac{m}{2}}(\zeta_n^{\frac{m}{2}} + \zeta_n^{-\frac{m}{2}})$ um inteiro algébrico de $\mathbb{K} = \mathbb{Q}(\zeta_n+\zeta_n^{-1})$, e substituindo esses valores na expressão obtida

no Teorema 5.2.2, segue o resultado. ■

14 a8a5-120lSBTHTD[1146.91-135[114658168.96i23m35.576.91 06TD[(K)]TJ a2 + 2a1a3 + a2) a3a

Exemplo 5.2.5 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_n)$ *e* $x = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \ldots + a_{\frac{\phi(n)}{2}}(\zeta_n^{\frac{\phi(n)}{2}} + \zeta_n^{-\frac{\phi(n)}{2}})$ *um inteiro algébrico do subcorpo maximal* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. *Na tabela abaixo explicitamos a função* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$ *para alguns valores de* n, *quando* $n = p^r$, $2p^r$ *ou* pq, *onde* p *e* q *são primos distintos e* r *é um número natural maior do que ou igual a* 1.

n	$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$
9	$6(a_1^2 + a_2^2) + 3a_3^2$ ¡ $6a_1a_2$
10	$3(a_1^2 + a_2^2) + 4a_1a_2$
14	

onde $A_j = a_0a_j + a_1a_{j+1} + \cdots + a_{p-2-j}a_{p-2}$. Mas $\sum_{j=1}^{p-2} A_j = \sum_{0\leq i<j\leq p-2} a_ia_j$, e assim, substituindo $\sum_{j=1}^{p-2} A_j$ na Equação 5.3.6, segue o resultado.

5.3.1 Forma quadrática via os subcorpos de $\mathbb{Q}(\zeta_p)$

Nesta seção veremos que o corpo ciclotômico $\mathbb{Q}(\zeta_p)$, onde p é primo, é particularmente importante, pois dado um corpo $\mathbb{K}$, tal que $\mathbb{Q} \subsetneq \mathbb{K} \subsetneq \mathbb{Q}(\zeta_p)$, conseguimos determinar a estrutura do corpo $\mathbb{K}$, o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$, e também podemos obter a forma quadrática via o subcorpo $\mathbb{K}$. O conteúdo desta seção encontra-se em [14], mas fizemos adaptações na demonstração de alguns resultados a seguir, assim existem lemas que são de nossa autoria.

Lema 5.3.1 ([14]) *Se $\mathbb{K}$ é um corpo tal que $\mathbb{K} \subsetneq \mathbb{Q}(\zeta_p)$, onde p é primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, e $\alpha \in \mathbb{Z}$ é tal que σ_α gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então o conjunto*

$$\{\zeta_p^{\alpha^{s+1}}, .., \zeta_p^{\alpha^{rs+1}}, \zeta_p^{\alpha^{s+2}}, .., \zeta_p^{\alpha^{rs+2}}, \ldots, \zeta_p^{\alpha^{s+s}}, .., \zeta_p^{\alpha^{rs+s}}\}$$

é linearmente independente.

Demonstração: Como G é isomorfo a $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, segue pelo Teorema 2.7.4, que $\mathbb{Q}(\zeta_p)$ é uma extensão cíclica, e por hipótese σ_α gera G. Logo ${\mathbb{Z}_p}^* = \langle\alpha\rangle$ e $G = \{\sigma_\alpha, \sigma_{\alpha^2}, \ldots, \sigma_{\alpha^{p-1}}\}$. Tomemos a seguinte combinação

$$\sum_{j=1}^{s}\sum_{i=1}^{r} a_{ji}\zeta_p^{\alpha^{is+j}} = 0, \tag{5.3.7}$$

onde $a_{ji} \in \mathbb{Q}$. Observemos que, para $1 \leq i_1, i_2 \leq r$ e $1 \leq j_1, j_2 \leq s$, se ${\zeta_p}^{\alpha^{i_1s+j_1}} = {\zeta_p}^{\alpha^{i_2s+j_2}}$ então $i_1 = i_2$ e $j_1 = j_2$, pois nos demais casos a igualdade não se verifica. De fato:

1. Se $i_1 = i_2$, $j_1 \neq j_2$ e ${\zeta_p}^{\alpha^{i_1s+j_1}} = {\zeta_p}^{\alpha^{i_2s+j_2}}$,então $\alpha^{i_1s+j_1} \equiv \alpha^{i_2s+j_2} \pmod p$, ou seja, $p \mid \alpha^{i_1s+j_1} - \alpha^{i_2s+j_2}$. Logo, $p \mid \alpha^{i_1s+j_1} - \alpha^{i_1s+j_2}$, ou seja, $p \mid \alpha^{i_1s}(\alpha^{j_1} - \alpha^{j_2})$. Como p é primo, segue que $p \mid \alpha^{i_1s}$ ou $p \mid \alpha^{j_1} - \alpha^{j_2}$. Se $p \mid \alpha^{i_1s}$, novamente usando o fato de p ser primo, segue que $p \mid \alpha$, o que é um absurdo, pois $\alpha \in \{1, 2, \ldots, p-1\}$. Agora, suponhamos $j_1 > j_2$, e deste modo existe $t \in \mathbb{N}$ tal que $j_1 = j_2 + t$. Assim, se $p \mid \alpha^{j_1} - \alpha^{j_2}$ então $p \mid \alpha^{j_2+t} - \alpha^{j_2}$, ou seja, $p \mid \alpha^{j_2}(\alpha^t - 1)$. Como p é primo, $p \mid \alpha^{j_2}$ ou $p \mid \alpha^t - 1$. Se $p \mid \alpha^{j_2}$, então $p \mid \alpha$, o que é um absurdo. Se $p \mid \alpha^t - 1$ então $\alpha^t \equiv 1 \pmod p$. Como $t = j_1 - j_2 \leq s - 1 < s < p - 1$, segue que a ordem do subgrupo gerado por α é menor que $p - 1$, o que é um absurdo, pois a ordem é exatamente $p - 1$.

2. Se $i_1 \neq i_2$ e $j_1 = j_2$, segue de modo análogo ao caso anterior.

3. Se $i_1 \neq i_2$ e $j_1 \neq j_2$, então suponhamos $i_1 > i_2$ e $j_1 > j_2$. Logo existem $t_1, t_2 \in \mathbb{N}$ tais que $i_1 = i_2 + t_1$ e $j_1 = j_2 + t_2$, onde $t_1 = i_1 - i_2 \leq r - 1$ e $t_2 = j_1 - j_2 \leq s - 1$. Assim se $p \mid \alpha^{i_1s+j_1} - \alpha^{i_2s+j_2}$, então $p \mid \alpha^{(i_2+t_1)s+(j_2+t_2)} - \alpha^{i_2s+j_2}$, ou seja $p \mid \alpha^{i_2s+j_2}(\alpha^{t_1s+t_2} - 1)$. Como p é primo, segue que $p \mid \alpha^{i_2s+j_2}$ ou $p \mid \alpha^{t_1s+t_2} - 1$. Se $p \mid \alpha^{i_2s+j_2}$, então $p \mid \alpha$, o que

é um absurdo. Se $p \mid \alpha^{t_1 s+t_2} - 1$, então $\alpha^{t_1 s+t_2} \equiv 1 \ (mod\ p)$, o que é um absurdo, pois como $t_1 \cdot r - 1$ e $t_2 \cdot s - 1$, segue que $t_1 s \cdot (r-1)s$ e assim $t_1 s + t_2 \cdot p - 2 < p - 1$, ou seja, analogamente ao ítem (1), teríamos que a ordem do subgrupo gerado por α seria menor que $p - 1$.

Assim, os ζ_p's da Equação (5.3.7) são todos distintos num total de $p - 1$ elementos. Logo podemos reescrevê-la da seguinte forma

$$\sum_{k=1}^{p-1} b_k {\zeta_p}^k = 0,$$

onde $b_k \in \mathbb{Q}$, para todo $k = 1, 2, \cdots, n$. Como $\{\zeta_p, {\zeta_p}^2, \ldots, {\zeta_p}^{p-1}\}$ é uma base de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, segue que $b_k = 0$ para todo $k = 1, 2, \ldots, p-1$ e conseqüentemente $a_{ji} = 0$, para todo $j = 1, 2, \ldots, s$ e $i = 1, 2, \ldots, r$. Portanto, o conjunto $\{\zeta_p^{\alpha^{s+1}}, .., \zeta_p^{\alpha^{rs+1}}, \zeta_p^{\alpha^{s+2}}, .., \zeta_p^{\alpha^{rs+2}}, \ldots, \zeta_p^{\alpha^{s+s}}, .., \zeta_p^{\alpha^{rs+s}}\}$ é linearmente independente. ∎

Teorema 5.3.2 ([14]) *Se $\mathbb{K}$ é um corpo tal que $\mathbb{K} \subsetneq \mathbb{Q}(\zeta_p)$, onde p é primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e $\alpha \in \mathbb{Z}$ tal que σ_α gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então $\mathbb{K} = \mathbb{Q}(\theta)$.*

Demonstração: Como $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$, segue que $\theta \in \mathbb{K}$, e portanto $\mathbb{Q}(\theta) \subseteq \mathbb{K}$. Como $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, segue que o subgrupo cíclico H que fixa o corpo $\mathbb{K}$ possui ordem r. Como $\{\overline{\alpha^s}, \overline{\alpha^{2s}}, \ldots, \overline{\alpha^{rs}} = \overline{1}\}$ é o único subgrupo de $\mathbb{Z}_p^*$ de ordem r e a ordem de H é r, segue que $H = \langle \sigma_{\alpha^s} \rangle = \{\sigma_{\alpha^s}, \sigma_{\alpha^{2s}}, \ldots, \sigma_{\alpha^{rs}}\}$, onde $H = Gal(\mathbb{Q}(\zeta_p)/\mathbb{K})$. Assim

$$\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) = \sigma_{\alpha^s}(\zeta_p) + \sigma_{\alpha^{2s}}(\zeta_p) + \ldots + \sigma_{\alpha^{rs}}(\zeta_p),$$

e deste modo $\theta = {\zeta_p}^{\alpha^s} + {\zeta_p}^{\alpha^{2s}} + \ldots + {\zeta_p}^{\alpha^{rs}}$. Como $\mathbb{Q}(\theta)$ é fixado por um subgrupo cíclico (logo um subgrupo normal) segue que $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão galoisiana. Agora, se $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ é o polinômio irredutível de θ sobre $\mathbb{Q}$, então

$$\theta^m + a_{m-1}\theta^{m-1} + \ldots + a_1\theta + a_0 = 0, \text{onde } a_i \in \mathbb{Q}, \text{ para todo } i = 0, 1, \cdots, m-1. \quad (5.3.8)$$

Aplicando σ_{α^i}, para $i = 1, 2, \cdots, s$, na Equação (5.3.8) obtemos

$$\begin{aligned} 0 &= \sigma_{\alpha^i}(\theta^m + a_{m-1}\theta^{m-1} + \ldots + a_1\theta + a_0) = \sigma_{\alpha^i}(\theta^m) + a_{m-1}\sigma_{\alpha^i}(\theta^{m-1}) + \ldots + a_1\sigma_{\alpha^i}(\theta) + a_0 = \\ &= [\sigma_{\alpha^i}(\theta)]^m + a_{m-1}[\sigma_{\alpha^i}(\theta)]^{m-1} + \ldots + a_1[\sigma_{\alpha^i}(\theta)] + a_0. \end{aligned}$$

ou seja, $\sigma_{\alpha^i}(\theta)$ é raiz de $f(x)$, para todo $i = 1, 2, \cdots, s$. Mas como $\mathbb{Q}(\theta)/\mathbb{Q}$ é galoisiana, tomando $i = 1, 2, \ldots, s$, segue que $\sigma_\alpha(\theta), \sigma_{\alpha^2}(\theta), \ldots, \sigma_{\alpha^s}(\theta) \in \mathbb{Q}(\theta)$. Agora, sejam $a_1, a_2, \cdots, a_s \in \mathbb{Q}$ tais que

$$a_1\sigma_\alpha(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta) = 0.$$

Assim

$$a_1({\zeta_p}^{\alpha^{s+1}} + \ldots + {\zeta_p}^{\alpha^{rs+1}}) + a_2({\zeta_p}^{\alpha^{s+2}} + \ldots + {\zeta_p}^{\alpha^{rs+2}}) + \ldots + a_s({\zeta_p}^{\alpha^{s+s}} + \ldots + {\zeta_p}^{\alpha^{rs+s}}) = 0,$$

ou seja,

$$a_1{\zeta_p}^{\alpha^{s+1}} + \ldots + a_1{\zeta_p}^{\alpha^{rs+1}} + a_2{\zeta_p}^{\alpha^{s+2}} + \ldots + a_2{\zeta_p}^{\alpha^{rs+2}} + \ldots + a_s{\zeta_p}^{\alpha^{s+s}} + \ldots + a_s{\zeta_p}^{\alpha^{rs+s}} = 0.$$

Mas pelo Lema 5.3.1, temos que o conjunto $\{\zeta_p^{\alpha^{s+1}}, .., \zeta_p^{\alpha^{rs+1}}, \zeta_p^{\alpha^{s+2}}, .., \zeta_p^{\alpha^{rs+2}}, \ldots, \zeta_p^{\alpha^{s+s}}, .., \zeta_p^{\alpha^{rs+s}}\}$ é linearmente independente. Logo $a_i = 0$, para todo $i = 1, 2, \ldots, s$, e portanto $\{\sigma_\alpha(\theta), \sigma_{\alpha^2}(\theta), \ldots, \sigma_{\alpha^s}(\theta)\}$ é um conjunto linearmente independente contido em $\mathbb{Q}(\theta)$. Portanto $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq s$. Mas como $\mathbb{Q}(\theta) \subseteq \mathbb{K}$ e $[\mathbb{K} : \mathbb{Q}] = s$, segue que $\mathbb{K} = \mathbb{Q}(\theta)$.

Corolário 5.3.1 ([14]) *Se $\mathbb{K}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$, onde p é primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e $\alpha \in \mathbb{Z}$ tal que σ_α gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, então $\mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta)$ é o anel dos inteiros algébricos de $\mathbb{K}$.*

Demonstração: Pelo Teorema 5.3.2 temos que $\{\sigma_\alpha(\theta), \sigma_{\alpha^2}(\theta), \ldots, \sigma_{\alpha^s}(\theta)\}$ é uma base para $\mathbb{K} = \mathbb{Q}(\theta)$. Se $\alpha \in \mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta)$, então $\alpha = \sum_{i=1}^{s} a_i\sigma_{\alpha^i}(\theta)$, onde $a_i \in \mathbb{Z}$, para todo $i = 1, 2, \cdots, s$. Mas $\sigma_{\alpha^i}(\theta) = \zeta_p^{\alpha^{s+i}} + \ldots + \zeta_p^{\alpha^{rs+i}}$, ou seja, $\sigma_{\alpha^i}(\theta) = \zeta_p^{j_1} + \ldots + \zeta_p^{j_r}$, onde os j_i's são distintos. Assim podemos reescrever $\sigma_{\alpha^i}(\theta)$ da seguinte forma:

$$\sigma_{\alpha^i}(\theta) = 0\zeta_p + \ldots + 1\zeta_p^{j_1} + \ldots + 1\zeta_p^{j_r} + \ldots + 0\zeta_p^{p-1}.$$

Logo $\sigma_{\alpha^i}(\theta) \in \mathbb{Z}[\zeta_p]$ e como $\sigma_{\alpha^i}(\theta) \in \mathbb{K}$, segue que $\sigma_{\alpha^i}(\theta) \in \mathbb{Z}[\zeta_p] \cap \mathbb{K}$. Temos que $\mathcal{O}_\mathbb{K} = \mathfrak{B} \cap \mathbb{K}$, onde $\mathfrak{B} = \{\alpha \in \mathbb{C}; \ irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]\}$. Como $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, segue que $\mathbb{Z}[\zeta_p] = \mathfrak{B} \cap \mathbb{Q}(\zeta_p)$, ou seja, $\mathbb{Z}[\zeta_p] \subseteq \mathfrak{B}$ e assim $\mathbb{Z}[\zeta_p] \cap \mathbb{K} \subseteq \mathfrak{B} \cap \mathbb{K} = \mathcal{O}_\mathbb{K}$. Portanto, $\sigma_{\alpha^i}(\theta) \in \mathcal{O}_\mathbb{K}$, e como $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo, segue que $a_i\sigma_{\alpha^i}(\theta) \in \mathcal{O}_\mathbb{K}$, onde $a_i \in \mathbb{Z}$, para todo $i = 1, 2, \cdots, s$, e conseqüentemente $\sum_{i=1}^{s} a_i\sigma_{\alpha^i}(\theta) \in \mathcal{O}_\mathbb{K}$, ou seja $\alpha \in \mathcal{O}_\mathbb{K}$. Portanto,

$$\mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta) \subseteq \mathcal{O}_\mathbb{K}.$$

Reciprocamente, dado $\alpha \in \mathcal{O}_\mathbb{K}$, podemos escrever

$$\alpha = a_1\sigma_\alpha(\theta) + a_2\sigma_{\alpha^2}(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta), \text{ onde } a_i \in \mathbb{Q}, \text{ para todo } i = 1, 2, \cdots, s,$$

pois $\alpha \in \mathcal{O}_\mathbb{K} \subseteq \mathbb{K}$, e $\{\sigma_\alpha(\theta), \sigma_{\alpha^2}(\theta), \ldots, \sigma_{\alpha^s}(\theta)\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim

$$\alpha = a_1\zeta_p^{\alpha^{s+1}} + \ldots + a_1\zeta_p^{\alpha^{rs+1}} + a_2\zeta_p^{\alpha^{s+2}} + \ldots + a_2\zeta_p^{\alpha^{rs+2}} + \ldots + a_s\zeta_p^{\alpha^{s+s}} + \ldots + a_s\zeta_p^{\alpha^{rs+s}}.$$

Repetindo o argumento que foi usado na demonstração do Teorema 5.3.2, podemos reescrever α da seguinte maneira

$$\alpha = b_1\zeta_p + b_2\zeta_p^2 + \ldots + b_{p-1}\zeta_p^{p-1}, \text{ onde } b_i \in \mathbb{Q}, \text{ para todo } i = 1, 2, \cdots, p - 1.$$

Como $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$, segue que $\mathfrak{B} \cap \mathbb{K} \subseteq \mathfrak{B} \cap \mathbb{Q}(\zeta_p)$, ou seja $\mathcal{O}_\mathbb{K} \subseteq \mathbb{Z}[\zeta_p]$. Assim, $\alpha \in \mathbb{Z}[\zeta_p]$, e $b_i \in \mathbb{Z}$, para todo $i = 1, 2 \ldots, p - 1$. Conseqüentemente $a_i \in \mathbb{Z}$, para todo $i = 1, 2, \ldots, s$. Assim, $\alpha \in \mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta)$. Portanto,

$$\mathcal{O}_\mathbb{K} \subseteq \mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta).$$

Assim concluímos que $\mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta) = \mathcal{O}_\mathbb{K}$. ∎

Proposição 5.3.1 ([5]) *Sejam $\mathbb{K}$ um corpo tal que $\mathbb{K} \neq \mathbb{Q}(\zeta_p)$, onde p é primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e $\alpha \in \mathbb{Z}$ tal que σ_α gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Se $y \in O_{\mathbb{K}}$, com $y = a_1\sigma_\alpha(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta)$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{s} a_i^2 + r \sum_{1\leq i<j\leq s} (a_i - a_j)^2 = Q_{s,r}(y).$$

Demonstração: Seja $y = a_1\sigma_\alpha(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta)$, onde $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$. Pela demonstração do Teorema 5.3.2 temos que $\theta = {\zeta_p}^{\alpha^s} + {\zeta_p}^{\alpha^{2s}} + \ldots + {\zeta_p}^{\alpha^{rs}}$. Logo $\sigma_{\alpha^i}(\theta) = {\zeta_p}^{\alpha^{s+i}} + \ldots + {\zeta_p}^{\alpha^{rs+i}}$, para todo $i = 1, 2, \cdots, s$, e assim

$$y = a_1({\zeta_p}^{\alpha^{s+1}} + \ldots + {\zeta_p}^{\alpha^{rs+1}}) + a_2({\zeta_p}^{\alpha^{s+2}} + \ldots + {\zeta_p}^{\alpha^{rs+2}}) + \ldots + a_s({\zeta_p}^{\alpha^{s+s}} + \ldots + {\zeta_p}^{\alpha^{rs+s}}).$$

Agora, repetindo o argumento que foi usado na demonstração do Corolário 5.3.1, e pela definição de forma quadrática, podemos associar a y a $(p-1)$-upla $\underline{y} = (a_1, \ldots, a_1, a_2, \ldots, a_2, \ldots, a_s, \ldots, a_s)$, onde cada a_i, para $i = 1, 2, \cdots, s$, aparece r vezes. Assim

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = Q_{p-1,1}(y),$$

e deste modo

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = r\sum_{i=1}^{s} a_i^2 + r^2 \sum_{1\leq i<j\leq s} (a_i - a_j)^2.$$

Usando as propriedades da função traço, temos que

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}) = [\mathbb{Q}(\zeta_p) : \mathbb{K}]\ Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}),$$

ou seja,

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \frac{1}{r} Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(y\overline{y}),$$

e assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{s} a_i^2 + r \sum_{1\leq i<j\leq s} (a_i - a_j)^2,$$

o que prova o proposição. ∎

Exemplo 5.3.1 *Tomando $p = 7$ e $r = 2$ temos que $s = 3$. Assim, se $y \in O_{\mathbb{K}}$ então $y = a_1\sigma_\alpha(\theta) + a_2\sigma_{\alpha^2}(\theta) + a_3\sigma_{\alpha^3}(\theta)$. Logo*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{3} a_i^2 + 2 \sum_{1\leq i<j\leq 3} (a_i - a_j)^2,$$

e portanto

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = 5\sum_{i=1}^{3} a_i^2 - 4(a_1a_2 + a_1a_3 + a_2a_3).$$

Exemplo 5.3.2 *Tomando $p = 11$ e $r = 2$ temos que $s = 5$. Assim, se $y \in \mathcal{O}_{\mathbb{K}}$ então $y = a_1\sigma_\alpha(\theta) + \ldots + a_5\sigma_{\alpha^5}(\theta)$. Logo*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{5} a_i^2 + 2 \sum_{1\leq i<j\leq 5} (a_i - a_j)^2,$$

e portanto

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = 9\sum_{i=1}^{5} a_i^2 - 4(a_1a_2 + a_1a_3 + a_1a_4 + a_1a_5 + a_2a_3 + a_2a_4 + a_2a_5 + a_3a_4 + a_3a_5 + a_4a_5).$$

5.3.2 Minimização da forma quadrática sobre os subcorpos de $\mathbb{Q}(\zeta_p)$

Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p)$, onde p é primo, $\mathbb{K} \subset \mathbb{L}$, $[\mathbb{L} : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)$, $\alpha \in \mathbb{Z}$ tal que σ_α gera $G = Gal(\mathbb{L}/\mathbb{Q})$ e $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$ os anéis dos inteiros algébricos de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Nesta seção veremos a minimização da forma quadrática obtida na Proposição 5.3.1, tomando os elementos y no ideal $\mathcal{P}_{\mathbb{K}} = \mathcal{P}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$, onde $\mathcal{P}_{\mathbb{L}} = (1 - \zeta_p)\mathcal{O}_{\mathbb{L}}$, pois estamos interessados em ideais que se ramificam totalmente em $\mathcal{O}_{\mathbb{L}}$, e $\mathcal{P}_{\mathbb{K}}$ satisfaz esta condição. Com efeito, pelo Teorema 2.7.2, temos que $\mathfrak{D}_{\mathbb{L}} = (-1)^{(p-1)/2}p^{p-2}$. Como p divide $\mathfrak{D}_{\mathbb{L}}$, segue pelo Teorema 2.8.6, que o ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ e pelo Lema 2.8.1, sua decomposição é dada por

$$p\mathcal{O}_{\mathbb{L}} = \mathcal{P}_{\mathbb{L}}{}^{p-1},$$

onde $\mathcal{P}_{\mathbb{L}} = (1 - \zeta_p)\mathcal{O}_{\mathbb{L}}$. Tomando $\mathcal{P}_{\mathbb{K}} = \mathcal{P}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$, pela Proposição 2.8.1, temos que sua decomposição é dada por

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_{\mathbb{K}}{}^{s}.$$

Assim $p\mathcal{O}_{\mathbb{K}}$ se ramifica totalmente, e deste modo o grau residual de $\mathcal{P}_{\mathbb{L}}$ sobre $\mathcal{P}_{\mathbb{K}}$ é igual a 1. Portanto, $\mathcal{O}_{\mathbb{L}}/\mathcal{P}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ possuem a mesma cardinalidade, e assim $N(\mathcal{P}_{\mathbb{K}}) = N(\mathcal{P}_{\mathbb{L}}) = N_{\mathbb{L}/\mathbb{Q}}(1 - \zeta_p) = p$.

Observação 5.3.1 *O conteúdo desta seção encontra-se em [5], mas fizemos adaptações na demonstração de alguns resultados a seguir, assim existem lemas que são de nossa autoria.*

Lema 5.3.2 ([5]) *Se $\mathbb{L} = \mathbb{Q}(\zeta_p)$, onde p é primo e $\mathcal{P}_{\mathbb{L}} = (1 - \zeta_p)\mathcal{O}_{\mathbb{L}}$, então*

$$\mathcal{P}_{\mathbb{L}} \cap \mathbb{Z} = p\mathbb{Z}.$$

Demonstração: Como $irr_{\mathbb{Q}}(\zeta_p) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \prod_{i=1}^{p-1}(x - \zeta_p^i)$, segue que $p = (1 - \zeta_p)(1 - \zeta_p^2)\ldots(1 - \zeta_p^{p-1})$. Assim $p \in (1 - \zeta_p)\mathcal{O}_{\mathbb{L}}$, e como $p \in \mathbb{Z}$, segue que $p\mathbb{Z} \subset (1 - \zeta_p)\mathcal{O}_{\mathbb{L}} \cap \mathbb{Z}$. Para mostrarmos a outra inclusão, suponhamos que $p\mathbb{Z} \subsetneq (1 - \zeta_p)\mathcal{O}_{\mathbb{L}} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal, segue que $(1 - \zeta_p)\mathcal{O}_{\mathbb{L}} \cap \mathbb{Z} = \mathbb{Z}$. Mas como $1 \in \mathbb{Z}$, ou seja, $1 = (1 - \zeta_p)a$, com $a \in \mathcal{O}_{\mathbb{L}}$, segue que $N(1) = N(1 - \zeta_p)N(a)$, o que implica que $1 = pN(a)$, com $N(a) \in \mathbb{Z}$, o que é um absurdo. Portanto $\mathcal{P}_{\mathbb{L}} \cap \mathbb{Z} = p\mathbb{Z}$. ∎

Os próximos lemas caracterizam os elementos de $\mathcal{P}_{\mathbb{L}}$ e $\mathcal{P}_{\mathbb{K}}$.

Lema 5.3.3 ([5]) *Se* $\mathbb{L} = \mathbb{Q}(\zeta_p)$, *onde* p *é primo,* $y = a_1\zeta_p + a_2\zeta_p^2 + \ldots + a_{p-1}\zeta_p^{p-1}$ *é um elemento de* $O_{\mathbb{L}}$ *e* $P_{\mathbb{L}} = (1 - \zeta_p)O_{\mathbb{L}}$, *então*

$$y \in P_{\mathbb{L}} \Leftrightarrow \sum_{i=1}^{p-1} a_i \equiv 0 (mod\ p).$$

Demonstração: Como $P_{\mathbb{L}} = (1 - \zeta_p)O_{\mathbb{L}}$, segue que $\zeta_p \equiv 1 (mod P_{\mathbb{L}})$. Como $a_1 \equiv a_1 (mod\ P_{\mathbb{L}})$, segue que $a_1\zeta_p \equiv a_1 (mod P_{\mathbb{L}})$. Como $1 - \zeta_p^i = (1 - \zeta_p)(\zeta_p^{i-1} + \zeta_p^{i-2} + \ldots + \zeta_p + 1)$, para qualquer i, segue que $1 - \zeta_p^i \in P_{\mathbb{L}}$, ou seja, $\zeta_p^i \equiv 1 (mod\ P_{\mathbb{L}})$. Assim $a_i\zeta_p^i \equiv a_1 (mod\ P_{\mathbb{L}})$, para todo $i = 2, 3, \ldots, p - 1$, e portanto

$$y \equiv \sum_{i=1}^{p-1} a_i (mod\ P_{\mathbb{L}})$$

Logo

$$y \in P_{\mathbb{L}} \Leftrightarrow \sum_{i=1}^{p-1} a_i \in P_{\mathbb{L}},$$

e como $\sum_{i=1}^{p-1} a_i \in \mathbb{Z}$, pelo Lema 5.3.2, segue que $\sum_{i=1}^{p-1} a_i \in p\mathbb{Z}$. Assim

$$y \in P_{\mathbb{L}} \Leftrightarrow \sum_{i=1}^{p-1} a_i \equiv 0 (mod\ p)$$

o que prova o lema. ∎

Lema 5.3.4 ([5]) *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_p)$, *onde* p *é primo,* $\mathbb{K} \subset \mathbb{L}$, $[\mathbb{L} : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$, $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)$ *e* $\alpha \in \mathbb{Z}$ *tal que* σ_α *gera* $G = Gal(\mathbb{L}/\mathbb{Q})$. *Se* $y = a_1\sigma_\alpha(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta)$ *é um elemento de* $O_{\mathbb{K}}$ *e* $P_{\mathbb{K}} = P_{\mathbb{L}} \cap O_{\mathbb{K}}$ *então*

$$y \in P_{\mathbb{K}} \Leftrightarrow \sum_{i=1}^{s} a_i \equiv 0 (mod\ p).$$

Demonstração: Seja $y \in P_{\mathbb{K}}$. Pelo fato de $P_{\mathbb{K}} \subset P_{\mathbb{L}}$ temos que $y \in P_{\mathbb{L}}$. Usando o Lema 5.3.3 temos que $r\sum_{i=1}^{s} a_i \equiv 0 (mod\ p)$ e como p não divide r segue que $\sum_{i=1}^{s} a_i \equiv 0 (mod\ p)$. Reciprocamente, pelo Corolário 5.3.1 temos que $O_{\mathbb{K}} = \mathbb{Z}\sigma_\alpha(\theta) + \ldots + \mathbb{Z}\sigma_{\alpha^s}(\theta)$. Por hipótese $y \in O_{\mathbb{K}}$ é dado por

$$y = a_1(\zeta_p^{\alpha^{s+1}} + \ldots + \zeta_p^{\alpha^{rs+1}}) + a_2(\zeta_p^{\alpha^{s+2}} + \ldots + \zeta_p^{\alpha^{rs+2}}) + \ldots + a_s(\zeta_p^{\alpha^{s+s}} + \ldots + \zeta_p^{\alpha^{rs+s}}).$$

Repetindo o argumento que foi usado na demonstração do Corolário 5.3.1, podemos associar a y a $(p - 1)$-upla $\underline{y} = (a_1, \ldots, a_1, a_2, \ldots, a_2, \ldots, a_s, \ldots, a_s)$, onde cada a_i, para $i = 1, 2, ¢¢¢, s$, aparece r vezes. Assim se $\sum_{i=1}^{s} a_i \equiv 0 (mod\ p)$, então $r\sum_{i=1}^{s} a_i \equiv 0 (mod\ p)$. Como $y \in O_{\mathbb{K}} \subset O_{\mathbb{L}}$, novamente pelo Lema 5.3.3, segue que $y \in P_{\mathbb{L}}$, o que prova o lema. ∎

Lema 5.3.5 ([5]) *Sejam $\mathbb{Q} \subset \mathbb{K}$ uma extensão Galoisiana, G seu grupo de Galois e $p \in \mathbb{Z}$ um primo que decompõe completamente. Então*

1. *$\sigma(P_{\mathbb{K}}) \cap \mathbb{Z} = p\mathbb{Z}$, para todo $\sigma \in G$.*
2. *$\sigma(P_{\mathbb{K}}) = P_{\mathbb{K}}$, para todo $\sigma \in G$.*

Demonstração: Para o ítem (1), temos pelo Lema 5.3.2, que $P_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$. Assim, se $y \in p\mathbb{Z}$, então $y \in P_{\mathbb{K}}$. Também, $y = \sigma(y) \in \sigma(P_{\mathbb{K}}) \cap \mathbb{Z}$, para todo $\sigma \in G$, ou seja, $p\mathbb{Z} \subset \sigma(P_{\mathbb{K}}) \cap \mathbb{Z}$. Por outro lado, como $p\mathbb{Z}$ é maximal e $\sigma(P_{\mathbb{K}}) \cap \mathbb{Z} \neq \mathbb{Z}$, segue que $\sigma(P_{\mathbb{K}}) \cap \mathbb{Z} = p\mathbb{Z}$. Para o ítem (2), como $P_{\mathbb{K}} \cap \mathbb{Z} = \sigma(P_{\mathbb{K}}) \cap \mathbb{Z} = p\mathbb{Z}$, para todo $\sigma \in G$, e $P_{\mathbb{K}}$ é o único idel primo acima de p, segue que $\sigma(P_{\mathbb{K}}) = P_{\mathbb{K}}$, para todo $\sigma \in G$. ∎

Lema 5.3.6 ([5]) *Se $y \in P_{\mathbb{K}}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) \in p\mathbb{Z}$.*

Demonstração: Pelo Lema 5.3.5, temos que $\sigma_i(P_{\mathbb{K}}) = P_{\mathbb{K}}$, para todo $\sigma_i \in Gal(\mathbb{K} : \mathbb{Q})$, $i = 1, 2, \cdots, s$. Logo para todo $y \in P_{\mathbb{K}}$, temos que $\sigma_i(y) \in P_{\mathbb{K}}$, e portanto

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{s} \sigma_i(y\overline{y}) \in P_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z},$$

o que prova o lema. ∎

Lema 5.3.7 ([5]) *Sejam $\mathbb{K} \supset \mathbb{Q}(\zeta_p)$, onde p é primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = r$, $[\mathbb{K} : \mathbb{Q}] = s$ e $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$. Se $y, y' \in O_{\mathbb{K}}$, e associarmos a y e y', respectivamente, as s-uplas $\underline{y} = (a, m, \cdots, m)$ e $\underline{y'} = (a, m', \cdots, m')$, então*

$$Q_{s,r}(\underline{y}) > Q_{s,r}(\underline{y'}),$$

onde $a > b > 0$, $m = \left[\frac{a}{1+1/r}\right]$ e $m' = \left[\frac{b}{1+1/r}\right]$.

Demonstração: Sendo $b > 0$, tomemos $a = b + 1$. Assim temos que $\underline{y} = (b+1, m, \cdots, m)$ e $\underline{y'} = (b, m', \cdots, m')$, onde $m = \left[\frac{b}{1+1/r} + \frac{1}{1+1/r}\right]$ e $m' = \left[\frac{b}{1+1/r}\right]$. Logo:

$$Q_{s,r}(\underline{y}) = (b+1)^2 + (s - 1)(m^2 + r(b+1 - m)^2),$$

$$Q_{s,r}(\underline{y'}) = b^2 + (s - 1)(m'^2 + r(b - m')^2).$$

Agora, comparamos cada parcela, dessas duas últimas igualdades.

1. Como $b > 0$, segue que $(b+1)^2 > b^2$.
2. Como $\frac{b+1}{1+1/r} > \frac{b}{1+1/r}$, segue que $\left[\frac{b+1}{1+1/r}\right] \geq \left[\frac{b}{1+1/r}\right]$. Portanto, $m \geq m' \geq 0$ e daí $m^2 \geq m'^2$.
3. Agora, temos que $(b+1) - m \geq b - m'$ se, e somente se, $m - m' \leq 1$, e para provarmos essa última desigualdade observe que $\frac{1}{2} \cdot \frac{1}{1+1/r} < 1$. Logo $\frac{b}{1+1/r} + \frac{1}{2} \cdot \frac{b}{1+1/r} + \frac{1}{1+1/r} < \frac{b}{1+1/r} + 1$. E ainda temos:

$$\begin{array}{ccccc} \frac{b}{1+1/r}+\frac{1}{1+1/r} \text{ i } \frac{1}{2} & \cdot & m & \cdot & \frac{b}{1+1/r}+\frac{1}{1+1/r}+\frac{1}{2}, \\ \frac{b}{1+1/r} \text{ i } \frac{1}{2} & \cdot & m' & \cdot & \frac{b}{1+1/r}+\frac{1}{2} \end{array}$$

Tomando os casos extremos em que $m' = \frac{b}{1+1/r}$ i $\frac{1}{2}$ e $m = \frac{b}{1+1/r}+\frac{1}{1+1/r}+\frac{1}{2}$, temos que:

$$m \text{ i } m' = \frac{b}{1+1/r}+\frac{1}{1+1/r}+\frac{1}{2} \text{ i } \frac{b}{1+1/r}+\frac{1}{2} = \frac{1}{1+1/r}+1.$$

Logo, m i $m' < 2$, mas como m e m' são números inteiros, segue que m i $m' = 1$ ou m i $m' = 0$. Portanto m i $m' \cdot 1$. Assim $(b+1$ i $m) \, , \, b$ i m' e daí $(b+1$ i $m)^2 \, , \, (b$ i $m')^2$.

Portanto, de (1), (2) e (3), segue o resultado. ∎

Observação 5.3.2 *A forma quadrática da Proposição* 5.3.1 *pode ser escrita como*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = (p \text{ i } r)\sum_{i=1}^{s} a_i^2 \text{ i } 2r \sum_{1\leq i<j\leq s} a_i a_j.$$

Lema 5.3.8 ([5]) *Se y é um elemento não nulo de $P_{\mathbb{K}}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$ assume o valor $2p$.*

Demonstração: Vamos assumir que $s \, , \, 2$, ou seja, $\mathbb{K} \neq \mathbb{Q}$, assim, se tomarmos $y = \sigma_\alpha(\theta) \text{ i } \sigma_{\alpha^2}(\theta) + 0\sigma_{\alpha^3}(\theta) + ¢¢¢ + 0\sigma_{\alpha^s}(\theta)$, temos que

$$\begin{array}{rcl} Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) & = & (p \text{ i } r)\sum_{i=1}^{s} a_i^2 \text{ i } 2r \sum_{1\leq i<j\leq s} a_i a_j \\ & = & (p \text{ i } r)(1+1) \text{ i } 2r(\text{ i } 1) \\ & = & 2p, \end{array}$$

o que prova o lema. ∎

Lema 5.3.9 ([5]) *Se r é par então $[\frac{r}{1+1/r}] = r$ i 1.*

Demonstração: Como i $1 < 0 < \frac{r-1}{2}$ segue que somando r^2, em cada parcela, obtemos i $1+r^2 < r^2 < r^2+\frac{r}{2}$ i $\frac{1}{2}$. Assim, dividindo cada parcela por $r+1$, obtemos r i $1 < \frac{r^2}{r-1} < r$ i $\frac{1}{2}$, ou seja, r i $1 < \frac{r}{1-1/r} < r$ i $\frac{1}{2}$. Mas, isto implica que, $[\frac{r}{1-1/r}] = r$ i 1. ∎

Observação 5.3.3 *Tomamos $y \in \mathcal{O}_{\mathbb{K}}$, tal que a s-upla associada a y é dada por $\underline{y} = (r, r \text{ i } 1, ¢¢¢ , r \text{ i } 1)$, onde r é par. Agora, pelo Lema* 5.3.7*, temos que, para minimizarmos a forma quadrática $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$ devemos tomar uma s-upla $\underline{y'} = (b, m', ¢¢¢ , m') = (a_1, a_2, ¢¢¢ , a_s)$ onde $r > b > 0$ e $m' = \left[\frac{b}{1+1/r}\right]$. Como $r > b > 0$, segue que $|b| < r$, ou seja i $(r \text{ i } 1) \cdot b \cdot r \text{ i } 1$. Temos também que $\frac{b}{1+1/r} < \frac{r}{1+1/r}$, e assim $m' = \left[\frac{b}{1+1/r}\right] \cdot \left[\frac{r}{1+1/r}\right] = r \text{ i } 1$. Como $r > 0$, segue que i $r < 0$, e assim $\frac{b}{1+1/r} > \frac{-r}{1+1/r}$, logo $m' = \left[\frac{b}{1+1/r}\right] \, , \, \left[\frac{-r}{1+1/r}\right] = \text{ i } \left[\frac{r}{1+1/r}\right] = \text{ i } (r \text{ i } 1)$. Portanto, i $(r \text{ i } 1) \cdot b, m' \cdot (r \text{ i } 1)$, ou seja, i $(r \text{ i } 1) \cdot a_i \cdot (r \text{ i } 1)$, para $i = 1, 2, ¢¢¢ , s$.*

Finalmente, como queremos $y \in P_{\mathbb{K}}$, *pelo Lema* 5.3.4, *segue que* $\sum_{i=1}^{s} a_i \equiv 0 (mod\ p)$. *Mas, isso somente ocorre quando* $\sum_{i=1}^{a} a_i = 0$, *uma vez que* $i(p-1) < i(r-1)\frac{p-1}{r} \cdot \sum_{i=1}^{s} a_i \cdot (r-1)\frac{p-1}{r} < p-1$.

Lema 5.3.10 ([5]) *A forma quadrática* $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$ *para* $y \in P_{\mathbb{K}}$ *não atinge o valor* p.

Demonstração: Suponhamos que exista $y = a_1\sigma_\alpha(\theta) + \ldots + a_s\sigma_{\alpha^s}(\theta)$ um elemento $P_{\mathbb{K}}$ tal que

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = (p-r)\sum_{i=1}^{s} a_i^2 - 2r \sum_{1\leq i<j\leq a} a_i a_j = p.$$

Como $\sum_{i=1}^{s} a_i = 0$ segue que $\left(\sum_{i=1}^{s} a_i\right)^2 = 0$. Assim, $\sum_{i=1}^{a} a_i^2 + 2\sum_{1\leq i<j\leq s} a_i a_j = 0$, ou seja, $\sum_{i=1}^{s} a_i^2 = -2\sum_{1\leq i<j\leq s} a_i a_j$. Assim, $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = (p-r)\sum_{i=1}^{s} a_i^2 + r\sum_{i=1}^{s} a_i^2 = p$, ou seja, $p\sum_{i=1}^{s} a_i^2 = p$. Logo, $\sum_{i=1}^{s} a_i^2 = 1$. Mas isso, somente ocorre quando tivermos uma das entradas igual a ± 1 e as outras nulas. Mas isso, contraria o fato de que $\sum_{i=1}^{s} a_i = 0$. Deste modo, temos que $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) > p$. ∎

Teorema 5.3.3 ([5]) *Dado* $y \in P_{\mathbb{K}}$, $y \neq 0$, *então* $min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})\} = 2p$.

Demonstração: Segue diretamente dos Lemas 5.3.6, 5.3.8 e 5.3.10. ∎

Exemplo 5.3.3 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{13})$, $\mathbb{K} \subsetneq \mathbb{L}$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 3$, $P_{\mathbb{L}} = (1-\zeta_{13})O_{\mathbb{L}}$ *e* $P_{\mathbb{K}} = P_{\mathbb{L}} \cap O_{\mathbb{K}}$. *Sabemos que* $\mathfrak{D}_{\mathbb{K}} = \pm 13^2$, $N(P_{\mathbb{K}}) = 13$ *e pelo Teorema* 5.3.3 *temos que* $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y});\ y \in P_{\mathbb{K}},\ y \neq 0\} = 26$. *Logo*

$$\delta(\sigma_{\mathbb{K}}(P_{\mathbb{K}})) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(P_{\mathbb{K}})} = 0,09805.$$

Exemplo 5.3.4 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{29})$, $\mathbb{K} \subsetneq \mathbb{L}$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 4$, $P_{\mathbb{L}} = (1-\zeta_{29})O_{\mathbb{L}}$ *e* $P_{\mathbb{K}} = P_{\mathbb{L}} \cap O_{\mathbb{K}}$. *Sabemos que* $\mathfrak{D}_{\mathbb{K}} = \pm 29^3$, $N(P_{\mathbb{K}}) = 29$ *e pelo Teorema* 5.3.3 *temos que* $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y});\ y \in P_{\mathbb{K}},\ y \neq 0\} = 58$. *Logo*

$$\delta(\sigma_{\mathbb{K}}(P_{\mathbb{K}})) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(P_{\mathbb{K}})} = 0,04642.$$

Observação 5.3.4 *No corpo ciclotômico* $\mathbb{Q}(\zeta_p)$ *e em seus subcorpos não conseguimos obter reticulados algébricos com densidade de centro ótima.*

Capítulo

6

Reticulados via perturbações do homomorfismo de Minkowski

6.1 Introdução

Neste capítulo apresentamos um método de gerar reticulados através de duas perturbações diferentes do homomorfismo de Minkowski. Desse modo, na Seção 6.2, apresentamos a perturbação σ_α. Assim, fixados $\mathbb{L}$ um corpo de números e A um ideal contido no anel dos inteiros algébricos de $\mathbb{L}$, vimos que a imagem de A por σ_α é um reticulado e obtemos a expressão para a densidade de centro. Na Seção 6.3, de maneira análoga, vimos a perturbação $\sigma_{2\alpha}$. Para finalizar, na Seção 6.4, apresentamos um estudo comparando os reticulados obtidos via o ideal A através do homomorfismo de Minkowski e das perturbações, sempre com o intuito de encontrar reticulados de alta densidade. Destacamos que, o trabalho apresentado neste capítulo é de nossa autoria.

6.2 A perturbação σ_α

Sejam $\mathbb{L}$ um corpo de números de grau n e $\sigma_1, \sigma_2, ¢¢¢ , \sigma_n$ os homomorfismos de $\mathbb{L}$ em $\mathbb{C}$, ordenados de modo que σ_i é real para $i = 1, 2, ¢¢¢ , r_1$ e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ para $j = 1, 2, ¢¢¢ , r_2$, onde r_2 representa a metade dos homomorfismos imaginários.

Definição 6.2.1 *Seja x 2 $\mathbb{L}$ um elemento. A perturbação σ_α : $\mathbb{L}$ ¡ ! $\mathbb{R}^n$ do homomorfismo de Minkowski é definida como*

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \ldots, <(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), =(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))),$$

onde $\alpha_i = \sigma_i(\alpha) > 0$, $\sigma_i(\alpha)$ 2 $\mathbb{R}$, para todo $i = 1, 2, \ldots, r_1 + r_2$ e as notações $<(x)$ e $=(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Proposição 6.2.1 *Seja $\mathbb{L}$ um corpo de números de grau n. Se $M \subset \mathbb{L}$ 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 $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, com volume*

$$Vol(\sigma_\alpha(M)) = b_\alpha \left| \det_{1\leq j,k\leq n}(\sigma_j(x_k)) \right|,$$

onde

- $b_\alpha = (N(\alpha))^{\frac{1}{2}}$ *se* $\mathbb{L}$ *for totalmente real,*
- $b_\alpha = 2^{\frac{jn}{2}}(N(\alpha))^{\frac{1}{2}}$ *se* $\mathbb{L}$ *for totalmente imaginário, e*
- $N(\alpha)$ *é a norma do elemento* $\alpha \in \mathbb{L}$.

Demonstração: Para cada j fixo, as coordenadas de $\sigma_\alpha(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sqrt{\overline{\alpha_1}}\sigma_1(x_j), \ldots, \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_j), \ldots, <(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_j)), =(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_j)). \tag{6.2.1}$$

Agora, calculamos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (6.2.1) fazendo uso das seguintes fórmulas $<(z) = \frac{1}{2}(z+\overline{z})$, $=(z) = \frac{1}{2i}(z - \overline{z})$ 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 linha da sua posterior, para $l = 1, \ldots, r_2$. Assim,

$$D = \begin{vmatrix}
\sqrt{\overline{\alpha_1}}\sigma_1(x_1) & \ldots & \sqrt{\overline{\alpha_1}}\sigma_1(x_j) & \ldots & \sqrt{\overline{\alpha_1}}\sigma_1(x_n) \\
\sqrt{\overline{\alpha_2}}\sigma_2(x_1) & \ldots & \sqrt{\overline{\alpha_2}}\sigma_2(x_j) & \ldots & \sqrt{\overline{\alpha_2}}\sigma_2(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_1) & \ldots & \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_j) & \ldots & \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_n) \\
<(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_1)) & \ldots & <(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_j)) & \ldots & <(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_n)) \\
=(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_1)) & \ldots & =(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_j)) & \ldots & =(\sqrt{\overline{\alpha_{r_1+1}}}\sigma_{r_1+1}(x_n)) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
<(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_1)) & \ldots & <(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_j)) & \ldots & <(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_n)) \\
=(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_1)) & \ldots & =(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_j)) & \ldots & =(\sqrt{\overline{\alpha_{r_1+r_2}}}\sigma_{r_1+r_2}(x_n))
\end{vmatrix} =$$

$$= \begin{vmatrix}
\sqrt{\overline{\alpha_1}}\sigma_1(x_1) & \ldots & \sqrt{\overline{\alpha_1}}\sigma_1(x_n) \\
\sqrt{\overline{\alpha_2}}\sigma_2(x_1) & \ldots & \sqrt{\overline{\alpha_2}}\sigma_2(x_n) \\
\vdots & \ddots & \vdots \\
\sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_1) & \ldots & \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_n) \\
\frac{1}{2}[\sqrt{\overline{\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)})] & \ldots & \frac{1}{2}[\sqrt{\overline{\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)})] \\
\frac{1}{2i}[\sqrt{\overline{\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)})] & \ldots & \frac{1}{2i}[\sqrt{\overline{\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)})] \\
\vdots & \ddots & \vdots \\
\frac{1}{2}[\sqrt{\overline{\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)})] & \ldots & \frac{1}{2}[\sqrt{\overline{\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)})] \\
\frac{1}{2i}[\sqrt{\overline{\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)})] & \ldots & \frac{1}{2i}[\sqrt{\overline{\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)})]
\end{vmatrix} =$$

$$= \sqrt{\overline{\alpha_1\alpha_2\ldots\alpha_{r_1}}}\alpha_{r_1+1}\alpha_{r_1+2}\ldots\alpha_{r_1+r_2}\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2} 2^{r_2} D_1,$$

onde D_1 é o seguinte determinante

$$D_1 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+1}(x_1) \; i \; \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) \; i \; \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) \; i \; \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \\ \sigma_{r_1+r_2}(x_1) \; i \; \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) \; i \; \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) \; i \; \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

Assim,

$$D = p\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}\alpha_{r_1+1}\alpha_{r_1+2}\dots\alpha_{r_1+r_2}\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}D_2,$$

onde D_2 é o seguinte determinante

$$D_2 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}.$$

Portanto, $D = p\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}\alpha_{r_1+1}\alpha_{r_1+2}\dots\alpha_{r_1+r_2}(2i)^{-r_2}\det(\sigma_j(x_k))$, para todo j, $k = 1,\dots,n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, segue que $\det(\sigma_j(x_k))$ 6= 0, e portanto, D 6= 0. Assim, os vetores $\sigma_\alpha(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_\alpha(M)$, ou seja, $\sigma_\alpha(M)$ é um reticulado do $\mathbb{R}^n$. Agora, como $fx_1,\dots,x_ng$ é uma $\mathbb{Z}$-base de M, segue que dado m 2 M temos que $m = \sum_{j=1}^{n} a_j x_j$, com a_j 2 $\mathbb{Z}$, para $j = 1, 2, ¢¢¢ , n$. Assim, $\sigma_\alpha(m) = \sum_{j=1}^{n} a_j\sigma_\alpha(x_j)$, com a_j 2 $\mathbb{Z}$, para $j = 1, 2, ¢¢¢ , n$, ou seja, $\sigma_\alpha(M) = \left\{\sum_{j=1}^{n} a_j\sigma_\alpha(x_j);\ a_j \text{ 2 } \mathbb{Z}\right\}$. Logo,

$$Vol(\sigma_\alpha(M)) = \ jDj = p\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}\alpha_{r_1+1}\alpha_{r_1+2}\dots\alpha_{r_1+r_2}2^{-r_2}j\det_{1\leq j,\,k\leq n}(\sigma_j(x_k))j.$$

Deste modo, temos os seguintes casos

2 Se $r_2 = 0$, então

$$Vol(\sigma_\alpha(M)) = (\prod_{i=1}^{r_1}\sigma_i(\alpha))^{\frac{1}{2}}j\det_{1\leq j,\,k\leq n}(\sigma_j(x_k))j = (N(\alpha))^{\frac{1}{2}}j\det_{1\leq j,\,k\leq n}(\sigma_j(x_k))j.$$

² Se $r_1 = 0$, então $\mathbb{L}$ é totalmente complexo e $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

$Vol(\sigma_\alpha(M)) = 2^{-r_2} \prod_{i=1}^{r_2} \sigma_i(\alpha) \det_{1\le j,k\le n}(\sigma_j(x_k))$. Como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+r_2}}$, para $i = 1, 2, \ldots, r_2$, segue que $\sigma_{r_2+j}(\alpha) = \overline{\sigma_j(\alpha)} = \sigma_j(\alpha)$. Assim, $\prod_{i=1}^{r_2} \sigma_i(\alpha) = (N(\alpha))^{\frac{1}{2}}$ e como $n = 2r_2$ segue que

$$Vol(\sigma_\alpha(M)) = 2^{\frac{in}{2}} (N(\alpha))^{\frac{1}{2}} \det_{1\le j,k\le n}(\sigma_j(x_k)),$$

o que prova a proposição. ■

Corolário 6.2.1 *Se $\mathbb{L}$ é um corpo de números de grau n, $\mathfrak{D}_\mathbb{L}$ o discriminante de $\mathbb{L}$, $O_\mathbb{L}$ o anel dos inteiros algébricos de $\mathbb{L}$, A um ideal não nulo de $O_\mathbb{L}$ e $N(A)$ a norma do ideal A, então $\sigma_\alpha(O_\mathbb{L})$ e $\sigma_\alpha(A)$ são reticulados, com respectivos volumes,*

$$Vol(\sigma_\alpha(O_\mathbb{L})) = b_\alpha \sqrt{|\mathfrak{D}_\mathbb{L}|},$$

$$Vol(\sigma_\alpha(A)) = b_\alpha \sqrt{|\mathfrak{D}_\mathbb{L}|}\, N(A)$$

Demonstração: Como A e $O_\mathbb{L}$ são $\mathbb{Z}$-módulos livres de posto n, segue da Proposição 6.2.1, que $\sigma_\alpha(A)$ e $\sigma_\alpha(O_\mathbb{L})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_\alpha(O_\mathbb{L})) = b_\alpha \sqrt{|\mathfrak{D}_\mathbb{L}|}$, pois

Demonstração: Seja $\mathbb{L}$ um corpo de números de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_\alpha(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned}
\|\sigma_\alpha(x)\|^2 &= [\sqrt{\alpha_1}\sigma_1(x)]^2 + \cdots + [\sqrt{\alpha_{r_1}}\sigma_{r_1}(x)]^2 + \sqrt{\alpha_{r_1+1}}\,\Re(\sigma_{r_1+1}(x))]^2 + [\sqrt{\alpha_{r_1+1}}\,\Im(\sigma_{r_1+1}(x))]^2 + \\
&\quad + \cdots + [\sqrt{\alpha_{r_1+r_2}}\,\Re(\sigma_{r_1+r_2}(x))]^2 + [\sqrt{\alpha_{r_1+r_2}}\,\Im(\sigma_{r_1+r_2}(x))]^2 = \\
&= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + \alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))]^2 + \alpha_{r_1+1}[\Im(\sigma_{r_1+1}(x))]^2 \\
&\quad + \cdots + \alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))]^2 + \alpha_{r_1+r_2}[\Im(\sigma_{r_1+r_2}(x))]^2 = \\
&= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + \alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))^2 + +\Im(\sigma_{r_1+1}(x))^2] + \\
&\quad + \cdots + \alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))^2 + \Im(\sigma_{r_1+r_2}(x))^2].
\end{aligned}$$

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 $r_1 + 1 \cdot k \cdot r_1 + r_2$. Assim, temos os seguintes fatos.

- Se $r_1 = 0$, então

$$\begin{aligned}
\|\sigma_\alpha(x)\|^2 &= \alpha_1\sigma_1(x\overline{x}) + \cdots + \alpha_{r_2}\sigma_{r_2}(x\overline{x}) &&= \sigma_1(\alpha)\sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(\alpha)\sigma_{r_2}(x\overline{x}) = \\
&= \sigma_1(\alpha x\overline{x}) + \cdots + \sigma_{r_2}(\alpha x\overline{x}) &&= \sigma_{r_2+1}(\alpha x\overline{x}) + \cdots + \sigma_{r_2+r_2}(\alpha x\overline{x}).
\end{aligned}$$

pois sendo $\overline{\sigma}$ a conjugação complexa, temos que $\sigma_{r_2+j}(\alpha x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(\alpha x\overline{x}) = \sigma_j(\alpha x\overline{x})$, para $j = 1, \ldots, r_2$. Logo,

$$\begin{aligned}
2\|\sigma_\alpha(x)\|^2 &= \sigma_1(\alpha x\overline{x}) + \cdots + \sigma_{r_2}(\alpha x\overline{x}) + \sigma_{r_2+1}(\alpha x\overline{x}) + \cdots + \sigma_{r_2+r_2}(\alpha x\overline{x}) = \\
&= \sum_{i=1}^{n} \sigma_i(\alpha x\overline{x}) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}).
\end{aligned}$$

Portanto

$$\|\sigma_\alpha(x)\|^2 = \frac{1}{2}Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}).$$

- Se $r_2 = 0$, então

$$\|\sigma_\alpha(x)\|^2 = \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2,$$

e como $\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$ segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = [\sigma_i(x)]^2$. Assim,

$$\begin{aligned}
\|\sigma_\alpha(x)\|^2 &= \alpha_1\sigma_1(x\overline{x}) + \cdots + \alpha_{r_1}\sigma_{r_1}(x\overline{x}) &&= \sigma_1(\alpha)\sigma_1(x\overline{x}) + \cdots + \sigma_{r_1}(\alpha)\sigma_{r_1}(x\overline{x}) = \\
&= \sigma_1(\alpha x\overline{x}) + \cdots + \sigma_{r_1}(\alpha x\overline{x}).
\end{aligned}$$

Portanto,

$$\|\sigma_\alpha(x)\|^2 = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}),$$

e isto conclui a demonstração. ∎

Observação 6.2.1 *Se* $\mathbb{L}$ *é um corpo de números totalmente real ou totalmente imaginário,* $\mathcal{O}_{\mathbb{L}}$ *é o anel dos inteiros algébricos de* $\mathbb{L}$ *e* $\mathcal{A}$ *um ideal não nulo de* $\mathcal{O}_{\mathbb{L}}$*, então podemos reescrever o raio de empacotamento do reticulado* $\sigma_\alpha(\mathcal{A})$ *da seguinte forma:*

$$\rho(\sigma_\alpha(\mathcal{A})) = \frac{1}{2} min\{|\sigma_\alpha(x)|,\ x \in \mathcal{A},\ x \neq 0\} = \frac{1}{2} min\left\{\sqrt{c_\alpha Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x \overline{x})},\ x \in \mathcal{A},\ x \neq 0\right\},$$

onde

$$c_\alpha = \begin{cases} 1, & \text{se } \mathbb{L} \text{ for totalmente real} \\ \dfrac{1}{2}, & \text{se } \mathbb{L} \text{ for totalmente imaginário,} \end{cases}$$

6.3 A perturbação $\sigma_{2\alpha}$

Sejam $\mathbb{L}$

$$= \begin{vmatrix} \sqrt{\overline{\alpha_1}}\sigma_1(x_1) & \dots & \sqrt{\overline{\alpha_1}}\sigma_1(x_n) \\ \sqrt{\overline{\alpha_2}}\sigma_2(x_1) & \dots & \sqrt{\overline{\alpha_2}}\sigma_2(x_n) \\ \vdots & \ddots & \vdots \\ \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_1) & \dots & \sqrt{\overline{\alpha_{r_1}}}\sigma_{r_1}(x_n) \\ \frac{1}{2}[\sqrt{\overline{2\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)})] & \dots & \frac{1}{2}[\sqrt{\overline{2\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)})] \\ \frac{1}{2i}[\sqrt{\overline{2\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_1)\ i\ \overline{\sigma_{r_1+1}(x_1)})] & \dots & \frac{1}{2i}[\sqrt{\overline{2\alpha_{r_1+1}}}(\sigma_{r_1+1}(x_n)\ i\ \overline{\sigma_{r_1+1}(x_n)})] \\ \vdots & \ddots & \vdots \\ \frac{1}{2}[\sqrt{\overline{2\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)})] & \dots & \frac{1}{2}[\sqrt{\overline{2\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)})] \\ \frac{1}{2i}[\sqrt{\overline{2\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_1)\ i\ \overline{\sigma_{r_1+r_2}(x_1)})] & \dots & \frac{1}{2i}[\sqrt{\overline{2\alpha_{r_1+r_2}}}(\sigma_{r_1+r_2}(x_n)\ i\ \overline{\sigma_{r_1+r_2}(x_n)})] \end{vmatrix} =$$

$$= \sqrt{\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}}\ 2\alpha_{r_1+1}2\alpha_{r_1+2}\dots 2\alpha_{r_1+r_2}\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2} 2^{r_2} D_1,$$

onde D_1 é o seguinte determinante

$$D_1 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+1}(x_1)\ i\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j)\ i\ \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n)\ i\ \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n) \\ \sigma_{r_1+r_2}(x_1)\ i\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j)\ i\ \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n)\ i\ \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

Assim,

$$D = \sqrt{\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}}\ 2\alpha_{r_1+1}2\alpha_{r_1+2}\dots 2\alpha_{r_1+r_2}\left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2} 2^{r_2} D_2,$$

onde D_2 é o seguinte determinante

$$D_2 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n) \\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}.$$

Portanto, $D = \sqrt{\overline{\alpha_1\alpha_2\dots\alpha_{r_1}}}\ 2\alpha_{r_1+1}2\alpha_{r_1+2}\dots 2\alpha_{r_1+r_2}(2i)^{-r_2}\det(\sigma_j(x_k))$, para todo $j,\ k = 1,\dots,n$. Como $(x_j)_{1\le j\le n}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, segue que $\det(\sigma_j(x_k)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{2\alpha}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{2\alpha}(M)$, ou seja, $\sigma_{2\alpha}(M)$ é um reticulado do $\mathbb{R}^n$. Agora, como $\{x_1,\dots,x_n\}$ é uma $\mathbb{Z}$-base de M, segue que dado $m \in M$ temos que $m = \sum_{j=1}^{n} a_j x_j$, com $a_j \in \mathbb{Z}$, para $j = 1, 2, \dots, n$. Assim, $\sigma_{2\alpha}(m) =$

$\sum_{j=1}^{n} a_j\sigma_{2\alpha}(x_j)$, com $a_j \in \mathbb{Z}$, para $j = 1, 2, \ldots, n$, ou seja, $\sigma_{2\alpha}(M) = \left\{\sum_{j=1}^{n} a_j\sigma_{2\alpha}(x_j);\ a_j \in \mathbb{Z}\right\}$.
Logo,

$$Vol(\sigma_{2\alpha}(M)) = |D| = \sqrt{\alpha_1\alpha_2\ldots\alpha_{r_1}}\, 2\alpha_{r_1+1}2\alpha_{r_1+2}\ldots 2\alpha_{r_1+r_2}2^{-r_2}\left|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))\right|.$$

Deste modo, temos os seguintes casos.

- Se $r_2 = 0$, então

$$Vol(\sigma_{2\alpha}(M)) = (\prod_{i=1}^{r_1}\sigma_i(\alpha))^{\frac{1}{2}}\left|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))\right| = (N(\alpha))^{\frac{1}{2}}\left|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))\right|.$$

- Se $r_1 = 0$, então

$Vol(\sigma_{2\alpha}(M)) = 2^{r_2}\prod_{i=1}^{r_2}\sigma_i(\alpha)2^{-r_2}\left|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))\right|$. Como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $i = 1, 2, \ldots, r_2$, segue que $\sigma_{r_2+j}(\alpha) = \overline{\sigma_j(\alpha)} = \sigma_j(\alpha)$. Assim, $\prod_{i=1}^{r_2}\sigma_i(\alpha) = (N(\alpha))^{\frac{1}{2}}$ e portanto

$$Vol(\sigma_{2\alpha}(M)) = (N(\alpha))^{\frac{1}{2}}\left|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))\right|,$$

o que prova a proposição. ∎

Corolário 6.3.1 *Se $\mathbb{L}$ é um corpo de números de grau n, $\mathfrak{D}_{\mathbb{L}}$ o discriminante de $\mathbb{L}$, $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$, $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$ e $N(\mathcal{A})$ a norma do ideal $\mathcal{A}$, então $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})$ e $\sigma_{2\alpha}(\mathcal{A})$ são reticulados, com respectivos volumes,*

$$Vol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})) = (|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}},$$

$$Vol(\sigma_{2\alpha}(\mathcal{A})) = (|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}}N(\mathcal{A}).$$

Demonstração: Como $\mathcal{A}$ e $\mathcal{O}_{\mathbb{L}}$ são $\mathbb{Z}$-módulos livres de posto n, segue da Proposição 6.3.1, que $\sigma_{2\alpha}(\mathcal{A})$ e $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})) = (|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}}$, pois $\mathfrak{D}_{\mathbb{L}} = \det(\sigma_i(x_k))^2$, onde $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}}$. Para a segunda fórmula, temos que $\sigma_{2\alpha}(\mathcal{A})$ é um subgrupo de $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})$ de índice $N(\mathcal{A})$, uma vez que $\mathcal{O}_{\mathbb{L}}/\mathcal{A}$ é isomorfo a $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})/\sigma_{2\alpha}(\mathcal{A})$. Além disso, como a região fundamental de $\sigma_{2\alpha}(\mathcal{A})$ é a união disjunta de $N(\mathcal{A})$ cópias de uma região fundamental de $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})$, segue que $Vol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{L}})) = (|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}}$ e $Vol(\sigma_{2\alpha}(\mathcal{A})) = (|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}}N(\mathcal{A})$. ∎

Corolário 6.3.2 *Se $\mathbb{L}$ é um corpo de números de grau n, $\mathfrak{D}_{\mathbb{L}}$ o discriminante de $\mathbb{L}$, $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de $\mathbb{L}$, $\mathcal{A}$ um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$ e $N(\mathcal{A})$ a norma do ideal $\mathcal{A}$, então a*

densidade de centro do reticulado $\sigma_{2\alpha}(A)$ *é dada por*

$$\delta(\sigma_{2\alpha}(A)) = \frac{(\rho(\sigma_{2\alpha}(A)))^n}{(|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{\frac{1}{2}}N(A)},$$

onde ρ *é o raio de empacotamento do reticulado.*

Demonstração: Segue diretamente da Observação 3.3.1. ∎

Proposição 6.3.2 *Se* $\mathbb{L}$ *é um corpo de números e* $x \in \mathbb{L}$ *então*

$$|\sigma_{2\alpha}(x)|^2 = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}),$$

onde $\overline{x}$ *é o conjugado complexo de* x*.*

Demonstração: Seja $\mathbb{L}$ um corpo de números de grau n de forma que $r_1 + 2r_2 = n$. Como $\sigma_{2\alpha}(x) \in \mathbb{R}^n$, segue que

$$\begin{aligned}
|\sigma_{2\alpha}(x)|^2 &= [\sqrt{\alpha_1}\sigma_1(x)]^2 + \cdots + [\sqrt{\alpha_{r_1}}\sigma_{r_1}(x)]^2 + [\sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x))]^2 + [\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x))]^2 + \\
&\quad + \cdots + [\sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x))]^2 + [\sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))]^2 = \\
&= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + 2\alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))]^2 + 2\alpha_{r_1+1}[\Im(\sigma_{r_1+1}(x))]^2 + \\
&\quad + \cdots + 2\alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))]^2 + 2\alpha_{r_1+r_2}[\Im(\sigma_{r_1+r_2}(x))]^2 = \\
&= \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2 + 2\alpha_{r_1+1}[\Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2] + \\
&\quad + \cdots + 2\alpha_{r_1+r_2}[\Re(\sigma_{r_1+r_2}(x))^2 + \Im(\sigma_{r_1+r_2}(x))^2].
\end{aligned}$$

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, temos os seguintes fatos.

- Se $r_1 = 0$, então

$$\begin{aligned}
|\sigma_\alpha(x)|^2 &= 2\alpha_1\sigma_1(x\overline{x}) + \cdots + 2\alpha_{r_2}\sigma_{r_2}(x\overline{x}) = 2\sigma_1(\alpha)\sigma_1(x\overline{x}) + \cdots + 2\sigma_{r_2}(\alpha)\sigma_{r_2}(x\overline{x}) = \\
&= 2\sigma_1(\alpha x\overline{x}) + \cdots + 2\sigma_{r_2}(\alpha x\overline{x}),
\end{aligned}$$

pois sendo $\overline{\sigma}$ é a conjugação complexa, temos que $\sigma_{r_2+j}(\alpha x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(\alpha x\overline{x}) = \sigma_j(\alpha x\overline{x})$, para $j = 1, \ldots, r_2$. Logo,

$$\begin{aligned}
|\sigma_\alpha(x)|^2 &= \sigma_1(\alpha x\overline{x}) + \cdots + \sigma_{r_2}(\alpha x\overline{x}) + \sigma_{r_2+1}(\alpha x\overline{x}) + \cdots + \sigma_{r_2+r_2}(\alpha x\overline{x}) = \\
&= \sum_{i=1}^{n} \sigma_i(\alpha x\overline{x}) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}).
\end{aligned}$$

Portanto,

$$|\sigma_\alpha(x)|^2 = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}).$$

- Se $r_2 = 0$, então

$$|\sigma_\alpha(x)|^2 = \alpha_1[\sigma_1(x)]^2 + \cdots + \alpha_{r_1}[\sigma_{r_1}(x)]^2,$$

e como $\sigma_i(x) = (\overline{\sigma} \pm \sigma_i)(x) = \sigma_i(\overline{x})$ segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = [\sigma_i(x)]^2$. Assim,

$$\begin{aligned} |\sigma_\alpha(x)|^2 &= \alpha_1\sigma_1(x\overline{x}) + ¢¢¢ + \alpha_r \end{aligned}$$

1. **Relação entre os reticulados gerados pelos homomorfismos**
   Comparando $\sigma_{\mathbb{L}}$, σ_α e $\sigma_{2\alpha}$, temos os seguintes fatos:

   - Os reticulados $\sigma_{\mathbb{L}}(A)$ e $\sigma_\alpha(A)$ são iguais se $\alpha_i = 1$, para todo $i = 1, 2, \cdots, r_1 + r_2$.
   - Os reticulados $\sigma_{\mathbb{L}}(A)$ e $\sigma_{2\alpha}(A)$ são iguais se $\mathbb{L}$ for totalmente real e $\alpha_i = 1$, para todo $i = 1, 2, \cdots, r_1$.
   - Os reticulados $\sigma_\alpha(A)$ e $\sigma_{2\alpha}(A)$ são iguais se $\mathbb{L}$ for totalmente real.

2. **Relação entre as densidades de centro dos reticulados gerados pelos homomorfismos**

   - Os reticulados $\sigma_\alpha(A)$ e $\sigma_{2\alpha}(A)$ possuem a mesma densidade de centro, conforme podemos observar nas Proposições 6.2.3 e 6.3.3.
   - Entre os reticulados $\sigma_{\mathbb{L}}(A)$ e $\sigma_\alpha(A)$ (ou $\sigma_{2\alpha}(A)$), podem ocorrer os seguintes casos:

(a) $\delta(\sigma_{\mathbb{L}}(A)) < \delta(\sigma_\alpha(A))$.

Exemplo 6.4.1 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt[p]{2})$, $A = (3 - 2\sqrt[p]{2})\mathcal{O}_{\mathbb{L}}$ *um ideal de* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt[p]{2}]$, *e* $\alpha = 10 + 7\sqrt[p]{2} + 2\mathcal{O}_{\mathbb{L}}$. *Temos que* $n = [\mathbb{L} : \mathbb{Q}] = 2$, $\mathfrak{D}_{\mathbb{L}} = 8$, $N(A) = 1$ *e* $N(\alpha) = 2$. *Dado* $x \in A$, *temos que* $x = (3 - 2\sqrt[p]{2})(a_0 + a_1\sqrt[p]{2})$, *com* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 34a_0^2 + 68a_1^2 - 96a_0a_1$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}) = 4a_0^2 + 8a_1^2 - 8a_0a_1$. *Portanto* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 2$ *e* $t_\alpha = 4$, *e as densidades de centro são dadas por:*

1. *sem perturbação*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,17677.$$

2. *com perturbação*

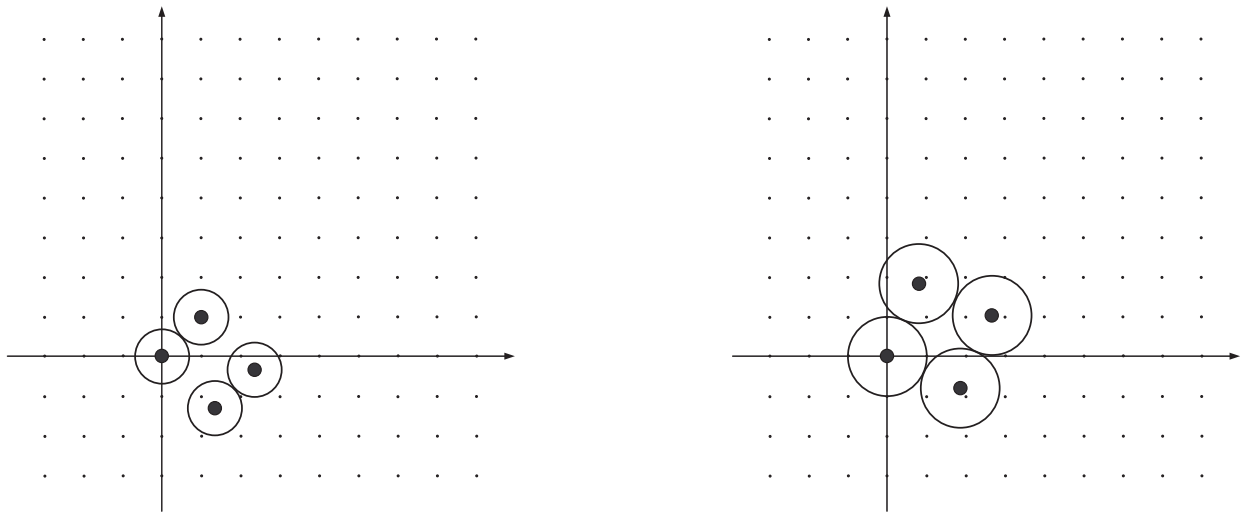
$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n (|\mathfrak{D}_{\mathbb{L}}| N(\alpha))^{1/2}} \frac{{t_\alpha}^{n/2}}{N(A)} = 0,25.$$

Na figura abaixo, damos um esboço do arranjo das esferas do empacotamento dos reticulados $\sigma_{\mathbb{L}}(A)$ e $\sigma_\alpha(A)$, respectivamente:

Exemplo 6.4.2 *Sejam o corpo* $\mathbb{L} = \mathbb{Q}(\zeta_5)$, $A = (1 + 2\zeta_5 + \zeta_5^2 + \zeta_5^3)\mathcal{O}_{\mathbb{L}}$ *um ideal de* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_5]$ *e* $\alpha = 7 + 4\zeta_5^2 + 4\zeta_5^3 \in \mathcal{O}_{\mathbb{L}}$. *Temos que* $n = [\mathbb{L} : \mathbb{Q}] = 4$, $\mathfrak{D}_{\mathbb{L}} = 125$, $N(A) = 41$ *e* $N(\alpha) = 25$. *Dado* $x \in A$, *temos que* $x = (1 + 2\zeta_5 + \zeta_5^2 + \zeta_5^3)(a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3)$, *com* $a_i \in \mathbb{Z}$, *para* $i = 0, 1, 2, 3$. *Assim,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 26(a_0^2 + a_1^2 + a_2^2 + a_3^2) - 18(a_0a_2 + a_0a_3 + a_1a_3) - 8(a_0a_1 + a_1a_2 + a_2a_3)$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}) = 110(a_0^2 + a_1^2 + a_2^2 + a_3^2) - 160(a_0a_1 + a_1a_2 + a_2a_3) + 50(a_0a_2 + a_0a_3 + a_1a_3)$. *Portanto* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 26$ *e* $t_\alpha = 60$, *e deste modo as densidades de centro são dadas por:*

1. *sem perturbação*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,09216.$$



2. com perturbação

$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n(|\mathfrak{D}_\mathbb{L}|N(\alpha))^{1/2}}\frac{{t_\alpha}^{n/2}}{N(A)} = 0,09816.$$

(b) $\delta(\sigma_\mathbb{L}(A)) = \delta(\sigma_\alpha(A))$.

Exemplo 6.4.3 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt[p]{2})$, $A = (6+4\sqrt[p]{2})O_\mathbb{L}$ *um ideal de* $O_\mathbb{L} = \mathbb{Z}[\sqrt[p]{2}]$, *e* $\alpha = 2 \in O_\mathbb{L}$. *Temos que* $n = [\mathbb{L} : \mathbb{Q}] = 2$, $\mathfrak{D}_\mathbb{L} = 8$, $N(A) = 4$ *e* $N(\alpha) = 4$. *Dado* $x \in A$, *temos que* $x = (6 + 4\sqrt[p]{2})(a_0 + a_1\sqrt[p]{2})$, *com* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 136a_0^2 + 272a_1^2 + 384a_0a_1$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}) = 272a_0^2 + 544a_1^2 + 768a_0a_1$. *Portanto* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 8$ *e* $t_\alpha = 16$, *e as densidades de centro são dadas por:*

1. sem perturbação

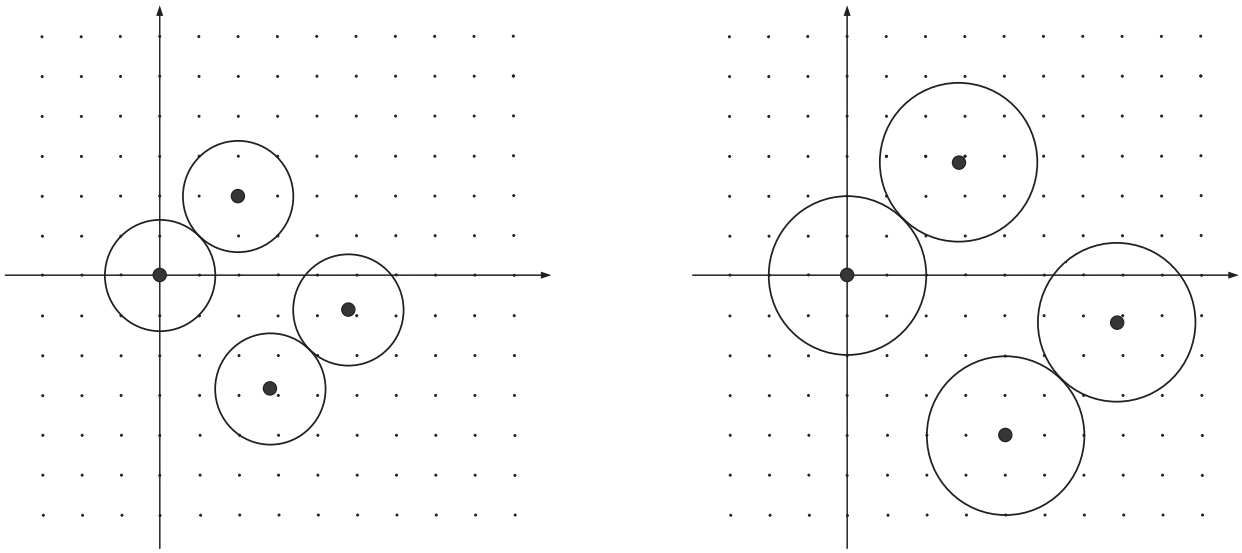
$$\delta(\sigma_\mathbb{L}(A)) = \frac{1}{2^n|\mathfrak{D}_\mathbb{L}|^{1/2}}\ \frac{t^{n/2}}{N(A)} = 0,17677.$$

2. com perturbação

$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n(|\mathfrak{D}_\mathbb{L}|N(\alpha))^{1/2}}\frac{{t_\alpha}^{n/2}}{N(A)} = 0,17677.$$

Na figura abaixo, damos um esboço do arranjo das esferas do empacotamento dos reticulados $\sigma_\mathbb{L}(A)$ e $\sigma_\alpha(A)$, respectivamente:

Exemplo 6.4.4 *Sejam o corpo* $\mathbb{L} = \mathbb{Q}(\zeta_9)$, $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ *seu subcorpo maximal,* $A = (2(\zeta_9^2 + \zeta_9^{-2}) + (\zeta_9^3 + \zeta_9^{-3}))O_\mathbb{K}$ *um ideal de* $O_\mathbb{K} = \mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$ *e* $\alpha = 3 \in O_\mathbb{K}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 3$, $\mathfrak{D}_\mathbb{K} = 81$, $N(A) = 3$ *e* $N(\alpha) = 27$. *Dado* $x \in A$, *temos que* $x = (2(\zeta_9^2 + \zeta_9^{-2}) + (\zeta_9^3 + \zeta_9^{-3}))(a_1(\zeta_9 + \zeta_9^{-1}) + a_2(\zeta_9^2 + \zeta_9^{-2}) + a_3(\zeta_9^3 + \zeta_9^{-3}))$, *com* $a_i \in \mathbb{Z}$, *para* $i = 1, 2, 3$. *Assim,* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = 18a_1^2 + 90a_2^2 + 27a_3^2 - 54a_1a_2 + 72a_2a_3$ *e*



$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x\overline{x}) = 54a_1^2 + 270a_2^2 + 81a_3^2 - 162a_1a_2 + 216a_2a_3$. *Portanto* $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 9$ *e* $t_\alpha = 27$, *e deste modo as densidades de centro são dadas por:*

1. *sem perturbação*

$$\delta(\sigma_{\mathbb{K}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,125.$$

2. *com perturbação*

$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n (|\mathfrak{D}_{\mathbb{K}}| N(\alpha))^{1/2}} \frac{{t_\alpha}^{n/2}}{N(A)} = 0,125.$$

(c) $\delta(\sigma_{\mathbb{L}}(A)) > \delta(\sigma_\alpha(A))$.

Exemplo 6.4.5 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{3})$, $A = (3 - \sqrt{3})O_{\mathbb{L}}$ *um ideal de* $O_{\mathbb{L}} = \mathbb{Z}[\sqrt{3}]$, *e* $\alpha = 2+\sqrt{3} \in O_{\mathbb{L}}$. *Temos que* $n = [\mathbb{L}:\mathbb{Q}] = 2$, $\mathfrak{D}_{\mathbb{L}} = 12$, $N(A) = 6$ *e* $N(\alpha) = 1$. *Dado* $x \in A$, *temos que* $x = (3 - \sqrt{3})(a_0 + a_1\sqrt{3})$, *com* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 24a_0^2 + 72a_1^2 - 72a_0a_1$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}) = 12a_0^2 + 36a_1^2$. *Portanto* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 24$ *e* $t_\alpha = 12$, *e as densidades de centro são dadas por:*

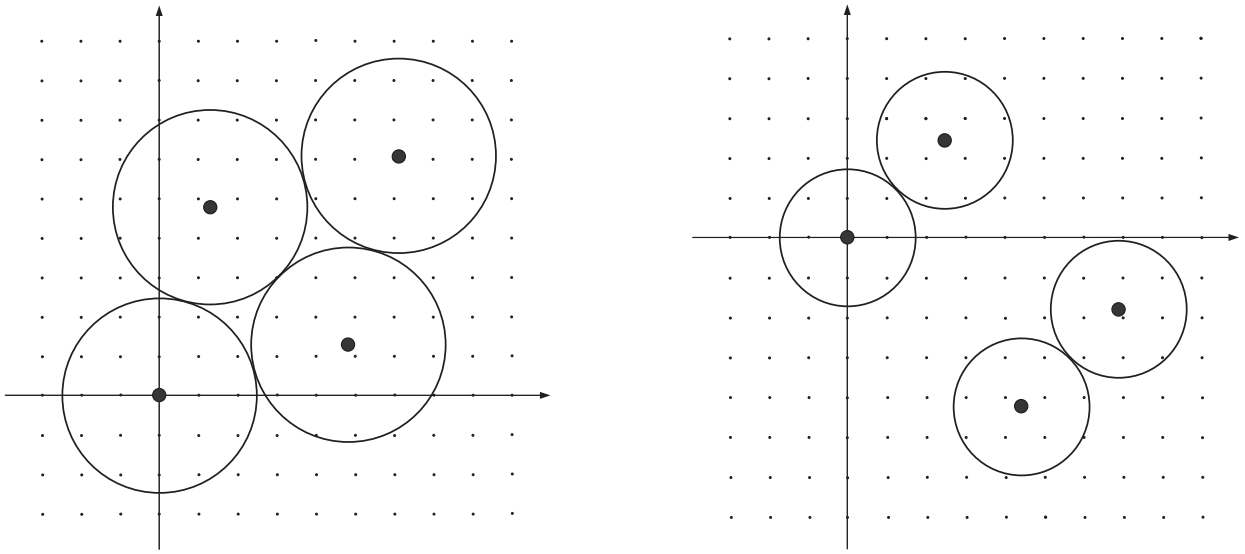
1. *sem perturbação*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,28868.$$

2. *com perturbação*

$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n (|\mathfrak{D}_{\mathbb{L}}| N(\alpha))^{1/2}} \frac{{t_\alpha}^{n/2}}{N(A)} = 0,14434.$$

Na figura abaixo, damos um esboço do arranjo das esferas do empacotamento dos reticulados $\sigma_{\mathbb{L}}(A)$ e $\sigma_\alpha(A)$, respectivamente:



Exemplo 6.4.6 *Sejam o corpo* $\mathbb{L} = \mathbb{Q}(\zeta_8)$, $A = (1+\zeta_8^3)O_{\mathbb{L}}$ *um ideal de* $O_{\mathbb{L}} = \mathbb{Z}[\zeta_8]$ *e* $\alpha = 2+\zeta_8$ *¡* ζ_8^3 *2* $O_{\mathbb{L}}$. *Temos que* $n = [\mathbb{L}:\mathbb{Q}] = 4$, $\mathfrak{D}_{\mathbb{L}} = §256$, $N(A) = 2$ *e* $N(\alpha) = 4$. *Dado* x *2* A, *temos que* $x = (1+\zeta_8^3)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$, *com* a_i *2* $\mathbb{Z}$, *para* $i = 0,1,2,3$. *Assim,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 8(a_0^2+a_1^2+a_2^2+a_3^2$ *¡* $a_0a_1+a_0a_3$ *¡* a_1a_2 *¡* $a_2a_3)$ *e* $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x\overline{x}) = 8(a_0^2+a_1^2+a_2^2+a_3^2)$. *Portanto* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x$ *2* A, x *6=* $0\} = 8$ *e* $t_\alpha = 8$, *e deste modo as densidades de centro são dadas por:*

1. *sem perturbação*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n|\mathfrak{D}_{\mathbb{L}}|^{1/2}}\,\frac{t^{n/2}}{N(A)} = 0,125.$$

2. *com perturbação*

$$\delta(\sigma_\alpha(A)) = \frac{1}{2^n(|\mathfrak{D}_{\mathbb{L}}|N(\alpha))^{1/2}}\frac{{t_\alpha}^{n/2}}{N(A)} = 0,0625.$$

Capítulo

7

Famílias de reticulados rotacionados em dimensões pares

7.1 Introdução

Na referência [15], Flores apresenta exemplos de reticulados algébricos, com densidade de centro ótimas, que são versões rotacionadas dos reticulados A_2, D_4 e E_6. Através do parâmetro densidade de centro estes eram os únicos exemplos conhecidos na literatura. Deste modo, neste capítulo apresentamos novos exemplos de reticulados algébricos com densidade de centro ótima, de dimensões 2,4, 6 e 8, que são versões rotacionadas dos reticulados A_2, D_4 e E_6, respectivamente. Na Seção 7.2, apresentamos famílias de reticulados algébricos, com densidade de centro ótima, que são versões rotacionadas do reticulado A_2, via os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$ e via os subcorpos maximais $\mathbb{Q}(\zeta_n+\zeta_n^{-1}$

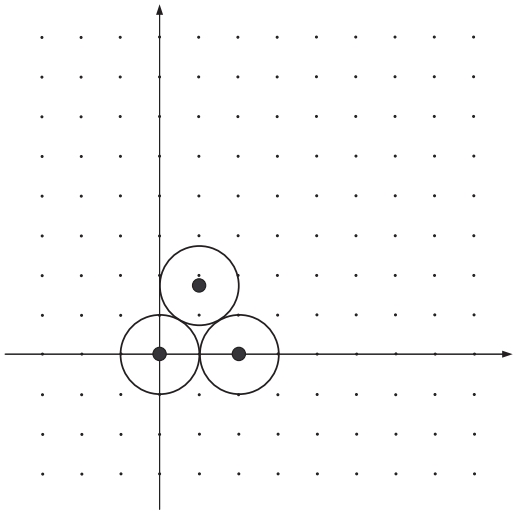
temos que $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 2$, *pois é suficiente tomar* $a_0 = 1$ *e* $a_1 = 0$, *e deste modo a densidade de centro é dada por:*

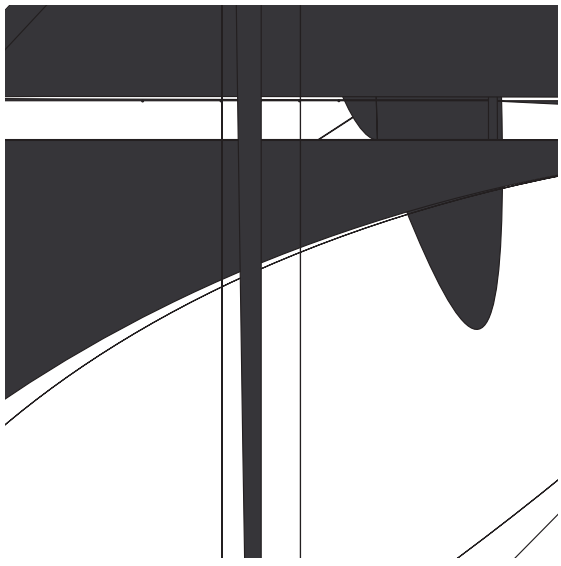
$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,28868.$$

Observação 7.2.1 *No Exemplo* 7.2.1, *o reticulado* $\sigma_{\mathbb{L}}(A)$ *possui a mesma densidade de centro do reticulado* $\Lambda_2 = A_2$, *assim como os reticulados gerados por outros ideais de* $\mathbb{Z}[\zeta_6]$, *conforme tabela abaixo.*

A	$N(A)$	t
$(1+\zeta_6)\mathcal{O}_{\mathbb{L}}$	3	6
$2\mathcal{O}_{\mathbb{L}}$	4	8
$(1+2\zeta_6)\mathcal{O}_{\mathbb{L}}$	7	14
$(3\zeta_6)\mathcal{O}_{\mathbb{L}}$	9	18
$(2 + 4\zeta_6)\mathcal{O}_{\mathbb{L}}$	12	24
$(4 + \zeta_6)\mathcal{O}_{\mathbb{L}}$	13	26
$(4\zeta_6)\mathcal{O}_{\mathbb{L}}$	16	32
$(3 + 5\zeta_6)\mathcal{O}_{\mathbb{L}}$	19	38
$(5 + \zeta_6)\mathcal{O}_{\mathbb{L}}$	21	42
$(5 + 5\zeta_6)\mathcal{O}_{\mathbb{L}}$	25	50
$6\mathcal{O}_{\mathbb{L}}$	36	72

Na figura abaixo, temos um esboço do arranjo das esferas do empacotamento dos reticulados $\sigma_{\mathbb{L}}(A)$, para $A = 2\mathcal{O}_{\mathbb{L}}$ e $A = (1+2\zeta_6)\mathcal{O}_{\mathbb{L}}$, respectivamente.





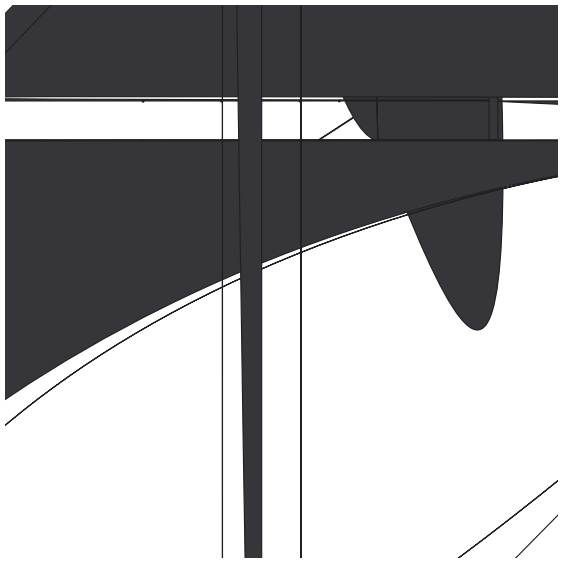
[2] Via o subcorpo maximal de $\mathbb{Q}(\zeta_n)$

Exemplo 7.2.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{12})$, $\mathbb{K} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1}) = \mathbb{Q}(\sqrt{3})$ *e* $A = ((\zeta_{12} + \zeta_{12}^{-1}) + 3(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$ *um ideal de* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{12} + \zeta_{12}^{-1}]$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathfrak{D}_{\mathbb{K}} = 12$ *e* $N(A) = 6$.

Dado $\alpha \in A$, *temos que* $\alpha = ((\zeta_{12} + \zeta_{12}^{-1}) + 3(\zeta_{12}^2 + \zeta_{12}^{-2}))(a_1(\zeta_{12} + \zeta_{12}^{-1}) + a_2(\zeta_{12}^2 + \zeta_{12}^{-2}))$, *com* $a_1, a_2 \in \mathbb{Z}$, *e assim pelo Teorema* 5.2.2 *segue que* $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = 72a_1^2 + 24a_2^2 + 72a_1a_2$. *Portanto, temos que* $t = min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) : \alpha \in A, \alpha \neq 0\} = 24$, *e a densidade de centro é dada por*

$$\delta(\sigma_{\mathbb{K}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,28868.$$

Na figura abaixo damos um esboço do arranjo das esferas do empacotamento do reticulado $\sigma_{\mathbb{K}}(A)$.



Observação 7.2.2 *No Exemplo* 7.2.2, *o reticulado* $\sigma_{\mathbb{K}}(A)$ *possui a mesma densidade de centro do reticulado* $\Lambda_2 = A_2$, *assim como os reticulados gerados por outros ideais de* $\mathbb{Z}[\zeta_{12} + \zeta_{12}^{-1}]$, *conforme tabela abaixo.*

A	$N(A)$	t
$(i\,19(\zeta_{12} + \zeta_{12}^{-1}) + 33(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	6	24
$(71(\zeta_{12} + \zeta_{12}^{-1}) + 123(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	6	24
$(10(\zeta_{12} + \zeta_{12}^{-1}) + 18(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	24	96
$(2(\zeta_{12} + \zeta_{12}^{-1})\ i\ 6(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	24	96
$(i\,38(\zeta_{12} + \zeta_{12}^{-1})\ i\ 66(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	24	96
$(4(\zeta_{12} + \zeta_{12}^{-1})\ i\ 12(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	96	384
$(i\,20(\zeta_{12} + \zeta_{12}^{-1}) + 36(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	96	384
$(8(\zeta_{12} + \zeta_{12}^{-1})\ i\ 24(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	384	1536
$(i\,40(\zeta_{12} + \zeta_{12}^{-1})\ i\ 72(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	384	1536
$(i\,16(\zeta_{12} + \zeta_{12}^{-1}) + 48(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	1536	6144
$(80(\zeta_{12} + \zeta_{12}^{-1}) + 144(\zeta_{12}^2 + \zeta_{12}^{-2}))\mathcal{O}_{\mathbb{K}}$	1536	6144

Observação 7.2.3 *Na verdade, existe uma infinidade de reticulados algébricos rotacionados de dimensão* 2, *o resultado a seguir garante este fato.*

Teorema 7.2.1 *Se* $\mathbb{L} = \mathbb{Q}(\zeta_3)$ *e* A *é um ideal principal não nulo de* $O_{\mathbb{L}}$*, então o reticulado* $\sigma_{\mathbb{L}}(A)$ *possui a mesma densidade de centro do reticulado* $\Lambda_2 = A_2$*.*

Demonstração: Se A é um ideal principal não nulo de $O_{\mathbb{L}}$, então $A = (a + b\zeta_3)O_{\mathbb{L}}$, onde $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. Assim,

$$N(A) = N(|a + b\zeta_3 i|) = |N(a + b\zeta_3)| = |a^2 + b^2 - ab| = a^2 + b^2 - ab.$$

pois $a^2 + b^2 - ab > 0$. Dado $x \in A$, temos que

$$x = (a + b\zeta_3)(a_0 + a_1\zeta_3) = (aa_0 - ba_1) + (aa_1 + ba_0 - ba_1)\zeta_3,$$

onde $a_0, a_1 \in \mathbb{Z}$. Pelo Teorema 5.2.1, segue que

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) &= 2[(aa_0 - ba_1)^2 + (aa_1 + ba_0 - ba_1)^2 - (aa_0 - ba_1)(aa_1 + ba_0 - ba_1)] = \\ &= 2a^2a_0^2 - 2a^2a_0a_1 + 2a^2a_1^2 - 2aba_0^2 + 2aba_0a_1 - 2aba_1^2 + 2b^2a_0^2 - 2b^2a_0a_1 + 2b^2a_1^2 \\ &= 2(a^2 + b^2 - ab)(a_0^2 + a_1^2 - a_0a_1). \end{aligned}$$

Temos que $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 2(a^2 + b^2 - ab)$, e assim é suficiente tomar $a_0 = 1$ e $a_1 = 0$. Portanto,

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n\sqrt{|\mathfrak{D}_{\mathbb{L}}|}} \frac{t^{n/2}}{N(A)} = \frac{1}{4}\frac{\sqrt{3}}{3} \frac{2(a^2 + b^2 - ab)}{(a^2 + b^2 - ab)} = 0,28868,$$

e segue o resultado. ∎

7.3 Rotacionados de D_4

Nesta seção, apresentamos uma família de reticulados rotacionados em dimensão 4.

Exemplo 7.3.1 *Sejam o corpo* $\mathbb{L} = \mathbb{Q}(\zeta_8)$ *e* $A = (1 + \zeta_8^3)O_{\mathbb{L}}$ *um ideal de* $O_{\mathbb{L}} = \mathbb{Z}[\zeta_8]$*. Temos que* $n = [\mathbb{L} : \mathbb{Q}] = 4$*,* $\mathfrak{D}_{\mathbb{L}} = \S 256$ *e* $N(A) = 2$*. Dado* $x \in A$*, temos que* $x = (1 + \zeta_8^3)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$*, com* $a_0, a_1, a_2, a_3 \in \mathbb{Z}$*, e assim pelo Teorema* 5.2.1 *segue que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 8(a_0^2 + a_1^2 + a_2^2 + a_3^2 - a_0a_1 - a_1a_2 + a_0a_3 - a_2a_3)$*. Portanto, temos que* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in A, x \neq 0\} = 8$*, pois é suficiente tomar* $a_0 = a_1 = 1$ *e* $a_2 = a_3 = 0$*, e deste modo a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n|\mathfrak{D}_{\mathbb{L}}|^{1/2}} \frac{t^{n/2}}{N(A)} = 0,125.$$

Observação 7.3.1 *No Exemplo* 7.3.1*, o reticulado* $\sigma_{\mathbb{L}}(A)$ *possui a mesma densidade de centro do reticulado* $\Lambda_4 = D_4$*, assim como os reticulados gerados por outros ideais de* $\mathbb{Z}[\zeta_8]$*, conforme tabela abaixo.*

A	$N(A)$	t
$(1+\zeta_8+\zeta_8^2+\zeta_8^3)O_{\mathbb{L}}$	8	16
$(1\ i\ \zeta_8+2\zeta_8^3)O_{\mathbb{L}}$	18	24
$(2\zeta_8+2\zeta_8^2)O_{\mathbb{L}}$	32	32
$(2+2\zeta_8+\zeta_8^2+\zeta_8^3)O_{\mathbb{L}}$	50	40
$(\ i\ 3+5\zeta_8\ i\ 5\zeta_8^2+\zeta_8^3)O_{\mathbb{L}}$	72	48
$(2+6\zeta_8+6\zeta_8^2+2\zeta_8^3)O_{\mathbb{L}}$	128	64
$(1+3\zeta_8\ i\ 2\zeta_8^2+2\zeta_8^3)O_{\mathbb{L}}$	162	72
$(3+\zeta_8+\zeta_8^2\ i\ 3\zeta_8^3)O_{\mathbb{L}}$	200	80
$(1+4\zeta_8+2\zeta_8^2\ i\ \zeta_8^3)O_{\mathbb{L}}$	242	88
$(4\zeta_8+2\zeta_8^2+2\zeta_8^3)O_{\mathbb{L}}$	288	96
$(2+3\zeta_8\ i\ 3\zeta_8^2+2\zeta_8^3)O_{\mathbb{L}}$	338	104

7.4 Rotacionados de E_6

Nesta seção, apresentamos uma família de reticulados rotacionados em dimensão 6.

Exemplo 7.4.1 *Sejam o corpo* $\mathbb{L}=\mathbb{Q}(\zeta_9)$ *e* $A=(1+\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4+\zeta_9^5)O_{\mathbb{L}}$ *um ideal de* $O_{\mathbb{L}}=\mathbb{Z}[\zeta_9]$. *Temos que* $n=[\mathbb{L}:\mathbb{Q}]=6$, $\mathfrak{D}_{\mathbb{L}}=\S 3^9$ *e* $N(A)=9$. *Dado* $x\ 2\ A$, *temos que* $x=(1+\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4+\zeta_9^5)(a_0+a_1\zeta_9+a_2\zeta_9^2+a_3\zeta_9^3+a_4\zeta_9^4+a_5\zeta_9^5)$, *com* $a_i\ \ 2\ \ \mathbb{Z}$, *para* $i=0,1,2,3,4,5$, *e assim pelo Teorema* 5.2.1 *segue que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})=18(\sum_{i=0}^{5}a_i^2+a_0a_1+a_1a_2\ i\ a_0a_3+a_2a_3\ i\ a_0a_4\ i\ a_1a_4+a_3a_4\ i\ a_0a_5\ i\ a_1a_5\ i\ a_2a_5+a_4a_5)$. *Portanto, temos que* $t=minfTr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}):x\ 2\ A,x\ 6=0g=18$, *pois é suficiente tomar* $a_0=1$ *e* $a_1=a_2=a_3=a_4=a_5=0$, *e deste modo a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(A))=\frac{1}{2^n j\mathfrak{D}_{\mathbb{L}}j^{1/2}}\ \frac{t^{n/2}}{N(A)}=0,07217.$$

Observação 7.4.1 *No Exemplo* 7.4.1, *o reticulado* $\sigma_{\mathbb{L}}(A)$ *possui a mesma densidade de centro do reticulado* $\Lambda_6=E_6$, *assim como os reticulados gerados por outros ideais de* $\mathbb{Z}[\zeta_9]$, *conforme tabela abaixo.*

A	$N(A)$	t
$(2 \ i \ \zeta_9^4 \ i \ \zeta_9^5)O_{\mathbb{L}}$	9	18
$(1 \ i \ 2\zeta_9^2 + \zeta_9^3 + 2\zeta_9^4 \ i \ 2\zeta_9^5)O_{\mathbb{L}}$	9	18
$(1 + 2\zeta_9 + 2\zeta_9^4 + \zeta_9^5)O_{\mathbb{L}}$	9	18
$(1 + \zeta_9 + \zeta_9^2 \ i \ \zeta_9^3 \ i \ \zeta_9^4 \ i \ \zeta_9^5)O_{\mathbb{L}}$	243	54
$(\ i \ 2 + \zeta_9 + \zeta_9^2 \ i \ \zeta_9^3 \ i \ \zeta_9^4 + 2\zeta_9^5)O_{\mathbb{L}}$	243	54
$(2 + 2\zeta_9 + 2\zeta_9^2 + \zeta_9^3 \ i \ 2\zeta_9^4 \ i \ 2\zeta_9^5)O_{\mathbb{L}}$	243	54
$(2 + 2\zeta_9 + 2\zeta_9^2)O_{\mathbb{L}}$	576	72
$(\ i \ 2\zeta_9 \ i \ 2\zeta_9^3 \ i \ 2\zeta_9^5)O_{\mathbb{L}}$	576	72
$(\ i \ 2\zeta_9 + 2\zeta_9^2 + 2\zeta_9^3 \ i \ 2\zeta_9^4)O_{\mathbb{L}}$	576	72
$(1 + \zeta_9 + \zeta_9^2 \ i \ 2\zeta_9^3 \ i \ 2\zeta_9^4 \ i \ 2\zeta_9^5)O_{\mathbb{L}}$	3087	126
$(2 + 2\zeta_9 + 2\zeta_9^2 \ i \ \zeta_9^3 \ i \ \zeta_9^4 \ i \ \zeta_9^5)O_{\mathbb{L}}$	3087	126

7.5 Rotacionados de E_8

Nesta seção, apresentamos uma família de reticulados rotacionados em dimensão 8.

Exemplo 7.5.1 *Sejam o corpo* $\mathbb{L} = \mathbb{Q}(\zeta_{20})$ *e* $A = (\ i \ 1 \ i \ \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)O_{\mathbb{L}}$ *um ideal de* $O_{\mathbb{L}} = \mathbb{Z}[\zeta_{20}]$. *Temos que* $n = [\mathbb{L} : \mathbb{Q}] = 8$, $\mathfrak{D}_{\mathbb{L}} = \S 2^8 5^6$ *e* $N(A) = 80$. *Dado* $x \ 2 \ A$, *temos que* $x = (\ i \ 1 \ i \ \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)(a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7)$, *com* $a_i \ 2 \ \mathbb{Z}$, *para* $i = 0, 1, ¢¢¢, 7$, *e assim pelo Teorema* 5.2.1 *segue que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 40(\sum_{i=0}^{7} a_i^2 + a_0a_1 + a_1a_2 \ i \ a_0a_3 + a_2a_3 \ i \ a_0a_4 \ i \ a_1a_4 + a_3a_4 \ i \ a_1a_5 \ i \ a_2a_5 + a_4a_5 + a_0a_6 \ i \ a_2a_6 \ i \ a_3a_6 + a_5a_6 + a_0a_7 + a_1a_7 \ i \ a_3a_7 \ i \ a_4a_7 + a_6a_7)$. *Portanto, temos que* $t = min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \ 2 \ A, x \ 6= 0\} = 40$, *pois é suficiente tomar* $a_0 = a_1 = a_4 = \ i \ 1$, $a_2 = a_6 = 1$ *e* $a_3 = a_5 = a_7 = 0$, *e deste modo a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{1}{2^n |\mathfrak{D}_{\mathbb{L}}|^{1/2}} \ \frac{t^{n/2}}{N(A)}$$

428v80625TD[())]TD8F18=290TD[(2)-2:D[(8)]T.

A	$N(A)$	t
$(\zeta_{20}\ i\ \zeta_{20}^2\ i\ \zeta_{20}^3+\zeta_{20}^4\ i\ \zeta_{20}^5)\mathcal{O}_{\mathbb{L}}$	80	40
$(\ i\ 1\ i\ \zeta_{20}+\zeta_{20}^2\ i\ \zeta_{20}^5+\zeta_{20}^6\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	80	40
$(\zeta_{20}^3+\zeta_{20}^4\ i\ \zeta_{20}^5\ i\ \zeta_{20}^6\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	80	40
$(\ i\ 1+\zeta_{20}^2\ i\ \zeta_{20}^3\ i\ \zeta_{20}^4\ i\ \zeta_{20}^6)\mathcal{O}_{\mathbb{L}}$	80	40
$(\ i\ \zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4\ i\ \zeta_{20}^5+\zeta_{20}^6)\mathcal{O}_{\mathbb{L}}$	80	40
$(\ i\ 1\ i\ \zeta_{20}\ i\ \zeta_{20}^2\ i\ \zeta_{20}^3+\zeta_{20}^4+\zeta_{20}^5\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60
$(1\ i\ \zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4\ i\ \zeta_{20}^5+\zeta_{20}^6\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60
$(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^4\ i\ \zeta_{20}^5\ i\ \zeta_{20}^6\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60
$(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^3\ i\ \zeta_{20}^4\ i\ \zeta_{20}^5+\zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60
$(1+\zeta_{20}+\zeta_{20}^3+\zeta_{20}^4+\zeta_{20}^5+\zeta_{20}^6\ i\ \zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60
$(1\ i\ \zeta_{20}+\zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^5\ i\ \zeta_{20}^6+\zeta_{20}^7)\mathcal{O}_{\mathbb{L}}$	405	60

Observação 7.5.2 *Neste capítulo, apresentamos exemplos de reticulados algébricos rotacionados de dimensão* 2, 4, 6 *e* 8. *Para as dimensões* 3, 5 *e* 7, *não conseguimos obter reticulados algébricos com densidade de centro ótima.*

Referências Bibliográficas

[1] SAMUEL, P. **Algebraic theory of numbers**, Paris: Hermann, 1970.

[2] STEWART, I. N.; TALL, D. O. **Algebraic number theory**. London: Chapman and Hall, 1987.

[3] MONTEIRO, L. H. J. Teoria de Galois. In: Colóquio Brasileiro de Matemática, 7, 1969. Poços de Caldas. Atas ... Rio de Janeiro: Impa, 1969.

[4] FLORES, A. L. **Representação geométrica de ideais de corpos de números**. 1996, 86f. Dissertação (Mestrado em Matemática), Instituto de Matemática, Estatística e de Computação Científica, Universidade Estadual de Campinas, Campinas, 1996.

[5] MELO, F. D. **Uma forma quadrática no corpo de condutor primo**. 2005, 59f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[6] OLIVEIRA, C. M. **Discriminante, ramificação e diferente**. 2005, 131f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[7] WASHINGTON, L. **Introduction to cyclotomic fields**. New York: Springer-Verlag, 1982.

[8] LANG, S. **Algebra**. New York: Addison-Wesley, 1972.

[9] NOBREGA, T. P. Cúbicas reais, algumas aplicações, In: Encontro de Álgebra, 6, 1997. Campinas. Anais ... Campinas: Unicamp, 1997.

[10] MARCUS, D. A. **Number fields**. New-York: Springer-Verlag, 1977.

[11] BOUTROS, J.; VITERBO, E. Signal space diversity: a power and bandwidth-efficient diversity technique for the Rayleigh fading channel. **IEEE Transactions on Information Theory**, New-York, v. 44, n. 4, p. 1453-1467, 1998.

[12] CONWAY, J. H.; SLOANE, N. J. A. **Sphere packing, lattices and groups**. New-York: Springer-Verlag, 1999.

[13] RODRIGUES, T. M. **Cúbicas galoisianas**. 2003, 68f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2003.

[14] VICENTE, J. P. G. **Reticulados de posto 3 em corpos de números**. 2000, 91f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2000.

[15] FLORES, A. L. **Reticulados em corpos abelianos**. 2000, 115f. Tese (Doutorado em Engenharia Elétrica), Faculdade de Engenharia Elétrica e da Computação, Universidade Estadual de Campinas, Campinas, 2000.

[16] FERRARI, A. J.; ANDRADE, A. A. Rotated algebraic lattices in dimensions 2, 4 and 6. In: Congresso Nacional de Matemática Aplicada e Computacional, 30, 2007. Florianópolis. Atas ... Florianópolis: SBMAC, 2007.

[17] ANDRADE, A. A.; FERRARI, A. J.; ALVES, C.; CARLOS, T.B. Lattices via cyclotomic fields in dimensions 2 and 4. **International Journal of Applied Mathematics**, Sofia, v. 20, p. 1095-1105, 2007.

[18] FERRARI, A. J.; ANDRADE, A. A. Families of rotated lattices in even dimensions up to 8. **International Journal of Applied Mathematics**, 2008. No prelo.

[19] BOUTROS, J.; VITERBO, E.; RATELLO, C.; BELFIORE, J. C. Good lattice constellations for both Rayleigh fading and Gaussian channels. **IEEE Transactions Information Theory**, New-York, v. 42, No. 2, p. 502-517, 1996.

[20] ALVES, C. **Reticulados via corpos ciclotômicos**. 2005, 125f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[21] BAYER-FLUCKIGER, E. Lattices and number fields. **Contemporary Mathematics**, Providence, v. 241, p. 69-84, 1999.

[22] BAYER-FLUCKIGER, E. Ideal lattices. In: Conference in honor of Alan Baker, 2002, Cambridge. Proceedings ... Cambridge: Cambridge University Press, 2002, p. 168-184.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo