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

Plínio Gabriel Sicuti

Um estudo sobre reticulados algébricos bem arredondados

São José do Rio Preto
2020

Plínio Gabriel Sicuti

Um estudo sobre reticulados algébricos bem arredondados

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Orientadora: Prof[a]. Dr[a]. Carina Alves Severo

São José do Rio Preto

2020

S567e

Sicuti, Plínio Gabriel
Um estudo sobre reticulados algébricos bem arredondados / Plínio Gabriel Sicuti. -- São José do Rio Preto, 2020
125 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientadora: Carina Alves Severo

1. Corpos quadráticos. 2. Anel de inteiros. 3. Reticulados algébricos. 4. Reticulados bem arredondados. 5. Homomorfismo torcido. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Plínio Gabriel Sicuti

Um estudo sobre reticulados algébricos bem arredondados

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Profª. Drª. Carina Alves Severo
Professora Livre-Docente
UNESP - Rio Claro - SP
Orientadora

Prof. Dr. Antônio Aparecido de Andrade
Professor Livre-Docente
UNESP - São José do Rio Preto - SP

Prof. Dr. Agnaldo José Ferrari
Professor Doutor
UNESP - Bauru - SP

São José do Rio Preto

27 de fevereiro de 2020

Dedico à meus pais

Alcides e Ivani.

Agradecimentos

Ao concluir este trabalho, agradeço:

Aos meus pais Alcides Sidinei Sicuti e Ivani Ferreira Sicuti, pelo amor incondicional, por minha educação e todos os valores a mim ensinados. Obrigado por incentivarem meus estudos e saibam que dar-lhes orgulho é, e sempre será, minha maior motivação para viver;

À minha namorada Cecília Artico Banho, por todo amor e carinho ao longo dos últimos anos. Por me ouvir e amparar nos momentos difíceis e por sempre me incentivar;

À minha tia Sueli Andrelina da Silva, por todo carinho e apoio ao longo da minha jornada acadêmica;

Aos meus incríveis amigos, Maurício Rodrigues, por todos os incontáveis momentos que passamos juntos ao longo dos últimos anos e por todas as alegrias que compartilhamos; Raul Appis, por sempre me animar e mostrar o melhor lado da vida; Rodrigo Bononi, por acreditar em meu potencial, pelas viagens e pelos eventos que compartilhamos; Wesley Oliveira, por todos seus conselhos e por se fazer presente mesmo distante; e Mariele Souza, por todo o carinho ao longo de anos de amizade;

Aos amigos da Pós-Graduação, em especial, Eliton Moro, por compartilhar da mesma linha de pesquisa, pelas inúmeras discussões produtivas e por todo o carinho que sempre demonstrou comigo; André Antunes, por ser absolutamente atencioso e por seus inúmeros conselhos; Carol Signorini, por se fazer tão presente e solucionar todas as minhas dúvidas com o Latex; E também à Ana Lívia Rodero, Jarne Ribeiro, Jéssica Ventura, Karina Rampazzi, Livea Esteves, Lucas Queiroz, Otávio

Perez, Rodrigo Ishizaka, Yagor Carvalho e a todos os demais colegas com quem compartilhei ótimos momentos;

Aos amigos que fiz ao longo da graduação, especialmente, Isabela Mendes, minha companheira de estudos, Carlos Vicente, Daniel Ferreira, João Vinícius Aquino, Leonardo Serantola, Amanda de Souza e Vinicius Vitório;

Aos docentes do departamento de matemática do IBILCE, por todos os ensinamentos, incentivos e pela amizade. Em especial às professoras Luci Any Roberto, pela orientação ao longo da graduação, e Andréa Prokopczyk Arita, pelos inúmeros conselhos. Também aos professores Parham Salehyan, por incentivar meu amor pela álgebra, e Paulo Ricardo da Silva, por toda ajuda ao longo da pós-graduação.

À Profa. Dra. Maria Gorete Carreira, por todos os ensinamentos, conselhos e pela amizade o longo dos anos de PET.

À minha orientadora, Profa. Dra. Carina Alves Severo, por todo amparo e disponibilidade, por toda confiança que depositou em mim para o desenvolvimento deste trabalho e pela amizade.

Aos membros da comissão examinadora, Prof. Dr. Antônio A. de Andrade e Prof. Dr. Agnaldo J. Ferrari, por aceitarem o convite de compor a comissão examinadora e pelas valorosas contribuições ao trabalho. Também ao professor Antônio pela orientação ao longo da graduação e por me apresentar esta linha de pesquisa que tanto significa para mim.

Finalmente, à Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto, IBILCE, que me permitiu a realização deste sonho. E a todos que durante esses anos cruzaram meu caminho e acrescentaram conhecimentos e experiências.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, à qual agradeço.

"Sometimes it is the very people who no one imagines anything of who do the things that no one can imagine".

The Imitation Game (2014)

Resumo

Um reticulado de posto completo em um espaço euclidiano é bem arredondado se o conjunto formado por seus vetores de norma mínima constitui uma base para este espaço. Recentemente, um estudo provou que a imagem do anel de inteiros de corpos quadráticos pelo homomorfismo canônico é um reticulado bem arredondado apenas para dois corpos quadráticos imaginários. Neste trabalho, provamos que existem corpos quadráticos reais cuja imagem de seus respectivos anéis de inteiros, por meio de perturbações no homomorfismo canônico, também produzem reticulados bem arredondados. Em particular, apresentamos uma família infinita de elementos nesses corpos que definem perturbações no homomorfismo canônico, as quais produzem reticulados bem arredondados, além de outros exemplos por meio dessas perturbações. Também investigamos as relações entre reticulados bem arredondados e reticulados algébricos obtidos através do anel de inteiros de corpos ciclotômicos. Além disso, caracterizamos quais elementos, em uma família de ideais no anel de inteiros desses corpos, atingem a norma mínima do reticulado correspondente.

Palavras-chave: corpos quadráticos, anel de inteiros, reticulados algébricos, reticulados bem arredondados, homomorfismo torcido.

Abstract

A lattice of full rank in a Euclidean space is well-rounded if its set of minimal vectors spans the whole space. Recently, a study showed that the image of the ring of integers of quadratic fields by canonical homomorphism is a well-rounded lattice only for two imaginary quadratic fields. In this work, we proved that there are real quadratic fields, whose image of their respective rings of integers, by twisted homomorphism also yield well-rounded lattices. In particular, we presented an infinite family of elements in these fields, which define twisted homomorphism that yield well-rounded lattices, besides, we presented other examples through these twists. We also investigated the relationships between well-rounded lattices and algebraic lattices obtained by the ring of integers of cyclotomic fields. Moreover, we characterized which elements, in a family of ideals in the ring of integers of these fields, reach the minimum norm of the corresponding lattice.

Keywords: *quadratic number fields, ring of integers, algebraic lattices, well-rounded lattices, twisted homomorfism.*

Lista de Figuras

Lista de Símbolos

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{C}$	Conjunto dos números complexos
Σ	Somatório
Π	Produtório
$\#A$	Cardinalidade do conjunto A
$\overline{x}$	Conjugado complexo de x
$M = (a_{ij})$	Matriz de entradas a_{ij}
$det(A)$	Determinante da matriz A
I_n	Matriz identidade de ordem n
$a \mid b$	a divide b
$a \equiv b \ (mod\ m)$	a congruente a b módulo m
$\varphi(n)$	Função de Euler aplicada à n
$m_\alpha(x)$	Polinômio minimal de α
$\partial(f(x))$	Grau do polinômio $f(x)$
$\Re(z)$	Parte real do número complexo z
$\Im(z)$	Parte imaginária do número complexo z
$A[x]$	Anel de polinômios com coeficientes em A
$\mathbb{K}[x]$	Anel de polinômios com coeficientes em $\mathbb{K}$
$\mathcal{I}, \mathcal{J}, \mathcal{Q}$	Ideais
$A/\mathcal{I}$	Anel quociente

$\mathbb{K}$, $\mathbb{L}$, $\mathbb{M}$	Corpos
$\mathbb{L}\|\mathbb{K}$	O corpo $\mathbb{L}$ é uma extensão do corpo $\mathbb{K}$
$[\mathbb{L} : \mathbb{K}]$	Grau da extensão $\mathbb{L}\|\mathbb{K}$
$Gal(\mathbb{L}\|\mathbb{K})$	O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$\mathcal{T}r_{\mathbb{L}\|\mathbb{K}}(\alpha)$	O traço de α em relação à $\mathbb{L}\|\mathbb{K}$
$\mathcal{N}_{\mathbb{L}\|\mathbb{K}}(\alpha)$	A norma de α em relação à $\mathbb{L}\|\mathbb{K}$
$\mathcal{N}(\mathcal{I})$	A norma do ideal $\mathcal{I}$
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$\mathcal{D}(\alpha_1, \ldots, \alpha_n)$	Discriminante de $(\alpha_1, \ldots, \alpha_n)$
$\mathcal{D}_{\mathbb{K}}$	Discriminante do corpo $\mathbb{K}$
ζ_n	Raiz n-ésima primitiva da unidade
$\mathbb{Q}(\zeta_n)$	n-ésimo corpo ciclotômico
Λ, Λ_1, Λ_2	Reticulados
Λ'	Sub-reticulado
$\mathcal{V}ol(\Lambda)$	Volume do reticulado Λ
$\Delta(\Lambda)$	Densidade de empacotamento do reticulado Λ
$\delta(\Lambda)$	Densidade de centro de Λ
$\|\Lambda\|$	Norma do reticulado Λ
$\mathcal{P}$	Região Fundamental do Reticulado
$\sigma_{\mathbb{K}}$	Homomorfismo canônico
σ_{α}	Homomorfismo torcido

Sumário

Introdução

Reticulados são estruturas algébricas, mais precisamente $\mathbb{Z}$-módulos livres de posto completo em $\mathbb{R}^n$, que desempenham um papel importante em diversas áreas da matemática, com extensas conexões com a Teoria Algébrica dos Números, a Teoria de Codificação, a Criptografia, entre outras áreas. O estudo de reticulados está diretamente relacionado a um dos seletos problemas destacados na famosa lista de 23 problemas, que foi apresentada pelo matemático alemão David Hilbert no Congresso Internacional de Matemáticos de 1900. Isso devido ao fato de que o $18^{\underline{o}}$ Problema de Hilbert está amplamente conectado com o Problema de Empacotamento Esférico, o qual consiste em preencher o espaço n-dimensional $\mathbb{R}^n$ com esferas idênticas de mesmo raio, de modo que duas quaisquer esferas não se tangenciem ou se tangenciem em no máximo um ponto e que essas cubram o maior espaço possível. Ao longo do Século XX muitos modelos e métodos foram propostos para resolver o problema citado.

Pode-se dizer, também, que um estímulo marcante para o estudo dos reticulados surgiu em 1948 no trabalho do matemático Claude E. Shannon apresentado em [31], onde o mesmo descreveu uma venerável relação entre códigos e reticulados. Até este momento, o principal interesse dos algebristas na Teoria dos Números se dava na procura da solução do Último Teorema de Fermat. Contudo, um dos modelos sugeridos para a solução do problema de empacotamento, originalmente sugerido pelo matemático Hermann Minkowski, consistia em fornecer uma representação geométrica de ideais nos anéis de inteiros de corpos de números. Essa representação estava relacionada a um reticulado e como sabemos hodiernamente para algumas dimensões, as melhores densidades de empacotamento, ou seja, as melhores disposições de esferas para que se obtenha o maior espaço coberto estão relacionadas com reticulados. Em outras palavras, em algumas dessas dimensões observa-se que o melhor empacotamento se dá para esferas cujo conjunto formado por seus centros forma um reticulado. Por meio do chamado homomorfismo de Minkowski é possível construir reticulados n-dimensionais utilizando ideais e $\mathbb{Z}$-módulos do anel de inteiros de um corpo de números algébricos, os quais são profundamente

estudados na Teoria dos Números.

A utilidade de um determinado reticulado para uma certa aplicação é descrita, muitas vezes, utilizando alguns invariantes relevantes do reticulado, como o raio de empacotamento, densidade de centro, distância produto mínima, dentre outros. Esse fato e várias propriedades que descrevemos têm relação com a Teoria Algébrica dos Números, que se originou com o matemático alemão Carl F. Gauss e teve sequência nos trabalhos dos matemáticos E. Kummer, R. Dedekind e L. Kronecker.

O principal objetivo deste trabalho, todavia, é estudar uma classe específica de reticulados algébricos, os reticulados bem arredondados, do inglês *well-rounded*. Um reticulado algébrico n-dimensional é bem arredondado se o conjunto formado por seus vetores de norma mínima constitui uma base para $\mathbb{R}^n$ como espaço vetorial.

Reticulados bem-arredondados surgem em uma ampla variedade de diferentes contextos, incluindo problemas de empacotamento, problema do número de contato, do inglês *kissing number*, descrito em [10], problemas de otimização discreta, aplicações em teoria de códigos, especialmente para canais MIMO e SISO sem fio como estudado em [19] e [20], conjectura de Minkowski, descrita em [22] e [23], entre outros. Ainda, a condição do reticulado ser bem arredondado é especial o suficiente para que se esperasse que os reticulados bem arredondados fossem relativamente escassos. Contudo, em 2005, C. McMullen, em [23], mostrou que, em certo sentido os reticulados unimodulares bem arredondados estão "bem distribuídos" entre todos os reticulados unimodulares no $\mathbb{R}^n$, lembrando que um reticulado unimodular é um reticulado com determinante igual a 1.

Diante do exposto, este trabalho está delineado como segue. No Capítulo 1 introduzimos aspectos dessa teoria que são pré-requisitos para o desenvolvimento da Teoria de Reticulados, nos permitindo inferir diversas propriedades aos reticulados construídos pelo método que descrevemos anteriormente e que são descritos em [11], [29], [30], [33], [32] e [37].

Dando continuidade ao trabalho, no Capítulo 2, estudamos detalhadamente dois tipos de corpos, os quadráticos e os ciclotômicos. Descrevemos suas principais características como seus respectivos anéis de inteiros, discriminantes e outros aspectos desenvolvidos no capítulo anterior.

No Capítulo 3 iniciamos o desenvolvimento da Teoria de Reticulados e apresentamos o Problema de Empacotamento Esférico, que citamos anteriormente, assim como alguns reticulados conhecidos da literatura. Muitos trabalhos apresentam diversas construções de reticulados em determinadas dimensões, como por exemplo [12], [14] e [36]. Dedicamos uma atenção especial ao estudo do homomorfismo que proporciona a construção de reticulados,

chamados de reticulados algébricos. Atualmente, existem alguns algoritmos para sistemas criptográficos e códigos corretores de erros baseados em reticulados. A relação entre a densidade de um empacotamento esférico e a eficiência de um código corretor de erros têm expandido o interesse neste estudo e novas técnicas para construção de reticulados têm sido obtidas, uma delas é também nosso objeto de estudo. Essa se refere a uma perturbação no homomorfismo de Minkowski, ou homomorfismo canônico, e também é alvo de estudo de trabalhos como [1], [2], [12] e [26].

Recentemente, têm surgido alguns trabalhos relacionando os reticulados bem arredondados aos reticulados algébricos, como [17] e [18], e este é o foco dos próximos capítulos.

No Capítulo 4, apresentamos resultados de [4], [15] e [18]. Salientamos que as demonstrações de alguns resultados foram adaptadas ou detalhadas da referência original. Nesse capítulo descrevemos com minudência uma série de propriedades geométricas desses reticulados para o caso em que $n = 2$ e que são encontradas em [15]. Ainda no caso bidimensional, caracterizamos os reticulados bem arredondados provenientes do anel de inteiros de corpos quadráticos por meio do homomorfismo canônico e exibimos uma família de ideais nesses anéis para os quais os reticulados correspondentes são bem arredondados, resultados encontrados em [18]. Também provamos que função densidade de empacotamento atinge seu máximo, dentre todos os reticulados em $\mathbb{R}^2$, no reticulado hexagonal. Ademais, utilizando a caracterização de reticulados bem arredondados para dimensões $n > 2$, através do resultado que garante que a imagem do anel de inteiros de um corpo de números $\mathbb{K}$ totalmente real ou totalmente imaginário é um reticulado bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico, destacamos quais elementos de reticulados p-dimensionais obtidos através de uma família de ideais nos anéis de inteiros de corpos ciclotômicos atingem a norma Euclidiana mínima.

No Capítulo 5 apresentamos, de forma detalhada, condições necessárias para que o anel de inteiros quadráticos possua um ideal cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado e que estão presentes em [17]. Esse estudo justifica que uma proporção significativa de corpos quadráticos reais e imaginários contém ideais que dão origem a reticulados bem arredondados. Finalizamos o presente trabalho apresentando os principais resultados de nossa autoria, em que estudamos reticulados provenientes de corpos quadráticos reais por uma perturbação no homomorfismo canônico. Provamos que existem corpos quadráticos reais cuja imagem do anel de inteiros, pela perturbação do homomorfismo canônico, é um reticulado bem arredondado. Em particular, apresentamos uma família infinita de elementos em um corpo quadrático real específico, cuja imagem pela perturbação do homomorfismo canônico por elementos dessa família é um reticulado bem arredondado, mais precisamente, o reticulado

hexagonal. Além de outros exemplos de reticulados via esse homomorfismo.

Salientamos que embora essa seja uma teoria altamente aplicável, este trabalho tem uma perspectiva teórica e que todos os resultados que não são de nossa autoria estão referenciados, ainda que alguns sejam amplamente conhecidos da literatura.

Capítulo

1

Teoria algébrica dos números

Neste capítulo apresentamos alguns pré-requisitos para o desenvolvimento dos demais. Omitimos as demonstrações de alguns resultados por serem, em sua maioria, amplamente conhecidos da Teoria Algébrica dos Números e da Teoria de Galois e existirem vários trabalhos sobre o assunto, como [4], [13] e [36]. Para um tratamento mais detalhado, o leitor interessado pode consultar às referências [11], [29], [30], [32] e [34].

Iniciamos a Seção 1.1 exibindo algumas definições elementares como as de corpos de números e elementos algébricos, bem como algumas caracterizações. Nas seguintes seções abordamos conceitos elementares da Teoria Algébrica dos Números como elementos inteiros algébricos, anel de inteiros, norma e traço, discriminante, norma de um ideal no anel de inteiros e as principais propriedades relacionadas a esses conceitos.

Embora apresentemos conceitos fundamentais, como o de extensões de corpos, espera-se que o leitor tenha familiaridade com a Teoria de Galois, sobretudo com extensões normais, separáveis e de Galois.

1.1 Corpos de números e elementos algébricos

Esta seção tem como principal objetivo apresentar brevemente os conceitos de corpos de números e elementos algébricos, simultaneamente com algumas de suas principais propriedades e alguns exemplos. A teoria apresentada nesta seção pode ser encontrada com minudência em [32].

Definição 1.1.1 *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{L}$ *é uma* ***extensão*** *de* $\mathbb{K}$ *se* $\mathbb{K} \subseteq \mathbb{L}$ *e*

denotamos $\mathbb{L}|\mathbb{K}$.

Evidentemente $\mathbb{L}$ é um espaço vetorial sobre $\mathbb{K}$ e portanto admite uma base. Em consequência deste fato podemos nos referir a dimensão do espaço vetorial $\mathbb{L}$ sobre $\mathbb{K}$, o que nos permite exibir a seguinte definição.

Definição 1.1.2 *Seja* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos. A dimensão do espaço vetorial* $\mathbb{L}$ *sobre* $\mathbb{K}$ *é chamada de* ***grau da extensão*** *e denotada por* $[\mathbb{L} : \mathbb{K}]$.

Se $[\mathbb{L} : \mathbb{K}]$ é finito, dizemos que a extensão $\mathbb{L}|\mathbb{K}$ é uma extensão finita. Caso contrário, dizemos que $\mathbb{L}$ é uma extensão infinita de $\mathbb{K}$. Particularmente, estamos interessados em extensões finitas, mais precisamente, em extensões finitas do corpo dos números racionais.

Definição 1.1.3 *Se* $\mathbb{K}$ *é uma extensão finita de* $\mathbb{Q}$*, então* $\mathbb{K}$ *é chamado de corpo de números algébricos, ou simplesmente,* ***corpo de números****.*

Exemplo 1.1.1 *O corpo* $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ *é um corpo de números, pois* $\left[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}\right] = 2$. *Assim como* $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$*, uma vez que* $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$.

O Teorema do Elemento Primitivo abaixo enunciado propicia uma caracterização para extensões finitas, as quais são simples e então podem ser geradas pela incorporação de um único elemento, chamado de elemento primitivo.

Teorema 1.1.1 (do Elemento Primitivo, [21], p. 287) *Se* $\mathbb{K}$ *é um corpo de números, então existe* $\theta \in \mathbb{K}$ *tal que* $\mathbb{K} = \mathbb{Q}(\theta)$.

Teorema 1.1.2 ([33], p. 41) *Se* $\mathbb{K}$ *é um corpo de números de grau* n*, então existem exatamente* n *monomorfismos distintos* $\sigma_i : \mathbb{K} \to \mathbb{C}$*, com* $i = 1, 2, \ldots, n$.

Os monomorfismos apresentados no Teorema 1.1.2, que fixam $\mathbb{Q}$, são conceitos clássicos da Teoria de Galois e são de grande importância para o desenvolvimento das Seções 3.3 e 3.4. No caso em que $\mathbb{K}$ é uma extensão normal, os monomorfismos são automorfismos de $\mathbb{K}$. Ademais, se $\mathbb{K}$ é uma extensão de Galois, então os monomorfismos de $\mathbb{K}$ apresentados no Teorema 1.1.2 são os automorfismos do grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$.

Se porventura $\mathbb{L}$ é uma extensão de $\mathbb{K}$ de grau n, sendo $\mathbb{K}$ e $\mathbb{L}$ corpos de números, então o Teorema 1.1.2 também é satisfeito, isto é, existem n monomorfismos distintos de $\mathbb{L}$ em $\mathbb{C}$, os quais fixam $\mathbb{K}$.

Definição 1.1.4 *Um corpo de números $\mathbb{K}$ é totalmente real se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, para todo $i = 1, 2, \ldots, n$. Se $\sigma_i(\mathbb{K}) \not\subseteq \mathbb{R}$, para todo $i = 1, 2, \ldots, n$, então $\mathbb{K}$ é um corpo totalmente complexo, ou totalmente imaginário.*

Proposição 1.1.1 ([3], p. 194) *Se $\mathbb{K}$ é um corpo de números galoisiano, então $\mathbb{K}$ é totalmente real ou totalmente complexo.*

Demonstração: Seja $\mathbb{K}$ um corpo de números galoisiano. Então $\mathbb{Q} \subset \mathbb{K}$ é uma extensão normal, uma vez que é galoisiana, sendo assim, $\sigma_i(\mathbb{K}) = \mathbb{K}$, para todo $i = 1, 2, \ldots, n$. Se $\mathbb{K} \subseteq \mathbb{R}$, então $\mathbb{K}$ é totalmente real. Caso contrário, existe $\alpha \in \mathbb{K}$ tal que $\alpha \in \mathbb{C}$ e $\alpha \notin \mathbb{R}$, logo, $\mathbb{K}$ é totalmente complexo.

□

Definição 1.1.5 *Seja $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos. Um elemento $\alpha \in \mathbb{L}$ é dito **algébrico** sobre $\mathbb{K}$ se existe um polinômio não nulo $p(x) \in \mathbb{K}[x]$ tal que $p(\alpha) = 0$.*

Exemplo 1.1.2 *O elemento $\alpha = 1 + \sqrt{17} \in \mathbb{Q}(\sqrt{17}) = \{a + b\sqrt{17} \mid a, b \in \mathbb{Q}\}$ é algébrico sobre $\mathbb{Q}$, uma vez que é raiz do polinômio $p(x) = x^2 - 2x - 16 \in \mathbb{Q}[x]$.*

O termo algébrico na Definição 1.1.3 se deve ao fato de que toda extensão $\mathbb{K} \subseteq \mathbb{L}$ finita é algébrica, isto é, todo elemento $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$. Além disso, é amplamente conhecido o fato que se $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$, então existe um único polinômio mônico irredutível $m_\alpha(x) \in \mathbb{K}[x]$ tal que $m_\alpha(\alpha) = 0$, chamado de *polinômio minimal* de α sobre $\mathbb{K}$.

Teorema 1.1.3 ([32], p. 63) *Sejam $\mathbb{K} \subset \mathbb{L}$, com $\mathbb{L} = \mathbb{K}(\theta)$, uma extensão finita de $\mathbb{K}$, $m_\theta(x)$ o polinômio minimal de θ sobre $\mathbb{K}$ e $n = \partial(m_\theta(x))$, então $\mathbb{L} = \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} \mid a_i \in \mathbb{K}$, $i = 0, 1, \ldots, n-1\}$ e $[\mathbb{L} : \mathbb{K}] = \partial(m_\theta(x))$. Em particular, $\mathcal{B} = \{1, \theta, \ldots, \theta^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$.*

1.2 Anel de inteiros algébricos e bases integrais

Nesta seção estudamos os elementos de um corpo de números que são inteiros algébricos, apresentando a definição e certas propriedades. Destacamos que o conceito de elemento inteiro pode ser generalizado para uma extensão de anéis $A \subseteq B$, conforme descrito em [30]. Na presente seção, entretanto, particularizamos este estudo para o caso em que A e B são corpos de números.

Definição 1.2.1 *Um elemento $\alpha \in \mathbb{C}$ é um **inteiro algébrico** se existe um polinômio mônico não nulo $f(x) \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$.*

Se $\mathbb{K}$ é um corpo de números e $\alpha, \beta \in \mathbb{K}$ são inteiros algébricos, então $\alpha \pm \beta$, $\alpha\beta$ e α^{-1}, desde que $\alpha \neq 0$, também são inteiros algébricos. Este fato é significativamente conhecido e também pode ser encontrado em [30]. Mais precisamente, o conjunto formado por todos os elementos inteiros algébricos de $\mathbb{K}$ constitui um anel, conforme definimos a seguir.

Definição 1.2.2 *Se $\mathbb{K}$ é um corpo de números, chamamos de **anel de inteiros algébricos**, ou simplesmente de **anel de inteiros de** $\mathbb{K}$, o conjunto dos elementos inteiros de $\mathbb{K}$ e denotamos por $\mathcal{O}_{\mathbb{K}}$.*

Observação 1.2.1 *Obviamente para um corpo de números $\mathbb{K}$ o conjunto dos números inteiros é um subconjunto do anel de inteiros, $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{K}}$. A igualdade se verifica para $\mathbb{K} = \mathbb{Q}$, isto é, o conjunto dos elementos inteiros algébricos de $\mathbb{Q}$ é $\mathbb{Z}$. Uma consequência deste fato é que $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$, para todo corpo de números $\mathbb{K}$.*

O estudo dos anéis de inteiros de corpos de números é notório por diversos fatores. Um dos principais destes fatores são as inúmeras propriedades desdes anéis, sendo significativos não só nas aplicações à teoria de reticulados, mas também em suas propriedades algébricas, como o fato de serem Noetherianos e Dedekind, nos quais todo ideal não nulo pode ser escrito como um produto único de ideais primos. Estudamos alguns aspectos deste fato na Seção 1.5.

Outra característica do anel de inteiros de um corpo de números é a estrutura de $\mathbb{Z}$-módulo livre de posto finito n, no qual n é o grau da extensão $\mathbb{K}|\mathbb{Q}$. Essa característica é herdada por todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Essas circunstâncias estão em concordância com os dois próximos resultados. Para maiores detalhes sobre $\mathbb{Z}$-módulos o leitor pode consultar [24].

Proposição 1.2.1 ([3], p. 66) *Se $\mathbb{K}$ é um corpo de números de grau n, então o seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.*

Corolário 1.2.1 ([3], p. 67) *Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de um corpo de números $\mathbb{K}$ de grau n. Todo ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto n.*

Uma vez que o anel de inteiros de um corpo de números admite a estrutura de $\mathbb{Z}$-módulo livre de posto finito, podemos nos referir a uma base para $\mathcal{O}_{\mathbb{K}}$.

Definição 1.2.3 *Se $\mathbb{K}$ é um corpo de números, então qualquer base do $\mathbb{Z}$-módulo livre $\mathcal{O}_{\mathbb{K}}$ é chamada de **base integral** de $\mathbb{K}$.*

Observação 1.2.2 *Observamos que se* $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ *é uma base integral de* $\mathbb{K}$*, então* $\mathcal{B}$ *é também uma base do espaço vetorial* $\mathbb{K}$ *sobre* $\mathbb{Q}$*. De fato, se* $\frac{a_i}{b_i} \in \mathbb{Q}$*, ou seja,* $a_i, b_i \in \mathbb{Z}$ *e* $b_i \neq 0$*, para* $i = 1, \ldots, n$*, então*

$$\sum_{i=1}^{n} \frac{a_i}{b_i}\alpha_i = 0 \Rightarrow \sum_{i=1}^{n} \left(\prod_{j=1}^{n} b_j\right) a_i\alpha_i = 0 \Rightarrow \left(\prod_{j=1}^{n} b_j\right) a_i = 0, \ \forall\ 1 \leq i \leq n \Rightarrow a_i = 0,$$

para $1 \leq i \leq n$*, o que nos permite concluir que* $\mathcal{B} \subset \mathbb{K}$ *é linearmente independente sobre* $\mathbb{Q}$*. Visto que este conjunto possui* $[\mathbb{K} : \mathbb{Q}]$ *elementos, constatamos que* $\mathcal{B}$ *é uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *como espaço vetorial.*

1.3 Norma e traço

Nessa seção apresentamos brevemente os conceitos de norma e traço de um elemento sobre uma extensão. Estes conceitos são muito importantes para o desenvolvimento do trabalho e para o estudo dos discriminantes.

Definição 1.3.1 *Sejam* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos de números de grau* n *e* $\sigma_1, \ldots, \sigma_n$ *os* n *monomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$*. Para cada* $\alpha \in \mathbb{L}$*, definimos a* ***norma*** *de* α *sobre* $\mathbb{K}$ *por*

$$\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \tag{1.1}$$

Definição 1.3.2 *Sejam* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos de números de grau* n *e* $\sigma_1, \ldots, \sigma_n$ *os* n *monomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$*. Para cada* $\alpha \in \mathbb{L}$*, definimos o* ***traço*** *de* α *por*

$$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{1.2}$$

Observação 1.3.1 *Em alguns casos, quando conveniente, para uma extensão* $\mathbb{Q} \subseteq \mathbb{K}$*, denotamos a norma e o traço de um elemento* $\alpha \in \mathbb{K}$ *apenas por* $\mathcal{T}r_{\mathbb{K}}(\alpha)$ *e* $\mathcal{N}_{\mathbb{K}}(\alpha)$*.*

A próxima proposição apresenta uma série de propriedades sobre a norma e o traço de elementos.

Proposição 1.3.1 ([30], p. 36) *Sejam* $\mathbb{K}$*,* $\mathbb{M}$ *e* $\mathbb{L}$ *corpos de números tais que* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ *e* $[\mathbb{L} : \mathbb{K}] = n$*. Se* $\alpha, \beta \in \mathbb{L}$ *e* $a \in \mathbb{K}$*, então valem as seguintes propriedades*

(i) $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha + \beta) = \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) + \mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta)$

(ii) $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(a\alpha) = a\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha)$

(iii) $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(a) = na$

(iv) $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(a) = a^n$

(v) $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(a\alpha) = a^n\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$

(vi) $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = \mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha)\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\beta)$

(vii) $\mathcal{N}_{\mathbb{L}|\mathbb{K}}(\alpha) = \mathcal{N}_{\mathbb{M}|\mathbb{K}}(\mathcal{N}_{\mathbb{L}|\mathbb{M}}(\alpha))$

(viii) $\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha) = \mathcal{T}r_{\mathbb{M}|\mathbb{K}}(\mathcal{T}r_{\mathbb{L}|\mathbb{M}}(\alpha))$.

Teorema 1.3.1 ([30], p. 38) *Seja $\mathbb{K}$ um corpo de números. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}_{\mathbb{K}}(\alpha)$ e $\mathcal{T}r_{\mathbb{K}}(\alpha)$ são números inteiros.*

No Capítulo 2 exemplificamos e explicitamos o cálculo da norma e traço de alguns elementos em corpos de números quadráticos e ciclotômicos. Como descrito no início dessa seção, estes conceitos são fundamentais para o desenvolvimento do conceito de discriminante que apresentamos na seção seguinte.

1.4 Discriminante

Na presente seção enfocamos no conceito de discriminante e algumas de suas propriedades. Assim como nas seções anteriores, os conceitos apresentados nesta seção podem ser estudado de modo mais geral para uma extensão de anéis $A \subseteq B$, para B um A-módulo livre de posto finito. Estamos interessados, contudo, no caso em que $A = \mathbb{Q}$ e $B = \mathbb{K}$ é um corpo de números.

Este conceito é muito importante para a Teoria Algébrica dos Números. Alguns trabalhos estudam, por exemplo, o cálculo de discriminantes de polinômios. Iniciamos definindo, de modo geral, o discriminante de uma n-upla.

Definição 1.4.1 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de corpos de números e $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$. O* ***discriminante da n-upla*** *$(\alpha_1, \ldots, \alpha_n)$ é definido por*

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)), \tag{1.3}$$

com $i, j = 1, 2, \ldots, n$.

Assim como observamos para a definição de traço, quando a extensão da Definição 1.4.1 for um corpo de números, denotamos o discriminante de uma n-upla na Equação (1.3) apenas por $\mathcal{D}_{\mathbb{K}}(\alpha_1, \ldots, \alpha_n)$.

A próxima proposição nos permite particularizar a definição de discriminante. Para sua demonstração, porém, faz-se necessário o Lema de Dedekind que enunciamos a seguir.

Lema 1.4.1 (de Dedekind, [30], p. 39) *Se G é um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \ldots, \sigma_n$ são homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então os σ_i's são linearmente independentes sobre $\mathbb{K}$.*

Proposição 1.4.1 ([11], p. 40) *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos distintos de $\mathbb{L}$. Se $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0. \tag{1.4}$$

Demonstração: Por definição, o discriminante de $\mathcal{B}$ é $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j))$. Considerando a definição de traço para $\alpha_i\alpha_j$ e as propriedades dos monomorfismos, obtemos

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) = det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) = det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right).$$

Como

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j),$$

então $det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) = det\left(\sigma_i(\alpha_j)\right)^2$. Portanto, $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2$. Por outro lado, se $det(\sigma_i(\alpha_j)) = 0$, então existem $a_1, \ldots, a_n \in \mathbb{C}$, não todos nulos, tais que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$, com $j = 1, \ldots, n$. Dessa forma, $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{L}$, o que é uma contradição, tendo em vista que o Lema de Dedekind nos garante que os n monomorfismos são linearmente independentes. Portanto, $det(\sigma_i(\alpha_j))^2 \neq 0$, o que conclui o resultado.

□

Devido a Proposição 1.4.1, podemos reformular a Definição 1.4.1 para o caso particular de um corpo de números algébricos.

Definição 1.4.2 *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. O* ***discriminante*** *dessa base é definido por*

$$\mathcal{D}_{\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = (det(\sigma_j(\alpha_i)))^2, \tag{1.5}$$

isto é, o determinante da matriz com entradas $\sigma_j(\alpha_i)$ na i-ésima linha e j-ésima coluna.

Proposição 1.4.2 ([11], p. 39) *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpo de números e $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\mathcal{C} = \{\beta_1, \ldots, \beta_n\}$ é um conjunto de elementos de $\mathbb{L}$ tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in \mathbb{K}$, para $i = 1, \ldots, n$, então*

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\beta_1, \ldots, \beta_n) = (det(a_{ij}))^2 \mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n).$$

Demonstração: Pela Definição 1.4.1, $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\beta_1, \ldots, \beta_n) = det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_r\beta_s))$, com $r, s = 1 \ldots, n$. Como $\beta_r = \sum_{i=1}^{n} a_{ri}\alpha_i$ e $\beta_s = \sum_{j=1}^{n} a_{sj}\alpha_j$, então $\beta_r\beta_s = \sum_{i=1}^{n} a_{ri}a_{sj}\alpha_i\alpha_j$. Logo,

$$\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_r\beta_s) = \sum_{i=1}^{n} a_{ri}a_{sj}\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j),$$

Representando na forma matricial, obtemos $(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_r\beta_s)) = (a_{ri})(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j))(a_{sj})^t$, em que t denota a transposição. Portanto,

$$\begin{aligned}
\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\beta_1, \ldots, \beta_n) &= det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\beta_r\beta_s)) = det((a_{ri})(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j))(a_{sj})^t) \\
&= det(a_{ri})det(\mathcal{T}r_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j))det((a_{sj})^t) \\
&= (det(a_{i,j}))^2 \mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n).
\end{aligned}$$

□

Teorema 1.4.1 ([3], p. 69) *Sejam $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_{\mathbb{K}}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Se $\mathcal{D}_{\mathbb{K}}(\alpha_1, \ldots, \alpha_n)$ é livre de quadrados, então $\mathcal{B}$ é uma base integral.*

Demonstração: Seja $\mathcal{C} = \{\beta_1, \ldots, \beta_n\}$ uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Sendo assim, $\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_j$, com $a_{ij} \in \mathbb{Z}$ e pela Proposição 1.4.2, $\mathcal{D}_{\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = (det(a_{ij}))^2 \mathcal{D}_{\mathbb{K}}(\beta_1, \ldots, \beta_n)$. Admitindo que o discriminante $\mathcal{D}_{\mathbb{K}}(\alpha_1, \ldots, \alpha_n)$ é livre de quadrados, obtemos $det(a_{ij}) = \pm 1$, ou seja, $\mathcal{B}$ também é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, e portanto, uma base integral de $\mathbb{K}$.

□

Teorema 1.4.2 ([3], p. 68) *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} \subset \mathcal{O}_\mathbb{K}$, uma base integral de $\mathbb{K}$. Então $\mathcal{C} = \{\beta_1, \ldots, \beta_n\}$ é uma base integral de $\mathbb{K}$ se, e somente se,*

$$\mathcal{D}_\mathbb{K}(\alpha_1, \ldots, \alpha_n) = \mathcal{D}_\mathbb{K}(\beta_1, \ldots, \beta_n).$$

Observação 1.4.1 *Pelo Teorema 1.4.2, o discriminante do corpo $\mathbb{K}$ independe da base de $\mathcal{O}_\mathbb{K}$. Devido a este fato, chamamos de discriminante de $\mathbb{K}$ o valor do discriminante de qualquer base integral de $\mathbb{K}$ e denotamos por $\mathcal{D}_\mathbb{K}$.*

Para concluir a seção enunciamos uma proposição que nos fornece um método prático para o cálculo do discriminante de uma base para uma extensão de corpos de números utilizando o elemento primitivo da extensão.

Proposição 1.4.3 ([3], p. 54) *Sejam $\mathbb{K} \subseteq \mathbb{L}$, com $\mathbb{L} = \mathbb{K}(\theta)$, uma extensão de corpos finita e separável de grau n e $m_\theta(x) \in \mathbb{K}[x]$ o polinômio minimal de θ sobre $\mathbb{K}$. Então*

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}} = \mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathcal{N}_{\mathbb{L}|\mathbb{K}}(m'_\theta(\theta)).$$

em que $m'_\theta(\theta)$ representa a derivada do polinômio $m_\theta(x)$ aplicada em θ.

1.5 Norma de ideal e ramificação de ideais

Encerramos este capítulo apresentando os conceitos de norma de um ideal no anel de inteiros de um corpo de números. Também comentamos brevemente o conceito de ideal fracionário e alguns resultados relacionados a ramificação de ideais. Este estudo está relacionado principalmente aos anéis de Dedekind e é desenvolvido em [30].

Como comentamos na Seção 1.2, os anéis de inteiros de corpos de números são anéis de Dedekind, isto é, são anéis Noetherianos, integralmente fechados em que todo ideal primo não nulo é maximal. Estes anéis possuem inúmeras propriedades relacionadas a fatoração de elementos e ideais. Começamos apresentando a definição de norma de um ideal do anel de inteiros de um corpo de números.

Definição 1.5.1 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_\mathbb{K}$ seu anel de inteiros e $\mathcal{I}$ um ideal de $\mathcal{O}_\mathbb{K}$. Definimos a **norma do ideal** $\mathcal{I}$ como sendo o número de elementos do anel quociente $\mathcal{O}_\mathbb{K}/\mathcal{I}$, ou seja,*

$$\mathcal{N}(\mathcal{I}) = \#\mathcal{O}_\mathbb{K}/\mathcal{I}. \tag{1.6}$$

Observação 1.5.1 *A norma de qualquer ideal $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ é um número finito.*

Proposição 1.5.1 ([30], p. 52) *Seja $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, isto é, $\mathcal{I} = \langle\alpha\rangle = \alpha\mathcal{O}_{\mathbb{K}}$ para algum $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}(\mathcal{I}) = |\mathcal{N}_{\mathbb{K}}(\alpha)|$.*

Lema 1.5.1 ([30], p. 52) *Seja $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Se $\mathcal{I}$ e $\mathcal{J}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}(\mathcal{I}\mathcal{J}) = \mathcal{N}(\mathcal{I})\mathcal{N}(\mathcal{J})$.*

Teorema 1.5.1 ([33], p. 129) *Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então*

(i) $\mathcal{N}(\mathcal{I}) = 1$ se, e somente se, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$.

(ii) Se $\mathcal{N}(\mathcal{I})$ é um número primo, então o ideal $\mathcal{I}$ é primo.

A seguir formalizamos o comentário de que o anel de inteiros de um corpo de números é um anel de Dedekind. Estamos interessados, notoriamente, no caso em que o anel de Dedekind A citado no teorema a seguir é o conjunto dos números inteiros $\mathbb{Z}$.

Teorema 1.5.2 ([30], p. 49) *Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind.*

Uma consequência de um dos principais resultados deste trabalho, apresentado no Capítulo 4, está relacionada à uma classe de ideais do anel de inteiros, os ideais fracionários. Apresentamos sua definição de modo mais geral de acordo com [30] e particularizamos para o objetivo do estudo.

Definição 1.5.2 *Sejam A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Um **ideal fracionário** de A é um A-submódulo $\mathcal{I}$ de $\mathbb{K}$ tal que $d\mathcal{I} \subset A$, para algum $d \in A$, $d \neq 0$.*

Proposição 1.5.2 ([3], p. 61) *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Se $\mathcal{I}$ é um A-submódulo finitamente gerado de $\mathbb{K}$, então $\mathcal{I}$ é um ideal fracionário.*

Observamos que todo ideal é um ideal fracionário, basta considerarmos $d = 1$ na Definição 1.5.2. Além disso, os elementos de um ideal fracionário possuem denominador comum $d \in A$. No contexto da Teoria Algébrica dos Números, temos a seguinte definição.

Definição 1.5.3 *Sejam $\mathbb{K}$ um corpo de números. Um **ideal fracionário** de $\mathcal{O}_{\mathbb{K}}$ é um $\mathcal{O}_{\mathbb{K}}$-submódulo $\mathcal{J}$ de $\mathbb{K}$ tal que $d\mathcal{J} \subset \mathcal{O}_{\mathbb{K}}$ para algum $d \in \mathcal{O}_{\mathbb{K}}$, com $d \neq 0$.*

Um dos principais resultados relacionados aos anéis de Dedekind é o seguinte.

Teorema 1.5.3 ([30], p. 50) *Seja A um anel de Dedekind. Se $\mathcal{I} \neq A$ é um ideal não nulo de A, então existem ideais primos não nulos $\mathcal{Q}_1, \ldots, \mathcal{Q}_t$ de A e inteiros positivos $e_1, \ldots, e_t$ de tal forma que $\mathcal{I}$ pode ser expresso de maneira única como $\mathcal{I} = \prod_{i=1}^{t} \mathcal{Q}_i^{e_i}$.*

No contexto de ramificação de ideais, o índice $t \in \mathbb{Z}$ do Teorema 1.5.3 é chamado de *número de decomposição* do ideal $\mathcal{I}$. Além disso, o expoente e_i é chamado de *índice de ramificação* do ideal $\mathcal{Q}_i$. Se $e_i > 1$ para algum $i = 1, \ldots, t$, dizemos que $\mathcal{I}$ se ramifica no seu corpo de frações.

Considerações Finais

Ao longo deste capítulo apresentamos pré-requisitos de maneira superficial, evidentemente os conceitos presentes fazem parte de uma teoria muito mais extensiva. Na Seção 1.5, especialmente, existe uma ampla teoria relacionada a ramificação de ideais. Algumas caracterizações de reticulados e de reticulados bem arredondados, principal tópico deste trabalho, necessitam dos conceitos que tratamos nas Seções 1.3, 1.4 e 1.5.

No próximo capítulo caracterizamos conceitos apresentados neste, como o anel de inteiros, norma, traço e discriminante para corpos de números extremamente importantes, os corpos quadráticos e ciclotômicos.

Capítulo

2

Corpos quadráticos e ciclotômicos

Os corpos quadráticos e ciclotômicos são corpos de números que desempenham um papel crucial no desenvolvimento da Teoria dos Números. Os corpos quadráticos por se tratarem de corpos mais simples no que se refere a sua composição, visto que são obtidos agregando ao conjunto dos números racionais uma raiz quadrada de um elemento inteiro livre de quadrados. E os corpos ciclotômicos, obtidos por agregar uma raiz da unidade complexa ao conjunto dos números racionais, por demais estudos relacionados a álgebra moderna.

A teoria presente neste capítulo é amplamente conhecida, contudo, representa significativa importância para o trabalho e por isso a apresentamos. Os resultados presentes neste capítulo estão disponíveis em [3], [11], [21] e [32].

Nas Seções 2.1 e 2.2 enfatizamos o estudo de corpos quadráticos, caracterizando-os, bem como seus anéis de inteiros e bases integrais correspondentes. Nas Seções 2.3 e 2.4 realizamos o mesmo estudo, no entanto, para corpos ciclotômicos. Finalmente, na Seção 2.5 damos uma atenção especial aos discriminantes de tais corpos devido a sua relevância em alguns resultados do Capítulo 4.

2.1 Corpos quadráticos

Iniciamos a seção definindo formalmente um corpo quadrático.

Definição 2.1.1 *Todo corpo de números* $\mathbb{K}$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 2$ *é chamado de* ***corpo quadrático****.*

Proposição 2.1.1 ([34], p. 62) *Todo corpo quadráticos $\mathbb{K}$ é da forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, sendo $d \in \mathbb{Z}$ livre de quadrados.*

Demonstração: Se $\mathbb{K}$ é um corpo quadrático, então pelo Teorema do Elemento Primitivo (Teorema 1.1.1), existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Seja $m_\theta(x) = x^2 + ax + b \in \mathbb{Q}[x]$ o polinômio minimal de θ sobre $\mathbb{Q}$. Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$, obtemos

$$2\theta = -a \pm \sqrt{a^2 - 4b}.$$

Dessa forma, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$ e como $a^2 - 4b \in \mathbb{Q}$, existem $u, v \in \mathbb{Z}$, com $v \neq 0$ e $mdc(u, v) = 1$, tais que $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$. Note que u e v não são quadrados perfeitos simultaneamente, pois neste caso teríamos $\mathbb{Q}(\theta) = \mathbb{Q}$, o que contradiz o fato de $\mathbb{Q}(\theta)$ ser um corpo quadrático. Assim,

$$\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\frac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\frac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv}).$$

Escrevendo $uv = q^2 d$, sendo $q, d \in \mathbb{Z}$ e d livre de quadrados, concluímos que

$$\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{q^2 d}) = \mathbb{Q}(\sqrt{d}).$$

□

Um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, é chamado de ***corpo quadrático imaginário***, ou ***complexo***, se $d < 0$. Todavia, se $d > 0$, então $\mathbb{Q}(\sqrt{d})$ é chamado de ***corpo quadrático real***.

Exemplo 2.1.1 *Os corpos $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{5})$ são corpos quadráticos reais e o primeiro é de suma importância para este trabalho conforme justificamos no Capítulo 5. Por outro lado, os corpos $\mathbb{Q}(\sqrt{-13})$ e $\mathbb{Q}(\sqrt{-7})$ são exemplos de corpos quadráticos imaginários.*

Um fato amplamente conhecido da Teoria de Galois é que toda extensão de grau 2 é uma extensão de Galois. Dessa forma, os 2 monomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados, descritos pelo Teorema 1.1.2, são os automorfismos do grupo de Galois dados por

$$id = \sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \qquad \text{e} \qquad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

com $a, b \in \mathbb{Q}$. Em geral, se $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, então

$$\mathcal{N}_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\alpha) = \prod_{i=1}^{2} \sigma_i(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

e

$$\mathcal{T}r_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\alpha) = \sum_{i=1}^{2} \sigma_i(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

2.2 Anel de inteiros e base integral de corpos quadráticos

Nesta seção vamos determinar o anel de inteiros dos corpos quadráticos que caracterizamos na seção anterior. O Lema 2.2.1 que apresentamos a seguir é de grande valor para a demonstração do Teorema 2.2.1 que determina categoricamente o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, para $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados. Muitas vezes, por simplicidade, nos referimos a este anel de inteiros como anel de inteiros quadráticos.

Lema 2.2.1 ([11], p. 20) *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático. Um elemento $a + b\sqrt{d} \in \mathbb{K}$ pertence a $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $2a = u \in \mathbb{Z}$, $2b = v \in \mathbb{Z}$ e $u^2 - dv^2 \equiv 0 \ (mod\ 4)$.*

Demonstração: Suponhamos que $\alpha = a + b\sqrt{d}$ pertença a $\mathcal{O}_{\mathbb{K}}$. Então seu conjugado $\beta = a - b\sqrt{d} \in \mathbb{K}$ também é um elemento de $\mathcal{O}_{\mathbb{K}}$ e como $\mathcal{O}_{\mathbb{K}}$ é um anel, a soma $\alpha + \beta = 2a \in \mathcal{O}_{\mathbb{K}}$. Note que $2a \in \mathbb{Q}$, e pela Observação 1.2.1, $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$, o que nos garante que $2a \in \mathbb{Z}$. Analogamente, o produto $\alpha\beta = a^2 - db^2 \in \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$. Sendo assim,

$$u^2 - dv^2 = (2a)^2 - (2b^2)d = 4(a^2 - b^2 d) \equiv 0 \ (mod\ 4).$$

Como $2a \in \mathbb{Z}$, então $(2a)^2 \in \mathbb{Z}$, e consequentemente, $(2b)^2 d \in \mathbb{Z}$. Seja $2b = \dfrac{m}{n} \in \mathbb{Q}$, com $m, n \in \mathbb{Z}$, $n \neq 0$ e $mdc(m, n) = 1$. Então $n = 1$, pois caso contrário existiria um primo p divisor de n tal que $p^2 \mid d$, contrariando o fato de que d é livre de quadrados. Portanto, $v = 2b \in \mathbb{Z}$.

Reciprocamente, se $2a = u \in \mathbb{Z}$, $2b = v \in \mathbb{Z}$ e $u^2 - dv^2 \equiv 0 \ (mod\ 4)$, então $u^2 - dv^2 \in \mathbb{Z}$ e o polinômio mônico $p(x) = x^2 - ux + (u^2 - dv^2) \in \mathbb{Z}[x]$ admite $a + b\sqrt{d}$ como raiz, portanto, $a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$.

□

Teorema 2.2.1 ([11], p. 21) *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com $d \in \mathbb{Z}$ livre de quadrados. Então seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é dado por*

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z}[\sqrt{d}], \ \text{se } d \equiv 2, 3 \ (mod\ 4) \\ \\ \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right], \ \text{se } d \equiv 1 \ (mod\ 4). \end{cases} \tag{2.1}$$

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{K}$ um inteiro algébrico, ou seja, $\alpha \in \mathcal{O}_{\mathbb{K}}$. Pelo Lema 2.2.1, $a = \frac{u}{2}$, $b = \frac{v}{2}$ e $u^2 - dv^2 \in \mathbb{Z}$, com $u, v \in \mathbb{Z}$.

Se $d \equiv 2, 3 \ (mod\ 4)$, então u e v são pares, uma vez que se v fosse ímpar, então $v^2 \equiv 1 \ (mod\ 4)$ e como $u^2 - dv^2 \in 4\mathbb{Z}$, obteríamos $u^2 \equiv dv^2 \equiv d \ (mod\ 4)$. Logo, $d \equiv 0 \ (mod\ 4)$ ou $d \equiv 1 \ (mod\ 4)$, o que é uma contradição. Portanto, v é par. Como $v^2 \equiv 0 \ (mod\ 4)$ e $u^2 \equiv dv^2 \equiv 0 \ (mod\ 4)$, podemos concluir que u também é par. Ou seja, devido ao fato que u e v são pares, então $a, b \in \mathbb{Z}$ e assim, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Portanto $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\sqrt{d}]$. Em contrapartida, se $\alpha \in \mathbb{Z}[\sqrt{d}]$, então α é raiz do polinômio mônico $p(x) = x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois novamente pelo Lema 2.2.1, $2a, a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

Agora, se $d \equiv 1 \ (mod\ 4)$, então necessariamente u e v possuem a mesma paridade, isto é, são ambos pares ou ambos ímpares. De fato, se u é par, então $u^2 \equiv dv^2 \equiv 0 \ (mod\ 4)$, o que nos permite concluir, devido ao fato que $d \equiv 1 \ (mod\ 4)$, que $v^2 \equiv 0 \ (mod\ 4)$, ou seja, v também é par. Se u é ímpar, como $u^2 \equiv dv^2 \equiv 0 \ (mod\ 4)$, para o caso em que v é par teríamos $u^2 \equiv 0 \ (mod\ 4)$, o que é uma contradição com a suposição inicial. Então u e v admitem a mesma paridade.

Para o primeiro caso, u e v pares, temos $a, b \in \mathbb{Z}$ e $\alpha = a + b\sqrt{d} = (a - b) + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se u e v são ímpares, então

$$\alpha = a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d} = \frac{u - v}{2} + \frac{v(1+\sqrt{d})}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Observe que como u e v são ímpares, então $u - v$ é par. Portanto $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ e $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a, b \in \mathbb{Z}$, então $2a + b \in \mathbb{Z}$ e $\left(a + \frac{b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = a^2 + ab + \frac{(1-d)b^2}{4} \in \mathbb{Z}$, pois como $d \equiv 1 \ (mod\ 4)$, então $(1 - d)b^2 \in 4\mathbb{Z}$.

Logo, o polinômio mônico $p(x) = x^2 - (2a + b)x + a^2 + ab + \frac{(1-d)b^2}{4} \in \mathbb{Z}[x]$ e $p(\alpha) = 0$, ou seja, $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

□

Exemplo 2.2.1 *O corpo quadrático $\mathbb{Q}(i)$ é chamado de corpo gaussiano. Neste caso, $d = -1$ e como $-1 \equiv 3 \ (mod\ 4)$, o Teorema 2.2.1 nos garante que o anel de inteiros de $\mathbb{Q}(i)$ é $\mathbb{Z}[i]$, chamado de anel de inteiros gaussiano.*

Como descrito na Seção 1.2, uma base integral é uma base para o $\mathbb{Z}$-módulo $\mathcal{O}_{\mathbb{K}}$. Para corpos quadráticos é habitual, por conveniência, utilizarmos como base do anel de inteiros o conjunto $\mathcal{B} = \left\{1, \frac{1+\sqrt{d}}{2}\right\}$, se $d \equiv 1 \ (mod\ 4)$ e $\mathcal{B} = \left\{1, \sqrt{d}\right\}$, se $d \equiv 2, 3 \ (mod\ 4)$.

Exemplo 2.2.2 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{13})$, então o Teorema 2.2.1 garante que o anel de inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$, tendo em vista que $13 \equiv 1 \ (mod\ 4)$. Neste caso, uma base integral para $\mathcal{O}_{\mathbb{K}}$ é o conjunto $\mathcal{B} = \left\{1, \frac{1+\sqrt{13}}{2}\right\}$.*

Como destacamos anteriormente, uma base integral não é única. Na Seção 4.3 estudamos uma outra base para o anel de inteiros quadráticos, a qual é de grande relevância para as construções que apresentamos.

2.3 Corpos ciclotômicos

Nesta seção apresentamos os n-ésimos corpos ciclotômicos, um dos mais importantes tipos de corpos de números. Alguns resultados relacionados a este conceito, bem como os polinômios ciclotômicos e outros aspectos desta teoria. Nesta e na próxima seção exibimos as demonstrações de alguns resultados para o caso em que $n = p$ é um número primo e omitimos outras para o caso geral, estas, porém, podem ser encontradas em [3], [11] e [36].

Damos início a seção estabelecendo precisamente a definição de raiz n-ésima da unidade.

Definição 2.3.1 *Seja $n \in \mathbb{Z}$ um inteiro positivo.*

*(i) Uma raiz do polinômio $x^n - 1$ é dita uma **raiz n-ésima da unidade**, denotada por ζ_n.*

*(ii) Uma raiz n-ésima da unidade tal que $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$, é chamada de **raiz n-ésima primitiva da unidade**.*

É comum em diversas áreas da matemática encontrarmos uma raiz n-ésima da unidade representada por $\zeta_n = e^{\frac{2\pi i}{n}} = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$, em que $i = \sqrt{-1}$ é a unidade imaginária. Essa representação é conveniente em alguns exemplos que apresentamos nos capítulos subsequentes.

Definição 2.3.2 *Se ζ_n é uma raiz n-ésima primitiva da unidade, o corpo $\mathbb{Q}(\zeta_n)$ é chamado de n-ésimo **corpo ciclotômico**.*

Teorema 2.3.1 ([36], p. 49) *Se $n \in \mathbb{Z}$ é um inteiro positivo e ζ_n uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde $\varphi(n) = \#\{m \in \mathbb{N} \mid 0 < m < n \text{ e } mdc(m,n) = 1\}$ denota a função de Euler.*

Corolário 2.3.1 ([36], p. 50) *Se $mdc(m,n) = 1$, então $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.*

Um resultado amplamente conhecido é que toda extensão ciclotômica é uma extensão de Galois. Sendo assim, se $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é um corpo ciclotômico, então os $\varphi(n)$ monomorfismos de $\mathbb{K}$ são os automorfismos do grupos de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$, os quais permutam as raízes do polinômio minimal de ζ_n.

Definição 2.3.3 *Seja ζ_n uma raiz n-ésima primitiva da unidade, $n \geq 2$. O polinômio*

$$\Phi_n(x) = \prod_{j=1}^{n}(x - \zeta_n^j), \tag{2.2}$$

*onde $mdc(j,n) = 1$, é chamado de n-**ésimo polinômio ciclotômico**. O grau de $\Phi_n(x)$ é dado pela função de Euler $\varphi(n)$.*

O polinômio apresentado na Definição 2.3.3 é o polinômio minimal de ζ_n. Esse fato é justificado pela próxima proposição. Neste caso, pela própria definição, $\Phi_n(x)$ é mônico e de grau $\varphi(n)$, sendo necessário apenas verificar sua irredutibilidade.

Proposição 2.3.1 ([21], p. 299) *O n-ésimo polinômio ciclotômico $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Seja $m_{\zeta_n}(x)$ o polinômio minimal de ζ_n. Como consequência do Teorema 2.3.1, temos $\partial(m_{\zeta_n}(x)) = \partial(\Phi_n(x))$ e $\Phi_n(\zeta_n) = 0$. Portanto, $m_{\zeta_n} \equiv \Phi_n$, e dessa forma, $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$.

□

Proposição 2.3.2 ([21], p. 298) *Se $n \in \mathbb{Z}$ é um inteiro positivo, então*

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{2.3}$$

Demonstração: Sejam $f(x) = x^n - 1$ e $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ as raízes de $f(x)$. Então,

$$x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{n-1}).$$

Considerando o período de cada raiz de $f(x)$ e escrevendo todas as raízes de mesmo período como um polinômio da forma

$$\Phi_d(x) = \prod_{\substack{\text{período} \\ \zeta=d}} (x-\zeta),$$

concluímos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

□

Corolário 2.3.2 ([21], p. 299) *Se $n \in \mathbb{Z}$ é um inteiro positivo, então*

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}. \tag{2.4}$$

Demonstração: É uma consequência imediata da Proposição 2.3.2.

□

Observação 2.3.1 *Se $n = p$ é um número primo, então o p-ésimo polinômio ciclotômico é dado por*

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x].$$

No próximo resultado exibimos explicitamente a norma e o traço de alguns elementos de um p-ésimo corpo ciclotômico. Esse resultado contribui para determinar o anel de inteiros de um corpo ciclotômico.

Lema 2.3.1 ([30], p. 43) *Sejam $p \in \mathbb{Z}$ um primo e ζ_p uma raiz p-ésima primitiva da unidade. Para $j = 1, \ldots, p-1$, temos*

(i) $\mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p^j) = -1$.

(ii) $\mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p^j) = p$.

(iii) $\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$ *e* $\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p) = p$.

(iv) $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$.

Demonstração: Para o item (i), temos pela Observação 2.3.1, que o p-ésimo polinômio ciclotômico de ζ_p é dado por $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. As raízes de $\Phi_p(x)$ são $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. Logo,

$$0 = \Phi_p(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j + 1,$$

para $j = 1, \ldots, p-1$, e assim, $\zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j = -1$. Portanto,

$$\mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \ldots + \zeta_p^j = -1.$$

Para o item (ii), $\mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1-\zeta_p^j) = \mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1) - \mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p^j)$ e como $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, então $\mathcal{T}r_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1) = 1+1+\ldots+1 = p-1$. Do item (i) obtemos que $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p^j) = -1$, assim, $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(1-\zeta_p^j) = p-1+1 = p$. Para (iii), como $\zeta_p - 1$ é uma raiz do polinômio

$$f(x) = x^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} x^{j-1},$$

então $\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$ e

$$\begin{aligned}
\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1-\zeta_p) &= \mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}((-1)(\zeta_p - 1)) \\
&= \mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(-1)\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p - 1) \\
&= (-1)^{p-1}(-1)^{p-1}p \\
&= (-1)^{2(p-1)}p \\
&= p.
\end{aligned}$$

Por fim, como $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ são raízes do polinômio ciclotômico $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$, então

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = (x-\zeta_p)(x-\zeta_p^2)\ldots(x-\zeta_p^{p-1}).$$

Para $x = 1$, concluímos que $p = \Phi_p(1) = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$, o que completa o item (iv) e por consequência, o resultado.

□

2.4 Anel de inteiros e base integral de corpos ciclotômicos

Nosso principal objetivo nesta seção é caracterizar o anel de inteiros corpos ciclotômicos. Também estudamos algumas propriedades de uma classe de ideais do anel de inteiros que apresentam inúmeras propriedades no que se refere a ramificação.

Considere $p \in \mathbb{Z}$ um inteiro primo e ímpar, $p > 2$ e ζ_p uma raiz p-ésima primitiva da unidade. Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, então $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{K}}$, pois como descrito na Observação

2.3.1, $\Phi_p(x) \in \mathbb{Z}[x]$ é o polinômio minimal de ζ_p sobre $\mathbb{Q}$ e como ζ_p^i são as demais raízes de $\Phi_p(x)$, para $i = 1, 2, \ldots, p-1$, então são inteiros algébricos.

No Teorema 2.4.1 mostramos que a inclusão $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$ também se verifica, ou seja, o conjunto $\mathbb{Z}[\zeta_p]$ é de fato o anel de inteiros de $\mathbb{Q}(\zeta_p)$. Contudo, antes de enunciá-lo e demonstrá-lo apresentamos alguns resultados que são importantes para a demonstração do mesmo. Nos próximos resultados nos referimos ao anel de inteiros sem necessariamente explicitá-lo.

O primeiro dentre estes se refere as chamadas unidades ciclotômicas.

Lema 2.4.1 ([3], p. 88) *Se r e s são inteiros tais que $mdc(p, rs) = 1$, então $\dfrac{\zeta_p^r - 1}{\zeta_p^s - 1}$ é um elemento inversível de $\mathbb{Z}[\zeta_p]$, chamado de unidade ciclotômica.*

Demonstração: Como $mdc(p, rs) = 1$, existe um número inteiro t tal que $r \equiv st \ (mod\ p)$. Assim,

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} = \frac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + \ldots + \zeta_p^{s(t-1)} \in \mathbb{Z}[\zeta_p]. \tag{2.5}$$

Analogamente, $\dfrac{\zeta_p^s - 1}{\zeta_p^r - 1} \in \mathbb{Z}[\zeta_p]$. Portanto, $\dfrac{\zeta_p^r - 1}{\zeta_p^s - 1}$ é inversível em $\mathbb{Z}[\zeta_p]$.

□

Proposição 2.4.1 ([36], p. 51) *Sejam $p \in \mathbb{Z}$ um número primo ímpar, $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. O ideal $(1 - \zeta_p)\mathcal{O}_{\mathbb{K}}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$ e $((1 - \zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1} = p\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Pelo item (iv) do Lema 2.3.1,

$$p = \prod_{i=1}^{p-1}(1 - \zeta_p^i).$$

O Lema 2.4.1 garante que os ideais $(1-\zeta_p)\mathcal{O}_{\mathbb{K}}$ e $(1-\zeta_p^i)\mathcal{O}_{\mathbb{K}}$ são iguais, para $i = 1, 2, \ldots, p-1$. Portanto, $p\mathcal{O}_{\mathbb{K}} = ((1-\zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1}$. Pelo Teorema da Igualdade Fundamental de [30], $p\mathcal{O}_{\mathbb{K}}$ possui no máximo $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p - 1$ fatores primos em $\mathcal{O}_{\mathbb{K}}$. Portanto, $(1 - \zeta_p)\mathcal{O}_{\mathbb{K}}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$.

□

Lema 2.4.2 ([36], p. 51) *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Então*

$$(1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle.$$

Demonstração: Pela Proposição 2.4.1, $((1-\zeta_p)\mathcal{O}_{\mathbb{K}})^{p-1} = p\mathcal{O}_{\mathbb{K}}$. Sendo assim, $p \in (1-\zeta_p)\mathcal{O}_{\mathbb{K}}$ e $p\mathbb{Z} \subset (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$. Por outro lado, como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, então $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$ ou $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Se a segunda opção acontece, isto é, $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$, então $1-\zeta_p$ é um elemento invertível de $\mathcal{O}_{\mathbb{K}}$. Logo, p é invertível em $\mathcal{O}_{\mathbb{K}}$. Entretanto, p admite inverso em $\mathbb{Q}$ e assim, p tem um inverso em $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$, o que é uma contradição visto que p não possui inverso em $\mathbb{Z}$. Portanto, $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

□

Lema 2.4.3 ([36], p. 52) *Sejam $p \in \mathbb{Z}$ um número primo ímpar, $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $\mathcal{T}r_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in p\mathbb{Z}$.*

Demonstração: Sejam $\sigma_i(\alpha(1-\zeta_p)) = \alpha_i(1-\zeta_p^i)$ os conjugados de $\alpha(1-\zeta_p)$, em que σ_i são os automorfismos de $\mathbb{K}$, para $i = 1, \ldots, p-1$. Estes elementos são múltiplos de $(1-\zeta_p^i)$ em $\mathcal{O}_{\mathbb{K}}$. Como $1-\zeta_p^i = (1-\zeta_p)(\zeta_p^{i-1} + \zeta_p^{i-2} + \ldots + \zeta_p + 1)$, então $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathcal{O}_{\mathbb{K}}$. Assim, pela definição de traço,

$$\mathcal{T}r_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) = \alpha_1(1-\zeta_p) + \alpha_2(1-\zeta_p^2) + \ldots + \alpha_p(1-\zeta_p^p) = \beta(1-\zeta_p),$$

para algum $\beta \in \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{T}r_{\mathbb{K}}(\alpha(1-\zeta_p)) \in \mathcal{O}_{\mathbb{K}}$. Finalmente, como $\mathbb{Z}$ é integralmente fechado, segue que $\mathcal{T}r_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathbb{Z}$. Logo, $\mathcal{T}r_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

□

Em posse do comentário no início desta seção, do Lema 2.3.1 e do Lema 2.4.3, estamos aptos a expor e demonstrar o teorema que classifica o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$.

Teorema 2.4.1 ([30], p. 43) *Sejam $p \in \mathbb{Z}$ um primo e $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Então o anel de inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$.*

Demonstração: Como destacamos anteriormente, $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{K}}$, sendo assim, nos resta garantir que $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Seja $\mathcal{B} = \{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$. Então $\mathcal{B}$ é linearmente independente sobre $\mathbb{Q}$, pois caso contrário ζ_p seria raiz de um polinômio com grau estritamente menor do que $p-1$, o que é uma contradição devido ao fato de que $\Phi_p(x)$ é o polinômio minimal de ζ_p. Considere $\alpha \in \mathcal{O}_{\mathbb{K}} \subset \mathbb{Q}(\zeta_p)$, assim

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

com únicos $a_i \in \mathbb{Q}$, para todo $i = 0, 1, \ldots, p-2$. Mostremos que $a_i \in \mathbb{Z}$. De fato, multiplicando

a Equação (2.6) por $1-\zeta_p$ em ambos os lados, obtemos

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}). \tag{2.7}$$

Pelo item (i) do Lema 2.3.1, temos $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p^j) = -1$. Dessa forma, utilizando as propriedades de traço,

$$\begin{aligned} \mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\alpha(1-\zeta_p)) &= a_0\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(1-\zeta_p) + a_1\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p - \zeta_p^2) \\ &+ \ldots + a_{p-2}\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p^{p-2} - \zeta_p^{p-1}), \end{aligned} \tag{2.8}$$

e pelo Lema 2.4.3, segue que $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\alpha(1-\zeta_p)) \in p\mathbb{Z}$. Além disso, como $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \ldots, p-2$, então $a_0\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(1-\zeta_p) = a_0 p \in p\mathbb{Z}$, com $a_0 \in \mathbb{Z}$. Portanto, $a_0 \in \mathbb{Z}$. De modo análogo, como $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_{\mathbb{K}}$,

$$(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \ldots + a_{p-2}\zeta_p^{p-3}. \tag{2.9}$$

Multiplicando a Equação (2.9) por $1-\zeta_p$, obtemos

$$(\alpha - a_0)\zeta_p^{-1}(1-\zeta_p) = a_1(1-\zeta_p) + a_2\zeta_p(1-\zeta_p) + \ldots + a_{p-2}\zeta_p^{p-3}(1-\zeta_p). \tag{2.10}$$

e

$$\begin{aligned} \mathcal{T}r_{\mathbb{Q}(\zeta_p)}((\alpha - a_0)\zeta_p^{-1}(1-\zeta_p)) &= a_1\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(1-\zeta_p) + a_2\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p - \zeta_p^2) \\ &+ \ldots + a_{p-2}\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(\zeta_p^{p-3} - \zeta_p^{p-2}). \end{aligned}$$

Novamente, pelo Lema 2.4.3, $\mathcal{T}r_{\mathbb{Q}(\zeta_p)}((\alpha-a_0)\zeta_p^{-1}(1-\zeta_p)) \in p\mathbb{Z}$. Portanto, $a_1\mathcal{T}r_{\mathbb{Q}(\zeta_p)}(1-\zeta_p) = a_1 p \in p\mathbb{Z}$, com $a_1 \in \mathbb{Z}$. Repetindo o mesmo processo concluímos que $a_i \in \mathbb{Z}$, para todo $i = 1, \ldots, n$. Portanto, $\alpha \in \mathbb{Z}[\zeta_p]$, e consequentemente, $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{K}}$.

□

Corolário 2.4.1 ([30], p. 43) *O conjunto $\mathcal{B} = \{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ é uma base integral para $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ como $\mathbb{Z}$-módulo.*

Demonstração: Pelo Teorema 2.4.1, o conjunto $\mathcal{B}$ é uma base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ como $\mathbb{Z}$-módulo, portanto, é uma base integral.

□

Exemplo 2.4.1 *Se $\mathbb{K} = \mathbb{Q}(\zeta_5)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_5]$ e uma base integral para $\mathcal{O}_{\mathbb{K}}$ é $\mathcal{B} = \{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$.*

O Teorema 2.4.1 finaliza a caracterização do anel de inteiros de um p-ésimo corpo ciclotômico. Em geral, para uma raiz n-ésima primitiva da unidade, o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ conforme enunciamos abaixo.

Teorema 2.4.2 ([36], p. 63) *Se $n \in \mathbb{Z}$ é um inteiro positivo, $n > 2$, e ζ_n é uma raiz n-ésima primitiva da unidade, então $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ e $\mathcal{B} = \{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como $\mathbb{Z}$-módulo.*

2.5 Discriminante de corpos quadráticos e ciclotômicos

Finalizamos o capítulo com esta seção que tem como objetivo expressar o discriminante de corpos quadráticos e ciclotômicos.

Proposição 2.5.1 ([34], p. 63) *Seja $d \in \mathbb{Z}$ livre de quadrados. Então o discriminante de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é dado por*

(i) $\mathcal{D}_{\mathbb{Q}(\sqrt{d})} = d$, *se* $d \equiv 1 \ (mod\ 4)$,

(ii) $\mathcal{D}_{\mathbb{Q}(\sqrt{d})} = 4d$, *se* $d \not\equiv 1 \ (mod\ 4)$.

Demonstração: Se $d \equiv 1 \ (mod\ 4)$, então o conjunto $\mathcal{B} = \left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ é uma base integral de $\mathbb{Q}(\sqrt{d})$. Como os monomorfismos de $\mathbb{Q}(\sqrt{d})$ são $\sigma_1 = id$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$, então

$$\begin{aligned}\mathcal{D}_{\mathbb{Q}(\sqrt{d})} &= \mathcal{D}_{\mathbb{Q}(\sqrt{d})}\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\dfrac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\dfrac{1+\sqrt{d}}{2}\right) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & 1 \\ \dfrac{1+\sqrt{d}}{2} & \dfrac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d.\end{aligned}$$

Caso contrário, se $d \not\equiv 1 \ (mod\ 4)$, então $\mathcal{B} = \{1, \sqrt{d}\}$ é uma base integral para $\mathbb{Q}(\sqrt{d})$. Sendo assim,

$$\mathcal{D}_{\mathbb{Q}(\sqrt{d})} = \mathcal{D}_{\mathbb{Q}(\sqrt{d})}\left(1, \sqrt{d}\right) = \begin{vmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

□

Exemplo 2.5.1 *Considere o corpo quadrático* $\mathbb{Q}(\sqrt{17})$. *Como* $17 \equiv 1 \ (mod\ 4)$, *pela Proposição 2.5.1, seu discriminante* $\mathcal{D}_{\mathbb{Q}(\sqrt{17})}$ *é* 17. *O discriminante do corpo gaussiano* $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ *é* $\mathcal{D}_{\mathbb{Q}(i)} = -4$, *uma vez que* $-1 \not\equiv 1 \ (mod\ 4)$.

Assim como na Seção 2.4, também enfatizamos os p-ésimos corpos ciclotômicos para o cálculo do discriminante e enunciamos o resultado para o caso geral. A próxima proposição caracteriza o discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_p)$.

Proposição 2.5.2 ([34], p. 68) *Se* ζ_p *é uma raiz* p*-ésima primitiva da unidade,* $p > 2$, *então o discriminante de* $\mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é*

$$\mathcal{D}_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}. \tag{2.11}$$

Demonstração: Pelo Corolário 2.4.1, $\mathcal{B} = \{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base integral de $\mathcal{O}_{\mathbb{K}}$ e consequentemente, também é uma base de $\mathbb{K}$. Assim, pela Proposição 1.4.3,

$$\mathcal{D}_{\mathbb{Q}(\zeta_p)} = \mathcal{D}_{\mathbb{Q}(\zeta_p)}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} \mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\Phi_p'(\zeta_p)),$$

sendo $\Phi_p'(x)$ a derivada do p-ésimo polinômio ciclotômico $\Phi_p(x)$ que é dado como na Observação 2.3.1,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Derivando-o e avaliando em $x = \zeta_p$, obtemos

$$\Phi_p'(x) = \frac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2} \Rightarrow \Phi_p'(\zeta_p) = \frac{(\zeta_p - 1)p\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2}.$$

Como $\zeta_p^p = 1$, visto que ζ_p é uma raiz p-ésima da unidade, então

$$\Phi_p'(\zeta_p) = \frac{(\zeta_p - 1)p\zeta_p^{p-1}}{(\zeta_p - 1)^2} = \frac{p\zeta_p^{p-1}}{\zeta_p - 1} = \frac{-p\zeta_p^{p-1}}{1 - \zeta_p}.$$

Assim, aplicando a norma, usando sua linearidade e o item (iii) do Lema 2.3.1 no denominador, concluímos que

$$\begin{aligned} \mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\Phi_p'(\zeta_p)) &= \mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}\left(\frac{-p\zeta_p^{p-1}}{1 - \zeta_p}\right) = \frac{\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(-p)\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p)^{p-1}}{\mathcal{N}_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p)} \\ &= \frac{(-p)^{p-1}1^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

Ademais, como p é ímpar, $(-1)^{p-2} = -1$, logo, $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Portanto,

$$\mathcal{D}_{\mathbb{Q}(\zeta_p)} = \mathcal{D}_{\mathbb{Q}(\zeta_p)}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

□

Exemplo 2.5.2 *Seja $p = 3 \in \mathbb{Z}$ e considere $\mathbb{K} = \mathbb{Q}(\zeta_3)$. Como 3 é primo, pelo Teorema 2.5.2, temos que $\mathcal{D}_{\mathbb{Q}(\zeta_3)} = (-1)^{\frac{3-1}{2}} 3^{3-2} = (-1)^1 3^1 = -3$.*

No caso geral, isto é, para uma raiz n-ésima primitiva da unidade, o discriminante é dado como no teorema que segue.

Teorema 2.5.1 ([37], p. 12) *Seja $n \in \mathbb{Z}$ um inteiro positivo, com $n > 1$. Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então o discriminante de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{K}}(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Considerações Finais

Assim como no Capítulo 1, selecionamos aqui alguns resultados de acordo com sua relevância para o desenvolvimento dos próximos e principais capítulos do trabalho. Muitos estudos sobre os n-ésimos corpos ciclotômicos investigam com detalhes os casos $n = p$, $n = p^r$, com $r \in \mathbb{Z}$ um inteiro positivo, e o caso geral.

Uma vez apresentados estes conceitos damos início ao estudo dos reticulados. A classificação do anel de inteiros, assim como do discriminante, de corpos quadráticos e ciclotômicos é vital para a construção de reticulados algébricos, conceito que definimos no próximo capítulo.

Capítulo

3

Reticulados

Neste capítulo apresentamos os principais resultados e propriedades da Teoria de Reticulados. Essa teoria possui inúmeras aplicações, em especial na Teoria de Códigos, a qual consiste em transformar informações em objetos matemáticos, e consequentemente, usufruir das propriedades associadas a estes objetos, e na Criptografia, a qual consiste em proteger informações.

Pode-se dizer que o estudo de reticulados surgiu com o admirável e clássico problema de empacotamento esférico que descrevemos na Seção 3.2, que consiste em organizar esferas n-dimensionais de mesmo raio não sobrepostas entre si no $\mathbb{R}^n$, para que a maior proporção possível de espaço seja coberta.

Nas Seções 3.3 e 3.4 estudamos os homomorfismos canônico e torcido, o quais são métodos clássicos da literatura que nos permitem construir reticulados através de ideais e de $\mathbb{Z}$-módulos do anel do inteiros de um corpo de números algébricos, os chamados reticulados algébricos. Essas seções são de suma importância para as análises e construções de reticulados bem arredondados que exibimos no Capítulo 5, sendo necessário o desenvolvimento de propriedades relacionadas a tais homomorfismos. Podemos inferir inúmeras características aos reticulados obtidos dessa maneira, utilizando conceitos presentes no Capítulo 1 deste trabalho. Algumas das referências relevantes sobre o tema desenvolvido neste capítulo são [6], [11], [30], [33] e [34].

3.1 Reticulados no $\mathbb{R}^n$

Nesta seção são apresentados conceitos básicos da teoria de reticulados como matriz geradora e matriz de Gram, bem como os conceitos de sub-reticulado, região fundamental e volume de

um reticulado, essenciais para o desenvolvimento do capítulo. No fim da seção, apresentamos uma relação de equivalência no conjunto de reticulados no $\mathbb{R}^n$.

Definição 3.1.1 *Seja $\mathcal{B} = \{v_1, \ldots, v_m\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, $m \leq n$. Um **reticulado** com base $\mathcal{B}$ e dimensão m é o subconjunto do $\mathbb{R}^n$ da forma*

$$\Lambda = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{m} a_i v_i, \text{ com } a_i \in \mathbb{Z} \right\}.$$

*Se $m = n$, dizemos que Λ é um **reticulado completo** ou de **posto completo** e que $\mathcal{B} = \{v_1, \ldots, v_n\}$ é uma base completa do reticulado.*

Observação 3.1.1 *Um reticulado Λ pode ser expresso como*

$$\Lambda = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m,$$

ou seja, um reticulado é um $\mathbb{Z}$-módulo livre de posto finito contido no $\mathbb{R}^n$, cuja base é linearmente independente sobre $\mathbb{R}$.

Exemplo 3.1.1 *O conjunto $\mathcal{B} = \{(1,0),(0,1)\}$ é uma base para o reticulado $\Lambda = \mathbb{Z}^2 \subset \mathbb{R}^2$, conforme a Figura 3.1.*

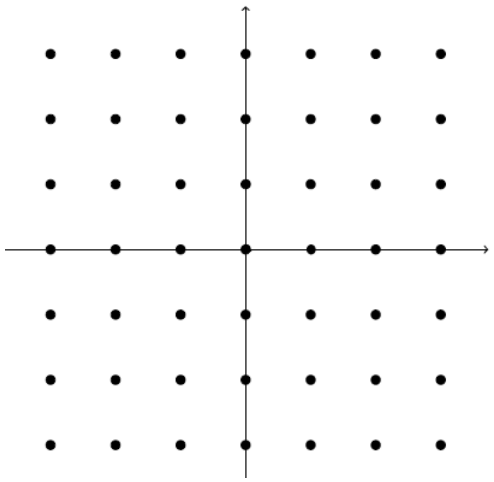

Figura 3.1: Reticulado $\Lambda = \mathbb{Z}^2$
Fonte: Elaborado pelo autor

Neste caso, o conjunto $\mathcal{B}' = \{(2,1),(-1,0)\}$ também é uma base para o reticulado $\mathbb{Z}^2$ e como justificamos ainda nesta seção, um reticulado possui mais de uma base. Em geral, o reticulado $\Lambda = \mathbb{Z}^n \subset \mathbb{R}^n$ é um exemplo de reticulado n-dimensional.

Exemplo 3.1.2 *O segundo reticulado que apresentamos é o célebre reticulado hexagonal* $\Lambda_{hex} \subset \mathbb{R}^2$*, que pode ser gerado por* $\mathcal{B} = \left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$ *e é imprescindível para o desenvolvimento deste trabalho. A Figura 3.2 representa* Λ_{hex}*.*

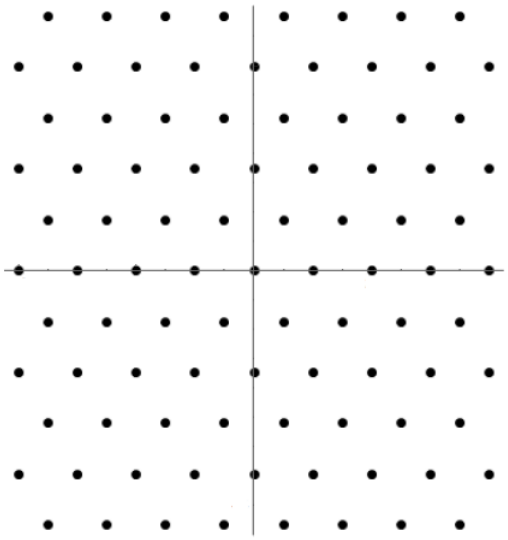

Figura 3.2: Reticulado Hexagonal $\Lambda_{hex} \subset \mathbb{R}^2$
Fonte: Elaborado pelo autor

Exemplo 3.1.3 *Um dos principais reticulados em* $\mathbb{R}^n$*, para* $n \geq 1$*, que não admite posto completo é o reticulado*

$$A_n = \{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid x_1 + x_2 + \ldots + x_{n+1} = 0\}.$$

No caso $n = 2$*, temos* $A_2 = \{(x_1, x_2, x_3) \in \mathbb{Z}^3 \mid x_1 + x_2 + x_3 = 0\}$*, que admite como uma de suas bases o conjunto* $\mathcal{B} = \{(1,0,-1), (0,1,-1)\}$ *e possui posto* 2 *em* $\mathbb{R}^3$*. O reticulado* A_2 *coincide com o reticulado hexagonal apresentado no Exemplo 3.1.2.*

Exemplo 3.1.4 *O conjunto* D_n *definido por*

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

também representa um reticulado em $\mathbb{R}^n$*. No caso* $d = 3$*, o reticulado* D_3*, conhecido como reticulado cúbico de face centrada, tem como base o conjunto* $\mathcal{B} = \{(2,0,0), (1,1,0), (1,0,1)\}$*.*

Definição 3.1.2 *Seja Λ um reticulado de $\mathbb{R}^n$ com base $\mathcal{B} = \{v_1, v_2, \ldots, v_m\}$, onde $m \leq n$. O conjunto*

$$\mathcal{P} = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{m} \lambda_i v_i,\ 0 \leq \lambda_i < 1 \right\}$$

*é chamado de **região fundamental** do reticulado Λ com relação a base $\mathcal{B}$.*

Exemplo 3.1.5 *No Exemplo 3.1.1 o quadrado cujos vértices são os pontos $(0,0)$, $(0,1)$, $(1,1)$ e $(1,0)$, exceto pelas arestas que ligam os pontos $(0,1)$ e $(1,1)$ e os pontos $(1,0)$, $(1,1)$ formam a região fundamental do reticulado $\Lambda = \mathbb{Z}^2$ conforme mostra a Figura 3.3.*

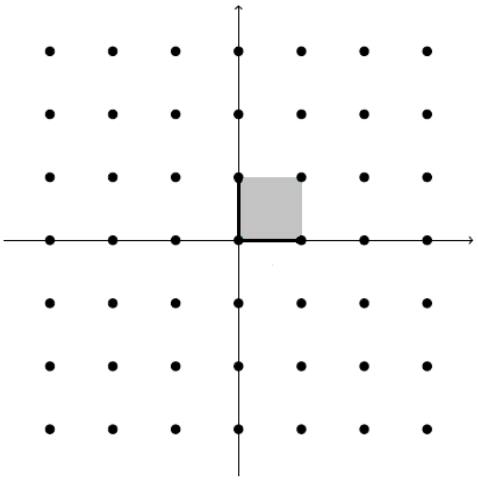

Figura 3.3: Região Fundamental de $\Lambda = \mathbb{Z}^2$
Fonte: Elaborado pelo autor

A região fundamental de um reticulado, também conhecida como região de Voronoi do reticulado, é um importante conceito para o desenvolvimento do problema de empacotamento esférico. Essa região nos permite construir uma decomposição de $\mathbb{R}^n$ por meio de uma translação pelos elementos de Λ.

O próximo resultado formaliza este fato.

Lema 3.1.1 ([34], p. 131) *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com região fundamental $\mathcal{P}$. Então cada elemento de $\mathbb{R}^n$ pertence a exatamente uma região $\mathcal{P} + l$, onde $l \in \Lambda$. Consequentemente,*

$$\mathbb{R}^n = \bigcup_{l \in \Lambda} \mathcal{P} + l.$$

Como é evidente pela Definição 3.1.2 e pelo Lema 3.1.1, essa decomposição é disjunta.

Definição 3.1.3 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\mathcal{B} = \{v_1, \ldots, v_m\}$, onde $m \leq n$. A* ***matriz geradora*** *do reticulado Λ é definida como sendo a matriz*

$$M = \begin{pmatrix} v_{11} & v_{21} & \cdots & v_{m1} \\ v_{12} & v_{22} & \cdots & v_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \cdots & v_{mn} \end{pmatrix},$$

onde $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para $i = 1, \ldots, m$, isto é, a matriz que admite como colunas os vetores da base $\mathcal{B}$. A matriz $G = M^t M$ é chamada de ***matriz de Gram*** *associada a matriz geradora, em que t denota a transposição de matrizes.*

Observamos que se M é uma matriz geradora de um reticulado $\Lambda \subset \mathbb{R}^n$ com base $\mathcal{B} = \{v_1, \ldots, v_m\}$, então podemos representá-lo da forma

$$\Lambda = \{M\lambda \mid \lambda \in \mathbb{Z}^m\}, \tag{3.1}$$

em que λ é um vetor de tamanho $m \times 1$.

Damos ênfase ao estudo de reticulados completos, sendo assim, por simplicidade, muitas vezes chamamos um reticulado completo apenas por reticulado.

Se $\Lambda \subset \mathbb{R}^n$ admite como base um conjunto de vetores $\mathcal{B}$, então uma condição necessária e suficiente para que um outro conjunto de vetores linearmente independentes $\mathcal{C}$ de $\mathbb{R}^n$ também seja uma base é que os vetores de $\mathcal{C}$ sejam vetores de Λ, ou seja, $\mathcal{C} \subset \Lambda$ e a matriz mudança de base de $\mathcal{B}$ para $\mathcal{C}$ possua entradas inteiras e determinante ± 1, fato que é justificado no próximo resultado.

Proposição 3.1.1 ([36], p. 94) *Sejam $\mathcal{B} = \{v_1, \ldots, v_n\} \subset \mathbb{R}^n$ uma base para um reticulado $\Lambda \subset \mathbb{R}^n$ e $\mathcal{C} = \{u_1, \ldots, u_n\}$ um conjunto de vetores de Λ linearmente independentes sobre $\mathbb{R}$ tal que*

$$u_i = \sum_{j=1}^{n} a_{ij} v_j,$$

com $a_{ij} \in \mathbb{Z}$. Então, $\mathcal{C}$ é uma base de Λ se, e somente se, $det(a_{ij}) = \pm 1$.

Demonstração: De fato, sejam $\mathcal{B} = \{v_1, \ldots, v_n\} \subset \mathbb{R}^n$ uma base de um reticulado Λ e $\mathcal{C} = \{u_1, \ldots, u_n\}$ um conjunto de vetores de Λ linearmente independentes sobre $\mathbb{R}$ tal que

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

O conjunto $\mathcal{C} = \{u_1, \ldots, u_n\}$ é uma base para Λ se, e somente se, a matriz $M = (a_{ij})$ é uma matriz de mudança de base, ou seja, é invertível. Equivalentemente, $\mathcal{C}$ é uma base para Λ se, e somente se, $det(a_{ij}) = \pm 1$.

□

Definição 3.1.4 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado, $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ uma base de Λ e $\mathcal{P}$ a região fundamental de Λ. O **volume da região fundamental** é definido como $\mathcal{V}ol(\mathcal{P}) = |det(M)|$, em que M é uma matriz geradora de Λ.*

Proposição 3.1.2 ([30], p. 55) *O volume da região fundamental de um reticulado $\Lambda \subset \mathbb{R}^n$ independe da escolha da base do reticulado.*

Demonstração: É uma consequência imediata da Proposição 3.1.1.

□

Como comentamos anteriormente, um reticulado possui diferentes bases e, por consequência, diferentes matrizes de Gram. Todavia, o determinante de cada matriz de Gram é o mesmo, pois independe da base escolhida.

Proposição 3.1.3 ([36], p. 95) *Se $\Lambda \subset \mathbb{R}^n$ é um reticulado com matriz de Gram G em relação a uma base $\mathcal{B}$, e G', em relação a uma base $\mathcal{B}'$, então $det(G) = det(G')$.*

Demonstração: Considere A a matriz de mudança de base de $\mathcal{B}$ para $\mathcal{B}'$. Se B e B' são as matrizes geradoras de Λ em relação a $\mathcal{B}$ e $\mathcal{B}'$, respectivamente, então $B' = AB$ e $|det(A)| = 1$. Logo, utilizando propriedades de determinante obtemos

$$\begin{aligned} det(G') &= det(B'^t B') = det(B^t A^t A B) = det(B^t) det(A^t) det(A) det(B) \\ &= det(B^t) det(B) = det(B^t B) = det(G). \end{aligned}$$

□

Devido a Proposição 3.1.3 o determinante do reticulado é definido como o determinante de uma matriz de Gram. Em moldes formais, temos a seguinte definição.

Definição 3.1.5 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. O determinante de Λ é o determinante de uma matriz de Gram de Λ,*

$$det(\Lambda) = det(G).$$

Definição 3.1.6 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$. O **volume do reticulado** Λ é definido como $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P})$.*

Note que se $\Lambda \subset \mathbb{R}^n$ é um reticulado de posto completo com matriz geradora M e matriz de Gram G, então $det(\Lambda) = det(G) = det(M^tM) = det(M^t)det(M) = (det(M))^2 = \mathcal{V}ol(\Lambda)^2$.

Exemplo 3.1.6 *Seja $\Lambda \subset \mathbb{R}^3$ o reticulado gerado por $\mathcal{B} = \{(1,0,3),(2,1,0),(1,1,-1)\}$, então o volume de Λ é dado por*

$$\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P}) = \left| det \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 3 & 0 & -1 \end{pmatrix} \right| = |2| = 2.$$

As definições apresentadas acima são fundamentais para o desenvolvimento da Seção 3.2. Primeiro, porém, apresentamos os conceitos de sub-reticulado e alguns exemplos.

Definição 3.1.7 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado, M sua matriz geradora e B uma matriz de ordem n e coordenadas inteiras. Um **sub-reticulado** de Λ é um reticulado dado por*

$$\Lambda' = \{MB\lambda \mid \lambda \in \mathbb{Z}^n\}.$$

Indubitavelmente os pontos de Λ' são pontos de Λ, ou seja, $\Lambda' \subseteq \Lambda$. No contexto de reticulados de posto completo, para um sub-reticulado Λ' também de posto completo, isto é, de mesmo posto que Λ, é corriqueiro nos referirmos ao índice de um sub-reticulado, o qual é definido como o quociente $\dfrac{det(\Lambda')}{det(\Lambda)}$.

Exemplo 3.1.7 *Em $\mathbb{R}^2$ o conjunto $\Lambda' = 2\mathbb{Z}^2$ formado por todas as coordenadas inteiras pares é um sub-reticulado de $\Lambda = \mathbb{Z}^2$. Neste caso, uma matriz geradora para Λ é*

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e tomando $B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ obtemos Λ' conforme a Figura 3.4.

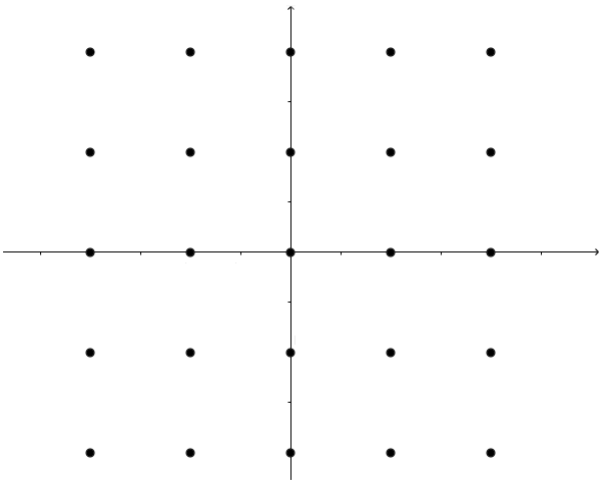

Figura 3.4: Sub-reticulado $\Lambda' = 2\mathbb{Z}^2 \subset \mathbb{Z}^2$
Fonte: Elaborado pelo autor

Exemplo 3.1.8 *O reticulado* $\Omega \subset \mathbb{R}^2$ *dado por*

$$\Omega = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x, y \in \mathbb{Z} \right\}$$

também é um sub-reticulado de $\Lambda = \mathbb{Z}^2$*. A Figura 3.5 representa este reticulado.*

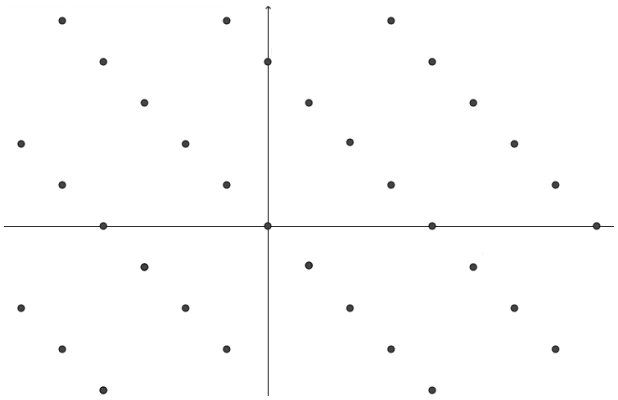

Figura 3.5: Reticulado $\Omega \subset \mathbb{R}^2$
Fonte: Elaborado pelo autor

Para concluir a seção exibimos o conceito de reticulados semelhantes mediante a relação de equivalência definida a seguir.

Definição 3.1.8 *Sejam $n \geq 2$ um inteiro e $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ reticulados de posto completo. Se existe uma matriz ortogonal real A de ordem n e uma constante $\alpha \in \mathbb{R}$ tal que $\Lambda_1 = \alpha A\Lambda_2$, dizemos que Λ_1 e Λ_2 são **semelhantes**, ou **equivalentes**, e denotamos por $\Lambda_1 \sim \Lambda_2$.*

Exemplo 3.1.9 *O reticulado $\Lambda' = 2\mathbb{Z}^2$ apresentado nos Exemplos 3.1.7 é semelhante a $\Lambda = \mathbb{Z}^2$. Neste caso, a matriz ortogonal da Definição 3.1.8 é a matriz identidade de ordem 2, I_2, e a constante é $\alpha = 2$.*

De modo geral, se $\Lambda \subset \mathbb{R}^n$ é um reticulado e $\alpha \in \mathbb{R}$ é uma constante, então os reticulados Λ e $\Lambda_\alpha = \alpha\Lambda$ são semelhantes, em que o reticulado Λ_α é obtido multiplicando todos os vetores de Λ pela constante α. Dizemos, neste caso, que Λ_α é um reticulado escalonado, ou uma versão escalonada, do reticulado Λ. Se $\alpha \in \mathbb{Z}$, então $\Lambda_\alpha \subseteq \Lambda$ é um sub-reticulado.

Observação 3.1.2 *A semelhança entre reticulados é uma relação de equivalência sobre o conjunto dos reticulados em $\mathbb{R}^n$. De fato, sejam $\Lambda_1, \Lambda_2, \Lambda_3 \subset \mathbb{R}^n$ reticulados de posto completo.*

(i) Temos que $\Lambda_1 \sim \Lambda_1$, uma vez que $\Lambda_1 = 1 \cdot I_n \cdot \Lambda_1$, onde I_n é a matriz identidade de ordem n.

(ii) Se $\Lambda_1 \sim \Lambda_2$, então $\Lambda_1 = \alpha A\Lambda_2$, com $\alpha \in \mathbb{R}$, obviamente podemos supor $\alpha \neq 0$, e $A \in M_n(\mathbb{R})$ uma matriz ortogonal. Assim,

$$A^t\Lambda_1 = A^t(\alpha A\Lambda_2) = \alpha(A^tA)\Lambda_2 = \alpha I_n\Lambda_2 \Rightarrow \Lambda_2 = \alpha^{-1}A^t\Lambda_1,$$

onde I_n é a matriz identidade de ordem n, $\alpha^{-1} \in \mathbb{R}$ e A^t é uma matriz ortogonal. Portanto, $\Lambda_2 \sim \Lambda_1$.

(iii) Por fim, se $\Lambda_1 \sim \Lambda_2$ e $\Lambda_2 \sim \Lambda_3$, então existem elementos não nulos $\alpha, \beta \in \mathbb{R}$ e $A, B \in M_n(\mathbb{R})$ matrizes ortogonais tais que $\Lambda_1 = \alpha A\Lambda_2$ e $\Lambda_2 = \beta B\Lambda_3$. Então

$$A^t\Lambda_1 = \alpha(A^tA)\Lambda_2 = \alpha I_n\Lambda_2 \Rightarrow \Lambda_2 = \alpha^{-1}A^t\Lambda_1. \tag{3.2}$$

Como $\Lambda_2 = \beta B\Lambda_3$, substituindo na Equação (3.2), temos

$$\alpha^{-1}A^t\Lambda_1 = \beta B\Lambda_3 \Rightarrow A^t\Lambda_1 = (\alpha\beta)B\Lambda_3 \Rightarrow AA^t\Lambda_1 = (\alpha\beta)AB\Lambda_3 \Rightarrow I_n\Lambda_1 = \Lambda_1 = (\alpha\beta)AB\Lambda_3,$$

onde I_n é a matriz identidade de ordem n, $\alpha\beta \in \mathbb{R}$ e AB é uma matriz ortogonal, uma vez que o produto de matrizes ortogonais é também uma matriz ortogonal. Portanto, $\Lambda_1 \sim \Lambda_3$, e assim,

a semelhança é uma relação de equivalência. As classes de equivalências dos reticulados são chamadas de classes de semelhança e a constante α é chamada de razão de semelhança.

A relação de equivalência apresentada na Definição 3.1.8 é muito importante para o desenvolvimento dos Capítulos 4 e 5. Existem muitos outros reticulados em diversas dimensões, além dos que exemplificamos nesta seção. Os conceitos que apresentamos na próxima seção nos permitem classificar alguns destes reticulados de acordo com critérios que apresentamos.

3.2 Empacotamento reticulado

Nesta seção apresentamos o problema de empacotamento. Conforme descrevemos anteriormente neste capítulo, o problema de empacotamento consiste em dispor esferas n-dimensionais de mesmo raio no $\mathbb{R}^n$ de modo a cobrir o maior espaço possível. Estamos interessados, particularmente, em empacotamentos cujos centros das esferas formam um reticulado, os chamados empacotamentos reticulados.

A importância do empacotamento reticulado se dá principalmente pelo fato de em algumas dimensões como 1, 2, 8 e 24, os empacotamentos mais densos possíveis, isto é, que cobrem a maior parte do espaço, são atingidos por empacotamentos reticulados.

Definição 3.2.1 *A **norma de um reticulado** $\Lambda \subset \mathbb{R}^n$ é definida por*

$$|\Lambda| = min\{||x|| \mid x \in \Lambda, x \neq 0\}, \tag{3.3}$$

em que $||\cdot||$ é a norma euclidiana usual em $\mathbb{R}^n$.

Definição 3.2.2 *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.*

Observamos que para descrever um empacotamento podemos indicar apenas o conjunto dos centros das esferas e o raio de uma e, por consequência, de todas as esferas.

Definição 3.2.3 *Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ em $\mathbb{R}^n$.*

Definição 3.2.4 *Dado um empacotamento associado a um reticulado $\Lambda \subset \mathbb{R}^n$ com base $\mathcal{B} = \{v_1, v_2 \ldots, v_n\}$, a **densidade de empacotamento** de Λ, denotada por $\Delta(\Lambda)$ é definida como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas de raio r.*

O valor $\rho = \dfrac{|\Lambda|}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de um reticulado $\Lambda \subset \mathbb{R}^n$ e obter um empacotamento. Sendo assim, o estudo de empacotamentos reticulado traduz-se ao estudo de reticulados. Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de Λ é igual a

$$\Delta(\Lambda) = \frac{\textit{Volume da região coberta pelas esferas}}{\textit{Volume da região fundamental}} = \frac{\mathcal{V}ol(\mathcal{B}(\rho))}{\mathcal{V}ol(\Lambda)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)}, \tag{3.4}$$

$$\text{onde } \mathcal{V}ol(\mathcal{B}(1)) = \begin{cases} \dfrac{\pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)!}, \text{ se } n \text{ é par} \\ \\ \dfrac{2^n \pi^{\left(\frac{n-1}{2}\right)} \left(\frac{n-1}{2}\right)!}{n!}, \text{ se } n \text{ é ímpar.} \end{cases}$$

Definição 3.2.5 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. A **densidade de centro** de Λ é definida por*

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)}, \tag{3.5}$$

onde $\mathcal{V}ol(\Lambda)$ é o volume e ρ é o raio de empacotamento de Λ.

Exemplo 3.2.1 *Considere o reticulado $\Lambda \subset \mathbb{R}^2$ com base $\mathcal{B} = \{(1,0),(0,2)\}$. O raio de empacotamento de Λ é $\rho = \dfrac{1}{2}$ e $\mathcal{V}ol(\mathcal{B}(1)) = \pi$. Logo, o volume do reticulado é $\mathcal{V}ol(\Lambda) = 2$, a densidade de empacotamento é*

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^2}{\mathcal{V}ol(\Lambda)} = \frac{\pi\left(\frac{1}{2}\right)^2}{2} = \frac{\pi}{8}$$

e a densidade de centro é $\delta(\Lambda) = \dfrac{1}{8}$.

Exemplo 3.2.2 *Os reticulados n dimensionais A_n e D_n, para $n \geq 3$, apresentados nos Exemplos 3.1.3 e 3.1.4, respectivamente, admitem mesmo raio de empacotamento, $\rho = \dfrac{\sqrt{2}}{2}$. As respectivas densidades de centro são $\delta(A_n) = 2^{-\frac{n}{2}}(n+1)^{-\frac{1}{2}}$ e $\delta(D_n) = 2^{-\frac{n+2}{2}}$.*

Exemplo 3.2.3 *Para determinar a densidade de empacotamento do reticulado hexagonal Λ_{hex} observamos que sua matriz geradora é*

$$M = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix},$$

cujo determinante é $det(M) = \frac{\sqrt{3}}{2}$ *e corresponde ao volume do reticulado,* $\mathcal{V}ol(\Lambda_{hex})$. *Como* $|\Lambda_{hex}| = 1$, *segue que o raio de empacotamento é* $\rho = \frac{|\Lambda_{hex}|}{2} = \frac{1}{2}$ *e o volume da circunferência euclidiana de raio* ρ *é* π. *Portanto,*

$$\Delta(\Lambda_{hex}) = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^2}{\mathcal{V}ol(\Lambda)} = \frac{\pi\left(\frac{1}{2}\right)^2}{\frac{\sqrt{3}}{2}} = \frac{\pi}{2\sqrt{3}} = 0,906899... \ .$$

Para a dimensão $n = 2$, ou seja, em $\mathbb{R}^2$, o reticulado hexagonal é o melhor reticulado em termos de densidade de empacotamento. No que se refere a características de um reticulado, a densidade de empacotamento é uma das mais importantes. No Capítulo 4 exibimos e provamos com formalidade o fato de que o reticulado hexagonal admite a melhor densidade de empacotamento dentre todos os reticulados bidimensionais.

A próxima proposição afirma que reticulados equivalentes de acordo com a Definição 3.1.8 possuem a mesma densidade de empacotamento.

Proposição 3.2.1 ([8], p. 20) *Sejam* Λ_1 *e* Λ_2 *dois reticulados em* $\mathbb{R}^n$. *Se* $\Lambda_1 \sim \Lambda_2$, *então ambos possuem a mesma densidade de empacotamento, ou seja,* $\Delta(\Lambda_1) = \Delta(\Lambda_2)$.

Demonstração: Como $\Lambda_1 \sim \Lambda_2$, existem uma matriz ortogonal real A e uma constante $\alpha \in \mathbb{R}$ tal que $\Lambda_2 = \alpha A\Lambda_1$. Se ρ_1 e ρ_2 são os raios de empacotamento de Λ_1 e Λ_2, respectivamente, então

$$\rho_2 = \frac{|\Lambda_2|}{2} = \frac{\alpha|\Lambda_1|}{2} = \alpha\rho_1.$$

Ou seja, o raio de empacotamento de Λ_2 é $\rho_2 = \alpha\rho_1$. Além disso, se M é a matriz geradora de Λ_1, então αAM é a matriz geradora de Λ_2 e

$$\begin{aligned} |det(\alpha AM)| &= |det(\alpha I_n)det(A)det(M)| = |det(\alpha I_n)||det(A)||det(M)| \\ &= |\alpha^n||-1||det(M)| \\ &= |\alpha^n det(M)|, \end{aligned}$$

o que nos permite concluir que $|det(\Lambda_2)| = |\alpha^n||det(\Lambda_1)|$. Logo, a densidade de empacotamento

é

$$\Delta(\Lambda_2) = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho_2^n}{\mathcal{V}ol(\Lambda_2)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho_2^n}{|det(\Lambda_2)|} = \frac{\mathcal{V}ol(\mathcal{B}(1))(\alpha\rho_1)^n}{|\alpha^n||det(\Lambda_1)|} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho_1^n}{\mathcal{V}ol(\Lambda_1)} = \Delta(\Lambda_1).$$

□

3.3 Homomorfismo canônico

Nesta seção apresentamos o homomorfismo canônico, descrito por Hermann Minkowski[1], o qual representa uma ferramenta fundamental para este trabalho e que nos fornece um método para obtenção de reticulados em $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números e são chamados de reticulados algébricos. Os conceitos desenvolvidos nessa seção estão disponíveis em [34], [30] e [11].

Conforme o Teorema 1.1.2, sabemos que dado um corpo de números $\mathbb{K}$ de grau n, existem n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$. Seja $\mu : \mathbb{C} \to \mathbb{C}$ a conjugação complexa, isto é, $\mu(i) = -i$. Assim, para qualquer $1 \leq j \leq n$, temos que $\mu \circ \sigma_j = \sigma_k$, $1 \leq k \leq n$. Além disso, $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, ou seja, se σ_j é um monomorfismo real de $\mathbb{K}$ de acordo com a Definição 1.1.4.

Consideramos r_1 o número de índices j tais que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Sendo assim, $n - r_1$ é um número par, ou seja, existe um número natural r_2 tal que $n = r_1 + 2r_2$, que corresponde a metade do número de monomorfismos complexos de $\mathbb{K}$. Podemos renumerar convenientemente os monomorfismos por σ_j, com $1 \leq j \leq r_1$, se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, e $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$, para $r_1 + 1 \leq j \leq r_1 + r_2$. Devido a renumeração citada acima, os primeiros $r_1 + r_2$ determinam os últimos r_2.

Uma vez dispostos os n monomorfismos de um corpo $\mathbb{K}$ de grau n podemos definir o homomorfismo canônico.

Definição 3.3.1 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$. O **homomorfismo de Minkowski** ou **homomorfismo canônico**, $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$, é definido por*

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

em que r_1 é o número de índices j tais que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, com $1 \leq j \leq r_1$, isto é, o número de monomorfismos reais de $\mathbb{K}$ e r_2 tal que $r_1 + 2r_2 = n$.

O homomorfismo canônico nos fornece uma representação geométrica de um corpo de números, a qual está associada a um reticulado, como descrito no Teorema 3.3.1.

[1] Matemático alemão (12/01/1909 - 22/06/1984) com enorme contribuição a Teoria dos Números

Exemplo 3.3.1 *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, *então* $r_1 = 2$ *e* $r_2 = 0$ *e os monomorfismos de* $\mathbb{K}$ *são dados por* $\sigma_1 = id$ *e* $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$, *com* $a, b \in \mathbb{Q}$. *Deste modo, para qualquer* $\alpha = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, *o homomorfismo canônico é dado por*

$$\sigma_{\mathbb{Q}(\sqrt{3})}(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha)) = (a + b\sqrt{3}, a - b\sqrt{3}).$$

Exemplo 3.3.2 *Se* $\mathbb{K} = \mathbb{Q}(i)$ *é o corpo gaussiano, então* $r_1 = 0$ *e* $r_2 = 1$ *e os monomorfismos de* $\mathbb{K}$ *são dados por* $\sigma_1 = id$ *e* $\sigma_2(a + bi) = a - bi$, *com* $a, b \in \mathbb{Q}$. *Note que* $\sigma_1 = \mu \circ \sigma_2 = \overline{\sigma_2}$ *e* $\sigma_1(\mathbb{K}), \sigma_2(\mathbb{K}) \not\subset \mathbb{R}$. *Logo, para qualquer* $\alpha = a + bi \in \mathbb{Q}(i)$, *o homomorfismo canônico é dado por*

$$\sigma_{\mathbb{Q}(i)}(\alpha) = (\Re(\alpha), \Im(\alpha)) = (a, b).$$

Exemplo 3.3.3 *Para o* 5*-ésimo corpo ciclotômico,* $\mathbb{K} = \mathbb{Q}(\zeta_5)$, *sendo* ζ_5 *uma raiz* 5*-ésima primitiva da unidade, os monomorfismos de* $\mathbb{K}$ *são os automorfismos do grupo de Galois de* $\mathbb{K}$, σ_1, σ_2, σ_3 *e* σ_4, *definidos por* $\sigma_i(\zeta_5) = \zeta_5^i$, *com* $i = 1, 2, 3, 4$. *Como* $\sigma_i(\zeta_5) \notin \mathbb{R}$, *para* $i = 1, 2, 3, 4$, *então* $\mathbb{K}$ *é um corpo totalmente complexo e assim,* $r_1 = 0$ *e* $r_2 = 2$. *Observamos que* $\mu \circ \sigma_1 = \overline{\sigma_1} = \sigma_4$ *e* $\mu \circ \sigma_2 = \overline{\sigma_2} = \sigma_3$. *Reordenando os automorfismos de modo conveniente, concluímos que o homomorfismo canônico* $\sigma_{\mathbb{Q}(\zeta_5)} : \mathbb{Q}(\zeta_5) \to \mathbb{R}^4$ *é dado por*

$$\sigma_{\mathbb{Q}(\zeta_5)}(\alpha) = (\Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)), \Re(\sigma_2(\alpha)), \Im(\sigma_2(\alpha))).$$

Teorema 3.3.1 ([30], p. 56) *Sejam* $\mathbb{K}$ *um corpo de números de grau* n, M *um* $\mathbb{Z}$*-módulo livre de posto* n *de* $\mathbb{K}$ *e* $\sigma_{\mathbb{K}}$ *o homomorfismo canônico associado a* $\mathbb{K}$. *Se* $\mathcal{B} = \{\omega_1, \omega_2, \ldots, \omega_n\}$ *é uma base de* M *como* $\mathbb{Z}$*-módulo, então* $\sigma_{\mathbb{K}}(M)$ *é um reticulado no* $\mathbb{R}^n$, *com base* $\sigma_{\mathbb{K}}(\mathcal{B}) = \{\sigma_{\mathbb{K}}(\omega_1), \sigma_{\mathbb{K}}(\omega_2), \ldots, \sigma_{\mathbb{K}}(\omega_n)\}$ *cujo volume é dado por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} \left| det_{1 \leq i,j \leq n}(\sigma_i(\omega_j)) \right|.$$

Se $\mathbb{K}$ é um corpo de números de grau n, então devido a Proposição 1.2.1 e ao Corolário 1.2.1, não só $\mathcal{O}_{\mathbb{K}}$, mas também qualquer ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n, isto é, admitem uma $\mathbb{Z}$-base de n elementos, digamos $\mathcal{B} = \{\omega_1, \omega_2, \ldots, \omega_n\}$.

Desse modo, podemos mergulhá-los em $\mathbb{R}^n$ através de $\sigma_{\mathbb{K}}$ para obter reticulados e nessas condições a matriz geradora de um reticulado algébrico é dada por

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \dots & \sigma_1(\omega_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_{r_1}(\omega_1) & \sigma_{r_1}(\omega_2) & \dots & \sigma_{r_1}(\omega_n) \\ \Re(\sigma_{r_1+1}(\omega_1)) & \Re(\sigma_{r_1+1}(\omega_1)) & \dots & \Re(\sigma_{r_1+1}(\omega_n)) \\ \Im(\sigma_{r_1+1}(\omega_1)) & \Im(\sigma_{r_1+1}(\omega_1)) & \dots & \Im(\sigma_{r_1+1}(\omega_n)) \\ \vdots & \vdots & \vdots & \vdots \\ \Re(\sigma_{r_1+r_1}(\omega_1)) & \Re(\sigma_{r_1+r_1}(\omega_1)) & \dots & \Re(\sigma_{r_1+r_1}(\omega_n)) \\ \Im(\sigma_{r_1+r_2}(\omega_1)) & \Im(\sigma_{r_1+r_2}(\omega_2)) & \dots & \Im(\sigma_{r_1+r_2}(\omega_n)) \end{pmatrix} \tag{3.6}$$

Corolário 3.3.1 ([30], p. 56) *Sejam $\mathbb{K}$ um corpo de números de grau n cujo discriminante é $\mathcal{D}_{\mathbb{K}}$ e $\sigma_{\mathbb{K}}$ o homomorfismo canônico associado a $\mathbb{K}$. Se $\mathcal{I}$ é um ideal não nulo do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{I})$ são reticulados em $\mathbb{R}^n$ com volumes dados por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}\sqrt{|\mathcal{D}_{\mathbb{K}}|} \quad e \quad \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-r_2}\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I}),$$

onde $\mathcal{N}(\mathcal{I})$ é a norma de $\mathcal{I}$.

Definição 3.3.2 *Um reticulado obtido a partir do homomorfismo de Minkowski $\sigma_{\mathbb{K}}$ associado a um corpo de números $\mathbb{K}$ é chamado de **reticulado algébrico**.*

Exemplo 3.3.4 *Seja $\mathbb{K} = \mathbb{Q}(i)$ o corpo gaussiano. Como descrito no Exemplo 2.2.1, o anel de inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$, que admite por base como $\mathbb{Z}$-módulo o conjunto $\mathcal{B} = \{1, i\}$. Pelo Exemplo 3.3.2, $r_1 = 0$, $r_2 = 1$ e para $\alpha = a + bi \in \mathbb{K}$, o homomorfismo canônico associado é $\sigma_{\mathbb{K}}(\alpha) = (a, b)$. Portanto, pelo Teorema 3.3.1, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado e como a matriz geradora de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é*

$$M = \begin{pmatrix} \Re(1) & \Re(i) \\ \Im(1) & \Im(i) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

cujo determinante é $det(M) = 1$. Logo, o volume de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dado por

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-1}|det(M)| = \frac{1}{2}.$$

O reticulado obtido através da imagem do anel de inteiros do corpo gaussiano é o reticulado $\mathbb{Z}^2$ que apresentamos no Exemplo 3.1.1.

Um dos problemas que surgem no estudo de reticulados é o de determinar a norma de seus vetores. Este fato reforça o interesse ao estudo de reticulados algébricos, uma vez que através

dos conceitos da Teoria Algébrica dos Números presentes no Capítulo 1, podemos inferir diversas características a estes reticulados, dentre elas a norma de um vetor.

O próximo resultado caracteriza a norma de um vetor através do traço do elemento correspondente a este vetor no anel de inteiros.

Proposição 3.3.1 ([12], p. 51) *Sejam $\mathbb{K}$ é um corpo de números de grau n e $\sigma_{\mathbb{K}}$ o homomorfismo canônico correspondente. Se $x \in \mathbb{K}$, então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}} \mathcal{T}r_{\mathbb{K}}(x\overline{x}), \tag{3.7}$$

onde $c_{\mathbb{K}} = \begin{cases} 1, \text{ se } \mathbb{K} \text{ for totalmente real, isto é}, r_2 = 0, \\ \dfrac{1}{2}, \text{ se } \mathbb{K} \text{ for totalmente imaginário, isto é}, r_1 = 0. \end{cases}$

Demonstração: Sejam $\sigma_1, \sigma_2, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ tal que $r_1 + 2r_2 = n$, onde r_1 é o número de monomorfismos reais e r_2 a metade do número de monomorfismos imaginários. Se $x \in \mathbb{K}$, então

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x) \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)).$$

Como $\sigma_{\mathbb{K}}(x) \in \mathbb{R}^n$, temos

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2 + (\Re\sigma_{r_1+1}(x))^2 + \ldots + (\Im\sigma_{r_1+r_2}(x))^2$$

e para $r_1 + 1 \leq j \leq r_1 + r_2$,

$$\begin{aligned} (\Re(\sigma_j(x)))^2 + (\Im(\sigma_j(x)))^2 &= \left(\frac{1}{2}\sigma_j(x) + \frac{1}{2}\overline{\sigma_j(x)}\right)^2 + \left(\frac{1}{2i}\sigma_j(x) - \frac{1}{2i}\overline{\sigma_j(x)}\right)^2 \\ &= \sigma_j(x)\overline{\sigma_j(x)} \\ &= \sigma_j(x\overline{x}). \end{aligned}$$

Sendo assim,

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

Se $r_1 = 0$, isto é, $\mathbb{K}$ é totalmente imaginário, então

$$|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \ldots + \sigma_{r_2}(x\overline{x}) = \sigma_{r_2+1}(x\overline{x}) + \ldots + \sigma_{r_2+r_2}(x\overline{x}).$$

Além disso, $\sigma_{r_2+j}(x\overline{x}) = (\mu\circ\sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, \ldots, r_2$ e μ a conjugação complexa. Logo,

$$\begin{aligned} 2|\sigma_{\mathbb{K}}(x)|^2 &= \sigma_1(x\overline{x}) + \ldots + \sigma_{r_2}(x\overline{x}) + \sigma_{r_2+1}(x\overline{x}) + \ldots + \sigma_{r_2+r_2}(x\overline{x}) \\ &= \sum_{i=1}^{n} \sigma_i(x\overline{x}) \end{aligned}$$

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

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}\mathcal{T}r_{\mathbb{K}}(x\overline{x}). \tag{3.8}$$

Em contrapartida, se $\mathbb{K}$ é um corpo totalmente real, $r_2 = 0$, então

$$|\sigma_{\mathbb{K}}(x)|^2 = (\sigma_1(x))^2 + \ldots + (\sigma_{r_1}(x))^2$$

e como $\sigma_j(x) = (\mu \circ \sigma_j)(x) = \sigma_j(\overline{x})$, concluímos que

$$\sigma_j(x\overline{x}) = \sigma_j(x)\sigma_j(\overline{x}) = \sigma_j(x)\sigma_j(x) = (\sigma_j(x))^2.$$

Logo,

$$\begin{aligned} |\sigma_{\mathbb{K}}(x)|^2 &= \sigma_1(x\overline{x}) + \ldots + \sigma_{r_1}(x\overline{x}) \\ &= \sum_{i=1}^{n} \sigma_i(x\overline{x}), \end{aligned}$$

ou seja,

$$|\sigma_{\mathbb{K}}(x)|^2 = \mathcal{T}r_{\mathbb{K}}(x\overline{x}). \tag{3.9}$$

Portanto, se $\mathbb{K}$ é totalmente real, então$|\sigma_{\mathbb{K}}(x)|^2$ é dado como na Equação (3.9) e se $\mathbb{K}$ for totalmente imaginário, é dada pela Equação (3.8), o que prova o resultado.

□

Em concordância com a Proposição 1.1.1 sabemos que se uma extensão $\mathbb{Q} \subseteq \mathbb{K}$ de grau n é galoisiana, então $\mathbb{K}$ é, necessariamente, totalmente real ou totalmente imaginário, pois $\sigma_i(\mathbb{K}) = \mathbb{K}$, para todo $i = 1, \ldots, n$. Em particular, quando $\mathbb{K}|\mathbb{Q}$ é uma extensão de Galois e n é ímpar, então $\mathbb{K}$ é totalmente real, tendo em vista que os monomorfismos complexos aparecem aos pares. Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é um corpo ciclotômico, $n > 1$, então $\mathbb{K}$ é totalmente complexo e pela Proposição 3.3.1, para cada $x \in \mathbb{K}$,

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}\mathcal{T}r_{\mathbb{K}}(x\overline{x}).$$

O Corolário 3.3.1 exibe o volume de um reticulado algébrico obtido através de um ideal do

anel de inteiros de um corpo de números. A próxima proposição, por sua vez, caracteriza a densidade de centro de um reticulado obtido nas mesmas condições para um corpo de números totalmente real ou totalmente complexo.

Proposição 3.3.2 ([12], p. 52) *Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente complexo de grau n, $\mathcal{O}_{\mathbb{K}}$ seu o anel de inteiros e $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$. Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{t^{\frac{n}{2}}}{2^n\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})}, \tag{3.10}$$

onde $t = min\{\mathcal{T}r_{\mathbb{K}}(x\overline{x}) \mid x \in \mathcal{I},\ x \neq 0\}$ e $\mathcal{N}(\mathcal{I})$ é a norma do ideal $\mathcal{I}$.

Demonstração: Admita que $\mathbb{K}$ é um corpo totalmente real, isto é, $r_2 = 0$. Então pela Proposição 3.3.1, o raio de empacotamento do reticulado pode ser escrito por

$$\rho = \frac{1}{2}min\left\{|\sigma_{\mathbb{K}}(x)| \mid x \in \mathcal{I},\ x \neq 0\right\} = \frac{1}{2}min\left\{\sqrt{\mathcal{T}r_{\mathbb{K}}(x\overline{x})} \mid x \in \mathcal{I},\ x \neq 0\right\}.$$

Note que neste caso o termo $c_{\mathbb{K}}$ da Equação (3.7) é $c_{\mathbb{K}} = 1$. Para $t = min\{\mathcal{T}r_{\mathbb{K}}(x\overline{x}) \mid x \in \mathcal{I},\ x \neq 0\}$, temos $\rho = \frac{1}{2}\sqrt{t}$, e portanto,

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{\left(\frac{1}{2}\sqrt{t}\right)^n}{\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})} = \frac{2^{-n}(\sqrt{t})^n}{\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})} = \frac{t^{\frac{n}{2}}}{2^n\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})}.$$

Por outro lado, se $\mathbb{K}$ é um corpo totalmente imaginário, então

$$\rho = \frac{1}{2}min\left\{\sqrt{\frac{1}{2}\mathcal{T}r_{\mathbb{K}}(x\overline{x})} \mid x \in \mathcal{I},\ x \neq 0\right\} = \frac{1}{2}\sqrt{\frac{1}{2}t}.$$

Além disso, $r_1 = 0$ e $r_2 = \frac{n}{2}$. Assim,

$$\delta(\sigma_{\mathbb{K}}(\mathcal{I})) = \frac{2^{\frac{n}{2}}\left(\frac{1}{2}\sqrt{\frac{1}{2}t}\right)^n}{\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})} = \frac{2^{\frac{n}{2}}\left(\frac{1}{2}\right)^n\left(\frac{t}{2}\right)^{\frac{n}{2}}}{\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})} = \frac{t^{\frac{n}{2}}}{2^n\sqrt{|\mathcal{D}_{\mathbb{K}}|}\mathcal{N}(\mathcal{I})},$$

o que conclui a proposição.

□

Embora o homomorfismo de Minkowski seja o principal método para construção de reticulados provenientes de corpos de números, existem outros homomorfismos também com domínio em um corpo de números de grau n e contradomínio $\mathbb{R}^n$ com tal propriedade. Deste fato tratamos na próxima seção.

3.4 Pertubação no homomorfismo canônico

Em conformidade com o comentário no fim da seção anterior, apresentamos um outro homomorfismo que nos permite construir reticulados através de ideais do anel de inteiros de um corpo de números, o qual contribui principalmente para a diversidade de reticulados algébricos e também é estudado em [1], [12] e [26].

Este método de construção se dá através de perturbações no homomorfismo canônico apresentado na Seção 3.3, por meio de específicos elementos do corpo de números. Inicialmente apresentamos duas definições que caracterizam os elementos citados e que são vitais para a construção de tal homomorfismo.

Definição 3.4.1 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$. Um elemento $\alpha \in \mathbb{K}$ é dito* ***totalmente real*** *se $\sigma_i(\alpha) \in \mathbb{R}$, para todo $1 \leq i \leq n$.*

Definição 3.4.2 *Seja $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$. Dizemos que um elemento totalmente real $\alpha \in \mathbb{K}$ é* ***totalmente positivo*** *se $\sigma_i(\alpha) > 0$, para todo $1 \leq i \leq n$.*

As Definições 3.4.1 e 3.4.2 representam as duas propriedades necessárias para que um elemento defina a perturbação no homomorfismo canônico, que exibimos a seguir.

Definição 3.4.3 *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$ e $\alpha \in \mathbb{K}$ um elemento totalmente real e totalmente positivo. O homomorfismo $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ dado por*

$$\begin{aligned}\sigma_\alpha(x) = \; & \big(\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots \\ & \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))\big)\end{aligned}$$

é chamado de ***perturbação do homomorfismo canônico*** *ou* ***homomorfismo canônico torcido****.*

Observação 3.4.1 *Por simplicidade vamos nos referir a tal homomorfismo por* ***homomorfismo torcido****.*

Assim como para o homomorfismo canônico, a imagem de qualquer $\mathbb{Z}$-módulo do corpo $\mathbb{K}$ é um reticulado em $\mathbb{R}^n$. Em especial, a imagem de qualquer ideal do anel de inteiros $\mathcal{O}_\mathbb{K}$ é um reticulado como ratifica o próximo resultado.

Corolário 3.4.1 ([26], p. 15) *Se $G \subseteq \mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\mathcal{B} = \{\omega_1, \omega_2, \ldots, \omega_n\}$, então a imagem $\sigma_\alpha(G)$ de G através de σ_α em $\mathbb{R}^n$ é um reticulado com base $\sigma_\alpha(\mathcal{B}) = \{\sigma_\alpha(\omega_1), \sigma_\alpha(\omega_2), \ldots, \sigma_\alpha(\omega_n)\}$.*

Assim como descrevemos no Teorema 3.3.1 da Seção 3.3 ao nos referir ao homomorfismo canônico, observamos que o principal fator que também define o resultado acima é o fato de G admitir uma $\mathbb{Z}$-base com n elementos.

Exemplo 3.4.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{17})$ um corpo quadrático. O elemento $\alpha = 17 + 4\sqrt{17} \in \mathbb{K}$ é totalmente real e totalmente positivo. Sendo assim, o homomorfismo torcido σ_α está bem definido e é dado por*

$$\begin{array}{rccl} \sigma_\alpha : & \mathbb{K} & \longrightarrow & \mathbb{R}^2 \\ & a + b\sqrt{17} & \longmapsto & \left(\sqrt{17 + 4\sqrt{17}}(a + b\sqrt{17}), \sqrt{17 - 4\sqrt{17}}(a - b\sqrt{17})\right). \end{array}$$

Como $17 \equiv 1 \pmod 4$, pelo Teorema 2.2.1, $\mathcal{O}_\mathbb{K} = \mathbb{Z}\left[\dfrac{1+\sqrt{17}}{2}\right]$ que admite como base integral o conjunto $\mathcal{B} = \left\{1, \dfrac{1+\sqrt{17}}{2}\right\}$. Pelo Corolário 3.4.1, $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado em $\mathbb{R}^2$.

Para um $\mathbb{Z}$-módulo livre G de $\mathcal{O}_\mathbb{K}$ com base $\mathcal{B} = \{\omega_1, \omega_2, \ldots, \omega_n\}$ a matriz geradora do reticulado obtido através do homomorfismo torcido é

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_1}\sigma_1(\omega_2) & \cdots & \sqrt{\alpha_1}\sigma_1(\omega_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_1) & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_n) \\ \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\omega_1)) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\omega_2)) & \cdots & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\omega_n)) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\omega_1)) & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\omega_2)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\omega_n)) \end{pmatrix}.$$

Um caso particular no qual estamos profundamente interessados é o caso em que $\mathcal{I} = \mathcal{O}_\mathbb{K}$, ou seja, nos reticulados da forma $\sigma_\alpha(\mathcal{O}_\mathbb{K}) \subset \mathbb{R}^n$ como no Exemplo 3.4.1. O próximo teorema caracteriza de modo geral o volume de um reticulado obtido através do homomorfismo torcido.

Teorema 3.4.1 ([12], p. 80) *Sejam $\mathbb{K}$ um corpo de números de grau n, M um $\mathbb{Z}$-módulo livre de posto n de $\mathbb{K}$ e σ_α uma perturbação do homomorfismo canônico associado a $\mathbb{K}$. Se $\mathcal{B} = \{\omega_1, \omega_2, \ldots, \omega_n\}$ é uma base de M como $\mathbb{Z}$-módulo, então $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, com base $\sigma_\alpha(\mathcal{B}) = \{\sigma_\alpha(\omega_1), \sigma_\alpha(\omega_2), \ldots, \sigma_\alpha(\omega_n)\}$ cujo volume é*

$$\mathcal{V}ol(\sigma_\alpha(M)) = b_\alpha \left| det_{1\leq j,i\leq n}(\sigma_j(\omega_i)) \right|,$$

onde

(i) $b_\alpha = \sqrt{\mathcal{N}_{\mathbb{K}}(\alpha)}$, *se $\mathbb{K}$ for totalmente real,*

(ii) $b_\alpha = 2^{\frac{-n}{2}}\sqrt{\mathcal{N}_{\mathbb{K}}(\alpha)}$, *se $\mathbb{K}$ for totalmente imaginário.*

Em decorrência deste resultado obtemos os dois seguintes corolários que determinam o volume dos reticulados da forma $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ e $\sigma_\alpha(\mathcal{I})$, com $\mathcal{I} \subset \mathcal{O}_\mathbb{K}$, e a densidade de centro de tais reticulados, respectivamente.

Corolário 3.4.2 ([12], p. 82) *Sejam $\mathbb{K}$ um corpo de números de grau n cujo discriminante é $\mathcal{D}_\mathbb{K}$ e σ_α uma perturbação no homomorfismo canônico. Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ e $\sigma_\alpha(\mathcal{I})$ são reticulados em $\mathbb{R}^n$ com volumes dados por*

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = b_\alpha\sqrt{|\mathcal{D}_\mathbb{K}|} \quad e \quad \mathcal{V}ol(\sigma_\alpha(\mathcal{I})) = b_\alpha\sqrt{|\mathcal{D}_\mathbb{K}|}\mathcal{N}(\mathcal{I}),$$

onde $\mathcal{N}(\mathcal{I})$ é a norma do ideal $\mathcal{I}$ e b_α é como no Teorema 3.4.1.

Corolário 3.4.3 ([12], p. 82) *Se $\mathbb{K}$ é um corpo de números de grau n cujo discriminante é $\mathcal{D}_\mathbb{K}$ e $\mathcal{I}$ um ideal não nulo do anel de inteiros $\mathcal{O}_\mathbb{K}$, então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{I})$ é dada por*

$$\delta(\sigma_\alpha(\mathcal{I})) = \frac{(\rho(\sigma_\alpha(\mathcal{I})))^n}{b_\alpha\sqrt{|\mathcal{D}_\mathbb{K}|}\mathcal{N}(\mathcal{I})},$$

onde ρ é o raio de empacotamento do reticulado $\sigma_\alpha(\mathcal{I})$.

Assim como para o homomorfismo canônico, é possível determinar a norma de um vetor de um reticulado algébrico obtido através do homomorfismo torcido por via da norma do elemento correspondente no anel de inteiros.

Proposição 3.4.1 ([36], p. 82) *Sejam $\mathbb{K}$ um corpo de números de grau n, $\alpha \in \mathbb{K}$ um elemento totalmente real e totalmente positivo e σ_α o homomorfismo torcido correspondente. Se $x \in \mathbb{K}$, então*

$$|\sigma_\alpha(x)|^2 = c_\alpha \mathcal{T}r_{\mathbb{K}}(\alpha x\overline{x}),$$

onde

$$c_\alpha = \begin{cases} 1, \text{ se } \mathbb{K} \text{ for totalmente real, } r_2 = 0, \\ \dfrac{1}{2}, \text{ se } \mathbb{K} \text{ for totalmente imaginário, } r_1 = 0 \end{cases}$$

e $\overline{x}$ é o conjugado complexo de x.

Demonstração: Sejam $\mathbb{K}$ um corpo de números de grau $n = r_1 + 2r_2$ e $x \in \mathbb{K}$. Assim, $\sigma_\alpha(x) \in \mathbb{R}^n$ e

$$\begin{aligned} |\sigma_\alpha(x)|^2 &= (\sqrt{\alpha_1}\sigma_1(x))^2 + \ldots + (\sqrt{\alpha_{r_1}}\sigma_{r_1}(x))^2 + (\sqrt{\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)))^2 \\ &+ (\sqrt{\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)))^2 + \ldots + (\sqrt{\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)))^2 + (\sqrt{\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)))^2 \\ &= \alpha_1(\sigma_1(x))^2 + \ldots + \alpha_{r_1}(\sigma_{r_1}(x))^2 + \alpha_{r_1+1}(\Re(\sigma_{r_1+1}(x)))^2 + \alpha_{r_1+1}(\Im(\sigma_{r_1+1}(x)))^2 \\ &+ \ldots + \alpha_{r_1+r_2}(\Re(\sigma_{r_1+r_2}(x)))^2 + \alpha_{r_1+r_2}(\Im(\sigma_{r_1+r_2}(x)))^2 \\ &= \alpha_1(\sigma_1(x))^2 + \ldots + \alpha_{r_1}(\sigma_{r_1}(x))^2 + \alpha_{r_1+1}[(\Re(\sigma_{r_1+1}(x)))^2 + (\Im(\sigma_{r_1+1}(x)))^2] \\ &+ \alpha_{r_1+r_2}[(\Re(\sigma_{r_1+r_2}(x)))^2 + (\Im(\sigma_{r_1+r_2}(x)))^2]. \end{aligned}$$

Note que, para $r_1 + 1 \leq k \leq r_1 + r_2$, $(\Re(\sigma_k(x)))^2 + (\Im(\sigma_k(x)))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x})$. Se $r_1 = 0$, então

$$\begin{aligned} |\sigma_\alpha(x)|^2 &= \alpha_1\sigma_1(x\overline{x}) + \ldots + \alpha_{r_2}\sigma_{r_2}(x\overline{x}) \\ &= \sigma_1(\alpha)\sigma_1(x\overline{x}) + \ldots + \sigma_{r_2}(\alpha)\sigma_{r_2}(x\overline{x}) \\ &= \sigma_1(\alpha x\overline{x}) + \ldots + \sigma_{r_2}(\alpha x\overline{x}) \\ &= \sigma_{r_2+1}(\alpha x\overline{x}) + \ldots + \sigma_{r_2+r_2}(\alpha x\overline{x}), \end{aligned}$$

uma vez que $\sigma_{r_2+j}(\alpha x\overline{x}) = (\mu \circ \sigma_j)(\alpha x\overline{x}) = \sigma_j(\alpha x\overline{x})$, para todo $j = 1, \ldots, r_2$ e μ a conjugação complexa. Sendo assim,

$$\begin{aligned} 2|\sigma_\alpha(x)|^2 &= \sigma_1(\alpha x\overline{x}) + \ldots + \sigma_{r_2}(\alpha x\overline{x}) + \sigma_{r_2+1}(\alpha x\overline{x}) + \ldots + \sigma_{r_2+r_2}(\alpha x\overline{x}) \\ &= \sum_{i=1}^{n} \sigma_i(\alpha x\overline{x}) \\ &= \mathcal{T}r_{\mathbb{K}}(\alpha x\overline{x}). \end{aligned}$$

Portanto,

$$|\sigma_\alpha(x)|^2 = \frac{1}{2}\mathcal{T}r_{\mathbb{K}}(\alpha x\overline{x}). \tag{3.11}$$

Por outro lado, se $r_2 = 0$, então

$$|\sigma_\alpha(x)|^2 = \alpha_1(\sigma_1(x))^2 + \ldots + \alpha_{r_1}(\sigma_{r_1}(x))^2$$

e como $\sigma_i(x) = (\mu \circ \sigma_i)(x) = \sigma_i(x)$, para todo $i = 1, \ldots, r_1$, temos $\sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$ e

$$\begin{aligned} |\sigma_\alpha(x)|^2 &= \alpha_1\sigma_1(x\overline{x}) + \ldots + \alpha_{r_1}\sigma_{r_1}(x\overline{x}) \\ &= \sigma_1(\alpha)\sigma_1(x\overline{x}) + \ldots + \sigma_{r_1}(\alpha)\sigma_{r_1}(x\overline{x}) \\ &= \sigma_1(\alpha x\overline{x}) + \ldots + \sigma_{r_1}(\alpha x\overline{x}) \\ &= \sum_{i=1}^{n} \sigma_i(\alpha x\overline{x}). \end{aligned}$$

Portanto,

$$|\sigma_\alpha(x)|^2 = \mathcal{T}r_{\mathbb{K}}(\alpha x\overline{x}), \tag{3.12}$$

o que conclui o resultado.

□

Este resultado é muito útil nos Capítulos 4 e 5, pois para o prosseguimento do estudo de reticulados bem arredondados é necessário, muitas vezes, calcular a norma de determinados vetores do reticulado. Finalmente, para concluir o capítulo descrevemos a seguinte versão do Corolário 3.4.3, que faz referencia aos corpos totalmente reais ou totalmente complexos.

Proposição 3.4.2 ([12], p. 84) *Sejam $\mathbb{K}$ um corpo de números de grau n totalmente real ou totalmente complexo, σ_α uma perturbação no homomorfismo canônico e $\mathcal{O}_\mathbb{K}$ seu anel de inteiros. Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{I})$ é dada por*

$$\delta(\sigma_\alpha(\mathcal{I})) = \frac{t_\alpha^{n/2}}{2^n\sqrt{|\mathcal{D}_\mathbb{K}\mathcal{N}_\mathbb{K}(\alpha)\mathcal{N}(\mathcal{I})}},$$

onde $t_\alpha = \min\{\mathcal{T}r_{\mathbb{K}}(\alpha x\overline{x}) \mid x \in \mathcal{I}, x \neq 0\}$.

Considerações Finais

A Teoria de Reticulados é muito ampla e existem inúmeros trabalhos relacionados a esta teoria. Pode-se dizer que o desenvolvimento apresentado neste capítulo representa uma síntese

dos principais aspectos que compõem esta teoria, enfatizando os reticulados algébricos.

Os poucos exemplos de reticulados que apresentamos na Seção 3.1 representam uma pequena fração dos inúmeros reticulados conhecidos da literatura, outros exemplos podem ser encontrados em [2]. Alguns trabalhos relacionados a estes conceitos classificam os demais reticulados conhecidos no que se refere aos parâmetros aqui apresentados, como densidade e volume.

Uma vez encerrado este capítulo, finalizamos a apresentação de todos os conceitos necessários para o estudo de uma classe de reticulados algébricos, os reticulados bem arredondados, que desenvolveremos a partir do Capítulo 4.

Capítulo

4

Reticulados bem arredondados

Neste capítulo, estudamos o principal assunto deste trabalho, os reticulados bem arredondados, do inglês *well-rounded*, apresentando conceitos básicos sobre essa teoria como definições, exemplos e algumas propriedades geométricas. Nas Seções 4.2 e 4.3 dedicamos uma atenção especial aos reticulados bem arredondados provenientes de corpos quadráticos e desenvolvemos detalhadamente resultados encontrados em [15] e [18]. Na Seção 4.4 estudamos reticulados bem arredondados em $\mathbb{R}^n$ e suas relações com o anel de inteiros de corpos ciclotômicos, assim como algumas propriedades relacionadas à ideais fracionários neste mesmo anel.

Embora ainda existam poucas referências sobre este assunto, tendo em vista seu surgimento recente, essa classe de reticulados apresenta muitas propriedades para aplicações, como nos problemas referentes ao número de contato, do inglês *kissing number*, e à diversidade de reticulados.

4.1 Definições e conceitos básicos

Nesta seção, apresentamos conceitos elementares da teoria de reticulados bem arredondados, além de alguns exemplos desses reticulados. A partir desta seção, com o propósito de simplificar notações, denotamos os reticulados $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{I})$ por $\Lambda_{\mathbb{K}}$ e $\Lambda_{\mathbb{K}}(\mathcal{I})$, respectivamente, em que $\mathbb{K}$ é um corpo de números de grau n, $\sigma_{\mathbb{K}}$ é o homomorfismo canônico correspondente, $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$ e $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$.

Definição 4.1.1 *Sejam $n \geq 2$ um inteiro e $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo. O*

conjunto de vetores mínimos *de* Λ *é definido por*

$$S(\Lambda) = \{v \in \Lambda \mid ||v|| = |\Lambda|\},$$

onde $|\Lambda| = min\{||v|| \mid v \in \Lambda, x \neq 0\}$.

No contexto da teoria de reticulados bem arredondados, devido ao conceito que definimos a seguir, é comum denotarmos a norma de um reticulado por $\lambda_1(\Lambda)$, ou simplesmente λ_1, e nos referirmos a tal valor como primeiro mínimo sucessivo.

Definição 4.1.2 *Sejam* $n \geq 2$ *um inteiro e* $\Lambda \subset \mathbb{R}^n$ *um reticulado de posto completo. Para cada* $1 \leq i \leq n$*, o* i*-ésimo* ***mínimo sucessivo*** *de* Λ *é definido como o número real*

$$\lambda_i = min\{\lambda \in \mathbb{R} \mid dim_{\mathbb{R}}\{v \in \Lambda \mid ||v|| \leq \lambda\} \leq i\}.$$

Em outras palavras, o i-ésimo mínimo sucessivo corresponde ao menor raio r tal que a bola centrada na origem de $\mathbb{R}^n$ e raio r contém i vetores linearmente independentes pertencentes a Λ. Como consequência,

$$0 < \lambda_1 \leq \ldots \leq \lambda_n. \tag{4.1}$$

Uma vez presentes os conceitos de conjunto de vetores mínimos e mínimos sucessivos, estamos aptos a exibir a definição de reticulado bem arredondado.

Definição 4.1.3 *Sejam* $n \geq 2$ *e* $\Lambda \subset \mathbb{R}^n$ *um reticulado de posto completo. O reticulado* Λ *é chamado de* ***bem arredondado*** *se* $S(\Lambda)$ *gera* $\mathbb{R}^n$*, ou seja, se* $S(\Lambda)$ *possui* n *vetores linearmente independentes.*

Observação 4.1.1 *A propriedade de ser bem arredondado é preservada pela relação de semelhança descrita na Definição 3.1.8. Em outros termos, se* $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ *são reticulados equivalentes e* Λ_1 *é bem arredondado, então* Λ_2 *também é bem arredondado.*

Em decorrência da Definição 4.1.2 e da Equação (4.1), um reticulado é bem arredondado se, e somente se, todos os seus mínimos sucessivos são iguais, isto é,

$$|\Lambda| = \lambda_1 = \lambda_2 = \ldots = \lambda_n. \tag{4.2}$$

Observação 4.1.2 *Com o intuito de simplificar os cálculos relacionados a norma do reticulado, constantemente utilizamos o quadrado da norma de um vetor* $v \in \Lambda$*,* $||v||^2$*, ao invés de* $||v||$.

Exemplo 4.1.1 *O reticulado $\Lambda_{\mathbb{K}} = \mathbb{Z}^2$ obtido através da imagem do anel de inteiros de $\mathbb{K} = \mathbb{Q}(i)$ pelo homomorfismo canônico e apresentado no Exemplo 3.1.1 é bem arredondado. De fato, como $-1 \equiv 3 \ (mod\ 4)$, o Teorema 2.2.1 nos garante que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ e $\mathcal{B} = \{1, i\}$ é uma base integral. O corpo $\mathbb{K}$ é totalmente imaginário e o homomorfismo canônico é dado como no Exemplo 3.3.2. Dessa forma, para todo $v \in \Lambda_{\mathbb{K}}$,*

$$v = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(i) \\ \Im\sigma_1(1) & \Im\sigma_1(i) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

com $x_1, x_2 \in \mathbb{Z}$. Sendo assim,

$$||v||^2 = x_1^2 + x_2^2,$$

cujo valor mínimo não nulo é atingido quando $x_1 = \pm 1$ e $x_2 = 0$ ou $x_1 = 0$ e $x_2 = \pm 1$. Logo,

$$S(\Lambda_{\mathbb{K}}) = \{(1,0), (0,1), (-1,0), (0,-1)\}.$$

Obviamente $S(\Lambda_{\mathbb{K}})$ gera $\mathbb{R}^2$, e portanto, $\Lambda_{\mathbb{K}} = \mathbb{Z}^2$ é bem arredondado.

Observação 4.1.3 *Em geral, o reticulado $\Lambda = \mathbb{Z}^n \subset \mathbb{R}^n$ é bem arredondado. Neste caso, o conjunto formado pela base canônica de $\mathbb{R}^n$ é um subconjunto do conjunto dos vetores mínimos do reticulado.*

Exemplo 4.1.2 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$, então o reticulado $\Lambda_{\mathbb{K}}$ é bem arredondado. Com efeito, pelo Teorema 2.2.1, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\dfrac{1+\sqrt{-3}}{2}\right]$, que admite como uma base integral o conjunto $\mathcal{B} = \left\{1, \dfrac{1+\sqrt{-3}}{2}\right\}$. Além disso, como $\mathbb{K}$ é um corpo totalmente imaginário, o homomorfismo canônico é dado por $\sigma_{\mathbb{K}}(x) = (\Re(x), \Im(x))$. Sendo assim, para todo $v \in \Lambda_{\mathbb{K}}$,*

$$v = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) \\ \Im\sigma_1(1) & \Im\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{2x_1+x_2}{2} \\ \frac{\sqrt{3}x_2}{2} \end{pmatrix},$$

com $x_1, x_2 \in \mathbb{Z}$. Logo,

$$||v||^2 = \left(\frac{2x_1 + x_2}{2}\right)^2 + \left(\frac{\sqrt{3}x_2}{2}\right)^2 = x_1^2 + x_1x_2 + \frac{x_2^2}{4} + \frac{3x_2^2}{4} = x_1^2 + x_1x_2 + x_2^2,$$

cujo valor mínimo não nulo é atingido quando $x_1 = \pm 1$ e $x_2 = 0$, $x_1 = 0$ e $x_2 = \pm 1$, $x_1 = 1$ e

$x_2 = -1$ *ou* $x_1 = -1$ *e* $x_2 = 1$. *Então,*

$$S(\Lambda_{\mathbb{K}}) = \left\{(1,0), (-1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right), \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)\right\}.$$

O reticulado $\Lambda_{\mathbb{K}}$ *é, na verdade, o reticulado hexagonal* Λ_{hex} *que apresentamos no Exemplo 3.1.2 e que possui a melhor densidade de empacotamento dentre todos os reticulados no plano. Claramente* $S(\Lambda_{\mathbb{K}})$ *gera* $\mathbb{R}^2$*, e portanto,* $\Lambda_{\mathbb{K}}$ *é bem arredondado.*

Os reticulados apresentados nos Exemplos 4.1.1 e 4.1.2 são os únicos bem arredondados em $\mathbb{R}^2$ obtidos através da imagem do anel dos inteiros de um corpo quadrático pelo homomorfismo canônico, resultado que verificamos na próxima seção e está disponível em [18].

Exemplo 4.1.3 *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$*. O grau da extensão* $\mathbb{K}|\mathbb{Q}$ *é* $[\mathbb{K} : \mathbb{Q}] = \varphi(8) = 4$*, e pelo Teorema 2.4.2,* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$*, cuja base integral é* $\mathcal{B} = \{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$*. Recordamos que* $\zeta_n = e^{\frac{2\pi i}{n}} = cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$ *e que, se* $\alpha \in \mathcal{O}_{\mathbb{K}}$*, então* $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i\zeta_n^i \in \mathcal{O}_{\mathbb{K}}$*. Diante disso,*

$$\zeta_8 = e^{\frac{2\pi i}{8}} = cos\left(\frac{2\pi}{8}\right) + isen\left(\frac{2\pi}{8}\right) = cos\left(\frac{\pi}{4}\right) + isen\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

e $\alpha = \sum_{i=0}^{\varphi(8)-1} a_i\zeta_8^i = \sum_{i=0}^{3} a_i\zeta_8^i = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3$*. O grupo de Galois de* $\mathbb{K}$ *é* $G = \{\sigma_i \mid \sigma_i(\zeta_8) = \zeta_8^i, i = 1,3,5,7\} \simeq \mathbb{Z}_8^* = \{1,3,5,7\}$ *e* $\sigma_i(\mathbb{K}) \not\subset \mathbb{R}$*, para* $i = 1,2,3,4$*, assim,* $r_1 = 0$ *e* $r_2 = 2$*. Portanto, o homomorfismo canônico,* $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^4$*, associado a* $\mathbb{K}$ *é dado por*

$$\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \Re\sigma_3(x), \Im\sigma_3(x)). \tag{4.3}$$

Além disso, para todo $v \in \Lambda_{\mathbb{K}} = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) \subset \mathbb{R}^4$*,*

$$v = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(\zeta_8) & \Re\sigma_1(\zeta_8^2) & \Re\sigma_1(\zeta_8^3) \\ \Im\sigma_1(1) & \Im\sigma_1(\zeta_8) & \Im\sigma_1(\zeta_8^2) & \Im\sigma_1(\zeta_8^3) \\ \Re\sigma_2(1) & \Re\sigma_2(\zeta_8) & \Re\sigma_2(\zeta_8^2) & \Re\sigma_2(\zeta_8^3) \\ \Im\sigma_2(1) & \Im\sigma_2(\zeta_8) & \Im\sigma_2(\zeta_8^2) & \Im\sigma_2(\zeta_8^3) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix},$$

com $x_i \in \mathbb{Z}, i = 1,2,3,4$*. Como*

$$\zeta_8^2 = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)^2 = \frac{1}{2} + \frac{2i}{2} - \frac{1}{2} = i \quad e \quad \zeta_8^3 = \zeta_8^2\zeta_8 = i\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = i\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2},$$

segue que

$$v = \begin{pmatrix} 1 & \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & \frac{\sqrt{2}}{2} & 1 & \frac{\sqrt{2}}{2} \\ 1 & -\frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ 0 & \frac{\sqrt{2}}{2} & -1 & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + \frac{\sqrt{2}}{2}x_2 - \frac{\sqrt{2}}{2}x_4 \\ \frac{\sqrt{2}}{2}x_2 + x_3 + \frac{\sqrt{2}}{2}x_4 \\ x_1 - \frac{\sqrt{2}}{2}x_2 + \frac{\sqrt{2}}{2}x_4 \\ \frac{\sqrt{2}}{2}x_2 - x_3 + \frac{\sqrt{2}}{2}x_4 \end{pmatrix}.$$

Dessa forma,

$$\begin{aligned} ||v||^2 &= \left(x_1 + \tfrac{\sqrt{2}}{2}x_2 - \tfrac{\sqrt{2}}{2}x_4\right)^2 + \left(\tfrac{\sqrt{2}}{2}x_2 + x_3 + \tfrac{\sqrt{2}}{2}x_4\right)^2 + \left(x_1 - \tfrac{\sqrt{2}}{2}x_2 + \tfrac{\sqrt{2}}{2}x_4\right)^2 \\ &+ \left(\tfrac{\sqrt{2}}{2}x_2 - x_3 + \tfrac{\sqrt{2}}{2}x_4\right)^2 \\ &= \left(x_1 + \tfrac{\sqrt{2}}{2}(x_2 - x_4)\right)^2 + \left(\tfrac{\sqrt{2}}{2}(x_2 + x_4) + x_3\right)^2 + \left(x_1 + \tfrac{\sqrt{2}}{2}(x_4 - x_2)\right)^2 \\ &+ \left(\tfrac{\sqrt{2}}{2}(x_2 + x_4) - x_3\right)^2 \\ &= x_1^2 + \sqrt{2}(x_2 - x_4)x_1 + \tfrac{1}{2}(x_2 - x_4)^2 + \tfrac{1}{2}(x_2 + x_4)^2 + \sqrt{2}(x_2 + x_4)x_3 + x_3^2 \\ &+ x_1^2 + \sqrt{2}(x_4 - x_2)x_1 + \tfrac{1}{2}(x_4 - x_2)^2 + \tfrac{1}{2}(x_2 + x_4)^2 - \sqrt{2}(x_2 + x_4)x_3 + x_3^2 \\ &= x_1^2 + \sqrt{2}(x_2 - x_4)x_1 + \tfrac{1}{2}(x_2 - x_4)^2 + x_1^2 + \sqrt{2}(x_4 - x_2)x_1 + \tfrac{1}{2}(x_4 - x_2)^2 \\ &+ (x_2 + x_4)^2 + 2x_3^2 = 2x_1^2 + (x_2 - x_4)^2 + (x_2 + x_4)^2 + 2x_3^2 \\ &= 2(x_1^2 + x_3^2) + x_2^2 - 2x_2x_4 + x_4^2 + x_2^2 + 2x_2x_4 + x_4^2 \\ &= 2(x_1^2 + x_2^2 + x_3^2 + x_4^2), \end{aligned}$$

que assume valor mínimo não nulo quando $x_i = \pm 1$ *e* $x_j = 0$*, para todo* $j \neq i$*,* $i = 1, 2, 3, 4$*. Portanto,* $S(\Lambda_{\mathbb{K}}) = S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \left\{\pm(1,0,1,0), \pm\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right), \pm(0,1,0,-1), \pm\left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)\right\}$*. Uma simples verificação constata que* $S(\Lambda_{\mathbb{K}})$ *possui* 4 *vetores linearmente independentes. Logo, este conjunto gera* $\mathbb{R}^4$*, e portanto, o reticulado* $\Lambda_{\mathbb{K}}$ *é bem arredondado.*

Assim como para corpos quadráticos, existe uma caracterização para reticulados obtidos através da imagem do anel de inteiros pelo homomorfismo canônico para corpos ciclotômicos, conforme apresentamos na Seção 4.4.

4.2 Reticulados bem arredondados em $\mathbb{R}^2$

Nesta seção, damos ênfase aos reticulados bem arredondados em $\mathbb{R}^2$ formalizando o comentário feito na seção anterior, o qual nos permite caracterizar os reticulados da forma $\Lambda_{\mathbb{K}}$, sendo $\mathbb{K}$ um corpo quadrático. Também estudamos os vetores mínimos destes reticulados,

tendo em vista que apresentam algumas propriedades geométricas particulares, especialmente no que se refere ao ângulo entre estes.

O próximo resultado é de suma importância para o estudo e corresponde a primeira caracterização de reticulados algébricos bem arredondados em $\mathbb{R}^2$.

Lema 4.2.1 ([18], p. 192) *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado de posto completo. Então Λ contém 2, 4 ou 6 vetores mínimos e é bem arredondado se, e somente se, $\#S(\Lambda) = 4$ ou $\#S(\Lambda) = 6$. Além disso, $\#S(\Lambda) = 6$ se, e somente se, Λ é semelhante ao reticulado hexagonal $\Lambda_{hex} = \Lambda_{\mathbb{Q}(\sqrt{-3})}$.*

Demonstração: Seja $v \in S(\Lambda)$. Como $-v \in \Lambda$ e $||v||^2 = ||-v||^2$, então $-v \in S(\Lambda)$. Note ainda que se $v_1, v_2 \in S(\Lambda)$ são vetores distintos e linearmente dependentes, ou seja, $v_1 = \lambda v_2$ para algum $\lambda \in \mathbb{R}$, então v_1 e v_2 são opostos entre si, uma vez que

$$||v_1|| = ||\lambda v_2|| = |\lambda|||v_2|| \Rightarrow |\lambda| = 1 \Rightarrow \lambda = \pm 1.$$

Como v_1 e v_2 são distintos, segue que $\lambda = -1$. Dessa forma, $S(\Lambda)$ possui um número par de elementos e contém dois vetores linearmente independentes se, e somente se, $\#S(\Lambda) \geq 4$. Sejam $v, u \in S(\Lambda)$ vetores distintos e suponhamos que o ângulo θ entre estes dois vetores seja tal que $0 < \theta < \dfrac{\pi}{3}$. Pela Lei dos cossenos, temos

$$||v-u||^2 = ||v||^2 - 2||v||||u||cos(\theta) + ||u||^2 < ||v||^2 - ||v||||u|| + ||u||^2$$

e como $||v|| = ||u||$, uma vez que são vetores de $S(\Lambda)$, temos

$$||v-u||^2 < ||v||^2 = ||u||^2,$$

o que é uma contradição, visto que encontramos um vetor $v - u \in \Lambda$, com $v - u \neq 0$ e norma menor do que $||v|| = ||u||$. Portanto, o ângulo entre dois vetores distintos de $S(\Lambda)$ é necessariamente maior ou igual à $\dfrac{\pi}{3}$. Por definição, os vetores de $S(\Lambda)$ estão compreendidos na circunferência de centro na origem e raio $|\Lambda|$. Assim,

$$\frac{2\pi}{\#S(\Lambda)} \geq \frac{\pi}{3}.$$

A desigualdade acima também nos permite concluir que $\#S(\Lambda) \leq 6$. Assim,

$$\#S(\Lambda) = 2, 4 \text{ ou } 6.$$

Se $\#S(\Lambda) = 2$, então Λ não é bem arredondado, uma vez que dois vetores linearmente dependentes não geram $\mathbb{R}^2$. Portanto, Λ é bem arredondado se, e somente se, $\#S(\Lambda) = 4$ ou 6.

Nos resta garantir que se $\#S(\Lambda) = 6$, então $\Lambda \sim \Lambda_{hex}$. De fato, se Λ possui 6 vetores de norma mínima, então necessariamente $S(\Lambda) = \{\pm v_1, \pm v_2, \pm v_3\}$ e podemos escolher um par de vetores v_i e v_j, com $1 \leq i, j \leq 3$ e $i \neq j$, tal que o ângulo entre esses vetores seja $\frac{\pi}{3}$, por conseguinte, v_i e v_j são linearmente independentes. Logo, como Λ tem posto 2, os vetores v_i e v_j formam uma base para Λ. Dessa forma, Λ_{hex} pode ser obtido através de rotação e dilatação dos vetores escolhidos, o que nos permite concluir a primeira implicação, isto é, $\Lambda \sim \Lambda_{hex}$. Em contrapartida, se $\Lambda \sim \Lambda_{hex}$, então $\#S(\Lambda) = \#S(\Lambda_{hex}) = 6$, concluindo o resultado.

□

Embora intuitivo, formalizamos, no Lema 4.2.9, o argumento utilizado no fim da demonstração do Lema 4.2.1 de que dois reticulados com mesmo ângulo entre seus vetores são semelhantes. A próxima proposição, por sua vez, caracteriza quais corpos quadráticos possuem anéis de inteiros cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado.

Lema 4.2.2 ([18], p. 193) *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático. Então $\Lambda_{\mathbb{K}} = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $d = -1$ ou $d = -3$.*

Demonstração: Seja $v \in \Lambda_{\mathbb{K}}$. Suponhamos inicialmente que $d \not\equiv 1 \ (mod\ 4)$. Neste caso, $\mathcal{B} = \{1, \sqrt{d}\}$ é uma base integral para $\mathcal{O}_{\mathbb{K}}$, e assim, se $d > 0$, então

$$v = \begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + y\sqrt{d} \\ x - y\sqrt{d} \end{pmatrix},$$

com $x, y \in \mathbb{Z}$. Logo,

$$||v||^2 = (x + y\sqrt{d})^2 + (x - y\sqrt{d})^2 = 2(x^2 + dy^2) \geq 2$$

e $||v||^2$ assume valor mínimo quando $x = \pm 1$ e $y = 0$. Dessa forma, $S(\Lambda_{\mathbb{K}}) = \{(1, 1), (-1, -1)\}$ e $\Lambda_{\mathbb{K}}$ não é bem arredondado. Se $d < 0$, consequentemente $-d > 0$, então

$$v = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(\sqrt{d}) \\ \Im\sigma_1(1) & \Im\sigma_1(\sqrt{d}) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-d} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y\sqrt{-d} \end{pmatrix},$$

com $x, y \in \mathbb{Z}$, e

$$||v||^2 = x^2 + (y\sqrt{-d})^2 = x^2 - dy^2 \geq 1,$$

que assume valor mínimo para $x = \pm 1$ e $y = 0$, exceto quando $d = -1$, pois neste caso, $x = 0$ e $y = \pm 1$ também fornecem norma mínima para v. Portanto, se $d \not\equiv 1 \ (mod\ 4)$, $\Lambda_{\mathbb{K}}$ é bem arredondado se, e somente se, $d = -1$. Neste caso, $S(\Lambda_{\mathbb{K}}) = \{(1,0),(0,1),(-1,0),(0,-1)\}$.

Suponhamos agora que $d \equiv 1 \ (mod\ 4)$ e consideramos a base integral $\mathcal{B} = \left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ de $\mathcal{O}_{\mathbb{K}}$. Se $d > 0$, consequentemente $d \geq 5$, então

$$v = \begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & \dfrac{1+\sqrt{d}}{2} \\ 1 & \dfrac{1-\sqrt{d}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \dfrac{2x+y}{2} + \dfrac{y\sqrt{d}}{2} \\ \dfrac{2x+y}{2} - \dfrac{y\sqrt{d}}{2} \end{pmatrix},$$

com $x, y \in \mathbb{Z}$. Logo,

$$||v||^2 = \left(\frac{2x+y}{2} + \frac{y\sqrt{d}}{2}\right)^2 + \left(\frac{2x+y}{2} - \frac{y\sqrt{d}}{2}\right)^2 = \frac{1}{2}\left(4x^2 + (d+1)y^2 + 4xy\right) \geq 2,$$

que assume menor valor quando $x = \pm 1$ e $y = 0$. Sendo assim, $S(\Lambda_{\mathbb{K}}) = \{(1,1),(-1,-1)\}$ e $\Lambda_{\mathbb{K}}$ não é bem arredondado. Por outro lado, se $d < 0$, consequentemente $d \leq -3$, então

$$v = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1\left(\frac{1+\sqrt{d}}{2}\right) \\ \Im\sigma_1(1) & \Im\sigma_1\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & \dfrac{1}{2} \\ 0 & \dfrac{\sqrt{|d|}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \dfrac{2x+y}{2} \\ \dfrac{y\sqrt{|d|}}{2} \end{pmatrix},$$

com $x, y \in \mathbb{Z}$ e

$$||v||^2 = \left(\frac{2x+y}{2}\right)^2 + \left(\frac{y\sqrt{|d|}}{2}\right)^2 = x^2 + xy + \frac{(|d|+1)y^2}{4} \geq 2,$$

que assume valor mínimo quando $x = \pm 1$ e $y = 0$, a menos que $d = -3$, pois neste caso quando $x = 0$ e $y = \pm 1$, $x = 1$ e $y = -1$ ou $x = -1$ e $y = 1$, o valor mínimo é atingido. Portanto, se $d \equiv 1 \ (mod\ 4)$, $\Lambda_{\mathbb{K}}$ é bem arredondado se, e somente se, $d = -3$. Neste caso,

$$S(\Lambda_{\mathbb{K}}) = \left\{(1,0),(-1,0),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right),\left(\frac{1}{2},-\frac{\sqrt{3}}{2}\right),\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right),\left(-\frac{1}{2},-\frac{\sqrt{3}}{2}\right)\right\}.$$

Portanto, $\Lambda_{\mathbb{K}}$ é bem arredondado se, e somente se, $d = -1$ ou $d = -3$.

□

Lema 4.2.3 ([18], p. 195) *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático totalmente imaginário. Se $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal principal e $\mathcal{J} = \alpha\mathcal{I}$, para algum $\alpha \in \mathbb{K}$, $\alpha \neq 0$, é um ideal fracionário,*

então $\Lambda_{\mathbb{K}}(\mathcal{J}) \sim \Lambda_{\mathbb{K}}$.

Demonstração: Como $\mathcal{I}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, existe $\beta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{I} = \langle\beta\rangle$. Sendo assim, como $\mathcal{J} = \alpha\mathcal{I}$, então $\mathcal{J} = \alpha\beta\mathcal{O}_{\mathbb{K}}$, com $\alpha\beta \in \mathbb{K}$. Observamos que $\mathbb{K} \subset \mathbb{C}$, logo, existem $r, \theta \in \mathbb{R}$ para os quais podemos escrever $\alpha\beta = re^{i\theta}$.

A ação de multiplicação à esquerda do elemento $\alpha\beta$ por um elemento $\gamma = se^{i\phi} \in \mathbb{C}$ é $\alpha\beta\gamma = rse^{i(\theta+\phi)}$ e corresponde a uma rotação e dilatação de γ. Como $\mathcal{J}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então $\Lambda_{\mathbb{K}}(\mathcal{J}) = \sigma_{\mathbb{K}}(\mathcal{J})$ é um reticulado e uma vez que $\Lambda_{\mathbb{K}} = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, esta é a ação de $\alpha\beta$ no reticulado, de rotação e translação. Isso significa que $\Lambda_{\mathbb{K}}(\mathcal{J})$ é obtido de $\Lambda_{\mathbb{K}}$ por rotação e dilatação. Portanto, os reticulados são semelhantes.

□

Corolário 4.2.1 ([18], p. 195) *Sejam* $\mathbb{K}$ *um corpo quadrático tal que* $\mathbb{K} = \mathbb{Q}(i)$ *ou* $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ *e* $\mathcal{I} \subset \mathbb{K}$ *um ideal fracionário não nulo. Então o reticulado* $\Lambda_{\mathbb{K}}(\mathcal{I})$ *é bem arredondado. Além disso, se* $\mathbb{K}$ *é um corpo quadrático totalmente imaginário diferente de* $\mathbb{Q}(i)$ *e* $\mathbb{Q}(\sqrt{-3})$ *e* $\mathcal{I} \subset \mathbb{K}$ *é um ideal fracionário não nulo e principal, então* $\Lambda_{\mathbb{K}}(\mathcal{I})$ *não é bem arredondado.*

Demonstração: Os corpos $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$ são, em particular, anéis principais. Se $\mathbb{K}$ é um destes corpos e $\mathcal{I} \subset \mathbb{K}$ é um ideal fracionário, então existe $\alpha \in \mathbb{K}$ tal que $\mathcal{I} = \langle\alpha\rangle$, com $\alpha \in \mathbb{K}$. Como $\mathcal{I}$ é um ideal fracionário, pelo Lema 4.2.3, $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Lambda_{\mathbb{K}}$. Logo, a primeira parte do resultado segue do Lema 4.2.2, pois $\Lambda_{\mathbb{K}}$ é um reticulado bem arredondado para $\mathbb{K} = \mathbb{Q}(i)$ ou $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ e a semelhança entre reticulados preserva a propriedade de ser bem arredondado.

Por outro lado, se $\mathbb{K} \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, então a contra recíproca do Lema 4.2.2 nos garante que $\Lambda_{\mathbb{K}}$ não é um reticulado bem arredondado. Analogamente a primeira parte do resultado, para o ideal fracionário principal $\mathcal{I}$ o Lema 4.2.3 nos permite concluir que $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Lambda_{\mathbb{K}}$. Portanto, $\Lambda_{\mathbb{K}}(\mathcal{I})$ não é bem arredondado.

□

Em [15] encontramos um resultado que nos permite transformar um reticulado $\Lambda \subset \mathbb{R}^2$ que não é bem arredondado em um reticulado bem arredondado, o qual apresentamos detalhadamente. Contudo, para a demonstração do mesmo são necessários alguns lemas auxiliares. Lembramos que o produto escalar entre dois vetores $u, v \in \mathbb{R}^n$ pode ser escrito na forma $u \cdot v = ||u||||v||cos(\theta)$, onde θ é o ângulo entre os dois vetores.

Observação 4.2.1 *Ao nos referirmos aos vetores correspondentes a mínimos sucessivos em um reticulado no* $\mathbb{R}^2$*, consideraremos um par de vetores de modo que o ângulo* θ *entre eles*

esteja no intervalo $\left[0, \frac{\pi}{2}\right]$. *Portanto,* $cos(\theta) > 0$, *e assim, a seguinte equação é satisfeita*

$$v_1^t v_2 = ||v_1||||v_2||cos(\theta) > 0. \tag{4.4}$$

Lema 4.2.4 ([15], p. 4) *Sejam* $v_1, v_2 \in \mathbb{R}^2$ *dois vetores não nulos tal que o ângulo* θ *entre eles satisfaça* $0 < \theta < \frac{\pi}{3}$. *Então*

$$||v_1 - v_2|| < max\{||v_1||, ||v_2||\}.$$

Demonstração: Note que pela Equação (4.4), $v_1^t v_2 > 0$. Assim, como $\theta < \frac{\pi}{3}$, temos

$$\frac{1}{2} < cos(\theta) = \frac{v_1^t v_2}{||v_1||||v_2||},$$

e portanto,

$$\begin{aligned} ||v_1 - v_2||^2 &= (v_1 - v_2)^t(v_1 - v_2) = ||v_1||^2 + ||v_2||^2 - 2v_1^t v_2 \\ &< ||v_1||^2 + ||v_2||^2 - ||v_1||||v_2|| \\ &< max\{||v_1||, ||v_2||\}^2. \end{aligned}$$

□

Observação 4.2.2 *O Lema 4.2.4 implica prontamente o fato que utilizamos na demonstração do Lema 4.2.1, o qual nos diz que o ângulo entre os vetores correspondentes aos mínimos sucessivos em um reticulado não pode ser menor que* $\frac{\pi}{3}$.

Lema 4.2.5 ([15], p. 5) *Sejam* $\Lambda \subset \mathbb{R}^2$ *um reticulado de posto completo com mínimos sucessivos* $\lambda_1 \leq \lambda_2$ *e* $v_1, v_2 \in \Lambda$ *seus respectivos vetores correspondentes. Se* $\theta \in \left[0, \frac{\pi}{2}\right]$ *é o ângulo entre* v_1 *e* v_2, *então*

$$\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}.$$

Demonstração: Se $\theta < \frac{\pi}{3}$, então, pelo Lema 4.2.4, temos

$$||v_1 - v_2|| < ||v_2|| = \lambda_2,$$

o que contradiz a definição de λ_2, uma vez que os vetores v_1 e $v_1 - v_2$ são linearmente independentes.

□

Os Lemas 4.2.4 e 4.2.5 nos permitem provar que os vetores correspondentes aos mínimos sucessivos em um reticulado no plano formam uma base para o mesmo, fato que admitimos implicitamente, porém formalizamos a seguir.

Teorema 4.2.1 ([15], p. 5) *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado com mínimos sucessivos $\lambda_1 \leq \lambda_2$ e $v_1, v_2 \in \Lambda$ seus respectivos vetores correspondentes. Então $\mathcal{B} = \{v_1, v_2\}$ é uma base para Λ.*

Demonstração: Sejam $u_1 \in \Lambda$ um vetor cuja norma seja mínima, isto é, um vetor cuja distância para origem seja a menor, e $u_2 \in \Lambda$ o vetor de menor norma de modo que o conjunto $\mathcal{B}' = \{u_1, u_2\}$ forme uma base para Λ. Ao escolhermos um vetor entre $\pm u_1$ e $\pm u_2$ podemos garantir, se necessário, que o ângulo entre esses vetores não seja maior que $\frac{\pi}{2}$ de acordo com a Observação 4.2.1. Assim,

$$0 < ||u_1|| \leq ||u_2||$$

e devido a escolha de u_2, para qualquer vetor $z \in \Lambda$ tal que $||z|| < ||u_2||$, o conjunto $\{u_1, z\}$ não constitui uma base para Λ. Como $v_1, v_2 \in \Lambda$, existem $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tais que

$$v_1 = a_1u_1 + a_2u_2 \quad \text{e} \quad v_2 = b_1u_1 + b_2u_2, \tag{4.5}$$

ou ainda,

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}. \tag{4.6}$$

Se θ_v e θ_u são os ângulos entre v_1 e v_2 e u_1 e u_2, respectivamente, então pelo Lema 4.2.5,

$$\frac{\pi}{3} \leq \theta_u \leq \frac{\pi}{2}.$$

Além disso, $\frac{\pi}{3} \leq \theta_v \leq \frac{\pi}{2}$. De fato, se $\theta_u < \frac{\pi}{3}$, então pelo Lema 4.2.4,

$$||u_1 - u_2|| < ||u_2||,$$

entretanto, uma vez que $\{u_1, u_2\}$ é uma base para Λ, o conjunto $\{u_1, u_1 - u_2\}$ também forma uma base para Λ e este fato contradiz a escolha de u_2. Agora, se

$$d = \left| det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \right|, \tag{4.7}$$

então d é um inteiro positivo e tomando o determinante em ambos os lados da Equação (4.6), obtemos

$$||v_1||||v_2||sen(\theta_v) = d||u_1||||u_2||sen(\theta_u). \tag{4.8}$$

Todavia, pela definição de mínimo sucessivo, $||v_1||||v_2|| \leq ||u_1||||u_2||$, e assim, a Equação

(4.8) implica que

$$d = \frac{||v_1||||v_2||}{||u_1||||u_2||}\frac{sen(\theta_v)}{sen(\theta_u)} \leq \frac{2}{\sqrt{3}} < 2,$$

o que nos garante que $d = 1$, ou seja, a matriz $\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$ é inversível. Somando este fato à Equação (4.6), temos

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

Portanto $\mathcal{B} = \{v_1, v_2\}$ é uma base para Λ.

□

Observação 4.2.3 *Observamos que, se substituirmos $\mathbb{R}^2$ por $\mathbb{R}^n$, o Lema 4.2.1 não é necessariamente verdadeiro. Este fato e um estudo para o caso $n \geq 5$ estão presentes em [28].*

A base para o reticulado como no Lema 4.2.1 é, muitas vezes, chamada de base mínima.

Observação 4.2.4 *Antes de apresentarmos o próximo resultado observamos que, em geral, se $\Lambda \subset \mathbb{R}^2$ é um reticulado algébrico bem arredondado e $\mathcal{B} = \{v_1, v_2\}$ é uma base para Λ, então deve existir uma matriz de mudança de base, inversível,*

$$U = \begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix} \in M_2(\mathbb{Z}) \tag{4.9}$$

de modo que $M' = MU$ é a matriz base para Λ correspondente a base mínima do reticulado.

Embora já tenhamos comentado que a função densidade de empacotamento de um reticulado descrita na Seção 3.2 atinge seu máximo, para reticulados em $\mathbb{R}^2$, no reticulado hexagonal Λ_{hex} e que este reticulado é bem arredondado, conforme o Exemplo 4.1.2, os próximos lemas garantem que necessariamente este máximo é atingido em reticulados do conjunto dos reticulados bem arredondados.

Lema 4.2.6 ([15], p. 6) *Sejam Λ e Ω reticulados em $\mathbb{R}^2$ com mínimos sucessivos $\lambda_1(\Lambda)$, $\lambda_2(\Lambda)$, $\lambda_1(\Omega)$ e $\lambda_2(\Omega)$, respectivamente. Considere $\mathcal{B} = \{v_1, v_2\}$ e $\mathcal{C} = \{u_1, u_2\}$ o conjunto formado pelos vetores correspondentes aos mínimos sucessivos de Λ e Ω, respectivamente. Se $v_1 = u_1$, o ângulo entre os vetores v_1 e v_2 e u_1 e u_2 são iguais e $\lambda_1(\Lambda) = \lambda_2(\Lambda)$, então*

$$\Delta(\Lambda) \geq \Delta(\Omega).$$

Demonstração: Pelo Lema 4.2.1, os conjuntos $\mathcal{B}$ e $\mathcal{C}$ constituem uma base mínima para os correspondentes reticulados, Λ e Ω. Além disso,

$$\lambda_1(\Lambda) = \lambda_2(\Lambda) = ||v_1|| = ||v_2|| = ||u_1|| = \lambda_1(\Omega) \leq ||u_2|| = \lambda_2(\Omega).$$

Sendo assim, como o raio de empacotamento de Λ é $\rho = \dfrac{|\Lambda|}{2} = \dfrac{\lambda_1(\Lambda)}{2}$, e $n = 2$, então $\mathcal{V}ol(\mathcal{B}(1)) = \pi$ e a densidade de empacotamento de Λ é

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)} = \frac{\pi\left(\dfrac{\lambda_1(\Lambda)}{2}\right)^2}{det(\Lambda)} = \frac{\pi\lambda_1(\Lambda)^2}{4det(\Lambda)}.$$

Logo, denotando por θ o ângulo entre v_1 e v_2, semelhante ao ângulo entre u_1 e u_2 e utilizando o fato que $det(\Lambda) = ||v_1||||v_2||sen(\theta)$, temos

$$\Delta(\Lambda) = \frac{\pi\lambda_1(\Lambda)^2}{4||v_1||||v_2||sen(\theta)} = \frac{\pi}{4sen(\theta)} \geq \frac{\pi\lambda_1(\Omega)^2}{4||u_1||||u_2||sen(\theta)} = \frac{\pi\lambda_1(\Omega)^2}{4det(\Omega)} = \Delta(\Omega). \tag{4.10}$$

□

Lema 4.2.7 ([15], p. 6) *Sejam $\Lambda \subset \mathbb{R}^2$ um reticulado de posto completo, $\mathcal{B} = \{v_1, v_2\}$ uma base para Λ tal que $||v_1|| = ||v_2||$ e θ o ângulo entre v_1 e v_2 tal que $\theta \in \left[\dfrac{\pi}{3}, \dfrac{\pi}{2}\right]$. Então $\mathcal{B} \subset S(\Lambda)$ e em particular, Λ é bem arredondado.*

Demonstração: Se $z \in \Lambda$, então $z = av_1 + bv_2$, para convenientes $a, b \in \mathbb{Z}$. Assim,

$$||z||^2 = a^2||v_1||^2 + b^2||v_2||^2 + 2abv_1^tv_2 = (a^2 + b^2 + 2abcos(\theta))||v_1||^2.$$

Se $ab > 0$, então é imediato que $||z||^2 \geq ||v_1||^2$. Agora, se $ab < 0$, então

$$||z||^2 = (a^2 + b^2 - |ab|)||v_1||^2 \geq ||v_1||^2,$$

pois $cos(\theta) \leq \dfrac{1}{2}$, por hipótese. Portanto, v_1 e v_2 são os vetores não nulos mais próximos da origem em Λ, logo, correspondem a mínimos sucessivos, e assim, formam uma base mínima, o que nos permite concluir que Λ é bem arredondado e isso completa a prova.

□

Por fim, estamos aptos a demonstrar o resultado indicado anteriormente.

Lema 4.2.8 ([15], p. 7) *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado com mínimos sucessivos $\lambda_1 \leq \lambda_2$ e $v_1, v_2 \in \Lambda$ seus respectivos vetores correspondentes, os quais formam uma base para Λ. Então o reticulado Λ_{wr} gerado por $\mathcal{C} = \left\{v_1, \frac{\lambda_1}{\lambda_2}v_2\right\}$ é bem arredondado com mínimo sucessivo igual à λ_1.*

Demonstração: Pelo Lema 4.2.5, o ângulo θ entre v_1 e v_2 pertence ao intervalo $\left[\frac{\pi}{3}, \frac{\pi}{2}\right]$ e obviamente θ é também o ângulo entre os vetores v_1 e $\frac{\lambda_1}{\lambda_2}v_2$. Pelo Lema 4.2.7, Λ_{wr} é bem arredondado com mínimo sucessivo igual à λ_1.

□

Concluímos a partir dos Lemas 4.2.6 e 4.2.8 que, para qualquer $\Lambda \subset \mathbb{R}^2$,

$$\Delta(\Lambda_{wr}) \geq \Delta(\Lambda). \tag{4.11}$$

Destacamos ainda que a igualdade na Equação (4.11) ocorre se, e somente se, Λ é um reticulado bem arredondado, o que é evidente a partir do Lema 4.2.6. Portanto, a densidade máxima de empacotamento entre os reticulados em $\mathbb{R}^2$ deve ocorrer para um reticulado bem arredondado.

Observação 4.2.5 *Uma segunda consequência da Equação (4.10) é que para qualquer reticulado bem arredondados em $\mathbb{R}^2$ é válida a igualdade*

$$sen(\theta) = \frac{\pi}{4\Delta(\Lambda)}, \tag{4.12}$$

o que significa que $sen(\theta)$ é um invariante e não depende da escolha específica da base mínima, embora convencionalmente consideramos a base descrita no Lema 4.2.5, com $\theta \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$.

Lema 4.2.9 ([15], p. 7) *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado bem arredondado. Um reticulado $\Omega \subset \mathbb{R}^2$ é semelhante a Λ se, e somente se, Ω é bem arredondado e $\theta(\Lambda) = \theta(\Omega)$.*

Demonstração: Seja $\mathcal{B} = \{v_1, v_2\}$ uma base mínima para Λ e suponhamos que Λ e Ω sejam reticulados semelhantes. Sendo assim, existem uma constante $\alpha \in \mathbb{R}$ e uma matriz ortogonal real U de ordem 2 tais que $\Omega = \alpha U\Lambda$.

Se $\mathcal{C} = \{u_1, u_2\}$ é uma base para Ω, então $u_1 = \alpha U v_1$ e $u_2 = \alpha U v_2$. Logo, $||u_1|| = ||u_2||$ e o ângulo entre u_1 e u_2 é $\theta(\Lambda) \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$. Pelo Lema 4.2.7, concluímos que $\mathcal{C}$ forma uma base mínima para Ω, e portanto, Ω é bem arredondado e $\theta(\Lambda) = \theta(\Lambda)$. Reciprocamente, assuma que

Ω é bem arredondado e $\theta(\Lambda) = \theta(\Lambda)$ e sejam $\lambda(\Lambda)$ e $\lambda(\Omega)$ os respectivos valores dos primeiros mínimos sucessivos de Λ e Ω. Definimos

$$z_1 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}u_1 \quad \text{e} \quad z_2 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}u_2.$$

Então o par de vetores v_1 e v_2 do conjunto $\mathcal{B}$ e o par de vetores z_1 e z_2 estão na circunferência de centro na origem e raio $\lambda(\Lambda)$ de $\mathbb{R}^2$ com mesmo ângulos entre si. Portanto, existe uma matriz ortogonal U de ordem 2 tal que

$$u_1 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}z_1 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}Uv_1 \quad \text{e} \quad u_2 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}z_2 = \frac{\lambda(\Lambda)}{\lambda(\Omega)}Uv_2,$$

e assim, os reticulados Λ e Ω são semelhantes e isto completa a demonstração.

□

Teorema 4.2.2 ([15], p. 3) *Seja Λ um reticulado de posto 2 em $\mathbb{R}^2$. Então*

$$\Delta(\Lambda) \leq \Delta(\Lambda_{hex}) = \frac{\pi}{2\sqrt{3}} = 0,906899... \ . \tag{4.13}$$

sendo a igualdade da equação acima verificada se, e somente se, Λ é semelhante à Λ_{hex}.

Demonstração: Seja Λ um reticulado de posto completo em $\mathbb{R}^2$. A desigualdade de densidade presente na Equação (4.11) garante que a maior densidade de empacotamento de um reticulado em $\mathbb{R}^2$ é alcançada por um reticulado bem arredondado. Além disso, devido a Observação 4.2.5,

$$\Delta(\Lambda) = \frac{\pi}{4sen(\theta)},$$

onde $\theta = \theta(\Lambda)$ é o ângulo entre os vetores da base de Λ. Logo, determinar a maior densidade do reticulado é equivalente a determinar o menor valor possível para $sen(\theta)$.

Pelo Lema 4.2.5, $\frac{\pi}{3} \leq \theta$, e então $\frac{\sqrt{3}}{2} \leq sen(\theta)$. No entanto, o reticulado hexagonal Λ_{hex} admite como base $\mathcal{B} = \left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$ e o ângulo formado entre os vetores da base $\mathcal{B}$ é $\theta = \frac{\pi}{3}$. Portanto, a maior densidade de empacotamento para um reticulado $\Lambda \subset \mathbb{R}^2$ é alcançada pelo reticulado hexagonal. Como $sen\left(\frac{\pi}{3}\right) = \frac{\sqrt{3}}{2}$, este valor é precisamente

$$\Delta(\Lambda_{hex}) = \frac{\pi}{4\frac{\sqrt{3}}{2}} = \frac{\pi}{2\sqrt{3}} = 0,906899... \ .$$

Por fim, suponhamos que para algum reticulado Λ, $\Delta(\Lambda) = \Delta(\Lambda_{hex})$. Então pela Equações (4.11) e (4.12), respectivamente, Λ é um reticulado bem arredondado e

$$\Delta(\Lambda) = \Delta(\Lambda_{hex}) \Leftrightarrow \frac{\pi}{4sen(\theta(\Lambda))} = \frac{\pi}{4sen\left(\frac{\pi}{3}\right)}.$$

Portanto, $\theta(\Lambda) = \frac{\pi}{3}$ e pelo Lema 4.2.9, Λ é semelhante ao reticulado Λ_{hex}. Pela Proposição 3.2.1, reticulados equivalentes admitem a mesma densidade de empacotamento e isto concluí o resultado.

□

4.3 Construção de uma família infinita de reticulados bem arredondados em $\mathbb{R}^2$

Como visto na seção anterior, no que se refere a reticulados da forma $\Lambda_{\mathbb{K}}$, sendo $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, apenas dois corpos imaginários apresentam reticulados bem arredondados. Todavia, este fato não se verifica quando estudamos reticulados da forma $\Lambda_{\mathbb{K}}(\mathcal{I})$, onde $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal fracionário do anel de inteiros de um corpo quadrático.

Nesta seção destacamos reticulados dessa forma e verificamos que existem infinitos corpos quadráticos cujo anel dos inteiros contém um ideal cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado. Para a construção de uma família infinita de ideais fazemos uso de uma conveniente base integral para o anel de inteiros e ideais, a qual chamamos, neste contexto, de base canônica.

A existência e unicidade de tal base, bem como demais aspectos dessa teoria são descritos em [7] e são de suma importância para o desenvolvimento dos Teoremas 4.3.4 e 4.3.5. Os próximos resultados asseguram a existência da base canônica citada acima, contudo, suas demonstrações exigem pré-requisitos que fogem dos objetivos do trabalho e por isso as omitimos.

Teorema 4.3.1 ([7], p. 94) *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros e $\mathcal{I}$ um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$. Então existem únicos $a, b, g \in \mathbb{Z}$ tais que $\mathcal{I} = \{ax + (b + g\delta)y \mid x, y \in \mathbb{Z}\}$ satisfazendo*

(i) $0 < g \leq b < a$,

(ii) $g \mid a$ *e* $g \mid b$,

onde $\delta \in \mathcal{O}_{\mathbb{K}}$ é dado por $\delta = \begin{cases} -\sqrt{d}, & \text{se } d \equiv 2, 3 \ (mod\ 4) \\ \dfrac{1-\sqrt{d}}{2}, & \text{se } d \equiv 1 \ (mod\ 4) \end{cases}$.

Em suma, o Teorema 4.3.1 nos diz que se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal fracionário, então existem $a, b, g \in \mathbb{Z}$ tais que

$$\mathcal{I} = \mathcal{I}(a, b, g) = \{ax + (b + g\delta)y \mid x, y \in \mathbb{Z}\}. \tag{4.14}$$

A igualdade $\mathcal{I} = \langle a, b + g\delta \rangle$ não se verifica apenas por este fato, pois apesar de terem a mesma base, os coeficientes de $\langle a, b + g\delta \rangle$ são elementos de $\mathcal{O}_{\mathbb{K}}$. Entretanto, a seguinte proposição, também disponível em [7], assegura que

$$\mathcal{I} = \{ax + (b + g\delta)y \mid x, y \in \mathbb{Z}\} = \langle a, b + g\delta \rangle. \tag{4.15}$$

Proposição 4.3.1 ([7], p. 95) *Se $a, b, g \in \mathbb{Z}$ e $\delta \in \mathcal{O}_{\mathbb{K}}$ são como no Teorema 4.3.1, então $a \mid \mathcal{N}_{\mathbb{K}}(b + g\delta)$, ou seja, $\mathcal{N}_{\mathbb{K}}(b + g\delta) = ak$, para algum $k \in \mathbb{Z}$.*

Mediante a condição da Proposição 4.3.1, exibimos o seguinte teorema que justifica o fato comentado anteriormente.

Teorema 4.3.2 ([7], p. 96) *Sejam $a, b, g \in \mathbb{Z}$ e $\delta \in \mathcal{O}_{\mathbb{K}}$ como no Teorema 4.3.1. Se $\mathcal{N}_{\mathbb{K}}(b + g\delta) = ak$, para algum $k \in \mathbb{Z}$, então o ideal $\mathcal{I} = \{ax + (b + g\delta)y \mid x, y \in \mathbb{Z}\}$ possui única base $\mathcal{B} = \{a, b + g\delta\}$.*

A única base integral $\mathcal{B} = \{a, b + g\delta\}$ que é composta pelos elementos unicamente determinados é chamada de ***base canônica*** do ideal $\mathcal{I}$. Antes de demonstrar os teoremas que apresentam tal família de ideais, exibimos uma versão simplificada de um resultado relacionado a inteiros livre de quadrados que está disponível em [9].

Teorema 4.3.3 ([9], p. 920) *Existem infinitos primos $p \in \mathbb{Z}$ tais que $3p - 4$ é livre de quadrados.*

A construção de reticulados bem arredondados através da imagem de ideais do anel de inteiros de corpos quadráticos está diretamente ligada a construção de uma base canônica correspondente a cada ideal. No próximo teorema apresentamos uma demonstração mais detalhada do que a apresentada em [18].

Teorema 4.3.4 ([18], p. 196) *Existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $d \equiv 3 \pmod 4$ tais que o anel de inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja bem arredondado.*

Demonstração: Seja $t \in \mathbb{Z}$ um inteiro positivo ímpar. Então, definimos

$$g = 1, \quad b = \frac{t-1}{2}, \quad a = 2b + 2 = t + 1 \quad \text{e} \quad d = (t+2)(3t+2) = 3t^2 + 8t + 4.$$

Os inteiros a, b, g satisfazem as condições da base canônica para todo $t \in \mathbb{Z}$. Note ainda que $d \equiv 3 \ (mod\ 4)$, uma vez que, como t é ímpar, existe $k \in \mathbb{Z}$ tal que $t = 2k + 1$, assim,

$$\begin{aligned} d &= 3t^2 + 8t + 4 \\ &= 3(2k+1)^2 + 8(2k+1) + 4 \\ &= 3(4k^2 + 4k + 1)^2 + 8(2k+1) + 4 \\ &= 12k^2 + 12k + 3 + 16k + 8 + 4 \\ &= 4(3k^2 + 7k + 3) + 3, \end{aligned} \tag{4.16}$$

e $4(3k^2 + 7k + 3) + 3 \equiv 3 \ (mod\ 4)$, equivalentemente, $-d \equiv 1 \ (mod\ 4)$. Inicialmente, afirmamos que existem infinitos $t \in \mathbb{Z}$ ímpares tais que d é livre de quadrados. De fato, se $\mathbb{P}$ é o conjunto dos números primos ímpares, então $\mathbb{P} \subset \{t + 2 \mid t \in \mathbb{Z}, 2 \nmid t\}$. Tomando $t \in \mathbb{Z}$ tal que $p = t + 2 \in \mathbb{P}$ e substituindo na Equação (4.16), temos

$$d = p(3p - 4).$$

Considere a decomposição em fatores primos de d dada pelo Teorema Fundamental da Aritmética,

$$d = p \underbrace{\prod_{i=1}^{r} p_i^{\alpha_i}}_{3p-4},$$

em que $r \in \mathbb{N}$ e $p_i, \alpha_i \in \mathbb{Z}$, p_i primo, para todo $1 \leq i \leq r$. Como d é livre de quadrados é necessário que para todo $i = 1, 2, \ldots, r$, $\alpha_i = 1$ e que $p \neq p_i$.

Observamos que se $p \mid 3p - 4$, então existe $k \in \mathbb{Z}$ tal que $4 = p(3 - k)$, e assim, $p \mid 4$, o que é uma contradição, pois $p \in \mathbb{P}$. Portanto, $p \nmid 3p - 4$, ou seja,

$$p \nmid \prod_{i=1}^{r} p_i^{\alpha_i},$$

o que nos garante que $p \neq p_i$, para todo $i = 1, 2, \ldots, r$. Dessa forma, para que $p(3p - 4)$ seja livre de quadrados é suficiente que $\alpha_i = 1$, para todo $i = 1, 2, \ldots, r$. Em outras palavras, é suficiente que $3p - 4$ seja livre de quadrados

Pelo Teorema 4.3.3, existem infinitos primos p tais que $3p - 4$ é livre de quadrados e consequentemente, infinitos primos p tal que d seja livre de quadrados. Para cada uma dessas infinitas possibilidades, existe $t \in \mathbb{Z}$ ímpar tal que $t = p - 2$ e dessa forma, existem infinitos

$t \in \mathbb{Z}$ ímpares com d livre de quadrados. Para qualquer t satisfazendo essa condição, definimos $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ e

$$\mathcal{I} = \langle a, b + g\delta \rangle = \left\langle t+1, \frac{t-\sqrt{-d}}{2} \right\rangle \subset \mathcal{O}_{\mathbb{K}}.$$

Como

$$\begin{aligned} \mathcal{N}_{\mathbb{K}}(b+g\delta) &= \sigma_1(b+g\delta)\sigma_2(b+g\delta) = \left(\frac{t-\sqrt{-d}}{2}\right)\left(\frac{t+\sqrt{-d}}{2}\right) \\ &= \frac{t^2+d}{4} = (t+1)^2 \\ &= a^2 \\ &= a^2 g, \end{aligned}$$

então as condições do Teorema 4.3.2 são satisfeitas. Logo, $\mathcal{B} = \left\{t+1, \frac{1-\sqrt{-d}}{2}\right\}$ é base canônica de $\mathcal{I}$. A matriz M, geradora de $\Lambda_{\mathbb{K}}(\mathcal{I})$, é dada por

$$M = \begin{pmatrix} \Re\sigma_1(t+1) & \Re\sigma_1\left(\frac{t-\sqrt{-d}}{2}\right) \\ \Im\sigma_1(t+1) & \Im\sigma_1\left(\frac{t-\sqrt{-d}}{2}\right) \end{pmatrix} = \begin{pmatrix} t+1 & \frac{t}{2} \\ 0 & -\frac{\sqrt{d}}{2} \end{pmatrix}$$

e para todo $v \in \Lambda_{\mathbb{K}}(\mathcal{I})$, existem $x_1, x_2 \in \mathbb{Z}$ tal que

$$v = \begin{pmatrix} t+1 & \frac{t}{2} \\ 0 & -\frac{d}{2} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (t+1)x_1 + \frac{t}{2}x_2 \\ -\frac{\sqrt{d}}{2}x_2 \end{pmatrix}.$$

Assim,

$$||v||^2 = (t+1)^2x_1^2 + t(t+1)x_1x_2 + \frac{t^2+d}{4}x_2^2, \tag{4.17}$$

e substituindo $a = t+1$ e $d = 3t^2+8t+4$ na Equação (4.17), temos

$$||v||^2 = a^2x_1^2 + a(a-1)x_1x_2 + a^2x_2^2.$$

Deste modo, temos os subsequentes casos

(i) Se $(x_1, x_2) = (\pm 1, 0) = (0, \pm 1)$, então $||v||^2 = a^2$,

(ii) Se $(x_1, x_2) = (1, 1) = (-1, -1)$, então $||v||^2 = 3a^2 - a$,

(iii) Se $(x_1, x_2) = (1, -1) = (-1, 1)$, então $||v||^2 = a^2 + a$,

(iv) Se $(x_1, x_2) \neq (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$, então $||v||^2 > a^2, 3a^2 - a, a^2 + a$.

Como $a = t + 1 > 0$, segue que $||v||^2$ assume menor valor em a^2, isto é, quando $x_1 = \pm 1$ e $x_2 = 0$, ou quando $x_1 = 0$ e $x_2 = \pm 1$. Em outras palavras, para $(x_1, x_2) = (1, 0)$, $(-1, 0)$, $(0, 1)$ ou $(0, -1)$. Logo, o conjunto de vetores mínimos é

$$S(\Lambda_{\mathbb{K}}(\mathcal{I})) = \left\{(t+1, 0), (-t-1, 0), \left(\frac{t}{2}, -\frac{\sqrt{d}}{2}\right), \left(-\frac{t}{2}, \frac{\sqrt{d}}{2}\right)\right\}$$

e assim, $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado. Portanto existem infinitos corpos quadráticos totalmente imaginários tais que existe pelo menos um ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ tal que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado.

□

Exemplo 4.3.1 *Para $t = 1 \in \mathbb{Z}$ nas condições do Teorema 4.3.4, como $d = (t+2)(3t+2)$, então $d = 3(3+2) = 15$ e $\mathbb{K} = \mathbb{Q}(\sqrt{-15})$. O ideal $\mathcal{I} = \left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-15})}$ dá origem a um reticulado bem arredondado cujo conjunto de vetores mínimos é*

$$S(\Lambda_{\mathbb{K}}(\mathcal{I})) = \left\{(2, 0), (-2, 0), \left(\frac{1}{2}, -\frac{\sqrt{15}}{2}\right), \left(-\frac{1}{2}, \frac{\sqrt{15}}{2}\right)\right\},$$

que é composto pela imagem dos elementos $\pm 2, \pm\frac{1-\sqrt{-15}}{2} \in \mathcal{O}_{\mathbb{K}}$ pelo homomorfismo canônico.

Exemplo 4.3.2 *Também nas condições do Teorema 4.3.4, se $t = 11 \in \mathbb{Z}$, então $d = (t+2)(3t+2) = 13(33+2) = 455$ e $\mathbb{K} = \mathbb{Q}(\sqrt{-455})$. O ideal $\mathcal{I} = \left\langle 12, \frac{12-\sqrt{-455}}{2} \right\rangle \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-455})}$ dá origem a um reticulado bem arredondado cujo conjunto de vetores mínimos é*

$$S(\Lambda_{\mathbb{K}}(\mathcal{I})) = \left\{(12, 0), (-12, 0), \left(\frac{11}{2}, -\frac{\sqrt{455}}{2}\right), \left(-\frac{11}{2}, \frac{\sqrt{455}}{2}\right)\right\}.$$

Novamente, devido a construção dada na demonstração do Teorema 4.3.4, este conjunto é composto pela imagem dos elementos $\pm 12, \pm\frac{11-\sqrt{-455}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-455})}$.

Assim como no Teorema 4.3.4, no Teorema 4.3.5 também apresentamos uma demonstração mais detalhada do resultado presente em [18].

Teorema 4.3.5 ([18], p. 197) *Existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $d \equiv 1 \pmod 4$ tais que o anel de inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja bem arredondado.*

Demonstração: A demonstração segue de modo análogo a que exibimos no Teorema 4.3.4. Seja $t \in \mathbb{Z}$ um inteiro positivo ímpar e definimos

$$g = 1, \quad b = \frac{t+1}{2}, \quad a = 2b + 1 = t + 2 \quad \text{e} \quad d = (t+2)(t-2) = t^2 - 4.$$

Novamente, os inteiros a, b, g satisfazem as condições para que sejam uma base canônica, para todo $t \in \mathbb{Z}$. Neste caso, $d \equiv 1 \ (mod\ 4)$, pois como t é ímpar, existe $k \in \mathbb{Z}$ tal que $t = 2k+1$. Logo,

$$d = (2k+1)^2 - 4 = 4k^2 + 4k + 1 - 4 = 4(k^2 + k - 1) + 1. \tag{4.18}$$

Observe que $4(k^2 + k - 1) + 1 \equiv 1 \ (mod\ 4)$. Mais uma vez mostramos que existem infinitos $t \in \mathbb{Z}$ ímpares tais que d é livre de quadrados. Considere $\mathbb{P} = \{t + 2 \mid t \in \mathbb{Z}, 2 \nmid t\}$ e seja $t \in \mathbb{Z}$ tal que $p = t + 2 \in \mathbb{P}$. Assim, a Equação (4.18) pode ser escrita como

$$d = p(p-4)$$

Considerando a decomposição em fatores primos de d dada pelo Teorema Fundamental da Aritmética

$$d = p \underbrace{\prod_{i=1}^{r} p_i^{\alpha_i}}_{p-4},$$

novamente com $r \in \mathbb{N}$ e $p_i, \alpha_i \in \mathbb{Z}$, p_i primo, para todo $1 \leq i \leq r$, e seguindo o fato de que d é livre de quadrados, obtemos que $\alpha_i = 1$ e que $p \neq p_i$, para todo $i = 1, 2, \ldots, r$, pois $p \nmid p - 4$, visto que $p > p - 4$, ou seja,

$$p \nmid \prod_{i=1}^{r} p_i^{\alpha_i},$$

o que nos garante que $p \neq p_i$, para todo $i = 1, 2, \ldots, r$. Sendo assim, para que $d = p(p-4)$ seja livre de quadrados é suficiente que $\alpha_i = 1$, para todo $i = 1, 2, \ldots, r$. Ou seja, é suficiente que $p - 4$ seja livre de quadrados.

Novamente, o Teorema 4.3.3 nos garante que existem infinitos primos p tais que $p-4$ é livre de quadrados, e dessa forma, infinitos primos p tais que d seja livre de quadrados. Para cada uma dessas infinitas possibilidades, existe $t \in \mathbb{Z}$ ímpar tal que $t = p - 2$ e dessa forma, existem infinitos $t \in \mathbb{Z}$ ímpares com d livre de quadrados. Para qualquer t satisfazendo essa condição, definimos $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e

$$\mathcal{I} = \langle a, b + g\delta \rangle = \left\langle t + 2, \frac{t+2}{2} - \frac{\sqrt{d}}{2} \right\rangle \subset \mathcal{O}_{\mathbb{K}}.$$

Como

$$\begin{aligned}\mathcal{N}_{\mathbb{K}}(b+g\delta) &= \sigma_1(b+g\delta)\sigma_2(b+g\delta) = \left(\frac{t+2}{2}-\frac{\sqrt{d}}{2}\right)\left(\frac{t+2}{2}+\frac{\sqrt{d}}{2}\right)\\ &= \frac{t^2+4t+4-d}{4} = t+2\\ &= a = ag,\end{aligned}$$

o que nos permite concluir que $\mathcal{B} = \left\{t+2, \frac{t+2}{2}-\frac{\sqrt{d}}{2}\right\}$ é base canônica de $\mathcal{I}$ e a matriz geradora de $\Lambda_{\mathbb{K}}(\mathcal{I})$ é dada por

$$M = \begin{pmatrix} \sigma_1(t+2) & \sigma_1\left(\frac{t+2}{2}-\frac{\sqrt{d}}{2}\right) \\ \sigma_2(t+2) & \sigma_2\left(\frac{t+2}{2}-\frac{\sqrt{d}}{2}\right) \end{pmatrix} = \begin{pmatrix} t+2 & \frac{t+2}{2}-\frac{\sqrt{d}}{2} \\ t+2 & \frac{t+2}{2}+\frac{\sqrt{d}}{2} \end{pmatrix}.$$

Utilizamos uma conveniente mudança de base com o intuito de simplificar os cálculos da norma de um elemento do reticulado. Sendo assim, considere $U = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$. Note que $det(U) = 1$, ou seja, U é uma matriz inversível. Logo, a Proposição 3.1.1 garante que o produto M' entre a matriz M e a matriz U também é uma matriz geradora para o reticulado $\Lambda_{\mathbb{K}}(\mathcal{I})$, e neste caso,

$$M' = \begin{pmatrix} \frac{t+2+\sqrt{d}}{2} & \frac{t+2-\sqrt{d}}{2} \\ \frac{t+2-\sqrt{d}}{2} & \frac{t+2+\sqrt{d}}{2} \end{pmatrix}.$$

Para todo $v \in \Lambda_{\mathbb{K}}(\mathcal{I})$, existem $x_1, x_2 \in \mathbb{Z}$ tais que

$$v = \begin{pmatrix} \frac{t+2+\sqrt{d}}{2} & \frac{t+2-\sqrt{d}}{2} \\ \frac{t+2-\sqrt{d}}{2} & \frac{t+2+\sqrt{d}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{t+2+\sqrt{d}}{2}x_1 + \frac{t+2-\sqrt{d}}{2}x_2 \\ \frac{t+2-\sqrt{d}}{2}x_1 + \frac{t+2+\sqrt{d}}{2}x_2 \end{pmatrix}$$

e

$$\begin{aligned}||v||^2 &= \left(\frac{t+2+\sqrt{d}}{2}x_1 + \frac{t+2-\sqrt{d}}{2}x_2\right)^2 + \left(\frac{t+2-\sqrt{d}}{2}x_1 + \frac{t+2+\sqrt{d}}{2}x_2\right)^2 \\ &= t(t+2)x_1^2 + 4(t+2)x_1x_2 + t(t+2)x_2^2.\end{aligned} \tag{4.19}$$

Substituindo $a = t+2$ na Equação (4.19), obtemos

$$||v||^2 = a(a-2)x_1^2 + 4ax_1x_2 + a(a-2)x_2^2.$$

Logo,

(i) Se $(x_1, x_2) = (\pm 1, 0) = (0, \pm 1)$, então $||v||^2 = a(a-2) = a^2 - 2a$,

(ii) Se $(x_1, x_2) = (1, 1) = (-1, -1)$, então $||v||^2 = 2a(a-2) + 4a = 2a^2$,

(iii) Se $(x_1, x_2) = (1, -1) = (-1, 1)$, então $||v||^2 = 2a(a-2) - 4a = 2a^2 - 8a$,

(iv) Se $(x_1, x_2) \neq (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$, então $||v||^2 > a^2 - 2a, 2a^2, 2a^2 - 8a$.

Como $a = t + 2 > 0$ e t é ímpar concluímos que necessariamente $a \geq 5$. Além disso, $2a^2 - 8a > a^2 - 2a$ se, e somente se, $a^2 - 6a > 0$, o que ocorre para $a < 0$ ou $a > 6$. Sendo assim, $||v||^2$ assume valor mínimo em $a^2 - 2a$ para $a \geq 7$, $x_1 = \pm 1$ e $x_2 = 0$ ou para $a \geq 7$, $x_1 = 0$ e $x_2 = \pm 1$. Finalizamos a demonstração observando que $a = t + 2$, e dessa forma, a restrição para a não influencia na infinidade de possibilidades para t ímpar. Neste caso o conjunto de vetores mínimos é dado por

$$S(\Lambda_{\mathbb{K}}(\mathcal{I})) = \left\{ \pm \left(\frac{t+2+\sqrt{d}}{2}, \frac{t+2-\sqrt{d}}{2} \right), \pm \left(\frac{t+2-\sqrt{d}}{2}, \frac{t+2+\sqrt{d}}{2} \right) \right\}.$$

Portanto, existem infinitos corpos quadráticos totalmente reais tais que existe pelo menos um ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é um reticulado bem arredondado.

□

Exemplo 4.3.3 *Para $t = 5 \in \mathbb{Z}$, nas condições do Teorema 4.3.5, temos $d = (t+2)(t-2) = 25 - 4 = 21$ e $\mathbb{K} = \mathbb{Q}(\sqrt{21})$. Sendo assim, o ideal do anel de inteiros de $\mathbb{K}$ que dá origem a um reticulado bem arredondado é $\mathcal{I} = \left\langle 7, \frac{7-\sqrt{21}}{2} \right\rangle \subset \mathcal{O}_{\mathbb{K}}$ e, pela construção apresentada na demonstração do Teorema 4.3.5, os elementos do anel de inteiros cujas imagens pelo homomorfismo canônico compõem o conjunto de vetores mínimos são $\pm\frac{7-\sqrt{21}}{2}$ e $\pm\frac{7+\sqrt{21}}{2}$.*

Embora os Teoremas 4.3.4 e 4.3.5 apresentem uma família infinita de ideais cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado, é provável que existam muitos outros reticulados com tal propriedade. Em outros termos, possivelmente existem outros reticulados bem arredondados no plano que podem ser obtidos pelo homomorfismo canônico através de ideais em corpos quadráticos reais e imaginários.

Observamos ainda que devido a construção apresentada na demonstração dos Teoremas 4.3.4 e 4.3.5, todos os reticulados bem arredondados sujeitos a esta construção admitem quatro elementos mínimos, isto é, $\#S(\Lambda_{\mathbb{K}}(\mathcal{I})) = 4$. O próximo resultado justifica que, de fato, todos os elementos da família infinita de ideais que construímos na prova de ambos os teoremas têm quatro elementos mínimos.

Proposição 4.3.2 ([18], p. 200) *Sejam $d \in \mathbb{Z}$ livre de quadrados, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e $\mathcal{I}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Se $d \neq \pm 3$, então $\#S(\Lambda_{\mathbb{K}}(\mathcal{I})) \leq 4$.*

Demonstração: Se $\#S(\Lambda_{\mathbb{K}}(\mathcal{I})) > 4$, como $\Lambda_{\mathbb{K}}(\mathcal{I})$ é um reticulado de posto completo, então pelo Lema 4.2.1, $\#S(\Lambda_{\mathbb{K}}(\mathcal{I})) = 6$, e neste caso, $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Lambda_{hex}$. Pelo Lema 4.2.9, $\theta(\Lambda_{\mathbb{K}}(\mathcal{I})) = \dfrac{\pi}{3}$, sendo assim, existem $u, v \in \Lambda_{\mathbb{K}}(\mathcal{I})$ tais que o ângulo entre ambos é $\dfrac{\pi}{3}$, o que nos permite afirmar que um destes vetores, digamos u, é obtido através do outro, v, por uma rotação de $\dfrac{\pi}{3}$, tendo em vista que u e v possuem mesma norma, pois $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado.

Logo, rotacionando $\dfrac{\pi}{3}$ o vetor $v = \left(x_{11} + x_{12}\sqrt{|d|}, x_{21} + x_{22}\sqrt{|d|}\right)$, com $x_{ij} \in \mathbb{Q}$, para $i, j = 1, 2$, obtemos

$$u = \begin{pmatrix} \dfrac{1}{2} & -\dfrac{\sqrt{3}}{2} \\ \dfrac{\sqrt{3}}{2} & \dfrac{1}{2} \end{pmatrix} v \in \mathbb{Q}(\sqrt{|d|}) \times \mathbb{Q}(\sqrt{|d|}),$$

implicando prontamente que $\sqrt{3} \in \mathbb{Q}(\sqrt{|d|})$. Portanto, $d = \pm 3$. A contra recíproca que acabamos de demonstrar concluí a prova

□

No que se refere a classificação de reticulados bem arredondados em $\mathbb{R}^2$, pode-se dizer que os resultados apresentados nesta seção são, até este momento, um dos principais desta teoria. No Capítulo 5 voltamos a estudar reticulados bidimensionais bem arredondados e apresentando outros reticulados obtidos através do anel de inteiros de corpos quadráticos, porém através do homomorfismo torcido apresentado na Seção 3.4.

4.4 Reticulados bem arredondados em $\mathbb{R}^n$

O principal objetivo desta seção é estudar reticulados bem arredondados em $\mathbb{R}^n$. Mais precisamente, reticulados obtidos através do anel de inteiros de corpos ciclotômicos. Provamos minuciosamente que se $\mathbb{K}$ é um corpo totalmente real ou totalmente imaginário de grau $n \geq 2$, então o reticulado $\Lambda_{\mathbb{K}}$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico, resultado encontrado em [4] e [18].

Ademais, estudamos algumas particularidades de reticulados da forma $\Lambda_{\mathbb{K}}(\mathcal{I})$ para alguns ideais principais $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$, sendo $\mathbb{K}$ um p-ésimo corpo ciclotômico, que apresentam boas propriedades no que se refere a ramificação, dentre outros aspectos, que são estudado em [12] e que tratamos no Capítulo 2. Motivados por um resultado apresentado em [14], caracterizamos quais elementos de ideais do anel de inteiros de um corpo ciclotômico correspondem a vetores de norma mínima em $\Lambda_{\mathbb{K}}$.

Inicialmente, recordamos que se $\mathcal{I}$ é um ideal do anel de inteiros de um corpo de números $\mathbb{K}$, então a norma do ideal $\mathcal{I}$, $\mathcal{N}(\mathcal{I})$ como na Definição 1.5.1, é o número de elementos do quociente $\mathcal{O}_{\mathbb{K}}/\mathcal{I}$. Se $\mathcal{I} = \langle\alpha\rangle$, para algum $\alpha \in \mathcal{O}_{\mathbb{K}}$, é um ideal principal, então $\mathcal{N}(\mathcal{I}) = |\mathcal{N}_{\mathbb{K}}(\alpha)|$. Os dois próximos resultados são ferramentas essenciais para a demonstração do resultado principal. O primeiro deles, conhecido como desigualdade das médias aritméticas e geométricas, é um resultado clássico da análise matemática e pode ser encontrado em [18]. O segundo, conhecido como Teorema de Kronecker, é um dos mais importantes no que se refere à teoria algébrica dos números e pode ser encontrado em [27].

Lema 4.4.1 ([18], p. 201) *Se $a_1, \ldots, a_n$ são números reais não negativos, então*

$$\left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{i=1}^{n} a_i. \tag{4.20}$$

A igualdade ocorre se, e somente se, $a_1 = \ldots = a_n$.

Teorema 4.4.1 (Kronecker, [27], p. 175) *Seja α um inteiro algébrico não nulo. Se α não é uma raiz da unidade, então pelo menos um conjugado de α possui norma absoluta estritamente maior que* 1.

Com o objetivo de provar que a imagem do anel de inteiros de um corpo de números $\mathbb{K}$ totalmente real ou totalmente imaginário pelo homomorfismo canônico é um reticulado bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico, enunciamos e demonstramos os próximos lemas, os quais são essenciais para demonstração de tal resultado.

Lema 4.4.2 ([4], p. 81) *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_{\mathbb{K}}$ o homomorfismo canônico associado. Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então*

$$\frac{n\mathcal{N}(\mathcal{I})^{\frac{2}{n}}}{2} \leq |\Lambda_{\mathbb{K}}(\mathcal{I})|^2, \tag{4.21}$$

onde $|\Lambda_{\mathbb{K}}(\mathcal{I})|$ é a norma do reticulado $\Lambda_{\mathbb{K}}(\mathcal{I}) = \sigma_{\mathbb{K}}(\mathcal{I})$.

Demonstração: Sejam $\sigma_1, \ldots, \sigma_{r_1}$ os r_1 monomorfismos reais de $\mathbb{K}$ e $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ os r_2 monomorfismos complexos de $\mathbb{K}$ não conjugados entre si. Considere ainda $\sigma_{i+r_1+r_2}$, com $1 \leq i \leq r_2$, os monomorfismos complexos conjugados a σ_{i+r_1}.

Dessa forma, se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\begin{aligned} |\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{1}{r_1+r_2}} &= \left|\prod_{i=1}^{n}\sigma_i(\alpha)\right|^{\frac{1}{r_1+r_2}} \\ &= \left(\prod_{i=1}^{r_1}|\sigma_i(\alpha)|^2\prod_{i=1}^{r_2}|\sigma_{i+r_1}(\alpha)\sigma_{i+r_1+r_2}(\alpha)|^2\right)^{\frac{1}{2(r_1+r_2)}} \\ &= \left(\prod_{i=1}^{r_1}|\sigma_i(\alpha)|^2\prod_{i=1}^{r_2}\left(\Re\left(\sigma_{i+r_1}(\alpha)\right)^2+\Im\left(\sigma_{i+r_1}(\alpha)\right)^2\right)^2\right)^{\frac{1}{2(r_1+r_2)}}. \end{aligned} \tag{4.22}$$

A última igualdade da equação acima segue do fato que o produto de um elemento $\beta \in \mathbb{C}$ por seu conjugado complexo é dado por $\Re(\beta)^2+\Im(\beta)^2$. Pelo Lema 4.4.1 e da igualdade $n = r_1+2r_2$, temos

$$\begin{aligned} |\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{1}{r_1+r_2}} &\leq \left(\frac{1}{n}\left(\sum_{i=1}^{r_1}\sigma_i(\alpha)^2+2\sum_{i=1}^{r_2}\left(\Re\left(\sigma_{i+r_1}(\alpha)\right)^2+\Im\left(\sigma_{i+r_1}(\alpha)\right)^2\right)\right)\right)^{\frac{n}{r_1+n}} \\ &\leq \left(\frac{2}{n}\|\sigma_{\mathbb{K}}(\alpha)\|^2\right)^{\frac{n}{r_1+n}}. \end{aligned} \tag{4.23}$$

Além isso, como $\dfrac{r_1+n}{n\,(r_1+r_2)} = \dfrac{r_1+(r_1+2r_2)}{(r_1+2r_2)(r_1+r_2)} = \dfrac{2(r_1+r_2)}{(r_1+2r_2)(r_1+r_2)} = \dfrac{2}{r_1+2r_2} = \dfrac{2}{n}$, então

$$\frac{n}{2}\,|\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{r_1+n}{n(r_1+r_2)}} \leq \|\sigma_{\mathbb{K}}(\alpha)\|^2 \Leftrightarrow \frac{n}{2}\,|\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{2}{n}} \leq \|\sigma_{\mathbb{K}}(\alpha)\|^2. \tag{4.24}$$

Como a Equação (4.23) é válida para todo $\alpha \in \mathcal{O}_{\mathbb{K}}$, em particular, é válida para os elementos de $\mathcal{I}$. Logo,

$$\begin{aligned} |\Lambda_{\mathbb{K}}(\mathcal{I})|^2 &= |\sigma_{\mathbb{K}}(\mathcal{I})|^2 = min\{\|\sigma_{\mathbb{K}}(\alpha)\|^2 \mid \alpha \in \mathcal{I}, \alpha \neq 0\} \\ &\geq min\left\{\frac{n}{2}\,|\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{2}{n}} \mid \alpha \in \mathcal{I}, \alpha \neq 0\right\} \\ &\geq \frac{n\mathcal{N}(\mathcal{I})^{\frac{2}{n}}}{2}, \end{aligned} \tag{4.25}$$

sendo a última desigualdade resultante do fato que $|\mathcal{N}_{\mathbb{K}}(\omega)| \geq \mathcal{N}(\mathcal{I})$, para todo $\omega \in \mathcal{I} \setminus \{0\}$. Em outras palavras, a última igualdade segue do fato que se $\langle\omega\rangle \subset \mathcal{I}$, para todo $\omega \in \mathcal{I}$, então $\#\left(\mathcal{O}_{\mathbb{K}}/\mathcal{I}\right) \leq \#\left(\mathcal{O}_{\mathbb{K}}/\langle\omega\rangle\right)$.

□

Lema 4.4.3 ([4], p. 82) *Sejam $\mathbb{K}$ um corpo de números totalmente real de grau $n = r_1$ e $\sigma_{\mathbb{K}}$*

o homomorfismo canônico associado. Se $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então

$$n\mathcal{N}(\mathcal{I})^{\frac{1}{n}} \leq |\Lambda_\mathbb{K}(\mathcal{I})|^2 \tag{4.26}$$

sendo $\Lambda_\mathbb{K}(\mathcal{I}) = \sigma_\mathbb{K}(\mathcal{I})$.

Demonstração: Sejam $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$, todos reais, uma vez que $n = r_1$. Para todo $\alpha \in \mathcal{O}_\mathbb{K}$,

$$|\mathcal{N}_\mathbb{K}(\alpha)|^{\frac{1}{n}} = \left(\prod_{i=1}^{n} |\sigma_i(\alpha)|\right)^{\frac{1}{n}} = \left(\left(\prod_{i=1}^{n} \sigma_i(\alpha)^2\right)^{\frac{1}{n}}\right)^{\frac{1}{2}} = \left(\prod_{i=1}^{n} \sigma_i(\alpha)^2\right)^{\frac{1}{2n}} \tag{4.27}$$

e pelo Lema 4.4.1,

$$\left(\prod_{i=1}^{n} \sigma_i(\alpha)^2\right)^{\frac{1}{2n}} \leq \left(\frac{1}{n}\sum_{i=1}^{n} \sigma_i(\alpha)^2\right)^{\frac{1}{2}} = \left(\frac{1}{n}\|\sigma_\mathbb{K}(\alpha)\|^2\right)^{\frac{1}{2}}.$$

Sendo assim, obtemos, como na demonstração do Lema 4.4.2, que

$$|\Lambda_\mathbb{K}(\mathcal{I})|^2 = min\{\|\sigma_\mathbb{K}(\alpha)\|^2 \mid \alpha \in \mathcal{I}, \alpha \neq 0\} \geq min\{n\,|\mathcal{N}_\mathbb{K}(\alpha)|^{\frac{2}{n}} \mid \alpha \in \mathcal{I}, \alpha \neq 0\}. \tag{4.28}$$

Por fim, como $\mathcal{N}(\mathcal{I}) \geq 1$ e $\dfrac{2}{n} > \dfrac{1}{n}$, então

$$|\Lambda_\mathbb{K}(\mathcal{I})|^2 \geq min\{n\,|\mathcal{N}_\mathbb{K}(\alpha)|^{\frac{2}{n}} \mid \alpha \in \mathcal{I}, \alpha \neq 0\} = n\mathcal{N}(\mathcal{I})^{\frac{2}{n}} \geq n\mathcal{N}(\mathcal{I})^{\frac{1}{n}}, \tag{4.29}$$

o que conclui o resultado. □

Lema 4.4.4 ([4], p. 83) *Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente complexo de grau n e $\sigma_\mathbb{K}$ o homomorfismo canônico associado. Dado $\alpha \in \mathcal{O}_\mathbb{K}$, se $\sigma_\mathbb{K}(\alpha) \in S(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K}))$, então α é uma raiz da unidade.*

Demonstração: Suponhamos que $\mathbb{K}$ é totalmente complexo, isto é, $r_1 = 0$ e $n = 2r_2$. Aplicando o Lema 4.4.2 para $\mathcal{I} = \mathcal{O}_\mathbb{K}$, temos

$$|\Lambda_\mathbb{K}|^2 = |\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})|^2 \geq \frac{n\mathcal{N}(\mathcal{O}_\mathbb{K})^{\frac{2}{n}}}{2} = \frac{2r_2\mathcal{N}(\mathcal{O}_\mathbb{K})^{\frac{1}{r_2}}}{2} = r_2, \tag{4.30}$$

uma vez que $\mathcal{N}(\mathcal{O}_\mathbb{K}) = 1$. Por outro lado, $||\sigma_\mathbb{K}(1)||^2 = r_2$, assim,

$$r_2 \geq |\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|^2 \tag{4.31}$$

e das Equações (4.30) e (4.31), concluímos que $|\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|^2 = r_2$. Do mesmo modo que na demonstração do Lema 4.4.2, como $|\mathcal{N}_{\mathbb{K}}(\alpha)| \geq 1$, pois $\alpha \in \mathcal{O}_{\mathbb{K}}$, e portanto, $\mathcal{N}_{\mathbb{K}}(\alpha) \in \mathbb{Z}$, segue que, se $\sigma_{\mathbb{K}}(\alpha) \in S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$, então

$$\begin{aligned} 1 &\leq |\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{1}{r_2}} = \left(\prod_{i=1}^{r_2} \left(\Re\left(\sigma_i(\alpha)\right)^2 + \Im\left(\sigma_i(\alpha)\right)^2\right)\right)^{\frac{1}{r_2}} \\ &\leq \frac{1}{r_2}\sum_{i=1}^{r_2} \left(\Re\left(\sigma_i(\alpha)\right)^2 + \Im\left(\sigma_i(\alpha)\right)^2\right) = \frac{\|\sigma_{\mathbb{K}}(\alpha)\|^2}{r_2} = \frac{r_2}{r_2} = 1. \end{aligned} \tag{4.32}$$

Além disso, o Lema 4.4.1 assegura que

$$\Re\left(\sigma_1(\alpha)\right)^2 + \Im\left(\sigma_1(\alpha)\right)^2 = \ldots = \Re\left(\sigma_{r_2}(\alpha)\right)^2 + \Im\left(\sigma_{r_2}(\alpha)\right)^2 = 1. \tag{4.33}$$

Logo, todos os conjugados de α admitem valor absoluto igual a 1. Portanto, segue do Teorema de Kronecker (Teorema 4.4.1) que α é uma raiz da unidade.

Em contrapartida, se $\mathbb{K}$ é totalmente real, ou seja, $r_2 = 0$ e $n = r_1$, de modo análogo ao que foi feito no caso imaginário, o Lema 4.4.3 e sua demonstração garantem que $|\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|^2 = r_1$, isto é, aplicando o Lema 4.4.3 para $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, temos

$$|\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|^2 \geq n\mathcal{N}(\mathcal{O}_{\mathbb{K}})^{\frac{1}{n}} = r_1\mathcal{N}(\mathcal{O}_{\mathbb{K}})^{\frac{1}{r_1}} = r_1, \tag{4.34}$$

novamente pelo fato que $\mathcal{N}(\mathcal{O}_{\mathbb{K}}) = 1$. Da mesma forma, $||\sigma_{\mathbb{K}}(1)|| = r_1$, o que nos permite concluir que $|\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})|^2 = r_1$ e, para cada α tal que $\sigma_{\mathbb{K}}(\alpha) \in S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$,

$$1 \leq |\mathcal{N}_{\mathbb{K}}(\alpha)|^{\frac{1}{r_1}} \leq \left(\prod_{i=1}^{r_2} \left(\sigma_i(\alpha)\right)^2\right)^{\frac{1}{r_1}} \leq \frac{1}{r_1}\sum_{i=1}^{r_1} \left(\sigma_i(\alpha)\right)^2 = \frac{\|\sigma_{\mathbb{K}}(\alpha)\|^2}{r_1} = 1, \tag{4.35}$$

pois $||\sigma_{\mathbb{K}}(\alpha)||^2 = r_1$. Pelo Lema 4.4.1,

$$\sigma_1(\alpha) = \ldots = \sigma_{r_1}(\alpha) = 1. \tag{4.36}$$

Por fim, o Teorema de Kronecker garante que α é uma raiz da unidade.

□

Apresentados os lemas acima, podemos finalmente proclamar e demonstrar o Teorema 4.4.2.

O Teorema 4.4.2 foi apresentado em [18] e sua demonstração foi adaptada em [4].

Teorema 4.4.2 ([4], p. 81) *Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente complexo e $\sigma_{\mathbb{K}}$ o homomorfismo canônico associado. Então o reticulado $\Lambda_{\mathbb{K}}$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.*

Demonstração: Admita que $\mathbb{K}$ seja totalmente real. Se $\mathbb{K} = \mathbb{Q} = \mathbb{Q}(\zeta_1)$, então

$$\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = \sigma_{\mathbb{K}}(\mathbb{Z}) = \mathbb{Z},$$

que é bem arredondado. Se $\mathbb{K} \neq \mathbb{Q}$, então $\mathbb{K}$ não é um corpo ciclotômico e as únicas raízes da unidade são ± 1, pois caso contrário, $\mathbb{K}$ possuiria um subcorpo ciclotômico não trivial $\mathbb{L}$, o que contradiz o fato de $\mathbb{K}$ ser real.

O Lema 4.4.4 nos garante que o conjunto de vetores mínimos $S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) \subset \{\sigma_{\mathbb{K}}(1), \sigma_{\mathbb{K}}(-1)\}$ e como $\sigma_{\mathbb{K}}(1) = -\sigma_{\mathbb{K}}(-1)$, não há r_1 vetores linearmente independentes em $S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$. Logo, se $\mathbb{K}$ é totalmente real, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\mathbb{K} = \mathbb{Q}$, que de fato é o único dos corpos totalmente reais que é ciclotômico.

Por outro lado, se admitirmos que $\mathbb{K}$ é totalmente complexo, ou seja, $n = 2r_2$, então, novamente pelo Lema 4.4.4, os únicos elementos $\alpha \in \mathcal{O}_{\mathbb{K}}$ tais que $\sigma_{\mathbb{K}}(\alpha) \in S(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$ são as raízes da unidade. Se ζ é uma raiz da unidade, então

$$\|\sigma_{\mathbb{K}}(\zeta)\|^2 = \sum_{i=1}^{r_2} \left(\Re\left(\sigma_i(\zeta)\right)^2 + \Im\left(\sigma_i(\zeta)\right)^2\right) = \sum_{i=1}^{r_2} 1 = r_2, \tag{4.37}$$

pois $\sigma_i(\zeta)$ pertence ao bola centrada na origem de raio 1 em $\mathbb{C}$. Pelo Lema 4.4.2,

$$|\sigma_{\mathbb{K}}\left(\mathcal{O}_{\mathbb{K}}\right)|^2 = r_2$$

e $S\left(\sigma_{\mathbb{K}}\left(\mathcal{O}_{\mathbb{K}}\right)\right) = \{\sigma_{\mathbb{K}}(\alpha) \mid \alpha \in G\}$, onde G é o subgrupo cíclico de $\mathbb{K}^*$ formado pelas raízes da unidade de $\mathbb{K}$. Podemos supor que o subgrupo G é gerado por $\zeta_k = e^{\frac{2\pi i}{k}}$, para algum $k \in \mathbb{Z}$. Sendo assim, temos as seguintes inclusões

$$G \subset \mathbb{Z}[\zeta_k] \subset \mathcal{O}_{\mathbb{K}}.$$

A primeira inclusão nos permite concluir que todas as raízes da unidade de $\mathbb{K}$ são combinações lineares inteiras de $1, \zeta_k, \zeta_k^2, \ldots, \zeta_k^{\varphi(k)-1}$, sendo estas raízes da unidade linearmente independentes entre si. Logo, o subgrupo G tem exatamente $\varphi(k)$ raízes da unidade linearmente independentes,

o que implica que $S\left(\sigma_{\mathbb{K}}\left(\mathcal{O}_{\mathbb{K}}\right)\right)$ possui $\varphi(k) \leq n$ vetores linearmente independentes.

Portanto, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\varphi(k) = n$, o que só pode ocorrer quando $\mathbb{K} = \mathbb{Q}(\zeta_k)$, que é um corpo ciclotômico.

□

Na seção anterior vimos que os únicos corpos quadráticos cuja imagem do anel de inteiros pelo homomorfismo canônico é um reticulado bem arredondado são $\mathbb{K} = \mathbb{Q}(i)$ e $\mathbb{K} = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, que correspondem aos únicos corpos ciclotômicos em dimensão 2, pois i é uma raiz 4-ésima primitiva da unidade e $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ é uma raiz 3-ésima primitiva da unidade. Duas consequências do Teorema 4.4.2 são os seguinte corolários.

Corolário 4.4.1 ([4], p. 84) *Sejam $\mathbb{K}$ um corpo de números galoisiano e $\sigma_{\mathbb{K}}$ o homomorfismo canônico associado a $\mathbb{K}$. O reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.*

Demonstração: Como $\mathbb{K}$ é uma extensão galoisiana de $\mathbb{Q}$, a Proposição 1.1.1 garante que $\mathbb{K}$ é um corpo totalmente real ou totalmente complexo, satisfazendo assim as hipóteses do Teorema 4.4.2 e concluindo o resultado.

□

Um dos fatos que é preservado do caso $n = 2$ para o caso geral e nas condições do Teorema 4.4.2 é o de que a imagem de um ideal fracionário $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ para $\mathbb{K}$ um corpo ciclotômico também é um reticulado bem arredondado.

Corolário 4.4.2 ([18], p. 191) *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico para alguma raiz n-ésima primitiva da unidade ζ_n, com $n \geq 2$. Se $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então o reticulado $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado.*

Demonstração: Seja $\mathcal{I}$ um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\zeta_n)$ para alguma raiz n-ésima primitiva da unidade, com $n \geq 2$. Se $n = 2$, então o Corolário 4.2.1 garante que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado. Suponhamos que $n > 2$ e seja $\alpha \in \mathcal{I}$ tal que $\sigma_{\mathbb{K}}(\alpha) \in S(\Lambda_{\mathbb{K}}(\mathcal{I}))$.

Como $\mathbb{K}$ é um corpo ciclotômico, então

$$||\sigma_{\mathbb{K}}(\alpha)||^2 = \sum_{i=1}^{\varphi(n)} \sigma_i(\alpha)\overline{\sigma_i}(\alpha).$$

Logo, para todo $0 \leq k \leq n$, tem-se que

$$\begin{aligned} ||\sigma_{\mathbb{K}}(\zeta_n^k\alpha)||^2 &= \sum_{i=1}^{\varphi(n)} \sigma_i(\zeta_n^k\alpha)\overline{\sigma_i}(\zeta_n^k\alpha) = \sum_{i=1}^{\varphi(n)} \sigma_i(\zeta_n^k)\sigma_i(\alpha)\overline{\sigma_i}(\zeta_n^k)\overline{\sigma_i}(\alpha) \\ &= \sum_{i=1}^{\varphi(n)} \sigma_i(\alpha)\overline{\sigma_i}(\alpha) = ||\sigma_{\mathbb{K}}(\alpha)||^2. \end{aligned}$$

Portanto, $\sigma_{\mathbb{K}}(\zeta_n^k\alpha) \in S(\Lambda_{\mathbb{K}}(\mathcal{I}))$, para todo $0 \leq k \leq n$. Como o conjunto $\mathcal{B} = \{\zeta_n^i \in \mathcal{O}_{\mathbb{K}} \mid 0 \leq i \leq \varphi(n) - 1\}$ forma uma base integral para $\mathcal{O}_{\mathbb{K}}$, então o conjunto $\mathcal{B}_{\mathcal{I}} = \{\zeta_n^i\alpha \in \mathcal{I} \mid 0 \leq i \leq \varphi(n) - 1\}$ é linearmente independente, e consequentemente,

$$\{\sigma_{\mathbb{K}}(\zeta_n^k\alpha) \in \mathbb{R}^{\varphi(n)} \mid 0 \leq i \leq \varphi(n) - 1\} \subset S(\Lambda_{\mathbb{K}}(\mathcal{I}))$$

é um conjunto linearmente independente em $\mathbb{R}^{\varphi(n)}$. Portanto, o reticulado $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado.

□

Exemplo 4.4.1 *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_8)$, $\sigma_{\mathbb{K}}$ o homomorfismo canônico associado e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros. O Corolário 4.4.2 nos garante que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é um reticulado bem arredondado, para o ideal fracionário $\mathcal{I} = (1 + \zeta_8)\mathcal{O}_{\mathbb{K}}$. De fato,*

$$\begin{aligned} \alpha &= (1 + \zeta_8)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3) \\ &= a_0(1 + \zeta_8) + a_1(1 + \zeta_8)\zeta_8 + a_2(1 + \zeta_8)\zeta_8^2 + a_3(1 + \zeta_8)\zeta_8^3 \\ &= a_0 + a_0\zeta_8 + a_1\zeta_8 + a_1\zeta_8^2 + a_2\zeta_8^2 + a_2\zeta_8^3 + a_3\zeta_8^3 + a_3\zeta_8^4 \\ &= a_0 + \zeta_8(a_0 + a_1) + \zeta_8^2(a_1 + a_2) + \zeta_8^3(a_2 + a_3) + a_3\zeta_8^4 \end{aligned}$$

com $a_0, a_1, a_2, a_3 \in \mathbb{Z}$. Substituindo $\zeta_8 = \dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2}$, $\zeta_8^2 = i$, $\zeta_8^3 = -\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2}$ e $\zeta_8^4 = -1$, temos

$$\begin{aligned} \alpha &= a_0 + \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)(a_0 + a_1) + i(a_1 + a_2) + \left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)(a_2 + a_3) - a_3 \\ &= a_0 + \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)a_0 + \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)a_1 + i(a_1 + a_2) \\ &+ \left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)a_2 + \left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)a_3 - a_3. \end{aligned}$$

Considerando $a_i = 1$ e $a_j = 0$, para $j \neq i$, $i = 0, 1, 2, 3$, temos

$$\alpha_0 = 1 + \zeta_8 = \frac{\sqrt{2} + 2}{2} + i\frac{\sqrt{2}}{2}, \qquad \alpha_1 = (1 + \zeta_8)\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{(\sqrt{2} + 2)}{2},$$
$$\alpha_2 = (1 + \zeta_8)\zeta_8^2 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2} + 2}{2} \quad e \quad \alpha_3 = (1 + \zeta_8)\zeta_8^3 = -\frac{\sqrt{2} + 2}{2} + i\frac{\sqrt{2}}{2}$$

e $\mathcal{B}_{\mathcal{I}} = \{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$ *corresponde a uma base para o ideal* $\mathcal{I} = (1+\zeta_8)\mathcal{O}_{\mathbb{K}}$. *Uma matriz geradora para o reticulado* $\Lambda_{\mathbb{K}}(\mathcal{I}) = \sigma_{\mathbb{K}}(\mathcal{I}) \subset \mathbb{R}^4$ *é*

$$M = \begin{pmatrix} \Re\sigma_1\left(\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) & \Re\sigma_1\left(\frac{\sqrt{2}}{2} + i\frac{(\sqrt{2}+2)}{2}\right) & \Re\sigma_1\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}+2}{2}\right) & \Re\sigma_1\left(-\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) \\ \Im\sigma_1\left(\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) & \Im\sigma_1\left(\frac{\sqrt{2}}{2} + i\frac{(\sqrt{2}+2)}{2}\right) & \Im\sigma_1\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}+2}{2}\right) & \Im\sigma_1\left(-\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) \\ \Re\sigma_2\left(\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) & \Re\sigma_2\left(\frac{\sqrt{2}}{2} + i\frac{(\sqrt{2}+2)}{2}\right) & \Re\sigma_2\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}+2}{2}\right) & \Re\sigma_2\left(-\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) \\ \Im\sigma_2\left(\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) & \Im\sigma_2\left(\frac{\sqrt{2}}{2} + i\frac{(\sqrt{2}+2)}{2}\right) & \Im\sigma_2\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}+2}{2}\right) & \Im\sigma_2\left(-\frac{\sqrt{2}+2}{2} + i\frac{\sqrt{2}}{2}\right) \end{pmatrix}.$$

Para todo vetor $v \in \Lambda_{\mathbb{K}}(\mathcal{I})$, *existem* $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ *tais que*

$$v = \begin{pmatrix} \frac{\sqrt{2}+2}{2} & \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}+2}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}+2}{2} & \frac{\sqrt{2}+2}{2} & \frac{\sqrt{2}}{2} \\ \frac{2-\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}-2}{2} \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}-2}{2} & \frac{\sqrt{2}-2}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}+2}{2}x_1 + \frac{\sqrt{2}}{2}x_2 - \frac{\sqrt{2}}{2}x_3 - \frac{\sqrt{2}+2}{2}x_4 \\ \frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}+2}{2}x_2 + \frac{\sqrt{2}+2}{2}x_3 + \frac{\sqrt{2}}{2}x_4 \\ \frac{2-\sqrt{2}}{2}x_1 - \frac{\sqrt{2}}{2}x_2 + \frac{\sqrt{2}}{2}x_3 + \frac{\sqrt{2}-2}{2}x_4 \\ \frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}-2}{2}x_2 + \frac{\sqrt{2}-2}{2}x_3 + \frac{\sqrt{2}}{2}x_4 \end{pmatrix}.$$

Assim,

$$\begin{aligned} ||v||^2 &= \left(\tfrac{\sqrt{2}+2}{2}x_1 + \tfrac{\sqrt{2}}{2}x_2 - \tfrac{\sqrt{2}}{2}x_3 - \tfrac{\sqrt{2}+2}{2}x_4\right)^2 + \left(\tfrac{\sqrt{2}}{2}x_1 + \tfrac{\sqrt{2}+2}{2}x_2 + \tfrac{\sqrt{2}+2}{2}x_3 + \tfrac{\sqrt{2}}{2}x_4\right)^2 \\ &+ \left(\tfrac{2-\sqrt{2}}{2}x_1 - \tfrac{\sqrt{2}}{2}x_2 + \tfrac{\sqrt{2}}{2}x_3 + \tfrac{\sqrt{2}-2}{2}x_4\right)^2 + \left(\tfrac{\sqrt{2}}{2}x_1 + \tfrac{\sqrt{2}-2}{2}x_2 + \tfrac{\sqrt{2}-2}{2}x_3 + \tfrac{\sqrt{2}}{2}x_4\right)^2 \\ &= \left(\tfrac{\sqrt{2}+2}{2}(x_1+x_4) + \tfrac{\sqrt{2}}{2}(x_2-x_3)\right)^2 + \left(\tfrac{\sqrt{2}}{2}(x_1+x_4) + \tfrac{\sqrt{2}+2}{2}(x_2+x_3)\right)^2 \\ &+ \left(\tfrac{2-\sqrt{2}}{2}(x_1-x_4) - \tfrac{\sqrt{2}}{2}(x_2-x_3)\right)^2 + \left(\tfrac{\sqrt{2}}{2}(x_1+x_4) + \tfrac{\sqrt{2}-2}{2}(x_2+x_3)\right)^2 \\ &= 4x_1^2 + 4x_2^2 + 4x_3^2 + 4x_4^2 + 4x_1x_2 + 4x_2x_3 + 4x_3x_4 - 4x_1x_4, \end{aligned}$$

cujo valor mínimo é $||v||^2 = 4$, *atingido, por exemplo, tomando* $x_i = 1$ *e* $x_j = 0$, *para* $i \neq j$ *e* $i, j = 1, 2, 3, 4$. *Os vetores correspondentes a estes casos são as imagens dos elementos da base* $\mathcal{B}_{\mathcal{I}}$,.

O Corolário 4.4.2 garante que a imagem de um ideal fracionário do anel de inteiros pelo homomorfismo canônico é um reticulado bem arredondado. Embora em seu enunciado não apresente explicitamente como determinar os elementos do ideal que correspondem aos vetores de norma mínima em $\Lambda_{\mathbb{K}}(\mathcal{I})$, a demonstração do mesmo descreve um método para determinar quais elementos compõem o conjunto de vetores mínimos.

Motivados por este fato, aprimoramos um resultado disponível em [13] que se refere à norma mínima de um vetor no reticulado obtido através da imagem do ideal principal $\mathcal{I} = (1-\zeta_p)\mathcal{O}_{\mathbb{K}}$,

o qual estudamos na Seção 2.3. Omitimos a demonstração do mesmo, pois para esta faz-se necessário uma série de pré-requisitos referentes a formas quadráticas e que fogem do objetivo principal deste trabalho. Por conveniência apresentamos a seguinte versão do resultado.

Proposição 4.4.1 ([13], p. 72) *Sejam $p \in \mathbb{Z}$ um primo ímpar, $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e $\mathcal{O}_\mathbb{K}$ seu anel de inteiros. Se $\alpha \in (1-\zeta_p)\mathcal{O}_\mathbb{K}$, com $\alpha \neq 0$, então $|\sigma_\mathbb{K}(\alpha)|^2 \geq p$. Além disso, a igualdade $|\sigma_\mathbb{K}(\alpha)|^2 = p$ é satisfeita para $\alpha = 1-\zeta_p$.*

Em suma, a Proposição 4.4.1 afirma que a norma do reticulado $\Lambda_\mathbb{K}(\mathcal{I}) = \sigma_\mathbb{K}((1-\zeta_p)\mathcal{O}_\mathbb{K})$ é $|\Lambda_\mathbb{K}(\mathcal{I})| = p$. Conectando este fato ao Corolário 4.4.2, que garante que $\Lambda_\mathbb{K}(\mathcal{I})$ é bem arredondado, uma vez que $(1-\zeta_p)\mathcal{O}_\mathbb{K}$ é um ideal fracionário, concluímos que existem outros elementos, ao menos $p-2$, cuja norma ao quadrado também é p.

O corolário a seguir, de nossa autoria, descreve explicitamente quais elementos possuem essa norma. Para demonstração do mesmo utilizamos a Proposição 3.3.1, que nos permite determinar a norma de um vetor através do traço do elemento correspondente no anel de inteiros.

Corolário 4.4.3 *Sejam $p \in \mathbb{Z}$ um primo ímpar, $\mathbb{K} = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_\mathbb{K}$ seu anel de inteiros e $\mathcal{I} = (1-\zeta_p)\mathcal{O}_\mathbb{K}$. Então $\mathcal{F} = \{\sigma_\mathbb{K}(\zeta_p^i - \zeta_p^{i+1}) \in \mathbb{R}^{p-1} \mid i = 0, 1, \ldots, p-2\} \subset S(\Lambda_\mathbb{K}(\mathcal{I}))$.*

Demonstração: Considere o conjunto $\mathcal{F} = \{\sigma_\mathbb{K}(\zeta_p^i - \zeta_p^{i+1}) \in \mathbb{R}^{p-1} \mid i = 0, 1, \ldots, p-2\}$. Para $i = 0$, ou seja, para $\sigma_\mathbb{K}(1-\zeta_p)$ a Proposição 4.4.1 assegura que $|\sigma_\mathbb{K}(1-\zeta_p)|^2 = p$ é a norma mínima, e portanto, $\sigma_\mathbb{K}(1-\zeta_p) \in S(\Lambda_\mathbb{K}(\mathcal{I}))$. Com o intuito de utilizar a Proposição 3.3.1 e explicitar os demais elementos de norma mínima, considere $\alpha = 1-\zeta_p$. Como $\mathbb{K}$ é um corpo totalmente complexo, o termo $c_\mathbb{K}$ dado na Proposição 3.3.1 é $c_\mathbb{K} = \dfrac{1}{2}$. Sendo assim, $|\sigma_\mathbb{K}(\alpha)|^2 = \dfrac{\mathcal{T}r_\mathbb{K}(\alpha\overline{\alpha})}{2}$. Então

$$|\sigma_\mathbb{K}(1-\zeta_p)|^2 = \frac{\mathcal{T}r_\mathbb{K}((1-\zeta_p)\overline{(1-\zeta_p)})}{2} = \frac{\mathcal{T}r_\mathbb{K}((1-\zeta_p)(1-\zeta_p^{-1}))}{2}$$

e como $(1-\zeta_p)\overline{(1-\zeta_p^{-1})} = (1-\zeta_p)(1-\zeta_p^{-1}) = 1-\zeta_p^{-1}-\zeta_p+1 = 2-\zeta_p^{-1}-\zeta_p$, segue que

$$\begin{aligned}
\mathcal{T}r_\mathbb{K}((1-\zeta_p)(1-\zeta_p^{-1})) &= \mathcal{T}r_\mathbb{K}(2-\zeta_p^{-1}-\zeta_p) \\
&= \mathcal{T}r_\mathbb{K}(2) - \mathcal{T}r_\mathbb{K}(\zeta_p^{-1}) - \mathcal{T}r_\mathbb{K}(\zeta_p) \\
&= 2(p-1) - (-1) - (-1) \\
&= 2p.
\end{aligned}$$

Portanto, em concordância com a Proposição 4.4.1,

$$|\sigma_{\mathbb{K}}(1-\zeta_p)|^2 = \frac{2p}{2} = p.$$

Para $1 \leq i \leq p-2$, observamos que $\overline{\zeta_p^i - \zeta_p^{i+1}} = \overline{\zeta_p^i} - \overline{\zeta_p^{i+1}} = \zeta_p^{-i} - \zeta_p^{-i-1}$, assim

$$\begin{aligned}(\zeta_p^i - \zeta_p^{i+1})(\zeta_p^{-i} - \zeta_p^{-i-1}) &= \zeta_p^i\zeta_p^{-i} - \zeta_p^i\zeta_p^{-i-1} - \zeta_p^{-i}\zeta_p^{i+1} + \zeta_p^{i+1}\zeta_p^{-i-1} \\ &= 1 - \zeta_p^{-1} - \zeta_p + 1,\end{aligned}$$

logo, $\overline{\zeta_p^i - \zeta_p^{i+1}} = \zeta_p^{-i} - \zeta_p^{-i-1}$ e $(\zeta_p^i - \zeta_p^{i+1})(\zeta_p^{-i} - \zeta_p^{-i-1}) = 2 - \zeta_p^{-1} - \zeta_p$. Portanto,

$$\begin{aligned}|\sigma_{\mathbb{K}}(\zeta_p^i - \zeta_p^{i+1})|^2 &= \frac{\mathcal{T}r_{\mathbb{K}}((\zeta_p^i - \zeta_p^{i+1})(\zeta_p^{-i} - \zeta_p^{-i-1}))}{2} \\ &= \frac{\mathcal{T}r_{\mathbb{K}}(2 - \zeta_p^{-1} - \zeta_p)}{2} \\ &= \frac{\mathcal{T}r_{\mathbb{K}}(2) - \mathcal{T}r_{\mathbb{K}}(\zeta_p^{-1}) - \mathcal{T}r_{\mathbb{K}}(\zeta_p)}{2} \\ &= \frac{2(p-1) + 1 + 1}{2} \\ &= p,\end{aligned}$$

o que nos permite concluir que

$$|\sigma_{\mathbb{K}}(1-\zeta_p)|^2 = |\sigma_{\mathbb{K}}(\zeta_p^i - \zeta_p^{i+1})|^2,$$

para todo $i = 1, \ldots p-2$ e que $\mathcal{F} = \{\sigma_{\mathbb{K}}(\zeta_p^i - \zeta_p^{i+1}) \in \mathbb{R}^{p-1} \mid i = 0, 1, \ldots, p-2\} \subset S(\Lambda_{\mathbb{K}}(\mathcal{I}))$.

□

Considerações Finais

Finalizamos esta seção com o Corolário 4.4.3, resultado de nossa autoria, que relaciona a família de ideais principais gerados pelos elementos $1-\zeta_p$, com p primo, com a teoria de reticulados bem arredondados. Como já ressaltamos neste trabalho, muitas vezes determinar quais elementos admitem norma mínima nem sempre é uma tarefa trivial, sendo que este resultado é uma pequena contribuição para o problema.

O fato deste estudo ser recente contribui para que existam algumas questões em aberto sobre o mesmo. Um dos problemas em aberto faz referência ao caso em que o corpo $\mathbb{K}$ do Teorema 4.4.2 é um corpo misto, ou seja, em que alguns dos homomorfismos são reais e outros complexos, ou seja, $r_1, r_2 \neq 0$.

Ressaltamos que todo o trabalho desenvolvido neste capítulo faz referências aos reticulados algébricos obtidos por meio do homomorfismo canônico descrito na Seção 3.3. No próximo capítulo, contudo, investigamos reticulados algébricos bem arredondados obtidos por meio do homomorfismo torcido e verificamos que por meio deste homomorfismo, podemos obter outros reticulados da forma $\Lambda_{\mathbb{K}}$, para um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ que são bem arredondados.

Capítulo

5

Construções de reticulados bem arredondados

Concluímos este trabalho apresentando, neste capítulo, algumas construções de reticulados bem arredondados. Na Seção 5.1 apresentamos alguns resultados de [16] e [17]. Estes resultados, bem como outras caracterizações presentes no Capítulo 4, motivam o principal resultado do trabalho, o qual encontra-se na Seção 5.2, e que nos permite construir reticulados bem arredondados através de $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, mais precisamente, reticulados semelhantes ao reticulado hexagonal. Ainda nesta seção, apresentamos um resultado análogo, contudo, para $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Finalizamos o Capítulo na Seção 5.3 apresentando uma série de exemplos de reticulados bem arredondados obtidos através do homomorfismo torcido aplicado no anel de inteiros de corpos quadráticos reais.

5.1 Condição necessária para existência de reticulados bem arredondados em $\mathbb{R}^2$

Conforme descrito no Capítulo 4, mais precisamente na Seção 4.3, existem infinitos ideais no anel de inteiros de algum corpo quadrático cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado. O principal objetivo dessa seção é descrever, conforme apresentado em [17], condições necessárias para que o anel de inteiros de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ possua um ideal que dê origem a um reticulado bem arredondado.

Iniciamos apresentando uma propriedade aritmética de um inteiro positivo.

Definição 5.1.1 *Um inteiro positivo livre de quadrados d satisfaz a condição λ-quase-quadrado, $\lambda \in \mathbb{R}$, $\lambda > 1$, se d possui algum divisor q tal que* $\sqrt{\frac{d}{\lambda}} \leq q < \sqrt{d}$.

Não encontramos a Definição 5.1.1 em literaturas matemáticas em português. Sendo assim, por conveniência, sugerimos o termo λ-quase-quadrado, do inglês λ-*nearsquare*, para o desenvolvimento do trabalho.

Exemplo 5.1.1 *O inteiro* 21 *satisfaz a condição* 3*-quase-quadrado, pois para* $q = 3$*, temos* $3 \mid 21$ *e a desigualdade*

$$2,6457... = \sqrt{7} = \sqrt{\frac{21}{3}} \leq 3 < \sqrt{21} = 4,5825...$$

é satisfeita.

Exemplo 5.1.2 *Se* $p \in \mathbb{Z}$ *é um primo, então* p *não satisfaz a condição* λ*-quase-quadrado, para todo* $\lambda \in \mathbb{R}$ *tal que* $1 < \lambda < p$*. De fato, como os únicos divisores de* p *são* 1 *e* p*, pois* p *é primo, segue que se* $q = p$*, então a desigualdade* $p < \sqrt{p}$ *não é válida. Por outro lado, se* $q = 1$*, a desigualdade* $\sqrt{\frac{p}{\lambda}} \leq 1 < \sqrt{p}$ *é satisfeita quando* $1 < p \leq \lambda$ *e, portanto,* p *satisfaz a condição* λ*-quase-quadrado neste segundo caso.*

Essa condição é de suma importância, pois como provamos ainda nesta seção, se d satisfaz a condição da Definição 5.1.1 para $\lambda = 3$, então o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ admite um ideal cuja imagem pelo homomorfismo canônico é bem arredondado.

O resultado o qual nos referimos é consequência de uma série de lemas técnicos e para a compreensão dos mesmos definimos uma sequência de funções de contagem para soluções de Equações Diofantinas Ternária da forma $p^2 + r^2 d = q^2$, onde $p, r, d, q \in \mathbb{Z}$. Não desenvolvemos de modo minucioso a Teoria de Equações Diofantinas, pois este tópico dispersa dos objetivos principais do trabalho. Além disso, estamos interessados em um caso particular de tais equações, mais precisamente, quando d é um inteiro livre de quadrados e $r = 1$, em concordância com a teoria apresentada em [16].

Sejam $p, r, d, q \in \mathbb{Z}$, com $d > 0$ livre de quadrados e $r > 0$. A função f definida por

$$f(r) = \#\left\{(p,q) \in \mathbb{Z}^2 \mid 0 < p < q, q^2 - p^2 = r^2 d, mdc(p,q) = 1 \text{ e } 0 < \frac{p}{q} \leq \frac{1}{2}\right\} \tag{5.1}$$

determina, para cada $r \in \mathbb{Z}$, a quantidade de pares de inteiros positivos (p, q) que são soluções da equação $q^2 - p^2 = r^2 d$, satisfazendo as demais condições apresentadas. Em sequência, definimos as funções

$$f_1(r) = \#\left\{(p,q) \in \mathbb{Z}^2 \mid p > 0, q > 0, q^2 - p^2 = r^2 d, mdc(p,q) = 1\right\} \tag{5.2}$$

e

$$f_2(r) = \#\left\{(p,q) \in \mathbb{Z}^2 \mid 0 < p < q, q^2 - p^2 = r^2 d \text{ e } 0 < \frac{p}{q} \leq \frac{1}{2}\right\}. \tag{5.3}$$

A função $f_1(r)$ é bem conhecida, um dos principais resultados relacionados a mesma, o qual está disponível em [25], fornece uma cota superior ao número de soluções nas devidas condições, que é dado por

$$f_1(r) \leq 2^{\omega\left(r^2 d\right)-1} = 2^{\omega(rd)-1}, \tag{5.4}$$

em que $\omega(x)$ é a função que determina o número de divisores primos de x. Observamos ainda que

$$f(r) \leq min\left\{f_1(r), f_2(r)\right\}. \tag{5.5}$$

Podemos, entretanto, utilizar uma outra versão da função f_2 apresentada na Equação (5.3), conforme descrito em [16]. Essa versão se dá mediante uma mudança de variável. Considere a equação $p^2 + rd^2 = q^2$ e sejam $a = q - p$ e $b = p + q$. Assim, $q = \dfrac{a+b}{2}$, $p = \dfrac{b-a}{2}$, $ab = r^2 d$ e para $\dfrac{p}{q} \leq \dfrac{1}{2}$, temos

$$1 < \frac{b}{a} = \frac{1+\frac{p}{q}}{1-\frac{p}{q}} = \frac{1}{1-\frac{p}{q}} + \frac{\frac{p}{q}}{1-\frac{p}{q}} \leq \frac{1}{1-\frac{1}{2}} + \frac{\frac{p}{q}}{1-\frac{1}{2}} = 2 + 2\frac{p}{q} \leq 2 + \frac{1}{2} \leq 3. \tag{5.6}$$

Como $b > 0$, então

$$b = \sqrt{\frac{b^2 a}{a}} = \sqrt{\frac{b}{a}(ab)} = \sqrt{\frac{b}{a} r^2 d} = \sqrt{\frac{1+\frac{p}{q}}{1-\frac{p}{q}} r^2 d} = r\sqrt{\frac{1+\frac{p}{q}}{1-\frac{p}{q}} d}. \tag{5.7}$$

Combinando as Equações (5.6) e (5.7), concluímos que $r\sqrt{d} < b \leq r\sqrt{3d}$. Portanto, a função f_2 pode ser escrita da seguinte forma

$$f_2(r) = \#\left\{b \in \mathbb{Z} \mid b > 0, b \mid r^2 d \text{ e } r\sqrt{d} < b \leq r\sqrt{3d}\right\}. \tag{5.8}$$

Essa versão da equação é muito importante, pois está relacionada com a condição necessária para que um corpo quadrático admita ideais em seu anel de inteiros cujos reticulados correspondentes são bem arredondados. O próximo lema é o primeiro da série de resultados que concluem os pré-requisitos para a demonstração do Teorema 5.1.2 e o demonstramos aqui de modo mais detalhado do que a demonstração apresentada em [17].

Lema 5.1.1 ([17], p. 144) *Seja $d \in \mathbb{Z}$, com $d > 0$ e livre de quadrados. A equação $p^2 + d = q^2$ possui sulução inteira $p, q \in \mathbb{Z}$ satisfazendo $\dfrac{p}{q} \leq \dfrac{1}{2}$ se, e somente se, $d = d_1 d_2$, para $d_1, d_2 \in \mathbb{Z}$,*

tais que

$$0 < d_1 < d_2 \quad e \quad \sqrt{\frac{d}{3}} \leq d_1 < \sqrt{d}. \tag{5.9}$$

Se este for o caso, então $mdc(d_1, d_2) = 1$ *e a solução* (p, q) *é tal que* $mdc(p, q) = 1$. *Além disso, se* d *é par, então não existe solução para* $p^2 + d = q^2$.

Demonstração: Observamos nitidamente que a equação $p^2+d = q^2$ admite solução $p^2+d = q^2$, com $p, q \in \mathbb{Z}$, se, e somente se, admite solução (p, q) positiva, isto é, solução tal que $0 < p, q$. O número de soluções inteiras positivas tais que $\frac{p}{q} \leq \frac{1}{2}$ é dado por $f_2(1)$ como descrito na Equação (5.3). Logo, a equação tem soluções se, e somente se, $f_2(1) \geq 1$. Consequentemente, para $r = 1$, a Equação (5.8) é dada por

$$f_2(1) = \#\left\{b \in \mathbb{Z} \mid b > 0, b \mid d \text{ e } \sqrt{d} < b \leq \sqrt{3d}\right\}$$

e este fato se verifica se, e somente se, $d = d_1 d_2$, para convenientes $d_1, d_2 \in \mathbb{Z}$ tais que

$$0 < d_1 < d_2 \quad \text{e} \quad \sqrt{d} \leq d_2 < \sqrt{3d},$$

condições que são equivalentes as dadas em (5.9). Juntamente a este fato, se as condições de (5.9) são verificadas, então $mdc(d_1, d_2) = 1$, pois neste caso, se $mdc(d_1, d_2) = g_1$, então

$$g_1 \mid d_1 \text{ e } g_1 \mid d_2 \Rightarrow g_1^2 \mid (d_1 d_2)^2 = d^2 \Rightarrow g_1 = 1,$$

sendo a última implicação decorrente do fato de que d é livre de quadrados. Ademais, se (p, q) é uma solução inteira com $mdc(p, q) = g_2$, então $g_2^2 \mid d$, e assim, como d é livre de quadrados, segue que $g_2 = 1$.

Finalmente, se $2 \mid d = q^2 - p^2 = (p + q)(p - q)$, então, como 2 é primo, o Lema de Euclides garante que $2 \mid q - p$ ou $2 \mid q + p$, o que significa que 2 divide $q - p$ e $q + p$, uma vez que se $2 \mid q - p$, como $2 \mid 2p$, então $2 \mid q - p + 2p = q + p$ e analogamente para $2 \mid q + p$. Assim, $2^2 \mid d$, o que contradiz o fato de que d é livre de quadrados. Portanto, $p^2 + d = q^2$ não tem solução.

□

A teoria desenvolvida em [16], assim como resultados de [17], referem-se a reticulados bem arredondados integrais, que são reticulados bem arredondados cujas matrizes de Gram possuem coordenadas inteiras. Para estes reticulados, enunciamos o principal resultado de [16].

Teorema 5.1.1 ([16], p. 2) *Se $\Lambda \subset \mathbb{R}^2$ é um reticulado bem arredondado integral, então*

$$cos(\theta(\Lambda)) = \frac{p}{q} \quad e \quad sen(\theta(\Lambda)) = \frac{r\sqrt{d}}{q}, \tag{5.10}$$

para $p, r, d, q \in \mathbb{Z}$, com $d > 0$ livre de quadrados, tais que $q^2 - p^2 = r^2 d$, $mdc(p, q) = 1$ e $\frac{p}{q} \leq \frac{1}{2}$. Além disso, $\Lambda \sim \Omega_d(p, q)$, em que $\Omega_d(p, q)$ é o reticulado cuja matriz geradora é $\begin{pmatrix} q & p \\ 0 & r\sqrt{d} \end{pmatrix}$, e para quaisquer $p, r, d, q \in \mathbb{Z}$ satisfazendo as condições anteriores, o reticulado $\Omega_d(p, q)$ é bem arredondado integral com ângulo $\theta(\Omega_d(p, q))$ satisfazendo (5.10).

Note que as condições do Teorema 5.1.1 estão relacionadas com as condições das funções de contagem que apresentamos anteriormente. Em [17] são generalizadas algumas construções para reticulados bem arredondados em $\mathbb{R}^2$ apresentadas em [18] e que desenvolvemos na Seção 4.3 do Capítulo 4, mostrando que muitas classes de semelhança de reticulados bem arredondados integrais em $\mathbb{R}^2$ contêm reticulados obtidos através da construção de uma base canônica.

Para o entendimento dos demais lemas necessários e por conveniência, nos referimos novamente a base canônica de ideais apresentada na Seção 4.3, $\mathcal{B} = \{a, b + g\delta\}$. Devido ao fato de que o desenvolvimento dos próximos lemas envolvem outros requisitos, como propriedades relacionadas a reticulados integrais, que fogem do nosso objetivo principal, apenas os enunciamos. As demonstrações podem ser encontradas em [17].

Apresentamos, contudo, as matrizes geradoras dos reticulados descritos nos próximos resultados. Seja $d \in \mathbb{Z}$, com $d > 0$, livre de quadrados. Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, definimos

$$\delta = \begin{cases} -\sqrt{d}, \text{ se } d \not\equiv 1 \ (mod\ 4) \\ \dfrac{1 - \sqrt{d}}{2}, \text{ se } d \equiv 1 \ (mod\ 4) \end{cases} \tag{5.11}$$

Para o primeiro caso, $d \not\equiv 1 \ (mod\ 4)$, consideramos a base canônica de um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ como sendo $\mathcal{B} = \{a, b - g\sqrt{d}\}$ e para o segundo caso, $d \equiv 1 \ (mod\ 4)$, $\mathcal{B} = \left\{a, b + \frac{g}{2} - \frac{g\sqrt{d}}{2}\right\}$. Desse modo, as respectivas matrizes geradoras dos reticulados são

$$M_1 = \begin{pmatrix} a & b - g\sqrt{d} \\ a & b + g\sqrt{d} \end{pmatrix} \quad \text{e} \quad M_2 = \begin{pmatrix} a & \dfrac{2b+g}{2} - \dfrac{g\sqrt{d}}{2} \\ a & \dfrac{2b+g}{2} + \dfrac{g\sqrt{d}}{2} \end{pmatrix}. \tag{5.12}$$

Se $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$, então definimos

$$\delta = \begin{cases} -\sqrt{-d}, \text{ se } d \not\equiv 1 \ (mod\ 4) \\ \dfrac{1-\sqrt{-d}}{2}, \text{ se } d \equiv 1 \ (mod\ 4) \end{cases} \tag{5.13}$$

e novamente, para $d \not\equiv 1 \ (mod\ 4)$, consideramos a base canônica de um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ como sendo $\mathcal{B} = \left\{a, b - g\sqrt{-d}\right\}$ e para $d \equiv 1 \ (mod\ 4)$, $\mathcal{B} = \left\{a, b + \dfrac{g}{2} - \dfrac{g\sqrt{-d}}{2}\right\}$. Logo, as matrizes geradoras dos reticulados são, respectivamente,

$$M_3 = \begin{pmatrix} a & b \\ 0 & -g\sqrt{d} \end{pmatrix} \quad \text{e} \quad M_4 = \begin{pmatrix} a & \dfrac{2b+g}{2} \\ 0 & -\dfrac{g\sqrt{d}}{2} \end{pmatrix} \tag{5.14}$$

Encerradas as notações podemos apresentar os próximos resultados. O primeiro destes, sob as hipóteses do Lema 5.1.1, descreve os termos para construção da base canônica e consequentemente define os ideais que dão origem a reticulados bem arredondados.

Lema 5.1.2 ([17], p. 146) *Sejam $d \in \mathbb{Z}$, com $d > 0$, ímpar e livre de quadrados satisfazendo a condição (5.9) do Lema 5.1.1 e (p, q) a solução da equação $p^2 + d = q^2$, com $\dfrac{p}{q} \leq \dfrac{1}{2}$. Então a classe de semelhança de $\Omega_d(p, q)$ contém reticulados da forma $\Lambda_{\mathbb{K}}(\mathcal{I})$. Mais especificamente, sejam*

$$(a, b) = \begin{cases} \left(p + q, \dfrac{p+q-1}{2}\right), & \text{se } d \equiv 1 \ (mod\ 4) \\ (2p + 2q, p + q), & \text{se } d \equiv 3 \ (mod\ 4) \end{cases} \tag{5.15}$$

e definimos

$$\begin{gathered} \mathcal{I} = \mathcal{I}(p, q) = \{ax + (b + \delta)y \mid x, y \in \mathbb{Z}\} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\ e \\ \mathcal{J} = \mathcal{J}(p, q) = \{ax + (b + \delta)y \mid x, y \in \mathbb{Z}\} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}. \end{gathered} \tag{5.16}$$

Para esta escolha de (a, b), onde δ é definido como nas Equações (5.11) e (5.13) os ideais $\mathcal{I}$ e $\mathcal{J}$ são ideais tais que $\Lambda_{\mathbb{Q}(\sqrt{d})}(\mathcal{I})$ e $\Lambda_{\mathbb{Q}(\sqrt{-d})}(\mathcal{J})$ são reticulados bem arredondados e pertencem à classe de semelhança de $\Omega_d(p, q)$.

Como descrito em [16], o fato de os reticulados do Lema 5.1.2 pertencerem a classe de semelhança do reticulado $\Omega_d(p, q)$ apresentado no Teorema 5.1.1 nos permite concluir que estes reticulados também são integrais.

Lema 5.1.3 ([17], p. 147) *Sejam $d \in \mathbb{Z}$, com $d > 0$ e livre de quadrados e considere $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ tal que exista um ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado. Então d deve satisfazer as condições (5.9) do Lema 5.1.1 e $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Omega_d(p,q)$ para convenientes (p,q) tais que $p^2 + d = q^2$, $mdc(p,q) = 1$ e $\frac{p}{q} \leq \frac{1}{2}$.*

Em suma, o Lema 5.1.3 afirma que para o anel de inteiros quadráticos de um corpo imaginário admitir um ideal cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado, é necessário que as condições do Lema 5.1.1 sejam satisfeitas. Impondo mais uma condição temos o seguinte resultado.

Lema 5.1.4 ([17], p. 148) *Sejam $d \in \mathbb{Z}$, com $d > 0$ livre de quadrados e $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ tal que exista um ideal bem arredondado $\mathcal{I} = \langle a, b + g\delta \rangle \subset \mathcal{O}_{\mathbb{K}}$, com $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondado, onde $\mathcal{B} = \{a, b + g\delta\}$ é a base canônica de $\mathcal{I}$. Assuma, além disso, que $a \mid 2d$, então d deve satisfazer a condição do Lema 5.1.1 e $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Omega_d(p,q)$ para convenientes p, q tais que $p^2 + d = q^2$, $mdc(p,q) = 1$ e $\frac{p}{q} \leq \frac{1}{2}$. Em particular, se*

(i) $d \not\equiv 1 \pmod 4$ e $min\{a^2, b^2 + d\} \geq 2ab$, ou

(ii) $d \equiv 1 \pmod 4$ e $min\left\{a^2, \frac{(2b+1)^2 + d}{4}\right\} \geq 2a(b+1)$,

então $a \mid 2d$.

Por fim, o último dos resultados diz respeito a corpos quadráticos imaginários e nos permite apresentar o Teorema 5.1.2.

Lema 5.1.5 ([17], p. 150) *Se $d \in \mathbb{Z}$, com $d > 0$ e livre de quadrados satisfaz as condições (5.9) do Lema 5.1.1 e $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$, então $\mathbb{K}$ contém um número finito de ideais $\mathcal{I}$ tal que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado, até a semelhança dos reticulados correspondentes.*

Demonstração: Uma vez satisfeitas as condições do Lema 5.1.1, este nos garante que existe um par de inteiros (p,q) tal que $p^2 + d = q^2$, para convenientes p, q com $mdc(p,q) = 1$ e $\frac{p}{q} \leq \frac{1}{2}$. Por outro lado, o Lema 5.1.2 afirma que, se $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$, então existe um ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado semelhante ao reticulado $\Omega_d(p,q)$, isto é, $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Omega_d(p,q)$ para cada (p,q) satisfazendo (5.9).

Por fim, o Lema 5.1.3 implica que todo ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ tal que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondado corresponde a uma solução da Equação (5.9). Assim, o número de ideais de $\mathcal{O}_{\mathbb{K}}$, até a classe de semelhança de $\Lambda_{\mathbb{K}}(\mathcal{I})$, é precisamente o número de pares (p,q) como em (5.9).

□

O número de ideais do Lema 5.1.5 é precisamente $f(1)$ como definido na Equação (5.1), que é estimado na Equação (5.5) utilizando a cota superior descrita na Equação (5.4). Como consequência dos Lemas 5.1.2, 5.1.3 e 5.1.5 e com o propósito de sintetizar tais resultados, apresentamos o Teorema 5.1.2.

Teorema 5.1.2 ([17], p. 141) *Seja $d \in \mathbb{Z}$, com $d > 0$ e livre de quadrados. Se d satisfaz a condição 3-quase-quadrado, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ do corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{\pm d})$ contém ideais $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é bem arredondados. O resultado torna-se se, e somente se, quando $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$.*

Demonstração: Segue dos Lemas 5.1.2, 5.1.3 e 5.1.5.

□

Observação 5.1.1 *De acordo com [17], este resultado implica, em particular, que uma proporção significativa dos corpos de números quadráticos reais e imaginários contém os ideais em seus anéis de inteiros cujos reticulados obtidos por sua imagem são bem arredondados.*

Mais especificamente, se $\mathcal{H} = \{\mathbb{K} = \mathbb{Q}(\sqrt{\pm d}) \mid 0 < d \leq n, n \in \mathbb{Z}\}$ e $\mathcal{H}_{\mathcal{I}} = \{\mathbb{K} = \mathbb{Q}(\sqrt{\pm d}) \mid \mathcal{O}_{\mathbb{K}}$ contém um ideal $\mathcal{I}$ com $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondado, $0 < d \leq n, n \in \mathbb{Z}\}$, então

$$\liminf_{n\to\infty} \frac{\#\mathcal{H}_{\mathcal{I}}}{\#\mathcal{H}} \geq \frac{\sqrt{3}-1}{2\sqrt{3}}, \tag{5.17}$$

ou seja, é possível exibir uma cota inferior para a quantidade de corpos quadráticos que admitem ideais $\mathcal{I}$ com $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondado. Além disso, ainda de acordo com [17], para cada d que satisfaz a condição 3-quase-quadrado, o corpo quadrático imaginário correspondente $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ contém apenas um número finito de ideais $\mathcal{I}$, com $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondados, até a semelhança dos reticulados correspondentes mediante a relação de equivalência que apresentamos na Definição 3.1.8, e esse número ψ satisfaz

$$\psi \ll min\left\{2^{\omega(d)-1}, \frac{2^{\omega(d)}}{\sqrt{\omega(d)}}\right\}, \tag{5.18}$$

sendo $\omega(d)$ é o número de divisores primos de d e a constante na notação de Vinogradov não depende de d, isto é, $\psi < min\left\{2^{\omega(d)-1}, \frac{2^{\omega(d)}}{\sqrt{\omega(d)}}\right\} k$, para alguma constante k que não depende de d. Em outras palavras, é possível encontrar uma cota superior para o número de ideais $\mathcal{I}$ com $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondado não semelhantes entre si.

Os resultados presentes nesta seção, sobretudo a equivalência descrita no Teorema 5.1.2 para corpos quadráticos imaginários reforçam nosso interesse no estudo de corpos quadráticos reais.

Observamos que para o caso em que $d = p \in \mathbb{Z}$ é primo, $d > 3$, não podemos garantir a existência de um ideal devido ao Exemplo 5.1.2, onde justificamos que um número primo p não satisfaz a condição λ-quase-quadrado para todo $\lambda < p$, de modo consequente, não satisfaz a condição 3-quase-quadrado. Embora essa não seja uma condição suficiente, pois conforme vimos no Teorema 4.3.5, existem corpos quadráticos reais que possuem ideais que produzem reticulados bem arredondados via homomorfismo canônico, este fato também motiva o estudo da próxima seção, onde fazemos uso da perturbação no homomorfismo canônico para construção de reticulados bem arredondados através de corpos reais.

5.2 Construções de reticulados bem arredondados através do homomorfismo torcido

Nesta seção estudamos construções de reticulados bem arredondados em $\mathbb{R}^2$ através do homomorfismo torcido. Pode-se dizer que o Teorema 5.2.1, de nossa autoria, e apresentado nesta seção é o principal resultado do trabalho, tendo em vista sua contribuição na construção de reticulados bem arredondados semelhantes ao reticulado hexagonal, que como exibimos na Seção 4.2, apresenta melhor densidade de empacotamento dentre todos os reticulados no plano. O Teorema 5.2.1 também contribui por apresentar uma família de elementos de $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ que dão origem a elementos que perturbam o homomorfismo canônico.

Apresentamos um segundo resultado que segue os mesmos princípios do teorema citado e que também nos permite descrever uma família de elementos que dão origem ao homomorfismo torcido, e consequentemente, a reticulados bem arredondados através da imagem do anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$.

Estes resultados são motivado principalmente pelo Lema 4.2.1, pois ainda que utilizando o homomorfismo torcido ao invés do canônico, possibilita a construção de reticulados bem arredondados através do anel de inteiros, e não de seus ideais, de um corpo quadrático diferente de $\mathbb{K} = \mathbb{Q}(i)$ e $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. No que se refere a reticulados da forma $\Lambda_{\mathbb{K}}(\mathcal{I})$, para um corpo quadrático $\mathbb{K}$ e $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$, os Teoremas 4.3.4, 4.3.5 e 5.1.2 apresentam diferentes condições para que existam reticulados bem arredondados. Para os Teoremas 4.3.4 e 4.3.5, todavia, os reticulados obtidos possuem explicitamente 4 vetores mínimos, e portanto, não possuem densidade ótima.

Teorema 5.2.1 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *e* $\alpha = \beta + \gamma\sqrt{3} \in \mathbb{K}$ *um elemento totalmente real e*

totalmente positivo. Se $2\gamma = \beta$*, isto é,* $\alpha = \beta + \frac{\beta}{2}\sqrt{3}$*, então o reticulado* $\Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ *é bem arredondado e semelhante ao reticulado hexagonal.*

Demonstração: De fato, como $3 \not\equiv 1 \ (mod\ 4)$, a base canônica de $\mathcal{O}_\mathbb{K}$ é $\mathcal{B} = \{1, -\sqrt{3}\}$. Seja $\alpha = \beta + \gamma\sqrt{3} \in \mathbb{K}$ um elemento totalmente real e totalmente positivo. Assim, σ_α está bem definido e de acordo com a Definição 3.4.3 é dado por

$$\begin{array}{rccl} \sigma_\alpha : & \mathbb{K} & \longrightarrow & \mathbb{R}^2 \\ & a + b\sqrt{3} & \longmapsto & \left(\sqrt{\beta + \gamma\sqrt{3}}(a + b\sqrt{3}), \sqrt{\beta - \gamma\sqrt{3}}(a - b\sqrt{3})\right). \end{array}$$

A matriz geradora de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ correspondente a base $\mathcal{B}$ é dada por

$$M = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{3}} & 0 \\ 0 & \sqrt{\beta - \gamma\sqrt{3}} \end{pmatrix} \begin{pmatrix} 1 & -\sqrt{3} \\ 1 & \sqrt{3} \end{pmatrix} = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{3}} & -\sqrt{3(\beta + \gamma\sqrt{3})} \\ \sqrt{\beta - \gamma\sqrt{3}} & \sqrt{3(\beta - \gamma\sqrt{3})} \end{pmatrix}$$

e um elemento arbitrário $v \in \Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ é

$$v = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{3}} & -\sqrt{3(\beta + \gamma\sqrt{3})} \\ \sqrt{\beta - \gamma\sqrt{3}} & \sqrt{3(\beta - \gamma\sqrt{3})} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\sqrt{\beta + \gamma\sqrt{3}} - y\sqrt{3(\beta + \gamma\sqrt{3})} \\ x\sqrt{\beta - \gamma\sqrt{3}} + y\sqrt{3(\beta - \gamma\sqrt{3})} \end{pmatrix}$$

para $x, y \in \mathbb{Z}$. Assim,

$$\begin{array}{rcl} ||v||^2 & = & \left(x\sqrt{\beta + \gamma\sqrt{3}} - y\sqrt{3(\beta + \gamma\sqrt{3})}\right)^2 + \left(x\sqrt{\beta - \gamma\sqrt{3}} + y\sqrt{3(\beta - \gamma\sqrt{3})}\right)^2 \\ & = & x^2\left(\beta + \gamma\sqrt{3}\right) - 2xy\sqrt{3}\left(\beta + \gamma\sqrt{3}\right) + 3y^2\left(\beta + \gamma\sqrt{3}\right) \\ & + & x^2\left(\beta - \gamma\sqrt{3}\right) + 2xy\sqrt{3}\left(\beta - \gamma\sqrt{3}\right) + 3y^2\left(\beta - \gamma\sqrt{3}\right) \\ & = & x^2\beta + x^2\gamma\sqrt{3} - 2xy\beta\sqrt{3} - 6xy\gamma + 3y^2\beta + 3y^2\gamma\sqrt{3} \\ & + & x^2\beta - x^2\gamma\sqrt{3} + 2xy\beta\sqrt{3} - 6xy\gamma + 3y^2\beta - 3y^2\gamma\sqrt{3} \\ & = & 2x^2\beta + 6y^2\beta - 12xy\gamma \\ & = & 2\left(x^2\beta + 3y^2\beta - 6xy\gamma\right). \end{array}$$

Substituindo a hipótese que $2\gamma = \beta$, obtemos

$$||v||^2 = 2\left(x^2\beta + 3y^2\beta - 3xy\beta\right) = 2\beta(x^2 + 3y^2 - 3xy).$$

Consequentemente, como $x^2 + 3y^2 - 3xy \geq 1$ para $x, y \in \mathbb{Z}$ não nulos simultaneamente, o conjunto de vetores mínimos de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ se dá para $x^2 + 3y^2 - 3xy = 1$, ou seja,

para os pares $(1,0)$, $(-1,0)$, $(1,1)$, $(-1,-1)$, $(2,1)$ e $(-2,-1)$. Portanto, $S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = \left\{\pm\left(\sqrt{\beta+\gamma\sqrt{3}}, \sqrt{\beta-\gamma\sqrt{3}}\right), \pm\left(\sqrt{\beta+\gamma\sqrt{3}} - \sqrt{3(\beta+\gamma\sqrt{3})}, \sqrt{\beta-\gamma\sqrt{3}} + \sqrt{3(\beta-\gamma\sqrt{3})}\right),\right.$ $\left.\pm\left(2\sqrt{\beta+\gamma\sqrt{3}} - \sqrt{3(\beta+\gamma\sqrt{3})}, 2\sqrt{\beta-\gamma\sqrt{3}} + \sqrt{3(\beta-\gamma\sqrt{3})}\right)\right\}$. Note que $\#S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = 6$, portanto, pelo Lema 4.2.1, $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é equivalente à Λ_{hex}.

□

Embora o Teorema 5.2.1 seja um resultado para um corpo real específico, o fato de o elemento β, que dá origem ao elemento que define a perturbação no homomorfismo canônico, ser racional, possibilita a construção de uma infinidade de reticulados semelhantes ao reticulado hexagonal. Em outras palavras, uma infinidade de reticulados de densidade ótima em $\mathbb{R}^2$. Ademais, este é resultado que se refere apenas ao anel de inteiros $\mathcal{O}_{\mathbb{Q}(\sqrt{3})}$ e não a seus ideais.

Exemplo 5.2.1 *Se $\beta = 1$ no Teorema 5.2.1, então $\alpha = 1 + \dfrac{\sqrt{3}}{2} \in \mathbb{Q}(\sqrt{3})$. A matriz geradora do reticulado $\sigma_\alpha(\mathcal{O}_{\mathbb{Q}(\sqrt{3})})$ e um vetor arbitrário $v \in \sigma_\alpha(\mathcal{O}_{\mathbb{Q}(\sqrt{3})})$ são, respectivamente,*

$$M = \begin{pmatrix} \sqrt{1+\frac{\sqrt{3}}{2}} & -\sqrt{3+\frac{3\sqrt{3}}{2}} \\ \sqrt{1-\frac{\sqrt{3}}{2}} & \sqrt{3-\frac{3\sqrt{3}}{2}} \end{pmatrix} \quad e \quad v = \begin{pmatrix} \sqrt{1+\frac{\sqrt{3}}{2}} & -\sqrt{3+\frac{3\sqrt{3}}{2}} \\ \sqrt{1-\frac{\sqrt{3}}{2}} & \sqrt{3-\frac{3\sqrt{3}}{2}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

com $x, y \in \mathbb{Z}$. Para os pares (x,y) como na demonstração do Teorema 5.2.1, o conjunto de vetores mínimos é $S(\sigma_\alpha(\mathcal{O}_{\mathbb{Q}(\sqrt{3})})) = \{\pm v_1, \pm v_2, \pm v_3\}$, em que $v_1 = \left(\sqrt{1+\frac{\sqrt{3}}{2}}, \sqrt{1-\frac{\sqrt{3}}{2}}\right)$, $v_2 = \left(\sqrt{1+\frac{\sqrt{3}}{2}} - \sqrt{3+\frac{3\sqrt{3}}{2}}, \sqrt{1-\frac{\sqrt{3}}{2}} + \sqrt{3-\frac{3\sqrt{3}}{2}}\right)$ e $v_3 = \left(2\sqrt{1+\frac{\sqrt{3}}{2}} - \sqrt{3+\frac{3\sqrt{3}}{2}}, 2\sqrt{1-\frac{\sqrt{3}}{2}} + \sqrt{3-\frac{3\sqrt{3}}{2}}\right)$

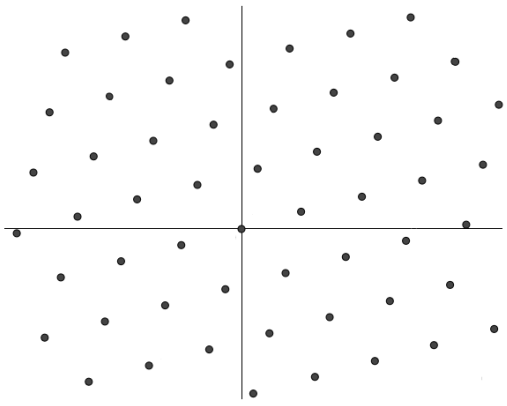

Figura 5.1: Reticulado $\Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ para $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ e $\alpha = 1 + \frac{\sqrt{3}}{2}$
Fonte: Elaborado pelo autor

O próximo resultado segue os mesmos princípios do Teorema 5.2.1, isto é, também descreve uma família infinita de elementos de mesmas características, porém para $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Ainda que o reticulado obtido não possua melhor densidade, este também contribui para o propósito de obter reticulados bem arredondados através de anéis de inteiros de corpos quadráticos reais.

Teorema 5.2.2 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ e $\alpha = \beta + \gamma\sqrt{2} \in \mathbb{K}$ um elemento totalmente real e totalmente positivo. Se $2\gamma = \beta$, isto é, $\alpha = \beta + \frac{\beta}{2}\sqrt{2}$, então o reticulado $\Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ é bem arredondado.*

Demonstração: Assim como no Teorema 5.2.1, a base canônica de $\mathcal{O}_\mathbb{K}$ é $\mathcal{B} = \{1, -\sqrt{2}\}$. Considerando $\alpha = \beta + \gamma\sqrt{2} \in \mathbb{K}$ um elemento totalmente real e totalmente positivo, σ_α está bem definido e é dado por

$$\begin{array}{rccl} \sigma_\alpha : & \mathbb{K} & \longrightarrow & \mathbb{R}^2 \\ & a + b\sqrt{2} & \longmapsto & \left(\sqrt{\beta + \gamma\sqrt{2}}(a + b\sqrt{2}), \sqrt{\beta - \gamma\sqrt{2}}(a - b\sqrt{2})\right). \end{array}$$

A matriz geradora de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ correspondente a base $\mathcal{B}$ é

$$M = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{2}} & 0 \\ 0 & \sqrt{\beta - \gamma\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & -\sqrt{2} \\ 1 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{2}} & -\sqrt{2(\beta + \gamma\sqrt{2})} \\ \sqrt{\beta - \gamma\sqrt{2}} & \sqrt{2(\beta - \gamma\sqrt{2})} \end{pmatrix}$$

e um vetor arbitrário $v \in \Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ é dado por

$$v = \begin{pmatrix} \sqrt{\beta + \gamma\sqrt{2}} & -\sqrt{2(\beta + \gamma\sqrt{2})} \\ \sqrt{\beta - \gamma\sqrt{2}} & \sqrt{2(\beta - \gamma\sqrt{2})} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\sqrt{\beta + \gamma\sqrt{2}} - y\sqrt{2(\beta + \gamma\sqrt{2})} \\ x\sqrt{\beta - \gamma\sqrt{2}} + y\sqrt{2(\beta - \gamma\sqrt{2})} \end{pmatrix}$$

para $x, y \in \mathbb{Z}$, cuja norma é

$$\begin{aligned} ||v||^2 &= \left(x\sqrt{\beta + \gamma\sqrt{2}} - y\sqrt{2(\beta + \gamma\sqrt{2})}\right)^2 + \left(x\sqrt{\beta - \gamma\sqrt{2}} + y\sqrt{2(\beta - \gamma\sqrt{2})}\right)^2 \\ &= x^2\left(\beta + \gamma\sqrt{2}\right) - 2xy\sqrt{2}\left(\beta + \gamma\sqrt{2}\right) + 2y^2\left(\beta + \gamma\sqrt{2}\right) \\ &+ x^2\left(\beta - \gamma\sqrt{2}\right) + 2xy\sqrt{2}\left(\beta - \gamma\sqrt{2}\right) + 2y^2\left(\beta - \gamma\sqrt{2}\right) \\ &= x^2\beta + x^2\gamma\sqrt{2} - 2xy\beta\sqrt{2} - 4xy\gamma + 2y^2\beta + 2y^2\gamma\sqrt{2} \\ &+ x^2\beta - x^2\gamma\sqrt{2} + 2xy\beta\sqrt{2} - 4xy\gamma + 2y^2\beta - 2y^2\gamma\sqrt{2} \\ &= 2x^2\beta + 4y^2\beta - 8xy\gamma \\ &= 2\left(x^2\beta + 2y^2\beta - 4xy\gamma\right). \end{aligned}$$

Como $2\gamma = \beta$, então

$$||v||^2 = 2\left(x^2\beta + 2y^2\beta - 2xy\beta\right) = 2\beta\left(x^2 + 2y^2 - 2xy\right).$$

Analogamente ao Teorema 5.2.1, como $x^2 + 2y^2 - 2xy \geq 1$ para $x, y \in \mathbb{Z}$ não nulos simultaneamente, então o conjunto de vetores mínimos de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é obtido para $x^2 + 2y^2 - 2xy = 1$, ou seja, para os pares $(1,0)$, $(-1,0)$, $(1,1)$ e $(-1,-1)$. Portanto, $S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = \left\{\pm\left(\sqrt{\beta+\gamma\sqrt{2}}, \sqrt{\beta-\gamma\sqrt{2}}\right), \pm\left(\sqrt{\beta+\gamma\sqrt{2}} - \sqrt{2(\beta+\gamma\sqrt{2})}, \sqrt{\beta-\gamma\sqrt{2}} + \sqrt{2(\beta-\gamma\sqrt{2})}\right)\right\}$.

Além disso, $\#S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = 4$, portanto, novamente pelo Lema 4.2.1, $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ um reticulado bem arredondado.

□

Exemplo 5.2.2 *Considere $\beta = 1$ no Teorema 5.2.2, logo, $\alpha = 1 + \dfrac{\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2})$. A matriz geradora e um vetor arbitrário de $\sigma_\alpha(\mathcal{O}_{\mathbb{Q}(\sqrt{2})})$ são respectivamente, para $x, y \in \mathbb{Z}$*

$$M = \begin{pmatrix} \sqrt{1+\frac{\sqrt{2}}{2}} & -\sqrt{2+\frac{2\sqrt{2}}{2}} \\ \sqrt{1-\frac{\sqrt{2}}{2}} & \sqrt{2-\frac{2\sqrt{2}}{2}} \end{pmatrix} \quad e \quad v = \begin{pmatrix} \sqrt{1+\frac{\sqrt{2}}{2}} & -\sqrt{2+\frac{2\sqrt{2}}{2}} \\ \sqrt{1-\frac{\sqrt{2}}{2}} & \sqrt{2-\frac{2\sqrt{2}}{2}} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Como $||v||^2 = 2(x^2 - 2xy + 2y^2)$ e $x^2 - 2xy + 2y^2 = 1$ é o valor mínimo não nulo, atingido para $(1,0)$, $(-1,0)$, $(1,1)$ e $(-1,-1)$, então o valor mínimo é $||v||^2 = 2$. Neste caso, o conjunto de vetores mínimos é

$$S(\sigma_\alpha(\mathcal{O}_{\mathbb{Q}(\sqrt{2})})) = \left\{\pm\left(\sqrt{\tfrac{2+\sqrt{2}}{2}}, \sqrt{\tfrac{2-\sqrt{2}}{2}}\right), \pm\left(\sqrt{\tfrac{2+\sqrt{2}}{2}} - \sqrt{2+\sqrt{2}}, \sqrt{\tfrac{2-\sqrt{2}}{2}} + \sqrt{2-\sqrt{2}}\right)\right\}.$$

A construção de reticulados por meio da perturbação no homomorfismo canônico infere aos mesmos diversas propriedades como, por exemplo, o fato de estes definirem os chamados ideais reticulados, que são reticulados algébricos providos de uma forma bilinear que pode ser descrita por uma forma traço e que são estudados em [1].

Os Teoremas 5.2.1 e 5.2.2, ainda que representem construções para corpos reais particulares, são pilares para um desenvolvimento futuro de construções de reticulados bem arredondados através do homomorfismo torcido.

5.3 Reticulados $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ para $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \equiv 1 \pmod 4$

Antes de concluir o trabalho, apresentamos uma série de exemplos envolvendo a perturbação no homomorfismo canônico e o anel de inteiros de corpos quadráticos $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d > 0$ e $d \equiv 1 \pmod 4$. Os reticulados que apresentamos são versões rotacionadas de $\mathbb{Z}^2$. Em [26] são apresentadas construções de reticulados semelhantes ao reticulado $\mathbb{Z}^n$, com $n \geq 2$. Estes reticulados admitem uma matriz ortogonal como geradora com relação a determinada base e, em relação a mesma, a matriz de Gram associada é a matriz identidade I_n.

Também é descrito em [1] que uma das condições necessárias, porém não suficientes, para a obtenção de reticulados $\mathbb{Z}^n$-rotacionados da forma $\sigma_\alpha(\mathcal{I})$, com $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$, é que

$$\mathcal{N}(\mathcal{I})\mathcal{N}_\mathbb{K}(\alpha)|\mathcal{D}_\mathbb{K}| = c^n, \tag{5.19}$$

em que $\mathcal{N}(\mathcal{I})$ é a norma do ideal $\mathcal{I}$, $\mathcal{N}_\mathbb{K}(\alpha)$ é a norma do elemento $\alpha \in \mathbb{K}$, $\mathcal{D}_\mathbb{K}$ é o discriminante do corpo e $c \in \mathbb{Z}$, com $c > 0$, é um inteiro positivo. Para o caso em que $\mathcal{I} = \mathcal{O}_\mathbb{K}$, a Equação (5.19) pode ser simplificada, uma vez que $\mathcal{N}(\mathcal{O}_\mathbb{K}) = 1$, e escrita como

$$\mathcal{N}_\mathbb{K}(\alpha)|\mathcal{D}_\mathbb{K}| = c^n. \tag{5.20}$$

Estamos interessados em versões de reticulados bidimensionais bem arredondados, ou seja, versões de reticulados $\mathbb{Z}^2$-rotacionados obtidos via homomorfismo torcido e que sejam bem arredondados. Como descrito no Exemplo 4.1.1, o reticulado $\Lambda_\mathbb{K} = \mathbb{Z}^2$, obtido através da imagem do anel de inteiros do corpo gaussiano, $\mathbb{K} = \mathbb{Q}(i)$, pelo homomorfismo canônico é bem arredondado.

Nos próximos exemplos construímos reticulados bem arredondados através do homomorfismo torcido, usando a Equação (5.20), por meio dos anéis de inteiros de corpos quadráticos reais.

Exemplo 5.3.1 *Sejam $d = 5$, $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ e $\mathcal{O}_\mathbb{K}$ seu anel de inteiros. Pelo Teorema 2.2.1, $\mathcal{O}_\mathbb{K} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ e $\mathcal{B} = \left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral para $\mathcal{O}_\mathbb{K}$. Considere o elemento totalmente real e totalmente positivo $\alpha = \frac{5+\sqrt{5}}{2} \in \mathbb{K}$ e note que $\mathcal{N}_\mathbb{K}(\alpha) = 5$.*

Pela Proposição 2.5.1, $\mathcal{D}_\mathbb{K} = 5$, isto é, $\mathcal{N}_\mathbb{K}(\alpha)|\mathcal{D}_\mathbb{K}| = 5^2$ e uma das condições necessárias para obtenção do reticulado $\mathbb{Z}^2$-rotacionado está satisfeita. O elemento α define uma perturbação no homomorfismo canônico, a qual é dada por

$$\begin{array}{rccl} \sigma_\alpha : & \mathbb{K} & \longrightarrow & \mathbb{R}^2 \\ & a + b\sqrt{5} & \longmapsto & \left(\sqrt{\frac{5+\sqrt{5}}{2}}(a+b\sqrt{5}), \sqrt{\frac{5-\sqrt{5}}{2}}(a-b\sqrt{5})\right). \end{array}$$

A matriz geradora de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ com relação a base $\mathcal{B}$ é

$$M = \begin{pmatrix} \sqrt{\frac{5+\sqrt{5}}{2}} & \sqrt{\frac{5+\sqrt{5}}{2}}\left(\frac{1+\sqrt{5}}{2}\right) \\ \sqrt{\frac{5-\sqrt{5}}{2}} & \sqrt{\frac{5-\sqrt{5}}{2}}\left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix}$$

e um vetor arbitrário $v \in \sigma_\alpha(\mathcal{O}_\mathbb{K})$ *é da forma*

$$v = \begin{pmatrix} \sqrt{\frac{5+\sqrt{5}}{2}} & \sqrt{\frac{5+\sqrt{5}}{2}}\left(\frac{1+\sqrt{5}}{2}\right) \\ \sqrt{\frac{5-\sqrt{5}}{2}} & \sqrt{\frac{5-\sqrt{5}}{2}}\left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{5+\sqrt{5}}{2}}x + \sqrt{\frac{5+\sqrt{5}}{2}}\left(\frac{1+\sqrt{5}}{2}\right) y \\ \sqrt{\frac{5-\sqrt{5}}{2}}x + \sqrt{\frac{5-\sqrt{5}}{2}}\left(\frac{1-\sqrt{5}}{2}\right) y \end{pmatrix}$$

com $x, y \in \mathbb{Z}$. *A norma ao quadrado de um vetor* $v \in \sigma_\alpha(\mathcal{O}_\mathbb{K})$ *é* $||v||^2 = 5x^2 + 10xy + 10y^2$, *que assume valor mínimo não nulo* $||v||^2 = 5$ *para* $(x, y) = (1, 0)$, $(-1, 0)$, $(1, -1)$ *e* $(-1, 1)$. *Portanto,*

$$S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = \left\{ \pm\left(\sqrt{\tfrac{5+\sqrt{5}}{2}}, \sqrt{\tfrac{5-\sqrt{5}}{2}}\right), \pm\left(\sqrt{\tfrac{5+\sqrt{5}}{2}}\left(1 - \tfrac{1+\sqrt{5}}{2}\right), \sqrt{\tfrac{5-\sqrt{5}}{2}}\left(1 - \tfrac{1-\sqrt{5}}{2}\right)\right)\right\}.$$

Ressaltamos que $\#S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = 4$ *e então, pelo Lema 4.2.1, o reticulado* $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ *é bem arredondado. Por fim, a matriz de Gram* $G = M^t M$ *é dada por*

$$\begin{pmatrix} \sqrt{\frac{5+\sqrt{5}}{2}} & \sqrt{\frac{5-\sqrt{5}}{2}} \\ \sqrt{\frac{5+\sqrt{5}}{2}}\left(\frac{1+\sqrt{5}}{2}\right) & \sqrt{\frac{5-\sqrt{5}}{2}}\left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix} \begin{pmatrix} \sqrt{\frac{5+\sqrt{5}}{2}} & \sqrt{\frac{5+\sqrt{5}}{2}}\left(\frac{1+\sqrt{5}}{2}\right) \\ \sqrt{\frac{5-\sqrt{5}}{2}} & \sqrt{\frac{5-\sqrt{5}}{2}}\left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 10 \end{pmatrix}$$

que, embora seja uma matriz diagonal, não corresponde a matriz identidade.

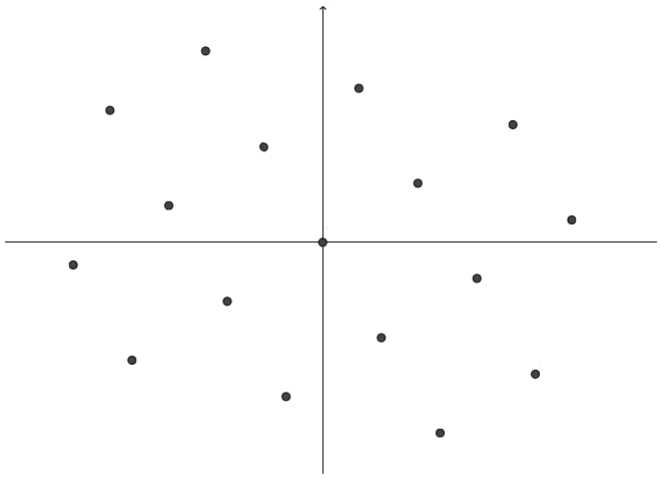

Figura 5.2: Reticulados $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ para $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ e $\alpha = \frac{5+\sqrt{5}}{2}$
Fonte: Elaborado pelo autor

Todavia, um simples cálculo monstra que o produto interno entre dois vetores linearmente independentes de $S(\sigma_\alpha(\mathcal{O}_\mathbb{K})$ *é* 0. *Em outras palavras, o ângulo* $\theta(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = \dfrac{\pi}{2}$, *e portanto, este reticulado é um* $\mathbb{Z}^2$*-rotacionado.*

Também poderíamos verificar que $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um $\mathbb{Z}^2$-rotacionado usando a matriz mudança de base $T=\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. *De fato, neste caso a matriz geradora do reticulado $\mathbb{Z}^2$ é* $R=\frac{1}{\sqrt{5}}MT$, *pois $R^tR=I_2$ é a matriz identidade de ordem 2.*

Exemplo 5.3.2 *No caso em que $d=13$, consideramos $\mathbb{K}=\mathbb{Q}(\sqrt{13})$ e* $\mathcal{B}=\left\{1, \frac{1+\sqrt{13}}{2}\right\}$ *uma base para* $\mathcal{O}_\mathbb{K}=\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$. *O elemento* $\alpha=\frac{13+3\sqrt{13}}{2}\in\mathbb{K}$ *é totalmente real e totalmente positivo e $\mathcal{N}_\mathbb{K}(\alpha)=13$. Logo, a condição da Equação (5.20), $\mathcal{N}_\mathbb{K}(\alpha)|\mathcal{D}_\mathbb{K}|=13^2$ é satisfeita. O homomorfismo torcido é*

$$\begin{array}{rccl} \sigma_\alpha: & \mathbb{K} & \longrightarrow & \mathbb{R}^2 \\ & a+b\sqrt{13} & \longmapsto & \left(\sqrt{\frac{13+3\sqrt{13}}{2}}(a+b\sqrt{13}), \sqrt{\frac{13-3\sqrt{13}}{2}}(a-b\sqrt{13})\right). \end{array}$$

De modo análogo ao Exemplo 5.3.1, a matriz geradora do reticulado com relação a base $\mathcal{B}$ é

$$M=\begin{pmatrix} \sqrt{\frac{13+3\sqrt{13}}{2}} & \sqrt{\frac{13+3\sqrt{13}}{2}}\left(\frac{1+\sqrt{13}}{2}\right) \\ \sqrt{\frac{13-3\sqrt{13}}{2}} & \sqrt{\frac{13-3\sqrt{13}}{2}}\left(\frac{1-\sqrt{13}}{2}\right) \end{pmatrix}$$

e um elemento $v\in\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é da forma

$$v=\begin{pmatrix} \sqrt{\frac{13+3\sqrt{13}}{2}} & \sqrt{\frac{13+3\sqrt{13}}{2}}\left(\frac{1+\sqrt{13}}{2}\right) \\ \sqrt{\frac{13-3\sqrt{13}}{2}} & \sqrt{\frac{13-3\sqrt{13}}{2}}\left(\frac{1-\sqrt{13}}{2}\right) \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} \sqrt{\frac{13+3\sqrt{13}}{2}}x+\sqrt{\frac{13+3\sqrt{13}}{2}}\left(\frac{1+\sqrt{13}}{2}\right)y \\ \sqrt{\frac{13-3\sqrt{13}}{2}}x+\sqrt{\frac{13-3\sqrt{13}}{2}}\left(\frac{1-\sqrt{13}}{2}\right)y \end{pmatrix}$$

com $x,y\in\mathbb{Z}$. Como

$$||v||^2=13x^2+52xy+65y^2=13(x^2+4xy+5y^2),$$

que assume valor mínimo $||v||^2=13$ para $(x,y)=(1,0)$, $(-1,0)$, $(-2,1)$ e $(1,-2)$, então $\#S(\sigma_\alpha(\mathcal{O}_\mathbb{K}))=4$, e portanto, $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado bem arredondado.

Assim como no Exemplo 5.3.1, podemos verificar que $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é um $\mathbb{Z}^2$-rotacionado usando a matriz mudança de base $T=\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$. *Neste caso, a matriz geradora de $\mathbb{Z}^2$ é* $R=\frac{1}{\sqrt{13}}MT$ *e $R^tR=I_2$.*

Exemplo 5.3.3 *Se $d=29$, consideramos $\mathbb{K}=\mathbb{Q}(\sqrt{29})$ o corpo quadrático real. O conjunto* $\mathcal{B}=\left\{1, \frac{1+\sqrt{29}}{2}\right\}$ *é uma base para $\mathcal{O}_\mathbb{K}$. Para* $\alpha=\frac{29+5\sqrt{29}}{2}$, *$\alpha$ é totalmente real e totalmente positivo, logo, define uma perturbação no homomorfismo canônico. Note ainda que $\mathcal{N}_\mathbb{K}(\alpha)=29$ e novamente, $\mathcal{N}_\mathbb{K}(\alpha)|\mathcal{D}_\mathbb{K}|=29^2$. O homomorfismo torcido é*

$$\begin{array}{rccl} \sigma_\alpha: & \mathbb{Q}(\sqrt{29}) & \longrightarrow & \mathbb{R}^2 \\ & a+b\sqrt{29} & \longmapsto & \left(\sqrt{\frac{29+5\sqrt{29}}{2}}(a+b\sqrt{29}), \sqrt{\frac{29-5\sqrt{29}}{2}}(a-b\sqrt{29})\right) \end{array}$$

Assim, a matriz geradora com relação a base $\mathcal{B}$ é

$$M = \begin{pmatrix} \sqrt{\frac{29+5\sqrt{29}}{2}} & \sqrt{\frac{29+5\sqrt{29}}{2}}\left(\frac{1+\sqrt{29}}{2}\right) \\ \sqrt{\frac{29-5\sqrt{29}}{2}} & \sqrt{\frac{29-5\sqrt{29}}{2}}\left(\frac{1-\sqrt{29}}{2}\right) \end{pmatrix}$$

e um vetor arbitrário de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é

$$v = \begin{pmatrix} \sqrt{\frac{29+5\sqrt{29}}{2}} & \sqrt{\frac{29+5\sqrt{29}}{2}}\left(\frac{1+\sqrt{29}}{2}\right) \\ \sqrt{\frac{29-5\sqrt{29}}{2}} & \sqrt{\frac{29-5\sqrt{29}}{2}}\left(\frac{1-\sqrt{29}}{2}\right) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{29+5\sqrt{29}}{2}}x + \sqrt{\frac{29+5\sqrt{29}}{2}}\left(\frac{1+\sqrt{29}}{2}\right)y \\ \sqrt{\frac{29-5\sqrt{29}}{2}}x + \sqrt{\frac{29-5\sqrt{29}}{2}}\left(\frac{1-\sqrt{29}}{2}\right)y \end{pmatrix}$$

cuja norma é dada por

$$||v||^2 = 29x^2 - 116xy + 145y^2.$$

Como o valor mínimo é $||v||^2 = 29$, obtido pelos pares de inteiros $(x,y) = (1,0)$, $(-1,0)$, $(2,1)$ e $(-2,-1)$, então $\#S(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = 4$ e, consequentemente, $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um reticulado bem arredondado.

De modo análogo aos exemplos anteriores podemos verificar que $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ é um $\mathbb{Z}^2$-rotacionado usando a matriz mudança de base $T = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$. Neste caso a matriz geradora de $\mathbb{Z}^2$ é $R = \frac{1}{\sqrt{29}}MT$, com $R^tR = I_2$.

Os reticulados apresentados nos Exemplos 5.3.1, 5.3.2 e 5.3.3 são apenas alguns dos que encontramos da forma $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ para $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d > 0$. Existem muitos outros, como para $d = 37$, $\mathbb{K} = \mathbb{Q}(\sqrt{37})$ e $\alpha = 37 + 6\sqrt{37} \in \mathbb{K}$. Observamos ainda que em todos os casos apresentados $d \equiv 1\ (mod\ 4)$.

Considerações Finais

Ao longo do trabalho, alternamos a utilização das bases integrais para a construção de reticulados de acordo com nossa conveniência, pois o reticulado obtido independe da base integral escolhida. Os resultados que apresentamos na Seção 5.2 abrangem o caso em que $d \equiv 2,3\ (mod\ 4)$, uma vez que $d = 3$ e $d = 2$ nos Teoremas 5.2.1 e 5.2.2, respectivamente. Na Seção 5.3, contudo, apresentamos exemplos para o caso em que $d \equiv 1\ (mod\ 4)$.

Ressaltamos que os $\mathbb{Z}^n$-rotacionados possuem inúmeras aplicações na Teoria dos Códigos e desempenham significativo papel no estudo de constelações de sinais, o leitor interessado nesta teoria pode consultar, por exemplo, [26]. Uma pergunta que surge naturalmente é se para todo $d \in \mathbb{Z}$ livre de quadrados, $d > 0$ e $d \equiv 1 \ (mod\ 4)$, existe $\alpha \in \mathbb{Q}(\sqrt{d})$ tal que o reticulado $\Lambda = \sigma_\alpha(\mathcal{O}_\mathbb{K})$ é bem arredondado? Esta ainda é uma questão em aberto e surge como motivação para trabalhos futuros.

Conclusões

Este trabalho foi dedicado principalmente ao estudo dos reticulados algébricos bem arredondados. Como ressaltamos anteriormente, o estudo dessa classe de reticulados é recente, tendo em vista publicações como [5], [17] e [18], portanto ainda existem diversas questões em aberto sobre o mesmo.

Nossa proposta inicial foi apresentar aspectos desta teoria de desenvolvê-los, em sua maioria, de forma minudente. Classificamos os reticulados algébricos bem arredondados obtidos por meio do anel de inteiros de um corpo quadrático através do homomorfismo canônico. Também desenvolvemos o estudo para corpos ciclotômicos por meio do mesmo homomorfismo. Em virtude da relação entre reticulados bem arredondados e a norma mínima de um reticulado, determinamos quais elementos em uma família de ideais atingem os vetores de norma mínima no reticulado correspondentes.

No Capítulo 5 nosso objetivo foi estudar algumas condições para existência de ideais no anel de inteiros de corpos quadráticos cuja imagem pelo homomorfismo canônico é um reticulado bem arredondado. Além disso, estudamos reticulados obtidos através do anel de inteiros de corpos quadráticos por meio de perturbações do homomorfismo canônico.

Devido às implicações do estudo de reticulados em outras áreas como na Teoria da Informação e Códigos, podemos dizer que as construções apresentadas, sobretudo nos Capítulos 4 e 5, representam uma pequena contribuição para esta teoria. Como perspectivas futuras temos por objetivo generalizar alguns resultados apresentados no Capítulo 5 para corpos quadráticos reais arbitrários e estudar diferentes famílias de ideais do anel de inteiros de corpos ciclotômicos.

Referências

[1] ALVES, C. **Reticulados e códigos.** 2008. 156 f. Tese (Doutorado em Matemática) - Instituto de Matemática, Estatística e Computação Científica, Universidade de Campinas, Campinas, nov. 2008.

[2] ANDRADE, A. A.; FERRARI, A. J.; BENEDITO, C. W. O.; COSTA, S. I. R. Constructions of algebraic lattices. **Computational & Applied Mathematics**, v. 29, n. 3, p. 493-505, 2010.

[3] ARAÚJO, R. R. **Anéis de inteiros de corpos de números e aplicações.** 2015. 215 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev. 2015.

[4] ARAÚJO, R. R. **Reticulados algébricos e aplicações a códigos e criptografia**. 2018. 128 f. Tese (Doutorado em Matemática) - Instituto de Matemática, Estatística e Computação Científica, Universidade de Campinas, Campinas, dez. 2018.

[5] ARAÚJO, R. R.; COSTA, S. I. R. Well-rounded algebraic lattices in odd prime dimension, **Archiv der Mathematik**, v. 112, p. 139-148, 2019.

[6] BAYER-FLUCKIGER, E. Lattices and Number Fields, **Contemporany Mathematics**, v. 241, p. 69-84, 1999.

[7] BUELL, D. A. **Binary Quadratic Forms**: Classical Theory and Modern Computations. 1. ed. New York: Springer-Velarg, 1989.

[8] CAMPELLO, A. C. A. **Reticulados, Projeções e Aplicações à Teoria da Informação**. 2014. 162 f. Tese (Doutorado em Matemática Aplicada) - Instituto de Matemática, Estatística e Computação Científica, Universidade de Campinas, Campinas, mar. 2014.

[9] CLARY, S.; FABRYKOWSKI, J. Arithmetic Progressions, Prime Numbers, and Squarefree Integers. **Czechoslovak Mathematical Journal**, v. 54, n. 4, p. 915-927, 2004.

[10] CONDWAY, J. H.; SLOANE, N. J. A. **Sphere packings, lattices and group**. 3. ed. New York: Springer-Verlag, 1998.

[11] ENDLER, O. **Teoria dos números algébricos**. 2. ed. Rio de Janeiro: Projeto Euclides, Instituto de Matemática Pura e Aplicada (IMPA), 2014.

[12] FERRARI, A. J. **Reticulados algébricos via corpos abelianos**. 2008. 115 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev, 2008.

[13] FLORES, A. L. **Representação Geométrica de Ideais de Corpos de Números**. 1996. 97 f. Dissertação (Mestrado em Matemática) - Instituto de Matemática, Estatística e Computação Científica, Universidade de Campinas, Campinas, mar. 1996.

[14] FLORES, A. L. **Reticulados em Corpos Abelianos**. 2000. 157 f. Tese (Doutorado em Engenharia Elétrica) - Faculdade de Engenharia Elétrica e de Computação, Universidade de Campinas, Campinas, mai. 2000.

[15] FUKSHANSKY, L. Revisiting the hexagonal lattice: On optimal lattice circle packing, **Elemente der Mathematik** v. 66, p. 1-9, 2011.

[16] FUKSHANSKY, L.; HENSHAW G.; LIAO, P.; *et al.* On Integral Well-Rounded Lattices in the Plane. **Discrete Comput. Geom**, v. 48, n. 3, p. 735-748, 2012.

[17] FUKSHANSKY, L.; HENSHAW, G.; LIAO, P.; *et al.* On Well-Rounded Ideal Lattices, II. **International Journal of Number Theory**, v. 9, n. 1, p. 139-154, 2013.

[18] FUKSHANSKY, L.; PETERSEN, K. On Well-Rounded Ideal Lattices, **International Journal of Number Theory**, v. 8, n. 1, p. 189-206, 2012.

[19] GNILKE, O. W.; BARREAL, A.; KARRILA, A.; TRAN, H. T. N. Well-rounded lattices for coset coding in MIMO wiretap channels. **26th International Telecommunication Networks and Applications Conference (ITNAC)**, p. 289-294, 2016.

[20] GNILKE, O. W.; TRAN, H. T. N.; KARRILA, A.; HOLLANTI, C. Well-rounded lattices for reliability and security in Rayleigh Fading SISO channels. **IEEE Information Theory Workshop (ITW)**, p. 359-363, 2016.

[21] HUNGERFORD, Thomas. **Algebra**. New York: Springer-Verlag, 1974.

[22] MARTINET, J. **Perfect Lattices in Euclidean Spaces**. New York: Springer-Verlag, 2003.

[23] MCMULLEN, C. T. Minkowski's conjecture, well-rounded lattices and topological dimension. **Journal of the American Mathematical Society**, v. 18, n. 3, p. 711-734, 2005.

[24] MILIES, F. C. P. **Anéis e Módulos**. São Paulo. Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, 1972.

[25] MOLLIN, R. A. **Fundamental Number Theory with Applications**. 2. ed., Chapman and Hall / CRC Press, 1998.

[26] OGGIER, F. **Algebraic Methods for Channel Coding**. 2005. 135 f. Tese (Doutorado em Ciências), Institut de mathématiques B, École Polytechnique fédérale de Lausanne, Lausanne, 2005.

[27] PLASOLOV, V. V. **Polynomials:** Algorithms and Computation in Mathematics. v. 11. Springer, 2004.

[28] POHST, M. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. **ACM SIGSAM Bulletin**, v. 15, n. 1, p. 37-44, 1981.

[29] RIBENBOIM, P. **Algebraic Numbers**. Wiley-Interscience, 1972.

[30] SAMUEL, P. **Algebraic Theory of Numbers**. Paris: Hermann, 1970.

[31] SHANNON, C. E. Mathematical Theory of Communication. **Bell Systems Technical Journal**, v. 27, pt. I: p. 379-423; pt. II: pp. 623-656, 1948.

[32] STEWART, I. **Galois Theory**. 3. ed. Chapman & Hall CRC , 1945.

[33] STEWART, I. TALL, D. **Algebraic Number Theory**. 2. ed. New York: Chapman & Hall, 1987.

[34] STEWART, I., TALL, D. **Algebraic Number Theory and Fermat's Las Theorem**. 3. ed. Natick: A K Peters, 2002.

[35] THE IMITATION Game. Direção de Morten Tyldum. Califórina: Black Bear Pictures, 2014. 1 DVD (114 min.).

[36] VICENTE, C. R. L. **Construções de reticulados algébricos via extensões galoisianas de grau prima**. 2018. 137 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista. São José do Rio Preto, fev. 2018.

[37] WASHINGTON, L. C. **Introduction to Cyclotomic Fields**. 2 ed. New York: Springer-Verlag, 1982.

Índice Remissivo