UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

JOSÉ CRISTIANO ALVES DA SILVA

Construção de Reticulados Algébricos nas Dimensões $2, 4$ e 8

Campinas

2022

José Cristiano Alves da Silva

Construção de Reticulados Algébricos nas Dimensões 2, 4 e 8

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática Aplicada e Computacional.

Orientadora: Cintya Wink de Oliveira Benedito

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno José Cristiano Alves da Silva e orientada pela Profa. Dra. Cintya Wink de Oliveira Benedito.

Campinas

2022

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Si38c

Silva, José Cristiano Alves da, 1989-
Construção de reticulados algébricos nas dimensões 2, 4 e 8 / José Cristiano Alves da Silva. – Campinas, SP : [s.n.], 2022.

Orientador: Cintya Wink de Oliveira Benedito.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Reticulados algébricos. 3. Matriz de Gram. 4. Homomorfismos (Matemática). 5. Algoritmo LLL. I. Benedito, Cintya Wink de Oliveira, 1985-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Construction of algebraic lattices in dimensions 2, 4 and 8
Palavras-chave em inglês:
Lattice theory
Algebraic lattices
Gram matrice
Homomorphisms (Mathematics)
LLL algorithm
Área de concentração: Matemática Aplicada e Computacional
Titulação: Mestre em Matemática Aplicada e Computacional
Banca examinadora:
Cintya Wink de Oliveira Benedito [Orientador]
Carina Alves
João Eloir Strapasson
Data de defesa: 15-12-2022
Programa de Pós-Graduação: Matemática Aplicada e Computacional

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-8430-4014
- Currículo Lattes do autor: http://lattes.cnpq.br/1836298270085924

Dissertação de Mestrado Profissional defendida em 15 de dezembro de 2022 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). CINTYA WINK DE OLIVEIRA BENEDITO

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). CARINA ALVES

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Ao concluir este trabalho agradeço:

Primeiramente à Deus.

Aos meus pais, Nair Alves Baliera e Ivair Candido da Silva (in memorian), por minha educação e valores ensinados.

A minha esposa, Danila Paulino, pelo amor, companheirismo, e por estar comigo em todos os momentos dando força e otimismo.

Ao meu filho, André Lucas, por todos os momentos que não pude brincar, mas esteve sempre do meu lado construindo labirintos.

A minha orientadora, Profa. Dra. Cintya Wink de Oliveira Benedito, por todo amparo e disponibilidade, por toda confiança que depositou em mim para o desenvolvimento deste trabalho e pela amizade. Agradeço muito pela paciência diante as minhas dificuldades.

Aos meus amigos da Pós-graduação, Paulo Lira (Paulinho), Ségio Mendes (Sérjão), Alan Di Maria pela amizade construída, além disso, por ajudar a construir os comando computacionais da minha pesquisa; Saris por ser companheiro do estudo de Análise real, e amigo para todas as horas. Não poderia faltar, Fabi, Brunão e Juliana grandes amigos e parceiros de estudos.

Aos professores do mestrado pelo conhecimento transmitido.

Aos professores da Banca examinadora.

"A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo".

(Albert Einstein)

Resumo

Este trabalho apresenta um estudo de reticulados e reticulados algébricos utilizando o homomorfismo canônico e suas perturbações. A partir deste estudo, apresentamos uma construção de reticulados algébricos nas dimensões $2, 4$ e 8 que são versões rotacionadas dos reticulados mais densos nestas dimensões. Além disso, iremos analisar essas construções por meio de suas matrizes geradores e matrizes de Gram. E, aplicando o Algoritmo LLL *(Lenstra, Lenstra e Lovász)*, encontramos uma matriz de base reduzida, que nos auxiliará na obtenção de um fator escala que expressa a razão entre os volumes dos reticulados obtidos com os reticulados mais densos nas respectivas dimensões. Com esta análise, podemos diferenciar as rotações obtidas e compará-las proporcionalmente em relação aos reticulados mais densos.

Palavras-chave: Reticulados, Reticulados Algébricos, Homomorfismo Canônico, Matriz de Gram, Algoritmo LLL.

Abstract

This work presents a study of lattices and algebraic lattices by using canonical embedding and its perturbations. From this study, we present a construction of algebraic lattices in the dimensions 2, 4 and 8 which are rotated versions of the densest lattices in these dimensions. Furthermore, we will analyze these constructions through their generator matrices and Gram matrices. And, applying the LLL (Lenstra, Lenstra e Lovász) Algorithm, find a matrix with reduced basis, which will help us to obtain a scale factor that expresses the ratio between the volumes of the lattices obtained with the densest lattices in the respective dimensions. With this analysis, we can differentiate the obtained rotations and compare them proportionally in relation to the densest lattices.

Keywords: Lattices, Algebraic Lattices, Canonical Embedding, Gram matrix, LLL Algorithm.

Lista de ilustrações

Lista de tabelas

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
$\sum$	Somatório
$\prod$	Produtório
$\mathbb{I}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$\mathbb{K}, \mathbb{L}, \mathbb{M}$	Corpos
$\mathbb{K}/\mathbb{L}$	Extensão de corpos $\mathbb{K}$ sobre $\mathbb{L}$
$\varphi(n)$	Função de Euler aplicada à n
$\mathcal{U}$	Ideal
$\mathcal{N}(\mathcal{U})$	Norma do ideal $\mathcal{U}$
$Gal(\mathbb{K}/\mathbb{L})$	Grupo de Galois de $\mathbb{K}$ sobre $\mathbb{L}$
$Tr_{\mathbb{K}/\mathbb{L}}(\alpha)$	Traço de α em relação à $\mathbb{K}$ sobre $\mathbb{L}$
$\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)$	Norma de α em relação à $\mathbb{K}$ sobre $\mathbb{L}$
$\mathcal{D}_{\mathbb{K}}$	Discriminante do corpo $\mathbb{K}$
ζ_n	Raiz n-ésima primitiva da unidade
$\mathbb{Q}(\zeta_n)$	n-ésimo corpo ciclotômico

Λ	Reticulado
$vol(\Lambda)$	Volume do reticulado Λ
$\mathcal{P}_\beta$	Região fundamental de Λ em relação a base β
ρ	Raio do empacotamento
Λ_{min}	Norma mínima
$\tau(\Lambda)$	Kissing number
$\delta(\Lambda)$	Densidade de centro do Λ
$\sigma_{\mathbb{K}}$	Homomorfismo canônico
σ_α	Perturbação σ_α
$\sigma_{2\alpha}$	Perturbação $\sigma_{2\alpha}$

Sumário

Introdução

Em 1611, Johannes Kepler estudando como organizar esferas no espaço, conjecturou como devemos proceder para colocar o maior número de esferas de mesmo tamanho visando ocupar o maior espaço possível [38]. David Hilbert no ICM *(Congresso Internacional de Matemática)* de 1900 em Paris, estabeleceu a conjectura de Kepler como o 18º problema de uma lista repleta de desafios que ocupariam destaque no desenvolvimento da ciência moderna [14]. A conjectura de Kepler está amplamente conectada com o problema de empacotamento de esferas, o qual consiste em: ocupar o espaço n-dimensional $\mathbb{R}^n$ da melhor forma possível com esferas de mesmo raio que se toquem apenas nos bordos. Durante o século XX muitos modelos e métodos foram propostos para resolver este problema, ver mais detalhes em [42].

Em 1910, o empacotamento de esferas ótimo para as dimensões 1 e 2 foram provadas por Axel Thue. Em 1998, Thomas Halles provou para a dimensão 3. No ano 2017, Maryna Viazoska, com H. Cohn, A. Kumar, S. Miller e D. Radchenko, provaram para as dimensões 8 e 24. Recentemente, em 2022, Maryna Viazoska recebeu a medalha Fields pela realização desse trabalho, para ver mais detalhes consultar [38].

Em 1948, Claude E. Shanonn publicou um artigo que viria mudar completamente a pesquisa na área das telecomunicações. Tal publicação deu início a teoria de códigos corretores de erros, estabelecendo que o problema de encontrar empacotamentos esféricos densos é equivalente a encontrar bons códigos corretores de erros [12]. A partir dessa percepção, passaram-se a associar o estudo dos códigos corretores de erros aos reticulados, com o interesse em resolver o problema 18º de Hilbert, e com essas técnicas surgiram várias famílias de reticulados, cada uma visando encontrar a melhor densidade de empacotamento, ver [6].

Dentre tais modelos, destaca-se o proposto inicialmente por Hermann Minkowski, modelo algébrico baseado na teoria algébrica dos números, o qual utilizamos neste trabalho. Este modelo consiste em tomar um corpo de números $\mathbb{K}$ de grau n, seu respectivo anel dos inteiros algébricos $\mathbb{I}_{\mathbb{K}}$ e, utilizando os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$, estabelecer

um homomorfismo de $\mathbb{K}$ em $\mathbb{R}$, conhecido como Homomorfismo canônico ou de Minkowski, de modo que a imagem de um ideal $\mathcal{U}$ não nulo de $\mathbb{I}_{\mathbb{K}}$, é um reticulado de posto n em $\mathbb{R}^n$, ver [6]. Para o cálculo da densidade de centro de tal reticulado construído algebricamente, utilizam-se elementos da teoria algébrica dos números como o grau e o discriminante do corpo de números utilizado, um ideal $\mathcal{U}$ não nulo e a norma deste ideal. Além disso, tem a minimização de uma forma quadrática pela função traço, ver [4]. A partir do homomorfismo de Minkowski, foram definidas perturbações deste homomorfismo adicionando um elemento α do corpo totalmente positivo. Utilizando estas perturbações também é possível obter reticulados algébricos e em alguns casos é possível calcular a densidade de centro destes reticulados, ver [12] e [14].

O objetivo deste trabalho é apresentar uma construção de reticulados algébricos nas dimensões 2, 4 e 8, utilizando a perturbação σ_α do homomorfismo canônico. A partir desta construção, iremos obter reticulados que são versões rotacionadas dos reticulados mais densos nestas dimensões, ou seja, versões rotacionadas dos reticulados A_2, D_4 e E_8, que apresentam as densidades de centro ótima nas dimensões 2, 4 e 8, respectivamente. A construção apresentada neste trabalho, baseia-se na construção apresentada principalmente em [3]. Além disso, analisaremos alguns exemplos de reticulados obtidos a partir desta construção por meio das suas matrizes geradoras e das matrizes de Gram. Utilizaremos o algoritmo LLL *(Lenstra, Lenstra e Lovász)* para obter uma matriz de base reduzida que nos auxiliará na obtenção de um fator escala c, o qual está associado a razão das regiões fundamentais dos reticulados, ver [23] e [41].

Este trabalho foi estruturado da seguinte forma. No Capítulo 1, apresentamos os conceitos básicos de álgebra, tais como, grupo, anéis, corpos, ideais, homomorfismos, monomorfismo, automorfismos, subcorpo, módulo, submódulo e teoria de Galois. Em seguida, dedicamos ao estudo de conceitos e resultados teoria algébrica dos números em que abordamos inteiros algébricos, anel dos inteiros algébricos, definição de traço e norma, norma de um ideal, discriminante de um corpo de números, resultados sobre corpos quadráticos e ciclotômicos. Resultados estes de suma importância para o desenvolvimento deste trabalho.

No Capítulo 2, apresentamos o conceito central deste trabalho que é o conceito de reticulado, abordamos a definição de reticulado, região fundamental, matriz geradora, matriz de Gram, determinante de um reticulado, volume do reticulado, definição de empacotamento esférico, conceito de kissing number e por fim apresentamos alguns reticulados mais conhecido da literatura e suas propriedades.

No Capítulo 3, temos o objetivo de apresentar o homomorfismo de Minkowski para a construção de reticulados algébricos, recorrendo a um ideal $\mathcal{U}$ não nulo do anel dos inteiros $\mathbb{I}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$ de grau n. E, a partir deste homomorfismo, definir perturbações deste homomorfismo e apresentar a construção de reticulados algébricos a

partir destas perturbações.

No Capítulo 4, apresentamos a construção de reticulados algébricos nas dimensões $2, 4$ e 8. Utilizamos as perturbações definidas no Capítulo 3 e a construção proposta em [3] para obter exemplos de reticulados algébricos que possuem densidade de centro ótima nas dimensões $2, 4$ e 8, ou seja, reticulados algébricos que são versões rotacionadas dos reticulados A_2, D_4 e E_8, respectivamente.

No Capítulo 5, analisamos alguns exemplos dos reticulados construídos no Capítulo 4, apresentando as matrizes geradora e de Gram destes exemplos, e por meio do uso de um algoritmo LLL que reduz a matriz de Gram do reticulado numa matriz de base reduzida, comparando proporcionalmente estes exemplos com os reticulados hexagonal Λ_H na dimensão 2, D_4 e E_8, nas dimensões 4 e 8, respectivamente.

Capítulo 1

Conceitos preliminares

Neste capítulo iremos apresentar conceitos e resultados que nos auxiliará no desenvolvimento dos demais capítulos. Na Seção 1.1 introduzimos alguns conceitos básicos de álgebra. Seção 1.2 apresentamos os principais conceitos da teoria de Galois. Em seguida, na Seção 1.3 tratamos dos principais assuntos da teoria algébrica dos números. As principais referências utilizadas neste capítulo foram [1], [2], [4], [6], [9], [10], [11], [12], [13], [15], [16], [22], [26], [29], [32], [34], [35], [37], [39], [40] e [43].

1.1 Conceitos básicos de álgebra

Nessa seção apresentamos alguns conceitos de álgebra tais como, grupo, anel, ideais principais, ideais primos, ideal maximal, homomorfismos, monomorfismos, isomorfismos, corpo, subcorpo, módulo e submódulo.

Definição 1.1.1. *Chama-se* ***grupo*** *um conjunto não vazio $G \neq \varnothing$, munido da operação $*$ que possui as seguintes propriedades:*

(i) Associativa: $(a * b) * c = a * (b * c), \forall a, b, c \in G$.

(ii) Admite elemento neutro e: $a * e = e * a = a, \forall a \in G$.

(iii) Para todo elemento $a \in G$, $\exists a' \in G$ *tal que* $a \cdot a' = a' \cdot a = e$.

Um grupo G é abeliano se a operação $*$ é comutativa

(iv) $a * b = b * a$.

Definição 1.1.2. *Um conjunto não vazio A e um par de operações $+$ (adição) e $\cdot$ (multiplicação) sobre A é chamado de* ***anel*** *e denotamos por $(A, +, \cdot)$, se A é um grupo abeliano em relação à operação $+$ e se a multiplicação satisfaz:*

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in A$ *(Associativa).*

(ii) $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in A$ *(distributiva).*

Definição 1.1.3. *Quando o anel A satisfaz $a \cdot b = b \cdot a, \forall a, b \in A$, chamamos de* ***anel comutativo****.*

Definição 1.1.4. *Quando a multiplicação admitir um elemento neutro, isto é, $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a, \forall a \in A$, neste caso chamamos A de* ***anel unitário****.*

Definição 1.1.5. *Seja $(A, +, \cdot)$ um anel. Um subconjunto não vazio $B \subset A$ é* ***subanel*** *de A quando:*

(i) As operações de A são operações em B, isto é, $\forall a, b \in B \Rightarrow a + b \in B$ e $a \cdot b \in B$.

(ii) $(B, +, \cdot)$ é anel.

Proposição 1.1.1. *[1] Sejam $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Então B é um subanel de A se, e somente se, as condições são verificadas*

(i) $0 \in B$.

(ii) $x, y \in B \Rightarrow x - y \in B$.

(iii) $x, y \in B \Rightarrow x \cdot y \in B$.

Exemplo 1.1.1. *O conjunto $(2\mathbb{Z}, +, \cdot)$ dos números pares é um subanel do anel $(\mathbb{Z}, +, \cdot)$. De fato, definimos $2\mathbb{Z} = \{2x; x \in Z\}$, $\forall a, b \in 2\mathbb{Z}, \exists x, y \in Z$ tais que $a = 2x$ e $b = 2y$, assim*

$$a - b = 2x - 2y = 2(x - y) \in 2\mathbb{Z} \quad e \quad a \cdot b = 2x \cdot 2y = 2(x \cdot y) \in 2\mathbb{Z}.$$

Portanto, $(2\mathbb{Z}, +, \cdot)$ é subanel de $(\mathbb{Z}, +, \cdot)$.

Definição 1.1.6. *Chama-se* ***domínio de integridade*** *todo anel comutativo $(A, +, \cdot)$ com elemento unidade e sem divisores de zero no qual é verdadeira a proposição*

(i) Se $a \cdot b = 0$, então $a = 0$ ou $b = 0 \Rightarrow$, $\forall a, b, c \in A$.

Num domínio de integridade $(A, +, \cdot)$, todo elemento não nulo $a \in A$ é simplificável para a operação de multiplicação, isto é,

(ii) $a \cdot b = a \cdot c \Rightarrow b = c, \forall a, b, c \in A, a \neq 0$.

Definição 1.1.7. *Seja $(A, +, \cdot)$ um anel comutativo. Um subconjunto $\mathcal{U} \subset A$, $\mathcal{U}$ não vazio é* ***ideal*** *em A se para quaisquer $x_1, x_2 \in \mathcal{U}$ e para quaisquer $\alpha \in A$, as seguintes condições são satisfeitas*

(i) $x_1 - x_2 \in \mathcal{U}$.

(ii) $\alpha \cdot x_1 \in \mathcal{U}$.

Definição 1.1.8. *Seja A um anel. Um ideal $\mathcal{U}$ gerado por um elemento $a \in A$, isto é, $\mathcal{U} = \langle\ a\ \rangle = \{ax; x \in A\}$ é* ***ideal principal*** *gerado por a. Ainda se todo ideal do anel A é principal dizemos que A é* ***anel principal****.*

Teorema 1.1.1. *[15] Todo ideal de $\mathbb{Z}$ é principal.*

Observação 1.1.1. *Sabemos que $\mathbb{Z}$ é um domínio principal. De fato, todos os seus ideias são principais.*

Exemplo 1.1.2. *Seja $(2\mathbb{Z}, +, \cdot)$ um ideal principal do anel $(\mathbb{Z}, +, \cdot)$, sabemos que $\langle 2\rangle = 2\mathbb{Z}$. De fato, definindo $2\mathbb{Z} = \{2n; n \in Z\}, \forall x \in 2\mathbb{Z}, \forall a \in \mathbb{Z}$, temos que $x \cdot a \in \mathbb{Z}$, tomando $x = 2n$, temos que $x \cdot a = 2n \cdot a = 2(na) \in \mathbb{Z}$. Portanto, $\langle 2\rangle$ é um ideal principal de $\mathbb{Z}$. O anel $(\mathbb{Z}, +, \cdot)$ é um anel principal, pois todos os seus ideais são principais.*

Definição 1.1.9. *Um ideal P será chamado de **ideal primo** de um anel comutativo A se*

(i) $P \neq A$.

(ii) Se $a, b \in A$ e $a \cdot b \in P$, então $a \in P$ ou $b \in P$.

Definição 1.1.10. *Um ideal M será chamado de **ideal maximal** de um anel comutativo A se*

(i) $M \neq A$.

(ii) Se I é um ideal de A e $M \subset I$, então $I = A$.

Teorema 1.1.2. *[10] Seja A um anel comutativo com unidade e $\mathcal{U}$ um ideal em A. Então,*

*(i) $\mathcal{U}$ é um **ideal primo** se, e somente se, $\dfrac{A}{\mathcal{U}}$ é um domínio de integridade.*

*(ii) $\mathcal{U}$ é um **ideal maximal** se, e somente se, $\dfrac{A}{\mathcal{U}}$ é um corpo.*

Exemplo 1.1.3. *$\mathbb{Z}_6$ não é ideal maximal e nem ideal primo de $\mathbb{Z}$. De fato, respectivamente,*

(i) Seja $\mathbb{Z}_2$ um ideal de $\mathbb{Z}$, tal que, $\mathbb{Z}_6 \nsubseteq \mathbb{Z}_2$.

(ii) Tomando $2, 3 \in \mathbb{Z}, 2 \cdot 3 \in \mathbb{Z}_6$, mas $2 \notin \mathbb{Z}_6$ e $3 \notin \mathbb{Z}_6$.

Definição 1.1.11. *Seja A um anel qualquer e $\mathcal{U}$ um ideal de A. A relação em A, $x, x' \in A$, $x \equiv x' mod(\mathcal{U}) \Leftrightarrow\ x - x' \in \mathcal{U}$.*

A Definição 1.1.11 expressa uma relação de equivalência em A. Denotaremos por $\overline{x}$ $= \{y \in A;\ y \equiv x\ mod(\mathcal{U})\}$, a qual chamaremos de **classe de equivalência** do elemento $x \in A$, relativamente a relação $\equiv mod(\mathcal{U})$.

Observação 1.1.2. *Observe que $y \in \overline{x} \Leftrightarrow\ y - x \in \mathcal{U}$ e por isso também denotamos a classe $\overline{x}$ por*

$$\overline{x} = x + \mathcal{U} = \{x + z; z \in \mathcal{U}\}.$$

Definição 1.1.12. *Sejam A um anel e $\mathcal{U}$ um ideal. O conjunto $\dfrac{A}{\mathcal{U}}$, munido de duas operações definidas acima, é chamado de **anel quociente** de A pelo ideal $\mathcal{U}$. Os ideais de $\dfrac{A}{\mathcal{U}}$*

são da forma $\frac{\mathcal{U}'}{\mathcal{U}}$ *onde* $\mathcal{U}'$ *pertence ao conjunto dos ideais de* A *que contém* $\mathcal{U}$*. Chamaremos de conjunto quociente de* A *pelo ideal* $\mathcal{U}$ *ao conjunto* $\frac{A}{\mathcal{U}} = \overline{x} = \{x + \mathcal{U}; x \in A\}$.

Definição 1.1.13. *Sejam* $(A, +, \cdot)$ *e* $(B, +, \cdot)$ *anéis. Um* ***homomorfismo*** *entre os anéis* A *e* B *é uma função,* $f : A \to B$*, tal que*

(i) $f(a + b) = f(a) + f(b)$.

(ii) $f(a \cdot b) = f(a) \cdot f(b)$.

Definição 1.1.14. *Sejam* $f : A \to B$ *de anéis. Dizemos que* f *é um* ***monomorfismo*** *quando* f *é injetora, isto é,* $f(x) = f(y) \Rightarrow x = y$.

Definição 1.1.15. *Seja* $f : A \to B$ *é um homomorfismo de anéis. Dizemos que* f *é um* ***isomorfismo*** *quando* f *é bijetora.*

Definição 1.1.16. *Seja* $(A, +, \cdot)$ *um anel. Chama-se* ***automorfismo*** *de* $(A, +, \cdot)$ *todo isomorfismo de* $(A, +, \cdot)$ *em si mesmo.*

Observação 1.1.3. *Um automorfismo de* $(A, +, \cdot)$ *é toda função bijetora* $f : A \to A$*, tal que*

(i) $f(a + b) = f(a) + f(b)$.

(ii) $f(a \cdot b) = f(a) \cdot f(b)$.

Definição 1.1.17. *Seja* $f : A \to B$ *um homomorfismo de anéis. O* ***núcleo*** *de* f *é formado pelos elementos de* A *cuja* ***imagem*** *por* f *é* $0 \in B$*, isto é,* $N(f) = \{a \in A; f(a) = 0\}$.

Definição 1.1.18. *Seja* $f : A \to B$ *um homomorfismo de anéis. A imagem de* f *é a* ***imagem da função****, isto é,* $Im(f) = \{f(a); a \in A\}$.

Exemplo 1.1.4. *Para o homomorfismo* $f : \mathbb{Z} \to \mathbb{R}$ *definido por* $f(x) = x$*, temos que* $N(f) = 0$ *e* $Im(f) = \mathbb{Z}$.

Teorema 1.1.3. *[16] Sejam* A *e* A' *anéis e* $f : A \to A'$ *um homomorfismo, então*

(i) $Im(f) = \{f(a) : a \in A\}$ *é um subanel de* A'.

(ii) $N(f) = \{a \in A : f(a) = 0\}$ *é um ideal de* A*, e* f *é injetiva* $\Rightarrow N(f) = \{0\}$.

(iii) Os anéis $\frac{A}{N}$ *e* $Im(f)$ *são isomorfos.*

Definição 1.1.19. *Chama-se* ***corpo*** *todo anel comutativo* $(\mathbb{K}, +, \cdot)$ *com elemento unidade tal que todo elemento não nulo de* $\mathbb{K}$ *é inversível para operação multiplicação* $(\cdot)$.

Observação 1.1.4. *Em outras palavras, corpo é toda ordenada* $(\mathbb{K}, +, \cdot)$ *que vale as seguintes propriedades,*

(i) $(\mathbb{K}, +, \cdot)$ *é grupo abeliano.*

(ii) $(\mathbb{K}^*, \cdot)$ *é grupo abeliano,* $(\mathbb{K}^* = \mathbb{K} - \{0\})$.

(iii) A $(\cdot)$ *é distributiva em relação a* $(+)$.

Definição 1.1.20. *Um conjunto não vazio* $S \subset \mathbb{K}$ *é chamado* ***subcorpo*** *de* $\mathbb{K}$ *se* S *é um corpo com as operações de* $\mathbb{K}$ *restritas a* S.

Proposição 1.1.2. *[10] Seja* $\mathbb{K}$ *um corpo e* S *um subconjunto de* $\mathbb{K}$ *tal que* $S \neq \varnothing$*, para que* S *seja um subcorpo de* $\mathbb{K}$ *é necessário e suficiente que*

(i) 0 *e* $1 \in S$.

(ii) Se $x, y \in S$*, então* $x - y \in S$.

(iii) Se $x, y \in S$ *e* $y \neq 0$*, então* $x \cdot y^{-1} \in S$.

Definição 1.1.21. *Para cada domínio de integridade* A*, tem-se um corpo* $\mathbb{K}$ *contendo* A *tal que* $a \in A$*,* $a \neq 0$*, existe* $x \in \mathbb{K}$ *satisfazendo* $a \cdot x = 1$*, este corpo é chamado de* ***corpo de frações****, munido das seguintes operações*

(i) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$.

(ii) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$.

Definição 1.1.22. *Seja* A *um anel. Um conjunto não vazio* M *é dito* ***A-módulo*** *se* M *for grupo abeliano com relação à operação de adição e munido de uma aplicação*

$$\phi : A \times M \to M.$$

Definida por $\phi(a, m) = a \cdot m$*, satisfazendo as condições*

(i) $a(m + n) = am + an$.

(ii) $(a + b)m = am + bm$.

(iii) $(ab)m = a(bm)$.

(iv) $1 \cdot m = m$.

Definição 1.1.23. *Sejam* A *um anel,* M *um* A*-módulo e* $N \subset M$*,* $N \neq \varnothing$ *. Dizemos que* N *é um* ***submódulo*** *do* A*-módulo* M*, se*

(i) N *é um subgrupo de* M.

(ii) $(\forall a \in A)\ (\forall n \in N) \Rightarrow a \cdot n \in N$.

Exemplo 1.1.5. *Sejam* $A = (\mathbb{Z}, +, \cdot)$ *um anel,* M *um* A*-módulo* M *tal que* $M = (\mathbb{Z}, +)$ *é um subgrupo abeliano e* $N = (P, +)$ *é o grupo dos inteiros pares, subgrupo de* M*, isto*

é, $N \subset M$ e $N \neq \emptyset$, então N é submódulo de A-módulo M. De fato, escolhendo elementos em A e N para testar as condições da Definição 1.1.23. Temos que $2 \in A$ e $8 \in N \Rightarrow 2 \cdot 8 \in N$. Concluímos que N é submódulo de A-módulo M.

Definição 1.1.24. *Um anel A é chamado de **finitamente gerado** e denotado por $f \cdot g$, se existem elementos $x_1, ..., x_n \in M$, tais que todo $m \in M$ é da forma $m = a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_n \cdot x_n$, com $a_i \in A$, $i = 1, 2, ..., n$. Neste caso, dizemos que $x_1, x_2, ..., x_n$ formam um sistema de geradores de M.*

Definição 1.1.25. *O conjunto de elementos $x_1, ..., x_n \in M$ é linearmente independente sobre A se cumpre com a condição*

$$a_1 \cdot x_1 + ... + a_n \cdot x_n = 0,$$

se, e somente se, $a_1 = a_2 = ... = a_n = 0$. Além disso, se os elementos $x_1, ..., x_n$ formam um sistema de geradores de M, então eles formam uma base[1] de M.

Definição 1.1.26. *Um A-módulo que possui uma base é chamado de **A-módulo livre**.*

Definição 1.1.27. *Sejam A um anel e M, N dois A-módulos. Dizemos que uma aplicação $f : M \to N$ é um homomorfismo de A-módulo se satisfaz as condições*

(i) $f(x + y) = f(x) + f(y)$.

(ii) $f(ax) = af(x)$, $\forall\ x, y \in M$ e $a \in A$.

Observação 1.1.5. *Se a aplicação f for injetora, dizemos que f é um homomorfismo de A-módulo e, se f for bijetora, dizemos que f é um isomorfismo de A-módulo.*

Exemplo 1.1.6. *Sejam A um anel e M, N dois A-módulos a aplicação $f : M \to N$ definida por $f(m) = 0$, com $m \in M$ e $0 \in N$, é um A-homomorfismo nulo. De fato,*

(i) $f(x + y) = f(x) + f(y) = 0 + 0 = 0$.

(ii) $f(ax) = af(x) = a \cdot 0 = 0$, $\forall x, y \in M$ e $a \in A$.

1.2 Teoria de Galois

Nesta seção apresentaremos os principais conceitos sobre a Teoria de Galois. Definiremos extensões, números algébricos, transcendentes, corpo de números, corpo de raízes, polinômio irredutível, polinômio mônico, extensões normais, separáveis, galoisianas, corpo fixo, grupo de Galois e involução.

Definição 1.2.1. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Dizemos que $\mathbb{K}$ é uma **extensão** de $\mathbb{L}$ se $\mathbb{L} \subset \mathbb{K}$ e denotamos está extensão por $\mathbb{K}/\mathbb{L}$.*

[1] O número de elementos da base é o posto de M.

Definição 1.2.2. *Seja $\mathbb{K}/\mathbb{L}$ uma extensão de corpos. O* ***grau*** *de $\mathbb{K}$ sobre $\mathbb{L}$ é a dimensão de $\mathbb{K}$ como espaço vetorial sobre $\mathbb{L}$, indicaremos o grau de $\mathbb{K}/\mathbb{L}$ por $[\mathbb{K} : \mathbb{L}]$*

Definição 1.2.3. *Seja $[\mathbb{K} : \mathbb{L}]$ finito, dizemos que $\mathbb{K}$ é uma* ***extensão finita*** *de $\mathbb{L}$.*

Exemplo 1.2.1. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$, por sua vez $\mathbb{C}$ é uma extensão de $\mathbb{R}$ e de $\mathbb{Q}$.*

Exemplo 1.2.2. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ um corpo com base $\{1, \sqrt{2}\}$ sobre $\mathbb{Q}$. Temos que $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ ($\mathbb{Q} \subset \mathbb{K}$) e tem uma dimensão $[\mathbb{K} : \mathbb{Q}] = 2$. Portanto, $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$.*

Teorema 1.2.1. *[12] Se $\mathbb{L} \subset \mathbb{K} \subset \mathbb{M}$ são corpos, então $[\mathbb{M} : \mathbb{L}] = [\mathbb{M} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{L}]$.*

Definição 1.2.4. *Sejam $\mathbb{K}$ uma extensão sobre $\mathbb{L}$ e $\alpha \in \mathbb{K}$. Dizemos que α é um* ***algébrico*** *sobre $\mathbb{L}$ se existe um $f(x) \in \mathbb{L}[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso contrário, dizemos que α é* ***transcendente*** *sobre $\mathbb{L}$.*

Definição 1.2.5. *Sejam $\mathbb{K}$ uma extensão de $\mathbb{L}$. Dizemos que $\mathbb{K}$ é uma* ***extensão algébrica*** *sobre $\mathbb{L}$ se todos os $\alpha \in \mathbb{K}$ são algébricos sobre $\mathbb{L}$.*

Exemplo 1.2.3. *Sabe-se que $\mathbb{R}$ é uma extensão dos $\mathbb{Q}$, e $\alpha = 2$ é algébrico sobre $\mathbb{Q}$. De fato, α é raiz do polinômio $f(x) = x^3 - x^2 - 4$ com coeficientes inteiros.*

Exemplo 1.2.4. *O corpo $\mathbb{R}$ é extensão dos $\mathbb{Q}$ e π é transcendente sobre $\mathbb{Q}$. De fato, π não é raiz de nenhum polinômio em $\mathbb{Q}[x]$.*

Observação 1.2.1. *Por outro lado, π é algébrico nos $\mathbb{R}$, pois é raiz do polinômio $p(x) = x - \pi \in \mathbb{R}[x]$.*

Exemplo 1.2.5. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$, todos os $\alpha \in \mathbb{R}$ são algébricos sobre $\mathbb{R}$, pois são raízes do polinômio $f(x) = x - \alpha$, assim essa extensão é uma extensão algébrica.*

Definição 1.2.6. *Dizemos que o polinômio não constante $p(x)$ é* ***irredutível*** *em $\mathbb{K}[x]$ se é impossível expressar $p(x)$ com um produto de dois polinômios $g(x) \cdot h(x)$ em $\mathbb{K}[x]$ cujos graus são ambos maiores ou iguais a 1.*

Exemplo 1.2.6. *O polinômio $p(x) = x^2 - 5 \in \mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$, pois é impossível escrever $p(x) = g(x) \cdot h(x)$ ambos de grau 1, caso fosse possível $p(x)$ teria duas raízes racionais o que não é verdade, pois*

$$x^2 - 5 = (x + \sqrt{5}) \cdot (x - \sqrt{5}), \quad com \quad \sqrt{5} \notin \mathbb{Q}.$$

Porém o polinômio $p(x)$ é redutível sobre $\mathbb{R}[x]$.

Definição 1.2.7. *Seja $\alpha \in \mathbb{K}$ um elemento algébrico sobre $\mathbb{L}$, raiz de um único* ***polinômio mônico*** *$p(x)$ de grau mínimo tal que $p(\alpha) = 0$, chamamos este polinômio de* ***polinômio minimal*** *de α sobre $\mathbb{K}$.*

Observação 1.2.2. *Um polinômio $f(x) = a_0 + ... + a_n x^n$ é mônico se $a_n = 1$, melhor dizendo, um polinômio é dito mônico se o coeficiente de maior grau é 1.*

O próximo teorema deixa claro que qualquer polinômio mônico de grau 1 irredutível sobre um corpo é minimal.

Teorema 1.2.2. *[39] Todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível.*

Demonstração: Seja α um elemento algébrico sobre $\mathbb{K}$ e seja $f(x) \in \mathbb{K}[x]$, mônico e de menor grau tal que $f(\alpha) = 0$. Pela minimalidade do grau de $f(x)$ segue que $f(x)$ é o único polinômio mônico irredutível em $\mathbb{K}[x]$ tal que $f(\alpha) = 0$. De fato, $f(x) \in \mathbb{K}[x]$, pelo algoritmo da divisão $\exists g(x), r(x) \in \mathbb{K}[x]$, tais que

$$f(x) = h(x)g(x) + r(x),$$

com $r(x) = 0$, como α é raiz de $f(x)$ temos

$$f(\alpha) = h(\alpha)g(\alpha) + r(\alpha),$$

$$0 = f(\alpha) = h(\alpha)g(\alpha) + r(\alpha),$$

$$r(\alpha) = f(\alpha) - h(\alpha)g(\alpha),$$

$$r(\alpha) = 0.$$

Mas $f(x)$ é o menor polinômio tal que $f(\alpha) = 0$ assim $r(\alpha) = 0$, temos que

$$f(x) = h(x)g(x).$$

Como $f(x)$ é mônico, então $h(x)$ e $g(x)$ são constantes, portanto $f(x)$ é irredutível em $\mathbb{K}[x]$. E $f(x)$ é único, supondo que exista $q(x) \in \mathbb{K}[x]$ tal que

$$q(\alpha) = 0.$$

Note que

$$q(\alpha) = 0 = f(\alpha) \Rightarrow q(\alpha) = f(\alpha),$$

como f e q são mônicos, então $q(x) = f(x)$. ■

Exemplo 1.2.7. *Seja $\mathbb{R}$ uma extensão de $\mathbb{Q}$ e $f(x) = x^2 - 3 \in \mathbb{Q}[x]$, temos que $\alpha = \sqrt{3}$ é um elemento algébrico sobre $\mathbb{Q}$. O polinômio $f(x)$ é mônico e sabemos que $f(x)$ é irredutível em $\mathbb{Q}[x]$, isto é, não existem polinômios $q(x), p(x) \in \mathbb{Q}[x]$ tal que $f(x) = x^2 - 3 = p(x) \cdot q(x)$, se fosse possível o polinômio teria duas raízes racionais, pois*

$$x^2 - 3 = (x + \sqrt{3}) \cdot (x - \sqrt{3}), \quad e \quad \sqrt{3} \notin \mathbb{Q},$$

então f é o polinômio minimal de α sobre $\mathbb{Q}$.

Observação 1.2.3. *Em [27] ilustra o fato do discriminante ($\Delta = b^2 - 4ac$) de um polinômio $f(x) = ax^2 + bx + c$ positivo, então esse polinômio $f(x)$ é redutível sobre $\mathbb{R}$, caso contrário o polinômio $f(x)$ é irredutível sobre $\mathbb{R}$.*

Definição 1.2.8. *Um **corpo de números** $\mathbb{K}$ é uma extensão finita do corpo $\mathbb{Q}$. Se a dimensão de $\mathbb{K}$ sobre $\mathbb{Q}$ é n, então dizemos que $\mathbb{K}$ é um corpo de números de grau n e denotado por $dim_{\mathbb{Q}}\mathbb{K} = n$.*

Teorema 1.2.3. *[40] Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$ para algum elemento algébrico $\alpha \in \mathbb{K}$.*

Exemplo 1.2.8. *Seja $\mathbb{Q}(\sqrt{2})$ uma extensão de $\mathbb{Q}$, então $\mathbb{Q}(\sqrt{2})$ é um corpo de números com dimensão 2. De fato, $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.*

Definição 1.2.9. *Sejam $\mathbb{K}$ um corpo de números e $\alpha \in \mathbb{K}$ uma raiz de um polinômio mônico $f(x) \in \mathbb{Z}[x]$, dizemos que α é um **inteiro algébrico** sobre $\mathbb{Z}$.*

Exemplo 1.2.9. *Considere o corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ e $\sqrt{3} \in \mathbb{K}$ é raiz do polinômio $f(x) = x^2 - 3$, o qual possui coeficientes em $\mathbb{Z}$, logo $\sqrt{3}$ é um inteiro algébrico sobre $\mathbb{Z}$.*

Definição 1.2.10. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os n-monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$. Dizemos que σ_i é um **homomorfismo real** se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$. Caso contrário dizemos que σ_i é um **homomorfismo imaginário**.*

Definição 1.2.11. *Se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$ para todo $(i = 1, ..., n)$, então dizemos que $\mathbb{K}$ é um **corpo totalmente real**, caso ocorra de σ_i ser imaginário para todo $(i = 1, ..., n)$, dizemos que $\mathbb{K}$ é um **corpo totalmente imaginário**.*

Teorema 1.2.4. *[40] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números e $[\mathbb{K} : \mathbb{Q}] = n$, então existem n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$ $(i = 1, ..., n)$. Os elementos $\sigma_i(\theta) = \theta_i$, são raízes distintas em $\mathbb{C}$ do polinômio minimal de θ em $\mathbb{Q}$.*

Exemplo 1.2.10. *Considere a extensão $\mathbb{Q}(\sqrt[4]{3})$ sobre $\mathbb{Q}$, seja o corpo de números $\mathbb{Q}(\sqrt[4]{3}) = \{a + b\sqrt[4]{3} + c(\sqrt[4]{3})^2 + d(\sqrt[4]{3})^3; a, b, c, d \in \mathbb{Q}\}$. A extensão tem grau 4 sobre $\mathbb{Q}$ e o polinômio minimal de $\sqrt[4]{3}$ sobre $\mathbb{Q}$ é $p(x) = x^4 - 3$. Usando a fórmula de De Moivre, obtemos o conjunto de raízes de $p(x)$,*

$$\{\sqrt[4]{3}, i\sqrt[4]{3}, -\sqrt[4]{3}, -i\sqrt[4]{3}\}.$$

Assim, temos 4 monomorfismos

$$\begin{cases} \sigma_1 : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}, \sigma_1(\sqrt[4]{3}) = \sqrt[4]{3} \\ \sigma_2 : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}, \sigma_2(\sqrt[4]{3}) = i\sqrt[4]{3} \\ \sigma_3 : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}, \sigma_3(\sqrt[4]{3}) = -\sqrt[4]{3} \\ \sigma_4 : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}, \sigma_4(\sqrt[4]{3}) = -i\sqrt[4]{3}. \end{cases}$$

Verifica-se que σ_1 e σ_3 são homomorfismos reais e σ_2 e σ_4 são homomorfismos imaginários.

Definição 1.2.12. *Sejam $\mathbb{L} \subset \mathbb{K}$ uma extensão de corpos e $f(x) \in \mathbb{L}[x]$. Dizemos que $\mathbb{K}$ é um **corpo de raízes** de $f(x)$, e denotamos por $\mathbb{K} = \mathbb{L}(R_{f(x)})$ se $\mathbb{K}$ é o menor corpo contendo $\mathbb{L}$ e todas as raízes de $f(x)$.*

Exemplo 1.2.11. *Sejam $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ uma extensão de $\mathbb{Q}$ e $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$, então $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de raízes de f, isto é, contém todas as raízes de f.*

Definição 1.2.13. *Sejam $\mathbb{L}$ um corpo e $f(x) \in \mathbb{L}[x]$ um polinômio não constante. Dizemos que $f(x)$ é **separável** se todas as raízes de $f(x)$ são simples no seu corpo de raízes.*

Observação 1.2.4. *Se $f(x) \in \mathbb{K}[x]$ é polinômio de grau $n \geqslant 1$ e $\alpha_1, ..., \alpha_n$ todas as raízes de $f(x)$ em $\mathbb{C}$, então*

$$f(x) = c(x - \alpha_1)^{m_1} \cdot ... \cdot (x - \alpha_r)^{m_r}.$$

*Em $\mathbb{C}[x]$ temos que $c \in \mathbb{K}$ e $r, m_1, ..., m_r$ são inteiros positivos. O inteiro m_i chama-se **multiplicidade** da raiz α_i. Se $m_i = 1$ dizemos que α_i é uma **raiz simples** de $f(x)$, o teorema a seguir formaliza esse conceito.*

Teorema 1.2.5. *[39] Sejam $f(x) \in \mathbb{K}[x]$, o grau de $f(x)$ é $n \geqslant 1$ e $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$, então*

(i) α é uma raiz simples de $f(x)$ se, e somente se, $f(\alpha) = 0$ e $f'(\alpha) \neq 0$.

(ii) Se $f(x)$ é irredutível sobre $\mathbb{K}$, então todas as raízes de $f(x)$ são simples.

Exemplo 1.2.12. *O polinômio $f(x) = x^2 - 2$ é irredutível em $\mathbb{Q}[x]$ e separável sobre $\mathbb{Q}$. De fato, o corpo de raízes de $f(x)$ é $\mathbb{Q}(\sqrt{2})$ e além disso, suas raízes são simples, pois*

$$f(\sqrt{2}) = 0 \Rightarrow \begin{cases} f'(\sqrt{2}) = 2\sqrt{2} \neq 0 \\ f'(-\sqrt{2}) = -2\sqrt{2} \neq 0. \end{cases}$$

Definição 1.2.14. *Uma extensão $[\mathbb{K} : \mathbb{L}]$ é dita **normal** se para todo $f(x) \in \mathbb{L}[x]$ é irredutível sobre $\mathbb{K}$ tal que possui uma raiz $\alpha \in \mathbb{L}$, então $f(x)$ possui todas as raízes em $\mathbb{L}$.*

Definição 1.2.15. *Uma extensão finita $\mathbb{K}/\mathbb{L}$ é **galoisiana** se $\mathbb{K}$ é o corpo de raízes de $\mathbb{L}$ para algum $f(x) \in \mathbb{L}[x]$ separável.*

Definição 1.2.16. *Seja uma extensão finita $\mathbb{K}/\mathbb{L}$, então esta extensão é galoisiana se for normal.*

Definição 1.2.17. *Chamamos de* ***corpo de decomposição*** *de um polinômio $f(x) \in \mathbb{K}[x]$ sobre $\mathbb{K}$, que denotamos por $L = Gal(f, \mathbb{K})$, o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e todas as raízes de $f(x)$ em $\mathbb{C}$.*

Exemplo 1.2.13. *Considere o polinômio $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ irredutível em $\mathbb{Q}$, as suas quatro raízes em $\mathbb{C}$ são*

$$\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\sqrt[4]{2}, \alpha_3 = -i\sqrt[4]{2}, \alpha_4 = -\sqrt[4]{2}.$$

O corpo $\mathbb{Q}(\sqrt[4]{2}, i)$ é o corpo de decomposição de $f(x)$. Além disso, a extensão $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}]$ é normal sobre $\mathbb{Q}$.

Podemos acrescentar que o polinômio $f(x) = x^4 - 2$ é separável pelo item (i) do Teorema 1.2.5, desse modo temos uma extensão galoisiana.

Definição 1.2.18. *Sejam $\mathbb{L} \subset \mathbb{K}$ uma extensão e $H \subset Aut(\mathbb{K})$. O Corpo*

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

é chamado de ***corpo fixo*** *pelo conjunto H.*

Definição 1.2.19. *Seja $\mathbb{L} \subset \mathbb{K}$ é uma extensão, então o* ***grupo de Galois*** *de $\mathbb{K}$ sobre $\mathbb{L}$ é dado por*

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

Exemplo 1.2.14. *Sejam $\mathbb{M} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ uma extensão de $\mathbb{K} = \mathbb{Q}$, $\mathbb{M}$ é o corpo de raízes do polinômio $p(x) = (x^2 - 2) \cdot (x^2 - 3)$ que contém 4 elementos $\{-\sqrt{2}, \sqrt{2}, \sqrt{3}, -\sqrt{3}\}$ e o grupo de Galois*

$$Gal(\mathbb{M}, \mathbb{K}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\},$$

que possui os subgrupos

$$H_0 = \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_1\}, H_2 = \{\sigma_0, \sigma_2\} \quad e \quad H_3 = \{\sigma_0, \sigma_3\}.$$

O grupo de Galois permuta as raízes do corpo de raízes e cada subgrupo do grupo de Galois fixam determinados subcorpos de $\mathbb{M}$. Os automorfismos σ_i permutam as raízes do polinômio $p(x)$, são elas

$$\textit{Permutações:} \begin{cases} \sigma_1 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \sigma_3 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \\ \sigma_4 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}. \end{cases}$$

$$\textit{Os corpos fixos por } H \textit{ são: } \begin{cases} K^{H_0} = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \textit{identidade} \\ K^{H_1} = \mathbb{Q}(\sqrt{3}) \\ K^{H_2} = \mathbb{Q}(\sqrt{2}) \\ K^{H_3} = \mathbb{Q}(\sqrt{6}), \textit{composição.} \end{cases}$$

Definição 1.2.20. *Seja $\mathbb{K}$ um corpo de números. Temos que*

*(i) Uma **involução** $\phi : \mathbb{K} \to \mathbb{K}$ é uma aplicação aditiva e multiplicativa tal que ϕ^2 é a identidade.*

*(ii) O conjunto $\mathbb{F} = \{x \in \mathbb{K}; \phi(x) = x\}$ é um corpo chamado **corpo fixo da involução**.*

Proposição 1.2.1. *[6] Se $\phi : \mathbb{K} \to \mathbb{K}$ é uma involução, então $\phi \in Gal(\mathbb{K}/\mathbb{Q})$, onde $Gal(\mathbb{K}/\mathbb{Q})$ denota o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$.*

Proposição 1.2.2. *[6] Seja $\mathbb{K}$ é um corpo de números, ϕ uma involução e $\mathbb{F}$ um corpo fixo da involução, então $[\mathbb{K} : \mathbb{F}] \leqslant 2$.*

Exemplo 1.2.15. *Sejam $\mathbb{C}$ uma extensão de $\mathbb{R}$ e α um $\mathbb{R}$-automorfismo em $\mathbb{C}$. Tomando $J = \alpha(i)$, onde $i = \sqrt{-1}$, então*

$$J^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1.$$

Para $\alpha(r) = r, \forall r \in \mathbb{R}$, então $J = i$ ou $J = -1$. Para todo $x, y \in \mathbb{R}$ temos

$$\alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y) = x + iy.$$

Desse modo temos dois candidatos a $\mathbb{R}$-automorfismos

$$\alpha_1 : x + iy \mapsto x + iy,$$

$$\alpha_2 : x + iy \mapsto x - iy.$$

Sendo α_1 identidade e α_2 a conjugação complexa. Fazendo α_2^2 temos uma involução, isto é,

$$\alpha_2^2 = \alpha_1 = id,$$

então, a extensão $\mathbb{C}/\mathbb{R}$ é um grupo de Galois de ordem 2, pois os únicos elementos fixos pelo $\mathbb{R}$-automorfismo são $\{id, \alpha_2^2\}$.

1.3 Teoria algébrica dos números

Nesta seção serão apresentados os principais conceitos e definições da teoria algébrica dos números necessários para o desenvolvimento deste trabalho. Na Subseção 1.3.1

definiremos os conceitos de inteiros algébricos e anel dos inteiros. Na Subsecção 1.3.2 apresentamos os conceitos de traço e norma de um corpo de números. Na Subsecção 1.3.3 trabalhamos com a norma de um ideal. Na Subsecção 1.3.4 apresentamos o conceito de discriminante de um corpo de números. Por fim, nas Subseções 1.3.5 e 1.3.6 apresentamos os corpos quadráticos e os corpos ciclotômicos.

1.3.1 Inteiros algébricos

Definição 1.3.1. *Sejam $A \subset B$ anéis. Dizemos que um elemento $\alpha \in B$ é **inteiro** sobre A se existe um polinômio mônico não nulo $f(x)$ com coeficientes em A tal que $f(\alpha) = 0$.*

Exemplo 1.3.1. *O elemento $x = \sqrt{2}$ é inteiro sobre $\mathbb{Z}$, pois satisfaz o polinômio $x^2 - 2 \in \mathbb{Z}[x]$ e $x \in \mathbb{Z}$.*

Teorema 1.3.1. *[13] Sejam A um anel, $B \in A$ subanel e $x \in A$, então são equivalentes*

(i) x é inteiro sobre B.

(ii) O anel $B[x]$ é um B-módulo finitamente gerado.

(iii) Existe um subanel A' de A que é um B-módulo finitamente gerado que contém B e x.

Demonstração: (i)$\Rightarrow$ (ii). Tome $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in B[x]$ tal que $x \in A$ é raiz de $p(x)$, isto é, x é um inteiro sobre B, ou seja, existem $a_1, ..., a_n \in B$ não todos nulos, tal que $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$. Assim, podemos escrever $x^n = -(a_{n-1}x^{n-1} + ... + a_1x + a_0)$. Seja $M = B + Bx + Bx^2 + ... + Bx^{n-1}$, evidentemente $M \in B[x]$, pois $M =< 1, x, x^2, ..., x^{n-1} >$ é um A-módulo finitamente gerado, provemos que $B[x] = M$. Temos que $x^n \in M$, pois x^n é uma combinação linear dos elementos geradores de M.

Agora mostremos por indução que $x^j \in M$, $\forall j \in N$, temos que para $j \leqslant n$ o resultado se verifica.

Supondo que $x^j \in M$, ou seja,

$$x^j = b_{n-1}x^{n-1} + ... + b_1x + b_0,$$

para, $b_0, ..., b_{n-1} \in B$. Mostremos que $x^{n+1} \in M$, de fato,

$x^{j+1} = x^j \cdot x$

$=(b_{n-1}x^{n-1} + ... + b_1x + b_0)x$

$=b_{n-1}x^n + ... + b_1x^2 + b_0x$

$=b_{n-1}(-a_{n-1}x^{n-1} - ... - a_1x - a_0) + ... + b_1x + b_0x$

$=-b_{n-1}b_0 + (b_0 - b_{n-1}a_1)x + ... + (b_{n-2} - b_{n-1}a_{n-1})x^{n-1}.$

Logo $x^{j+1} \in M$, o que mostra que $B[x] \subset M$, então $M = B[x]$.

(ii)$\Rightarrow$ (iii). Tome $A' = B[x]$, pois $B \subset B[x]$ e $x \in B[x]$.

(iii)$\Rightarrow$ (i). Seja $\{\beta_1, ..., \beta_n\}$ um conjunto finito gerador de A', um B-módulo finitamente gerado, ou seja,

$$A' = B\beta_1 + B\beta_2 + ... + B\beta_n.$$

Como $x \in A'$ e A' é subanel de A, segue que

$$x\beta_i \in A',\ \forall i = 1, ..., n.$$

Assim, $x\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j$, com $a_{ij} \in B$, para $1 \leqslant i, j \leqslant n$. Daí, $x\beta_i - \sum_{j=1}^{n} a_{ij}\beta_j = 0$ e, podemos reescrever como $\sum_{j=1}^{n}(x\frac{\beta_i}{\beta_j} - a_{ij})\beta_j = 0$. Tomando $\frac{\beta_i}{\beta_j} = \delta_{ij} = \begin{cases} 0, i \neq j \\ 1, i = j \end{cases}$,

temos que $\sum_{j=1}^{n}(x\delta_{ij} - a_{ij})\beta_j = 0$, para $i = 1, ..., n$. Assim, temos um sistema linear de n equações lineares homogêneas em que $\beta_1, ..., \beta_n$ é a solução:

$$\begin{cases} \sum_{j=1}^{n}(x\delta_{ij} - a_{ij})\beta_j = 0 \\ \sum_{j=1}^{n}(\delta_{2j} - a_{2j})\beta_j = 0 \\ \vdots \\ \sum_{j=1}^{n}(\delta_{nj} - a_{nj})\beta_j = 0. \end{cases}$$

Escrevendo na forma matricial obtemos:

$$\begin{bmatrix} x\delta_{11} - a_{11} & \dots & x\delta_{1n} - a_{1n} \\ x\delta_{21} - a_{21} & \dots & x\delta_{2n} - a_{2n} \\ \vdots & \ddots & \vdots \\ x\delta_{n1} - a_{n1} & \dots & x\delta_{nn} - a_{nn} \end{bmatrix} \cdot \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

O determinante $det(x_{ij}x - a_{ij}) = d$. Pela regra de Cramer, temos que $d\beta_j = 0$. Consequentemente, $dA' = 0$, pois A' é gerado por $\beta_1, ..., \beta_n$. Em particular $d1 = d = 0$. Mas, d é um polinômio mônico em x, $d = x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$, onde $a_i \in B$. Portanto, x é inteiro sobre B. ■

Proposição 1.3.1. *[13] Se $x_1, ..., x_n \in A$ forem inteiros sobre B, então $B[x_1, ..., x_n]$ é B-módulo finitamente gerado.*

Demonstração: Pelo Teorema 1.3.1, temos que x_1 é inteiro sobre B, então $B[x_1]$ é um B-módulo finitamente gerado. Suponhamos por indução que $C = B[x_1, ..., x_{n-1}]$ seja B-módulo finitamente gerado, ou seja, $C = \sum_{j=1}^{p} BC_i$, onde $c_1, ..., c_p \in C$. Pelo Teorema 1.3.1 temos que $B[x_1, ..., B_n] = C[x_n]$ é C-módulo finitamente gerado. Então

$$C[x_n] = \sum_{k=1}^{q} CW_k = \sum_{k=1}^{q}(\sum_{j=1}^{p} BC_i)W_k = \sum_{jk} BC_iW_k,$$

onde $W_k \in C[x_n]$. Logo $B[x_1, ..., x_n]$ é um B-módulo finitamente gerado por $\{C_iW_k\}$. ■

Corolário 1.3.1. *[35] Sejam A um anel, $B \subset A$ um subanel e $x, y \in A$. Se x e y são inteiros sobre B então $x + y$, $x - y$ e xy são inteiros sobre B.*

Demonstração: Pela Proposição 1.3.1, $B[x, y]$ é finitamente gerado, pois x, y são inteiros sobre B. Como $x, y \in B[x, y]$ e $B[x, y]$ é subanel de A, $x + y$, $x - y$ e xy são elementos de $B[x, y]$ e pelo Teorema 1.3.1 como $B \subset B[x, y] \subset A$ e $B[x, y]$ contém $x + y$, $x - y$ e xy estes são inteiros sobre B. ■

Exemplo 1.3.2. *Sejam $\mathbb{Z} \subset \mathbb{R}$ anéis, tomando $x = 1$ e $y = 2$ onde $x, y \in \mathbb{R}$, são inteiros sobre $\mathbb{Z}$, pois são raízes dos polinômios $x^2 - 1, x^2 - 4 \in \mathbb{Z}[x]$ respectivamente. E $x + y$, $x - y$ e xy são inteiros sobre $\mathbb{Z}$, pois são raízes de polinômios com coeficientes em $\mathbb{Z}[x]$. De fato,*

$$x + y = 3, \quad x - y = -1, \quad xy = 2,$$

são raízes de, por exemplo, $x^2 - 9$, $x^2 - 1$, $x^2 - 4$ em $\mathbb{Z}[x]$, respectivamente.

Definição 1.3.2. *Sejam $B \subset A$ anéis. Dizemos que A é **inteiro** sobre B se todo elemento de A for inteiro sobre B.*

Exemplo 1.3.3. *Seja $\mathbb{Z} \subset \mathbb{R}$ anéis, então $\forall a \in \mathbb{R}$ são inteiros sobre $\mathbb{Z}$, pois a é raiz de todo polinômio na forma $f(x) = x - a \in \mathbb{Z}[x]$, dessa forma $\mathbb{R}$ é inteiro sobre $\mathbb{Z}$.*

Proposição 1.3.2. *[35] Sejam $C \subset B \subset A$ anéis. Se A é inteiro sobre B e B é inteiro sobre C, então A é inteiro sobre C.*

Demonstração: Suponhamos que A é inteiro sobre C, todo elemento de A é inteiro sobre C, se $\alpha \in A$ então existe $a_0, ..., a_{n-1} \in C$, não nulos, tal que

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

Como $C \subset B$, segue que $a_i \in B$, para $i = 0, 1, ..., n$, ou seja, α é inteiro sobre B. Portanto, A é inteiro sobre B. Agora se $\beta \in B$, como $B \subset A$ segue que $\beta \in A$, então existem

$b_0, ..., b_{n-1} \in B$ não nulos tal que

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

Como $\beta \in A$, então β é inteiro sobre A, implica que β é inteiro sobre C, pois todo elemento de A é inteiro sobre B e de C, e como $C \subset B$, portanto B é inteiro sobre C. ■

Observação 1.3.1. *Na Proposição 1.3.2 a propriedade de ser inteiro é transitiva.*

Definição 1.3.3. *Sejam $A \subset B$ anéis.*

(i) O conjunto de elementos de B que são inteiros sobre A é denotado por

$$\mathbb{I}_B(A) = \{\alpha \in B : \alpha \text{ é inteiro sobre } A\} \text{ é dito } \textbf{\textit{anel dos inteiros}} \text{ de } B \text{ sobre } A.$$

*(ii) Se A é um domínio e $B = \mathbb{K}$ seu corpo de frações dizemos que $\mathbb{I}_B(A)$ é **anel dos inteiros** de A sobre $\mathbb{K}$.*

*(iii) Se todo elemento de B é inteiro sobre A, ou seja, $\mathbb{I}_B(A) = B$, então o **conjunto B é inteiro sobre** A.*

Definição 1.3.4. *Sejam A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Quando $\mathbb{I}_{\mathbb{K}}(A) = A$ o anel A é **integralmente fechado**.*

Observação 1.3.2. *Em outras palavras, um anel é integralmente fechado se todo elemento do seu corpo de frações que é inteiro sobre A e está em A.*

Exemplo 1.3.4. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Então $\mathbb{I}_{\mathbb{K}}(A)$ é anel integralmente fechado, ou seja, $\mathbb{I}_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}}(A)) = \mathbb{I}_{\mathbb{K}}(A) = A$. Visto que $A \subset \mathbb{I}_{\mathbb{K}} \subset \mathbb{K}$ e $\mathbb{K}$ é o menor corpo que contém A, logo $\mathbb{K}$ é o menor corpo que contém $\mathbb{I}_{\mathbb{K}}$, assim $\mathbb{K}$ é o corpo das frações de $\mathbb{I}_{\mathbb{K}}(A)$. Seja $\alpha \in \mathbb{K}$ um inteiro sobre $\mathbb{I}_{\mathbb{K}}$. Sendo $\mathbb{I}_{\mathbb{K}}$ inteiro sobre A, então pela Proposição 1.3.2 α é inteiro sobre A e $\alpha \in \mathbb{I}_{\mathbb{K}}$. Assim A é integralmente fechado.*

Proposição 1.3.3. *[35] Todo domínio principal é integralmente fechado.*

Exemplo 1.3.5. *O anel $\mathbb{Z}$ é um domínio de integridade, pois tem elemento unidade e sem divisor de zero. O conjunto $< 2 >$ é ideal de $\mathbb{Z}$ gerado pelo elemento 2, então todo ideal de $\mathbb{Z}$ é principal. Logo, $\mathbb{Z}$ é um domínio principal,implicando em $\mathbb{Z}$ ser integralmente fechado.*

Definição 1.3.5. *Um número complexo α é um **inteiro algébrico** se existe um polinômio mônico $f(x)$ com coeficientes inteiros tal que $f(\alpha) = 0$.*

Exemplo 1.3.6. *Seja $\alpha = \sqrt{2}$ inteiro algébrico, pois é raiz do polinômio mônico $f(x) = x^2 - 2$ com coeficientes em $\mathbb{Z}$.*

Teorema 1.3.2. *[40] Se α é um número complexo que satisfaz um polinômio mônico cujos coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Exemplo 1.3.7. *Dado $p(x) = x^2 - x + 10 \in \mathbb{Z}[x]$ mônico, os coeficientes de $p(x)$ são inteiros algébricos de outros polinômios em $\mathbb{Z}$. De fato, $\alpha = -1$ e $\beta = 10$ são raízes de $f(x) = x^2 - 1$ e $g(x) = x^2 - 100$ respectivamente.*

Teorema 1.3.3. *[40] Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$ para algum inteiro algébrico α.*

Exemplo 1.3.8. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt[3]{(-2)^2})$ corpo de números e $\alpha_1 = \sqrt[3]{(-2)^2}$ inteiro algébrico. De fato, α_1 é raiz do polinômio mônico $f(x) = x^3 - 4$.*

Exemplo 1.3.9. *Sabemos que $\mathbb{Z}$ é domínio, $\mathbb{Q}$ seu corpo de frações e $\mathbb{R}$ uma extensão de $\mathbb{Q}$. Dado um polinômio mônico $p(x) = x^2 - 2x + 1 \in \mathbb{Z}[x]$ onde $\alpha_1 = 1$ é inteiro sobre $\mathbb{Z}$. Como $\alpha_1 \in \mathbb{Q}$ e $\alpha_1 \in \mathbb{Z}$, temos que $\mathbb{I}_{\mathbb{Q}}(\mathbb{Z}) = \mathbb{Z}$ é integralmente fechado.*

Definição 1.3.6. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathbb{I}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$, chamamos de **base integral** de $\mathbb{K}$ ou de $\mathbb{I}_{\mathbb{K}}$ uma $\mathbb{Z}$-base para o grupo aditivo $\mathbb{I}_{\mathbb{K}}$.*

Observação 1.3.3. *Se $\{\alpha_1, ..., \alpha_n\}$ é uma base integral $\mathbb{I}_{\mathbb{K}}$, então todo elemento $\alpha \in \mathbb{I}_{\mathbb{K}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, ..., n$.*

Mostraremos em seções subsequentes propriedades e exemplos sobre bases integrais.

1.3.2 Traço e norma

Definição 1.3.7. *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão de grau n e $\sigma_1, ..., \sigma_2$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. O **traço** e **norma** de um elemento $\alpha \in \mathbb{K}$ relativamente a extensão $\mathbb{K}/\mathbb{L}$ são definidos por*

$$Tr_{\mathbb{K}/\mathbb{L}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \qquad e \qquad \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Observação 1.3.4. *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão de grau n, e denotaremos traço e norma por $Tr(\alpha)$ e $\mathcal{N}(\alpha)$. Se $\alpha, \beta \in \mathbb{K}$, então valem as seguintes propriedades*

1. $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
2. $Tr(x \cdot \alpha) = xTr(\alpha.)$
3. $Tr(x) = n \cdot x$.
4. $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$.
5. $\mathcal{N}(x\alpha) = x^n\mathcal{N}(\alpha)$.

6. $\mathcal{N}(x) = x^n$.

Temos outras propriedades para as extensões $\mathbb{M} \subset \mathbb{L} \subset \mathbb{K}$ *finitas e* $\alpha \in K$,

1. $Tr_{\mathbb{K}/\mathbb{M}}(\alpha) = Tr_{\mathbb{L}/\mathbb{M}}(Tr_{\mathbb{K}/\mathbb{L}}(\alpha))$.

2. $\mathcal{N}_{\mathbb{K}/\mathbb{M}}(\alpha) = \mathcal{N}_{\mathbb{L}/\mathbb{K}}(\mathcal{N}_{\mathbb{K}/\mathbb{L}})(\alpha)$.

3. $Tr_{\mathbb{K}/\mathbb{M}}(\alpha) = [\mathbb{K} : \mathbb{L}] \cdot Tr_{\mathbb{L}/\mathbb{M}}(\alpha)$.

4. $\mathcal{N}_{\mathbb{K}/\mathbb{M}}(\alpha) = \mathcal{N}_{\mathbb{L}/\mathbb{M}}(\alpha)^{[\mathbb{K}:\mathbb{L}]}$.

Exemplo 1.3.10. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{17})$ *um corpo de números e* $\mathbb{K}/\mathbb{Q}$ *uma extensão, com* $\alpha = 1 + \sqrt{17}$ *e* $\beta = \dfrac{3 + \sqrt{17}}{2}$ *elementos de* $\mathbb{K}$*, os monomorfismos de* $\mathbb{K}$ *e os elementos fixos por* $\mathbb{Q}$*, são*

$$\sigma_1 : \mathbb{Q}(\sqrt{17}) \to \mathbb{C}, \sqrt{17} \mapsto \sqrt{17} \qquad e \qquad \sigma_2 : \mathbb{Q}(\sqrt{17}) \to \mathbb{C}, \sqrt{17} \mapsto -\sqrt{17}.$$

Apresentamos a seguir, algumas propriedades de norma e traço.

$$\mathcal{N}(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) = (1 + \sqrt{17}) \cdot (1 - \sqrt{17}) = -16.$$

$$\mathcal{N}(\beta) = \sigma_1(\beta) \cdot \sigma_2(\beta) = \left(\frac{3 + \sqrt{17}}{2}\right) \cdot \left(\frac{3 - \sqrt{17}}{2}\right) = -2.$$

$$Tr(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (1 + \sqrt{17}) + (1 - \sqrt{17}) = 2.$$

$$Tr(\beta) = \sigma_1(\beta) + \sigma_2(\beta) = \left(\frac{3 + \sqrt{17}}{2}\right) + (3 - \sqrt{17}) = 3.$$

E com isso temos que

$$\begin{aligned} \mathcal{N}(\alpha \cdot \beta) &= \mathcal{N}\left((1 + \sqrt{17})\left(\frac{3 + \sqrt{17}}{2}\right)\right) \\ &= \mathcal{N}(10 + 2\sqrt{17}) \\ &= \sigma_1(10 + 2\sqrt{17}) \cdot \sigma_2(10 + 2\sqrt{17}) \\ &= (10 + 2\sqrt{17})(10 - 2\sqrt{17}) = 32 = (-16)(-2) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta), \end{aligned}$$

$$e$$

$$\begin{aligned} Tr(\alpha + \beta) &= Tr\left((1 + \sqrt{17}) + \left(\frac{3 + \sqrt{17}}{2}\right)\right) \\ &= Tr\left(\frac{5 + 3\sqrt{17}}{2}\right) \\ &= \sigma_1\left(\frac{5 + 3\sqrt{17}}{2}\right) + \sigma_2\left(\frac{5 + 3\sqrt{17}}{2}\right) \\ &= \frac{5 + 3\sqrt{17}}{2} + \frac{5 - 3\sqrt{17}}{2} = 5 = 2 + 3 = Tr(\alpha) + Tr(\beta). \end{aligned}$$

Proposição 1.3.4. *[35] Sejam $\mathbb{K}$ um corpo de característica zero ou um corpo finito, $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$ de grau n, $\alpha \in \mathbb{L}$ e $\alpha_1, ..., \alpha_n$ raízes do polinômio minimal de α sobre $\mathbb{K}$. Então, $Tr_{\mathbb{K}/\mathbb{L}}(\alpha) = \alpha_1 + \alpha_2 + ... + \alpha_n$ e $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_n$ e $g(x) = (x - \alpha_1)...(x - \alpha_n)$,* ***polinômio característico****.*

Proposição 1.3.5. *[35] Sejam A um domínio, $\mathbb{L}$ seu corpo de frações e $\mathbb{K}$ uma extensão finita de $\mathbb{L}$. Se $\alpha \in \mathbb{K}$ é um inteiro sobre A, então os coeficientes do polinômio característico $g(x)$ de α relativo a $\mathbb{K}$ e $\mathbb{L}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$, são inteiros sobre A.*

Corolário 1.3.2. *[35] Se A é anel integralmente fechado, então os coeficientes do polinômio característico de $\alpha \in \mathbb{K}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$ são elementos de A.*

Demonstração: Por definição esses coeficientes são elementos de $\mathbb{K}$. Pela Proposição 1.3.5 são inteiros sobre A. Logo são elementos de A, pois A é integralmente fechado. ■

Exemplo 1.3.11. *Sejam $\mathbb{Z}$ domínio e integralmente fechado, $\mathbb{Q}$ um corpo de frações, $\mathbb{R}/\mathbb{Q}$ uma extensão, $\mathbb{K} = \mathbb{Q}(\sqrt{17})$ um corpo de números e $p(x) = x^2 - 17$ um polinômio característico com $\alpha_1 = \sqrt{17}$ e $\alpha_2 = -\sqrt{17}$ raízes de $p(x)$, então*

$$\mathcal{N}(\alpha) = \sqrt{17} \cdot (-\sqrt{17}) = -17 \qquad e \qquad Tr(\alpha) = \sqrt{17} + (-\sqrt{17}) = 0,$$

são elementos de $\mathbb{Z}$ e inteiros sobre $\mathbb{Z}$, isto é, são coeficientes de $p(x)$.

Lema 1.3.1. *[13] Sejam A um anel integralmente fechado, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\mathbb{I}_{\mathbb{K}}$ anel dos inteiros algébricos $\mathbb{K}$. Se $\{\alpha_1, ..., \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}$ onde $det(Tr(\alpha_i\alpha_j)) \neq 0$ e $\alpha \in \mathbb{K}$. Se $tr(\alpha \cdot \beta) = 0$ para todo $\beta \in \mathbb{K}$, então $\alpha = 0$.*

Exemplo 1.3.12. *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\{1, \sqrt{7}\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, os monomorfismos e os corpos fixos por $\mathbb{Q}$*

$$\sigma_1 : \mathbb{Q} \to \mathbb{C}, \sqrt{7} \mapsto \sqrt{7} \qquad e \qquad \sigma_2 : \mathbb{Q} \to \mathbb{C}, \sqrt{7} \mapsto -\sqrt{7}.$$

Então,

$$det \begin{vmatrix} Tr(1 \cdot 1) & Tr(\sqrt{7} \cdot 1) \\ Tr(1 \cdot \sqrt{7}) & Tr(\sqrt{7} \cdot \sqrt{7}) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 14 \end{vmatrix} = 28.$$

Logo, $det(Tr(\alpha_1 \cdot \alpha_2)) \neq 0$.

Lema 1.3.2. *[32] Com as mesmas hipóteses do Lema 1.3.1 temos que a aplicação $\rho : \mathbb{L} \to Hom_{\mathbb{K}}(\mathbb{K}, \mathbb{L})$ um homomorfismo, dado por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = Tr_{\mathbb{K}/\mathbb{L}}(\alpha\beta)$, com $\beta \in \mathbb{L}$, um isomorfismo.*

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

$$\begin{cases} \rho(\alpha_1+\alpha_2)(\beta) = S_{\alpha_1,\alpha_2}(\beta) = Tr_{\mathbb{K}/\mathbb{L}}((\alpha_1+\alpha_2)(\beta)) = \\ Tr_{\mathbb{K}/\mathbb{L}}(\alpha_1\cdot\beta) + Tr_{\mathbb{K}/\mathbb{L}}(\alpha_2\cdot\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (\rho(\alpha_1)+\rho(\alpha_2))(\beta), \qquad e \\ \rho(a\alpha)(\beta) = S_{a\alpha}(\beta) = Tr_{\mathbb{K}/\mathbb{L}}(a\alpha\beta) = aTr_{\mathbb{K}/\mathbb{L}}(\alpha\beta) = aS_{\alpha}(\beta) = a\rho(\alpha)(\beta), \end{cases}$$

para todo $\beta \in \mathbb{L}$. Assim, ρ é um homomorfismo. Agora se $\alpha \in \mathbb{L}$ é tal que $\rho(\alpha) = 0$, então $\rho(\alpha)(\beta) = S_\alpha(\beta) = Tr_{\mathbb{K}/\mathbb{L}}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{L}$. Pelo Lema 1.3.1, segue que $\alpha = 0$. Assim ρ é injetora. Além disso, como $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{K},\mathbb{L}))$, segue que ρ é sobrejetora. Portanto, ρ é um isomorfismo. ■

Teorema 1.3.4. *[32] Se A é um anel integralmente fechado, $\mathbb{L}$ é seu corpo de fração, $\mathbb{K}/\mathbb{L}$ extensão finita de grau n e $\mathbb{I}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$, então $\mathbb{I}_{\mathbb{K}}$ é um A-módulo livre de posto n.*

Observação 1.3.5. *Seja $\{\alpha_1, ..., \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}$, de dimensão n, então todos os elementos da base são inteiros sobre $\mathbb{K}$*

1.3.3 Norma de um ideal

Definição 1.3.8. *Sejam $\mathbb{K}$ um corpo de números, $\mathbb{I}_{\mathbb{K}}(\mathbb{Z})$ anel, dos inteiros de $\mathbb{K}$ e $\mathcal{U}$ um ideal de $\mathbb{I}_{\mathbb{K}}(\mathbb{Z})$ não nulo. A **norma do ideal** $\mathcal{U}$ é definida como o número de elementos do anel quociente $\frac{\mathbb{I}_{\mathbb{K}}(\mathbb{Z})}{\mathcal{U}}$, ou seja,*

$$\mathcal{N}(\mathcal{U}) = \#\frac{\mathbb{I}_{\mathbb{K}}(\mathbb{Z})}{\mathcal{U}}.$$

Teorema 1.3.5. *[40] Sejam $\mathbb{K}$ um corpo de números e $\mathbb{I}_{\mathbb{K}}(\mathbb{Z})$ um anel dos inteiros de $\mathbb{K}$. Se $\mathcal{U} =< \alpha >$ é um ideal principal de $\mathbb{I}_{\mathbb{K}}(\mathbb{Z})$, então $\mathcal{N}(\mathcal{U}) = |\mathcal{N}(\alpha)|$.*

Observação 1.3.6. *Se α é um elemento não nulo de $\mathbb{I}_{\mathbb{K}}(\mathbb{Z})$, então $\mathcal{N}(\alpha) \in \mathbb{Z}$.*

Proposição 1.3.6. *[37] Se $\mathcal{U}$ é um ideal não nulo, então $\mathcal{N}(\mathcal{U})$ é finita.*

Lema 1.3.3. *[40] Se $\mathcal{U}$ e $\mathcal{A}$ são ideais não nulos de $\mathbb{I}_{\mathbb{K}}$, então $\mathcal{N}(\mathcal{U}\cdot\mathcal{A}) = \mathcal{N}(\mathcal{U})\cdot\mathcal{N}(\mathcal{A})$*

Proposição 1.3.7. *[35] Se $\mathcal{U}$ é um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$, então*

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

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

Exemplo 1.3.13. *Sejam $\mathcal{U}$ e $\mathcal{A}$ ideais de $\mathbb{Z}[i]$ inteiros de Gauss do corpo de números $\mathbb{Q}[i]$. Os ideais $\mathcal{U}$ e $\mathcal{A}$ são gerados por $z = a + bi$ e $w = c + di$ respectivamente, fazendo*

$$z\cdot w = (ac - bd) + (ad + bc)i,$$

Segundo o Lema 1.3.3, temos os seguintes cálculos

$$(i)\ \mathcal{N}(z)\cdot\mathcal{N}(w) = (a^2+b^2)\cdot(c^2+d^2) = (ac)^2+(ad)^2+(bc)^2+(bd)^2,$$

$$(ii)\ \mathcal{N}(zw) = (ac-bd)^2+(ad+bc)^2 = (ac)^2+(bd)^2+(ad)^2+(bc)^2.$$

Logo, $\mathcal{N}(zw) = \mathcal{N}(z)\cdot\mathcal{N}(w)$.

Agora vamos caracterizar aqueles anéis dos inteiros $\mathbb{I}_{\mathbb{K}}$ para os quais a fatoração de elementos irredutíveis é única.

Teorema 1.3.6. *[40] A fatoração dos elementos de* $\mathbb{I}_{\mathbb{K}}$ *em irredutíveis é unico se, e somente se, cada ideal de* $\mathbb{I}_{\mathbb{K}}$ *for principal.*

Exemplo 1.3.14. *Sejam* $\mathbb{Z}[i]$ *anel dos inteiros de Gauss e* $\mathcal{U} =< 3 >$ *ideal gerado por 3, irredutível em* $\mathbb{Z}[i]$. *Portanto,* $\mathcal{U}$ *é ideal primo em* $\mathbb{Z}[i]$, *pois tem fatoração única. Por outro lado,* $\mathcal{A} =< 5 >$ *ideal de* $\mathbb{Z}[i]$, *não é primo, pois* $5 = (2+i)(2-i)$.

1.3.4 Discriminante

Definição 1.3.9. *Sejam* $B \subset A$ *anéis tal que* A *é um* B*-módulo livre de posto* n *e* $\{\alpha_1,...,\alpha_n\} \in A^n$. *Definimos o* ***discriminante*** *de* $\{\alpha_1,...,\alpha_n\}$ *por*

$$\mathcal{D}_{A/B}(\alpha_1,...,\alpha_n) = det(Tr_{A/B}(\alpha_i\alpha_j)).$$

Corolário 1.3.3. *[25] O discriminante* $\mathcal{D}(\alpha_1,...,\alpha_n) \in \mathbb{Q}$ *se* α_i *é inteiro algébrico, então* $\mathcal{D}(\alpha_1,...,\alpha_n) \in \mathbb{Z}$.

Exemplo 1.3.15. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *um corpo de números e* $\{1,\sqrt{3}\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$. *Então*

$$\mathcal{D}(1,\sqrt{3}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{3}) \\ Tr(\sqrt{3} & Tr((\sqrt{3})^2)) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 6 \end{vmatrix} = 12.$$

Proposição 1.3.8. *[32] Sejam* $B \subset A$ *anéis. Se* $\{\alpha_1,...,\alpha_n\}$, $\{\beta_1,...,\beta_n\} \in A^n$ *são tais que* $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$ *com* $a_{ij} \in B$, *então*

$$\mathcal{D}_{A/B}(\beta_1,...,\beta_n) = (det(a_{ij}))^2\cdot\mathcal{D}_{A/B}(\alpha_1,...,\alpha_n).$$

Exemplo 1.3.16. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *um corpo de números e* $\{1,\sqrt{3}\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$, *sabemos que o discriminante de* $\{1,\sqrt{3}\}$ *é 12. Seja* $\{1+\sqrt{3},-4-\sqrt{3}\}$ *outra base de* $\mathbb{K}$, *pela Proposição 1.3.8, temos que*

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1+\sqrt{3},-4-\sqrt{3}) = \begin{vmatrix} 1 & 1 \\ -4 & -1 \end{vmatrix}^2 \mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\sqrt{3}) = 3^2\cdot(12).$$

Observação 1.3.7. *A Proposição 1.3.8, implica que o discriminante das bases de B sobre A são associadas, isto é, a matriz (a_{ij}) que expressa uma base em termos da outra tem uma matriz inversa com entradas em A. Portanto, ambos $det(a_{ij})$ e $det(a_{ij})^{-1}$ são inversíveis em A.*

Corolário 1.3.4. *[35] Sejam $A \subset B$ anéis tais que B é um A-módulo livre de posto finito n e A um domínio. Se $\{\alpha_1, ..., \alpha_n\}$ e $\{\beta_1, ..., \beta_n\}$ são bases de B, então $\mathcal{D}_{B/A}(\alpha_1, ..., \alpha_n)$ e $D_{B/A}(\beta_1, ..., \beta_n)$ são associadas ou possuem determinantes nulos.*

Demonstração: Como $\{\alpha_1, ..., \alpha_n\}$ e $\{\beta_1, ..., \beta_n\}$ são bases de B, segue que existem elementos $a_{ij} \in A$ tais que $\beta_i = \sum_{i=1}^{n} a_{ij}\alpha_i$, para todo $j = 1, ..., n$. Assim pela Proposição 1.3.8, temos que

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

como a_{ij} é uma matriz inversível, segue que o $det(a_{ij})$ é uma unidade de A. Assim $\mathcal{D}_{B/A}(\alpha_1, ..., \alpha_n)$ e $\mathcal{D}_{B/A}(\beta_1, ..., \beta_n)$ são elementos associados ou ambos são nulos. ■

Proposição 1.3.9. *[34] Sejam A um domínio, B um anel tal que $A \subset B$ e B um A-módulo livre de posto finito n. Se o conjunto $\{\alpha_1, ..., \alpha_n\}$ de elementos de B é linearmente dependente sobre A, então*

$$D_{B/A}(\alpha_1, ..., \alpha_n) = 0.$$

Definição 1.3.10. *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n, $\mathbb{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\{\alpha_1, ..., \alpha_n\}$ uma $\mathbb{Z}$-base de $\mathbb{I}_{\mathbb{K}}$. Definimos o **discriminante** de $\mathbb{K}$ como um ideal principal de $\mathbb{Z}$ gerado por $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, ..., \alpha_n)$ e denotado por $\mathcal{D}_{\mathbb{K}}$.*

Observação 1.3.8. *O discriminante de quaisquer duas bases que são associadas geram o mesmo ideal.*

Lema 1.3.4. *[35] **(Lema de Dedekind)** Sejam G um grupo e $\mathbb{K}$ um corpo. Se $\sigma_1, ..., \sigma_n$ são homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então $\{\sigma_1, ..., \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.*

Proposição 1.3.10. *[2] Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\sigma_1, ..., \sigma_n$ os monomorfismos distintos de $\mathbb{K}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{L}$. Se $\{\alpha_1, ..., \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$ então*

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

Exemplo 1.3.17. *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ um corpo de números, $\alpha = (a + b\sqrt{3}) \in \mathbb{K}$ e $[\mathbb{K} : \mathbb{L}] = 2$, existem dois homomorfismos distintos σ_1 e σ_2 tais que $\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$*

e $\sigma_2(a+b\sqrt{3}) = a - b\sqrt{3}$. *Como* $\{1, \sqrt{3}\}$ *é uma base de* $\mathbb{Q}(\sqrt{3})$ *sobre* $\mathbb{Q}$, *segue que*

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(1, \sqrt{3}) = \begin{vmatrix} 1 & 1 \\ \sqrt{3} & \sqrt{3} \end{vmatrix}^2 = (2\sqrt{3})^2 = 12.$$

Assim, o discriminante é linearmente independente.

Proposição 1.3.11. *[4] Se* $\mathbb{K}/\mathbb{L}$ *uma extensão finita de grau* n *tal que* $\mathbb{K} = \mathbb{L}(\alpha)$ *e* $f(x)$ *polinômio minimal de* α *sobre* $\mathbb{L}$, *então*

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(1, \alpha, ..., \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathcal{N}(f'(\alpha)),$$

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

Exemplo 1.3.18. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *corpo de números e* $f(x) = x^2 - 3$ *polinômio minimal de* $\alpha = \sqrt{3}$ *sobre* $\mathbb{Q}$. *Temos que* $f'(\alpha) = 2\sqrt{3}$, *e* $\mathcal{N}(2\sqrt{3}) = (2\sqrt{3})(-2\sqrt{3}) = -12$. *Assim pela Proposição 1.3.11 temos*

$$\mathcal{D}(1, \sqrt{3}) = (-1)^{\frac{2(2-1)}{2}} \mathcal{N}(f'(\alpha)) = (-1)(-12) = 12.$$

Teorema 1.3.7. *[6] O discriminante de qualquer base de* $\mathbb{K} = \mathbb{Q}(\theta)$ *é racional e não nulo. Se todos os* $\mathbb{K}$*-monomorfismos de* θ *são reais, então o discriminante de qualquer base é positivo.*

Definição 1.3.11. *Dizemos que* $n \in \mathbb{Z}$ *é* ***livre de quadrados*** *se, e somente se,* n *não tem divisor, que é quadrado de um número primo.*

Teorema 1.3.8. *[35] Seja um corpo de números de grau* n, $\mathbb{I}_{\mathbb{K}}$ *o anel dos inteiros de* $\mathbb{K}$ *e* $\{\alpha_1, ..., \alpha_n\} \in \mathbb{I}_{\mathbb{K}}$ *uma* $\mathbb{Q}$*-base de* $\mathbb{K}$. *Se* $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\alpha_1, ..., \alpha_n)$ *é livre de quadrados, então* $\{\alpha_1, ..., \alpha_n\}$ *é uma base integral.*

Corolário 1.3.5. *[13] Todo corpo de número possui uma base integral.*

Corolário 1.3.6. *[26] Sejam* $\{\alpha_1, ..., \alpha_n\}$ *e* $\{\beta_1, ..., \beta_n\}$ *duas bases integrais para um corpo de números* $\mathbb{K}$, *então*

$$\mathcal{D}(\alpha_1, ..., \alpha_n) = \mathcal{D}(\beta_1, ..., \beta_n).$$

Exemplo 1.3.19. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{13})$, $\alpha = \left(\frac{1+\sqrt{13}}{2}\right)$ *e* $\beta = \sqrt{13}$ *elementos de* $\mathbb{K}$ *e suas respectivas bases* $B_1 = \left\{1, \frac{1+\sqrt{13}}{2}\right\}$ *e* $B_2 = \left\{1, \sqrt{13}\right\}$ *de* $\mathbb{K}$. *A primeira base é integral e a segunda não é base integral. De fato, sejam os homomorfismos da base* B_2 *de* $\mathbb{K}$ *em* $\mathbb{C}$, $\sigma_1 : \sqrt{13} \mapsto \sqrt{13}$ *e* $\sigma_2 : \sqrt{13} \mapsto -\sqrt{13}$, *e o discriminante*

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{13}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{13}) \\ Tr(\sqrt{13}) & Tr((-\sqrt{13})^2) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 26 \end{vmatrix} = 52.$$

Pelo Teorema 1.3.8, temos que os divisores de 52 são $1, 2, 4, 13, 26$ e 52. Sendo que $4 = 2^2$, logo $\{1, \sqrt{13}\}$ não é integral, pois 52 não é livre de quadrados.
Para a base B_1, temos os homomorfismos $\sigma_1 : \frac{1+\sqrt{13}}{2} \mapsto \frac{1+\sqrt{13}}{2}$ e $\sigma_2 : \frac{1+\sqrt{13}}{2} \mapsto \frac{1-\sqrt{13}}{2}$ e o discriminante

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{13}}{2}\right) = \begin{vmatrix} Tr(1) & Tr\left(\frac{1+\sqrt{13}}{2}\right) \\ Tr\left(\frac{1+\sqrt{13}}{2}\right) & Tr\left(\left(\frac{1+\sqrt{13}}{2}\right)^2\right) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & 7 \end{vmatrix} = 13.$$

Logo, 13 é livre de quadrados, assim a base $\left\{1, \frac{1+\sqrt{13}}{2}\right\}$ é uma base integral.

Observação 1.3.9. *O caso inverso do Teorema 1.3.8 é falso. De fato, $\{1, \sqrt{2}\}$ é uma base integral, mas $\mathcal{D}(1, \sqrt{2}) = 8$ que não é livre de quadrados.*

1.3.5 Corpos quadráticos

Definição 1.3.12. *Um **corpo quadrático** é um corpo de números $\mathbb{K}$ de grau 2 sobre $\mathbb{Q}$. Mais especificamente, $\mathbb{K} = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico e θ é uma raiz de um polinômio do tipo*

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

Proposição 1.3.12. *[12] Os corpos quadráticos são da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados.*

Exemplo 1.3.20. *O corpo $\mathbb{K} = \mathbb{Q}(\sqrt{13})$ é um corpo quadrático, pois $\theta = \sqrt{13}$ é raiz de $f(x) = x^2 - 13$ e 13 é livre de quadrados.*

Observação 1.3.10. *(i) Pela Proposição 1.3.12, temos que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados. Portanto, $\{1, \sqrt{d}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$.*

(ii) Se $\sqrt{d}$ é raiz do polinômio $f(x) = x^2 - d$ sobre $\mathbb{Q}$ existe um automorfismo dado por $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ e $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$. Deste modo

$$Tr(\sigma) = \sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = 2a.$$

$$N(\sigma) = \sigma_1(a + b\sqrt{d}) \cdot \sigma_2(a + b\sqrt{d}) = a^2 - db^2.$$

Proposição 1.3.13. *[40] Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com d livre de quadrados e $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ um inteiro algébrico, então $2a$ e $a^2 - db^2$ são números inteiros.*

Exemplo 1.3.21. *Dado que $\mathbb{K}(\sqrt{5})$ é um corpo quadrático, como 5 livre de quadrados, então os monomorfismo são $\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ e $\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$. Logo $Tr(a + b\sqrt{5}) = 2a$ e $N(a + b\sqrt{5}) = a^2 - 5b^2$, ambos inteiros.*

Definição 1.3.13. *Se $d > 0$, a extensão $\mathbb{Q}(\sqrt{d})$ é dita* ***real*** *e se $d < 0$ a extensão $\mathbb{Q}(\sqrt{d})$ é dita* ***imaginária****.*

O Teorema 1.3.9 a seguir determina o anel dos inteiros algébricos $\mathbb{I}_{\mathbb{K}}$ de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados.

Teorema 1.3.9. *[9] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, tal que $d \equiv 0(mod 4)$.*

(i) Se $d \equiv 2(mod\ 4)$ ou $d \equiv 3(mod\ 4)$, então o anel dos inteiros $\mathbb{I}_{\mathbb{K}}$ de $\mathbb{K}$, consiste em todos os elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$.

(ii) Se $d \equiv 1(mod\ 4)$, então o anel dos inteiros algébricos $\mathbb{I}_{\mathbb{K}}$ de $\mathbb{K}$ consiste em todos os elementos da forma $\dfrac{a + b\sqrt{d}}{2}$, com $a, b \in \mathbb{Z}$ e de mesma paridade.

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com $a, b \in \mathbb{Q}$ inteiro algébrico. Então existe um polinômio $f(x) \in \mathbb{Z}[x], talque f(\alpha) = 0$. Vamos analisar duas situações

(1) Se $b = 0$, então o polinômio minimal de α sobre $\mathbb{Q}$ é dado por $\alpha = x - a$. Como α é inteiro algébrico, segue que $a \in \mathbb{Z}$.

(2) Se $b \neq 0$, então o polinômio minimal de α sobre $\mathbb{Q}$ é de grau 2 e obtido do seguinte modo

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

Logo, o polinômio minimal é $\alpha = x^2 - 2ax + a^2 - b^2 d$. Como α é inteiro algébrico, segue que $2a, a^2 - db^2 \in \mathbb{Z}$. Já que $a^2 - db^2 \in \mathbb{Z}$, então $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e como $2a \in \mathbb{Z}$ segue que $d(2b)^2 \in \mathbb{Z}$. Ainda, $2b \in \mathbb{Z}$, pois caso contrário, $2b$ seria da forma $\dfrac{w}{y}$, com w e y inteiros primos entre si e $y \neq 0$. Como $d(2b)^2 \in \mathbb{Z}$, segue que $d(\dfrac{w}{y})^2 \in \mathbb{Z}$ e, portanto ou $\dfrac{y^2}{w^2}$ ou $\dfrac{y^2}{d}$. O primeiro caso é impossível, pois $y \nmid w$. Logo, $y^2 \mid d$ e assim $d = y^2 \cdot k$, k inteiro, o que também é absurdo, pois d é livre de quadrados por hipótese. Portanto, $2b \in \mathbb{Z}$. Concluímos que se $\alpha = \{a + b\sqrt{d}; a, b \in \mathbb{Q}\}$ é algébrico, então $2a$ e $2b$ são números inteiros e podemos escrever

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

Temos também que $(2a)^2 - d(2b)^2 \in 4\mathbb{Z}$, pois $(2a)^2 - d(2b)^2 = 4a^2 - 4db^2 = 4(a^2 - db^2) \in \mathbb{Z}$. Substituindo por $\dfrac{u}{2}$ e b por $\dfrac{v}{2}$, segue que $u^2 - dv^2 \in \mathbb{Z}$. Então $4 \mid (u^2 - dv^2)$ ou equivalentemente,

$$u^2 - dv^2 \equiv 0\ (mod\ 4). \tag{1.1}$$

Agora vamos determinar em quais condições a Equivalência 1.1 é válida

(I) Se u e v são ímpares, então $\forall\ k_1, k_2 \in \mathbb{Z}$, temos

$$u^2 - dv^2 = (2k_1 + 1)^2 - d(2k_2 + 1)^2 = 4(k_1^2 + k_1 - dk_2^2 - dk_2) + 1 - d \in 4\mathbb{Z} \Leftrightarrow 4 \mid (1 - d).$$

A Equivalência 1.1 é válida se, e somente se, $d \equiv 1\ (mod\ 4)$.

(II) Se u e v são pares, então $\forall\ k_1, k_2 \in \mathbb{Z}$, temos

$$u^2 - dv^2 = (2k_1)^2 - d(2k_2)^2 = 4(k_1^2 - dk_2^2) \in \mathbb{Z}.$$

Nesse caso a Equivalência 1.1 é válida se, e somente se, $d \equiv 2\ (mod\ 4)$ ou $d \equiv 3\ (mod\ 4)$.

(III) Se u ímpar e v par, então $\forall\ k_1, k_2 \in \mathbb{Z}$, temos

$$u^2 - dv^2 = (2k_1 + 1)^2 - d(2k_2)^2 = 4(k_1^2 + k_1 - dk_2^2) + 1 \notin 4\mathbb{Z}.$$

Nesse caso a Equivalência 1.1 não é válida.

(IV) Se u par e v ímpar, então $\forall\ k_1, k_2 \in \mathbb{Z}$, temos

$$u^2 - dv^2 = (2k_1)^2 - d(2k_2 + 1)^2 = 4(k_1^2 - dk_2^2 - dk_2) - d \notin \mathbb{Z}.$$

Do item (I) concluímos que se $d \equiv 1\ (mod\ 4)$, os elementos do anel $\mathbb{I}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ são da forma $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$, isto é,

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

Já que u e v são ímpares, então $u - v$ é par e $\dfrac{u - v}{2}$ e $v \in \mathbb{Z}$. Portanto $\mathbb{I}_{\mathbb{K}} \in \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$.

Por outro lado, se $\alpha = a + b\left(\dfrac{1 + \sqrt{d}}{2}\right) \in \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$, com $a, b \in \mathbb{Z}$, então

$$2a + b \in \mathbb{Z} \quad e \quad \left(\frac{a + b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = \frac{a^2 + ab + (1 - d)b^2}{4} \in \mathbb{Z},$$

pois, $d \equiv 1\ (mod\ 4)$. Logo, $\mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right] \subset \mathbb{I}_{\mathbb{K}}$, pois os coeficientes do polinômio $x^2 - (2a + b)x + a^2 + ab + \dfrac{(1 - d)b^2}{4}$, estão em $\mathbb{Z}$. Portanto, $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$.

Do item (ii) concluimos que se $d \equiv 2$ ou $3(mod\ 4)$, o anel $\mathbb{I}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ é da forma $\alpha = a + b\sqrt{d}, a, b \in \mathbb{Z}$. Sendo assim, $\alpha \in \mathbb{Z}[\sqrt{d}]$ e então $\mathbb{I}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}$. Por outro lado, todo $\alpha \in \mathbb{Z}[\sqrt{d}]$ é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois $2a, a^2 - db^2 \in \mathbb{Z}$. Logo $\mathbb{Z}[\sqrt{d}] \subset \mathbb{I}_{\mathbb{K}}$. Portanto, $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$. ■

Observação 1.3.11. *Podemos verificar do Teorema 1.3.9, que* $\{1, \sqrt{d}\}$ *e* $\left\{1, \dfrac{1 + \sqrt{d}}{2}\right\}$ *são bases integrais do corpo quadrático* $\mathbb{K}$ *sobre* $\mathbb{Q}$.

Exemplo 1.3.22. *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ *o corpo quadrático. O anel dos inteiros algébricos de* $\mathbb{K}$ *é dado por* $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$, *onde* $i = \sqrt{-1}$, *pois* $d = -1 \equiv 3(mod\ 4)$. *Por outro lado, o anel dos inteiros algébricos do corpo quadrático* $\mathbb{Q}(\sqrt{-3})$ *é* $\mathbb{Z}\left[\dfrac{1 + \sqrt{-3}}{2}\right]$, *pois* $d = -3 \equiv 1(mod\ 4)$.

A próxima Proposição 1.3.14 determina o discriminante de corpos quadráticos.

Proposição 1.3.14. *[9] Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, onde d é um inteiro livre de quadrados, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

(i) $\mathcal{D}_{\mathbb{K}} = d$, se $d \equiv 1 (mod\ 4)$.

(ii) $\mathcal{D}_{\mathbb{K}} = 4d$, se $d \equiv 2 (mod\ 4)$ ou $d \equiv 3 (mod\ 4)$.

Demonstração: Sejam σ_1 e σ_2 os monomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com $d \in \mathbb{Z}$ livre de quadrados em $\mathbb{C}$, definimos por $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$.

(i) Se $d \equiv 1\ (mod\ 4)$, então

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

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

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

■

Exemplo 1.3.23. *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ um corpo quadrático com discriminante de $\mathbb{K}$ igual a $\mathcal{D}_{\mathbb{K}} = 5$, pois $5 \equiv 1 (mod\ 4)$. De fato, pelo Teorema 1.3.9 temos que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, onde $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathbb{I}_{\mathbb{K}}$ e os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são: $\sigma_1 : \frac{1+\sqrt{5}}{2} \mapsto \frac{1+\sqrt{5}}{2}$ e $\sigma_2 : \frac{1+\sqrt{5}}{2} \mapsto \frac{1-\sqrt{5}}{2}$ e o discriminante é dado por*

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{5} & \frac{1-\sqrt{5}}{5} \end{vmatrix}^2 = (\sqrt{5})^2 = 5,$$

que é livre de quadrados, observe que as hipóteses da Proposição 1.3.14 são satisfeitas.

1.3.6 Corpos ciclotômicos

Definição 1.3.14. *Seja n um inteiro positivo. Dizemos que ζ_n é uma raiz n-ésima primitiva da unidade se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$, para todo $1 \leqslant m \leqslant n-1$. Um **corpo ciclotômico** é um corpo da forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade.*

Observação 1.3.12. *(i) Pela Definição 1.3.14, temos que as raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$.*

(ii) O número de raízes n-ésimas primitivas da unidade é dada por

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

onde φ é a função de Euler.

Definição 1.3.15. *Seja n um inteiro positivo. Dizemos que* $\Phi_n(x) = \prod_{j=1, mdc(j,1)=1}^{n} (x - \zeta_n^j)$ *é chamado de* ***polinômio ciclotômico****.*

Proposição 1.3.15. *[22] Se n é um inteiro positivo, então* $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Corolário 1.3.7. *[22] Se m e n são primos entre si, então* $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

Exemplo 1.3.24. *Seja $f(x) = x^4 - 1$. As raízes de $f(x)$ são $1, \zeta_4, \zeta_4^2$ e ζ_4^3 que possuem períodos 1, 4, 2 e 4, respectivamente. Assim*

$$\begin{aligned} \Phi_1(x) &= x - 1 \\ \Phi_2(x) &= x - \zeta_4^2 = (x+1) \\ \Phi_4(x) &= (x - \zeta_4)(x - \zeta_4^3) = (x^2 + 1), \end{aligned}$$

como os divisores de 4 são $1, 2$, e 4 temos que

$$x^4 - 1 = \prod_{d|n} \Phi_d(x) = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) = (x-1)(x - \zeta_4^2)(x - \zeta_4)(x - \zeta_4^3).$$

Corolário 1.3.8. *[32] Se n é um inteiro positivo, então*

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

Observação 1.3.13. *O Corolário 1.3.8 permite calcular, por recorrência, cada polinômio ciclotômico.*

Proposição 1.3.16. *[32] O n-ésimo polinômio ciclotômico $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Exemplo 1.3.25. *Seja $\Phi_1(x) = x - 1$, pelo Corolário 1.3.8 calculamos os seguintes polinômios ciclotômicos,*

$$\begin{aligned} \Phi_1(x) &= x - 1, \quad \Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1, \\ \Phi_3(x) &= \frac{x^3 - 1}{x - 1} = x^2 + x + 1, \quad \Phi_4(x) = \frac{x^4 - 1}{(x+1)(x-1)} = x^2 + 1, \end{aligned}$$

e assim por diante.

Teorema 1.3.10. *[11] Se n é um inteiro positivo, ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ corpo ciclotômico correspondente, então $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler.*

Demonstração: É claro que $\Phi_n(x)$ é mônico e tem grau $\varphi(n)$. Devemos mostrar que os coeficientes estão em $\mathbb{Z}[x]$. Usamos indução em n. O resultado é verdadeiro para $n = 1$. Assumo por indução que $\Phi_d \in \mathbb{Z}[x]$, para todo $1 \leqslant d < n$. Então, $x^n - 1 = f(x)\Phi_n(x)$, onde $f(x) = \prod_{d|n, d<n} \Phi_d(x)$ é mônico e os coeficientes estão em $\mathbb{Z}[x]$. Desde que $f(x)$ divide $x^n - 1$ em $F[x]$, onde $F[x] = \mathbb{Q}(\zeta_n)$ é o corpo de raízes n-ésimas da unidade e ambos $f(x)$ e $x^n - 1$ tem coeficientes em $\mathbb{Q}$, $f(x)$ divide $x^n - 1$ em $\mathbb{Q}[x]$, pelo algoritmo da divisão, ver [30]. Pelo lema de Gauss, ver [4], temos que $f(x)$ divide $x^n - 1$ em $\mathbb{Z}[x]$, então $\Phi_d(x) \in \mathbb{Z}[x]$. Agora devemos mostrar que $\Phi_n(x)$ é irredutível. Se não, temos uma fatoração $\Phi_n(x) = f(x)g(x)$ com $f(x), g(x) \in \mathbb{Z}[x]$ mônicos, onde $f(x)$ com fator irredutível de $\Phi_n(x)$. Seja ζ uma raiz n-ésima primitiva da unidade que é uma raiz de $f(x)$, então $f(x)$ é polinômio mônico de ζ sobre $\mathbb{Q}$, e denotamos p um número primo que não divide n. Então ζ^p é novamente uma raiz primitiva da unidade e portanto é uma raiz de $f(x)$ ou $g(x)$. Supondo que $g(\zeta^p = 0)$, então ζ é uma raiz de $g(\zeta^p)$ e como $f(x)$ é polinômio mínimo para ζ, $f(x)$ deve dividir $g(x^p)$ em $\mathbb{Z}[x]$, digamos $g(x^p) = f(x)h(x), h(x) \in \mathbb{Z}[x]$. Se reduzimos esta em $(mod\ p)$, obtemos, $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$, em $F_p[x]$, onde $\overline{g}(x^p) = (\overline{g}(x))^p$, então teremos a seguinte: $(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x)$, que é um domínio de fatoração única (DFU) em $F_p[x]$. Segue que $\overline{f}(x)$ e $\overline{g}(x)$ tem fator comum em $F_p[x]$. Agora reduzindo $\Phi_n(x) = f(x)g(x)$ em $(mod\ p)$, temos $\overline{\Phi_n}(x) = \overline{f}(x)\overline{g}(x)$ segue que $\overline{\Phi_n}(x) \in F_p[x]$, tem uma raiz múltipla. Então $x^n - 1$ teria uma raiz múltipla sobre F_p, uma vez que tem $\overline{\Phi_n}(x)$ como fator, isto é uma contradição, visto que existem n raízes distintas de $x^n - 1$ sobre qualquer corpo de característica p que não divide n. Logo ζ_p deve ser uma raiz de $f(x)$ uma vez que isso se aplica a toda raiz de $f(x)$. Segue que ζ^a é uma raiz de $f(x)$ para todo a primo com n: $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, produtos de primos que não divide n. Então, ζ_1^p, ζ_2^p, etc são raízes de $f(x)$. Mas isso significa que cada raiz n-ésima primitiva da unidade é uma raiz de $f(x)$, isto é, $f(x) = \Phi_n(x)$, mostrando que $\Phi_n(x)$ é irredutível.

Logo, $\partial(f(x)) \geqslant \partial(\Phi_n(x)$, pois toda raiz de $f(x)$ é raiz de $\Phi_n(x)$, e como $f(x) \mid \Phi_n(x)$, segue que $\partial(\Phi_n(x) \geqslant \partial(f(x))$, portanto $\partial(\Phi_n(x)) = \partial(f(x)) = \varphi(n)$. ■

Exemplo 1.3.26. *Seja o corpo ciclotômico $\mathbb{Q}(\zeta_4)$ que tem duas raízes primitivas quartas da unidade $\{i, -i\}$ estas geram todas as raízes de $x^4 - 1$, isto é, $\{i^m; m \in \mathbb{Z}\} = \{1, i, i^2 = -1, i^3 = -i\}$ e $\{-i^m; m \in \mathbb{Z}\} = \{1, -i, (-i)^2 = -1, (-i)^3 = i\}$. Portanto, o grau de $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = \varphi(4) = 2$. Por outro lado, -1 é a única raiz primitiva quadrada da unidade de $x^2 - 1$, isto é, gera todas as raízes. Portando, $[\mathbb{Q}(\zeta_2) : \mathbb{Q}] = \varphi(2) = 1$.*

Uma aplicação direta do Teorema 1.3.10, seja $\mathbb{K} = \mathbb{Q}(\zeta_{12})$ corpo ciclotômico, temos que $[\mathbb{Q}(\zeta_{12}) : \mathbb{Q}] = \varphi(12) = 4$.

Proposição 1.3.17. *[4] Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico, onde ζ_n é uma raiz n-ésima primitiva da unidade. Se $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo*

maximal real de $\mathbb{K}$*, então* $[\mathbb{K} : \mathbb{L}] = 2$.

Demonstração: Como ζ_n não é real, então o polinômio $p(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ é irredutível em $\mathbb{L}$ e tem como raiz ζ_n. Logo, $p(x)$ é um polinômio minimal de ζ_n sobre $\mathbb{L}$. Desta forma $[\mathbb{K} : \mathbb{L}] = \partial(p) = 2$. ■

Observação 1.3.14. *Se* ζ_n *é uma raiz n-ésima primitiva da unidade, então* $(\zeta_n + \zeta_n^{-1})$ *é um número real. De fato,* ζ_n^{-1} *é o conjugado complexo de* $\zeta_n \in \mathbb{C}$*, então* $(\zeta_n + \zeta_n^1)$ *é igual a duas vezes a parte real de* ζ_n*. Portanto,* $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *está contido nos* $\mathbb{R}$.

Proposição 1.3.18. *[6] Os homomorfismos de* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{C}$ *são dados por*

$$\sigma_i; mdc(i, n) = 1 \quad e \quad \sigma_i = (\zeta) = \zeta^i, \quad onde \quad i = 1, ..., n-1.$$

Definição 1.3.16. *Nas condições da Proposição 1.3.17, o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *é chamado* ***subcorpo maximal real*** *de* $\mathbb{Q}(\zeta_n)$.

Definição 1.3.17. *Todo subcorpo do corpo ciclotômico* $\mathbb{Q}(\zeta_n)$ *será chamado* ***subcorpo ciclotômico****.*

Corolário 1.3.9. *[32] Se* ζ_n *é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \dfrac{\varphi(n)}{2}$*, onde* φ *é a função de Euler.*

Exemplo 1.3.27. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$ *subcorpo maximal real de* $L = \mathbb{Q}(\zeta_{12})$ *e* $[\mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1}) : \mathbb{Q}] = \dfrac{\varphi(12)}{2} = 2$*. De fato, pelo Corolário 1.3.9.*

Teorema 1.3.11. *[43] Se n é um inteiro positivo,* ζ_n *é uma raiz n-ésima primitiva da unidade e* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *o corpo ciclotômico correspondente, então o anel* $\mathbb{I}_\mathbb{K}$ *dos inteiros algébricos de* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *é* $\mathbb{Z}[\zeta_n]$ *e* $\{1, \zeta_n, \zeta_n^2, ..., \zeta_n^{\varphi(n)-1}\}$ *é uma base integral.*

Teorema 1.3.12. *[43] Se n é um inteiro,* ζ_n *uma raiz n-ésima primitiva da unidade e* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *o corpo ciclotômico correspondente, então* $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *é o subcorpo maximal real de* $\mathbb{K}$*,* $\mathbb{I}_\mathbb{L} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ *é o seu anel dos inteiros e* $\{1, \zeta_n + \zeta_n^{-1}, ..., \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-(\frac{\varphi(n)}{2}-1)}\}$ *uma base integral do subcorpo* $\mathbb{L}$.

Proposição 1.3.19. *[2] Seja* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *é um corpo ciclotômico, onde* ζ_p *é uma raiz p-ésima da unidade e p é um número primo ímpar, então o discriminante de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é dado por*

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

Exemplo 1.3.28. *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_5)$ *corpo ciclotômico e* $p = 5$ *primo ímpar, então o discriminante de* $\mathbb{K}$ *é* $\mathcal{D}_\mathbb{K} = (-1)^{\frac{(5-1)\cdot(5-2)}{2}} \cdot 5^(5-2) = (-1)^6 \cdot 125 = 125$.

Proposição 1.3.20. *[29] Seja $\mathbb{K} = \mathbb{Q}(\zeta_p)$ um corpo ciclotômico, e ζ_p é uma raiz p-ésima da unidade e p é um número primo. Se $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ é um subcorpo maximal real de $\mathbb{K}$, então o discriminante de $\mathbb{L}$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{L}} = p^{\frac{p-3}{2}}.$$

Proposição 1.3.21. *[37] Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ um corpo ciclotômico, e ζ_{p^r} é uma raiz p^r-ésima primitiva da unidade, o p é número primo e r um inteiro maior que 1, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, ..., \zeta_{p^r}^{\varphi(p^r)-1}) = \pm p^{p^{r-1}\cdot(r(p-1)-1)}.$$

Exemplo 1.3.29. *Dado $\mathbb{K} = \mathbb{Q}(\zeta_8)$ corpo ciclotômico e do discriminante de $\mathbb{K}$ é $\mathcal{D}_{\mathbb{K}} = 256$. De fato, $\zeta_8 = \zeta_{2^3}$, onde $p = 2$ e $r = 3$, então $\mathcal{D} = \pm 2^{2^{3-1}\cdot(3(2-1)-1)} = \pm 256$.*

Proposição 1.3.22. *[6] Seja $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, e r é um número inteiro positivo. Se $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ o subcorpo maximal real de $\mathbb{K}$, então o discriminante de $\mathbb{L}$ é dado por*

$$|\mathcal{D}_{\mathbb{L}}| = 2^{(r-1)n-1}.$$

Teorema 1.3.13. *[43] Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. O discriminante do corpo $\mathbb{K} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

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

Exemplo 1.3.30. *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_8)$ um corpo ciclotômico, seu discriminante $\mathcal{D}_{\mathbb{K}} = 256$ e $\varphi(8) = 4$. De fato, pelo Teorema 1.3.13 temos $\mathcal{D}_{\mathbb{K}} = (-1)^4 \dfrac{8^4}{2^4} = 256$.*

Observação 1.3.15. *Para calcular o discriminante de um subcorpo maximal real $\mathbb{K} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$ de $\mathbb{L} = \mathbb{Q}(\zeta_{12})$, aplicamos o Corolário 1.3.9, onde $\dfrac{\varphi(n)}{2} = 2$ e agora usamos o Teorema 1.3.13, temos*

$$\mathcal{D}_{\mathbb{K}} = (-1)^2 \frac{12^2}{2^2 \cdot 3^1} = 12.$$

Capítulo 2

Reticulados

Neste capítulo apresentamos um estudo sobre reticulados. Na Seção 2.1 definimos reticulados e apresentamos suas principais propriedades. Na Seção 2.2 apresentamos os conceitos de matriz geradora, matriz de Gram e determinante de um reticulado. Na Seção 2.3 os conceitos de empacotamento esférico, densidade de empacotamento, densidade de centro e $k$issing number são apresentados. E, na Seção 2.4 mostramos famílias de reticulados conhecidas na literatura e suas propriedades mais importantes. As principais referências utilizadas neste capítulo foram [2], [5], [6], [7], [8], [12], [14], [18], [17], [19], [20], [21], [24], [33], [35], [38] e [42].

2.1 Definição de reticulado

Veremos nesta seção a definição de reticulado no $\mathbb{R}^n$ e algumas de suas propriedades como a região fundamental, bem como apresentamos alguns exemplos.

Definição 2.1.1. *Seja $\beta = \{v_1, ..., v_m\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente independente sobre $\mathbb{R}$, chamamos de **reticulado** Λ o conjunto de todas as combinações lineares inteiras de v_i, ou seja,*

$$\Lambda = \{x \in \mathbb{R}^n; x = \sum_{i=1}^{m} a_i v_i, a_i \in \mathbb{Z}\},$$

e o conjunto $\beta = \{v_i, ..., v_m\}$ é uma base do reticulado Λ.

Exemplo 2.1.1. *Em $\mathbb{R}^2$, considere o reticulado $\Lambda = \{a(1,0) + b(0,1) : a, b \in \mathbb{Z}\}$ cuja base é a base canônica $\beta = \{(1,0),(0,1)\}$. Este reticulado é o reticulado $\Lambda = \mathbb{Z}^2$ e pode ser representado geometricamente na Figura 1.*

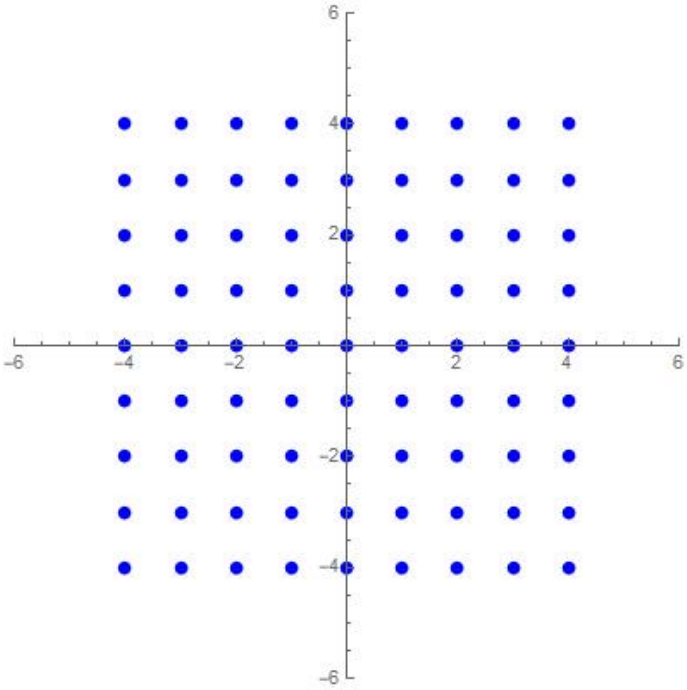


Figura 1 – Reticulado $\Lambda = \mathbb{Z}^2$.
Fonte: Autor.

Observação 2.1.1. *Note que um reticulado pode ter mais do que uma base. De fato,* $\beta_1 = \{(1,2),(3,5)\}$ *também é uma base para o reticulado* $\Lambda = \mathbb{Z}^2$*,*

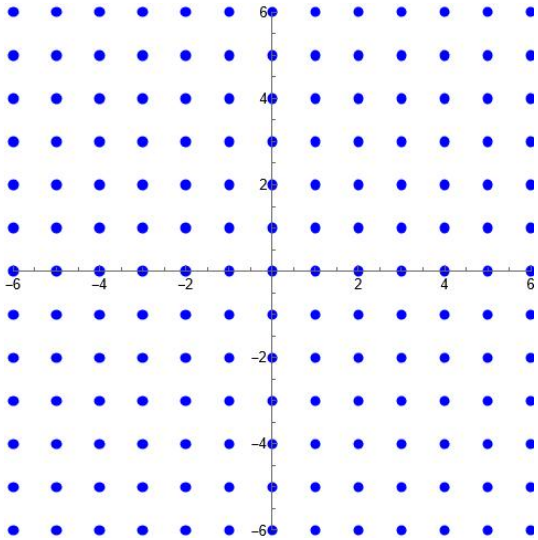


Figura 2 – Outra base para o reticulado $\Lambda = \mathbb{Z}^2$.
Fonte: Autor.

Observação 2.1.2. *Dado um reticulado* Λ *no* $\mathbb{R}^n$ *gerado por uma base* β *temos que uma condição necessária e suficiente para que um outro conjunto de vetores linearmente independentes* β' *de* $\mathbb{R}^n$ *também seja uma base deste reticulado é* β' *estar contida em* Λ *e a matriz de mudança de base de* β *para* β' *ter entradas inteiras e determinantes* ± 1*.*

Definição 2.1.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, com base $\beta = \{v_1, ..., v_n\}$. O conjunto*

$$\mathcal{P}_\beta = \{x \in \mathbb{R}^n : x = \sum_{i=1}^{n} \lambda_i v_i, 0 \leqslant \lambda_i < 1\},$$

é chamado de ***região fundamental*** *de Λ com relação à base β.*

Exemplo 2.1.2. *No Exemplo 2.1.1, o quadrado de vértices $\{(0,0),(0,1),(1,0),(1,1)\}$, hachurado abaixo, é a região fundamental do reticulado $\Lambda = \mathbb{Z}^2$,*

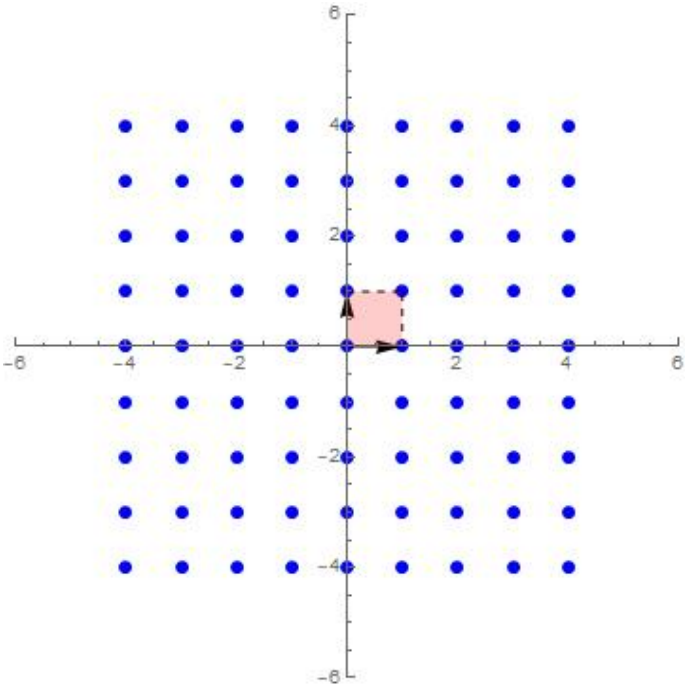


Figura 3 – Região fundamental do reticulado $\Lambda = \mathbb{Z}^2$.
Fonte: Autor.

Exemplo 2.1.3. *Neste exemplo apresentamos um reticulado muito importante na dimensão 2 conhecido como reticulado hexagonal, o qual iremos denotar por Λ_H. O conjunto de vetores $\beta = \left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$ forma uma base para o reticulado Λ_H. Este reticulado, assim como sua região fundamental, é apresentado na Figura 4.*

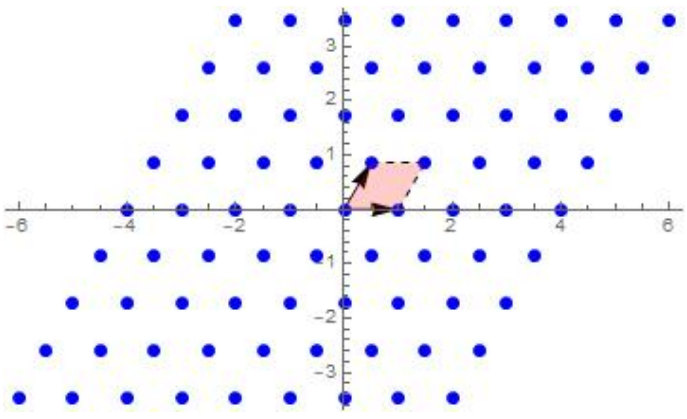


Figura 4 – Região fundamental do reticulado hexagonal.
Fonte: Autor.

A proposição a seguir nos diz que podemos obter outras regiões fundamentais por translações de $\mathcal{P}_\beta$.

Proposição 2.1.1. *[6] Cada elemento do $\mathbb{R}^n$ pertencem a exatamente um dos conjuntos $\mathcal{P}_\beta + l$, para todos $l \in \Lambda$.*

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

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

Mas podemos separar a parte inteira de cada coeficiente a_i, ou seja, $a_i = \alpha_i + \theta_i$, onde $\alpha_i \in \mathbb{Z}, 0 \leqslant \theta_i < 1$ e $\theta_i \in \mathbb{R}^n$, para $i = 1, ..., n$. Assim, podemos reescrever x da seguinte maneira

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

Portanto, $x \in \mathcal{P}_\beta + l$. Para unicidade, suponhamos que x pertença simultaneamente a $\mathcal{P}_\beta + l_1$ e $\mathcal{P}_\beta + l_2$, onde $l_1, l_2 \in \Lambda$, ou seja,

$$\begin{aligned} x &= \sum_{i=1}^{n} \theta_i e_i + \sum_{i=1}^{n} \alpha_i e_i, \quad com \quad \alpha_i \in \mathbb{Z}, 0 \leqslant \Theta_i < 1 \quad e \quad \theta_i \in \mathbb{R}^n, \quad para \quad i = 1, ..., n. \\ x &= \sum_{i=1}^{n} \gamma_i e_i + \sum_{i=1}^{n} \delta_i e_i, \quad com \quad \delta_i \in \mathbb{Z}, 0 \leqslant \gamma_i < 1 \quad e \quad \theta_i \in \mathbb{R}^n, \quad para \quad i = 1, ..., n, \end{aligned}$$

onde a primeira parcela das equações pertence a Λ e a segunda parcela são l_1 e l_2, respectivamente igualando, obtemos

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

Assim,

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

Como $\{e_i, ..., e_n\}$ é linearmente independente, segue que $(\theta_i + \alpha_i - \gamma_i \delta_i) = 0$, para $i = 1, ..., n$ e assim

$$\theta_i - \gamma_i = \delta_i - \alpha_i.$$

Como $0 \leqslant \theta_i, \gamma_i < 1$, segue que $-1 < \theta_i - \gamma_i < 1$. Mas, pela igualdade acima, e pelo fato de que $\delta_i - \alpha_i \in \mathbb{Z}$, concluímos que $\delta_i = \alpha_i$, para $i = 1, ..., n$. Assim, $l_1 = l_2$, portanto x pertence a exatamente a um dos conjuntos $\mathcal{P}_\beta + l$ com $l \in \Lambda$. ■

Exemplo 2.1.4. *A região fundamental $\mathcal{P}_\beta$ do reticulado $\Lambda = \mathbb{Z}^2$ e uma translação $\mathcal{P}_\beta + l$ são descritas na Figura 5.*

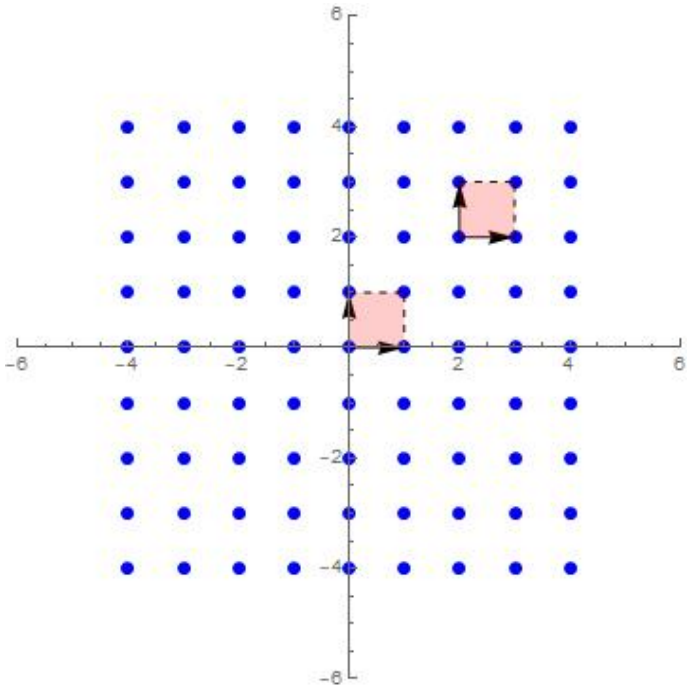


Figura 5 – Translação da região fundamental do reticulado $\Lambda = \mathbb{Z}^2$.
Fonte: Autor.

Observação 2.1.3. *A união disjunta de $\mathcal{P}_\beta$ por pontos do Λ ladrilha o $\mathbb{R}^n$. Qualquer região que satisfaça as propriedades (i) e (ii) é chamada de região fundamental de Λ*

(i) Se $x, y \in \Lambda, x \neq y$, então $(x + \mathcal{P}_\beta) \cap (y + \mathcal{P}_\beta = \varnothing)$.

(ii) $\bigcup_{x\in\Lambda}(x + \mathcal{P}_\beta) = \mathbb{R}^n$.

Definição 2.1.3. *Um subgrupo H do $\mathbb{R}^n$ é* ***discreto*** *se, para qualquer subconjunto compacto K do $\mathbb{R}^n$, tivemos $H \cap K$ finito.*

Teorema 2.1.1. *[35] Se Λ é subgrupo discreto do $\mathbb{R}^n$, então Λ é gerado como $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}^n$, com $r \leqslant n$.*

Demonstração: Seja $\beta = \{e_1, ..., e_r\}$ um conjunto de vetores de Λ que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível com $r \leqslant n$. Seja o paralelepípedo $\mathcal{P}_\beta = \{x \in \mathbb{R}^n : x = \sum_{i=1}^{r} \alpha_i e_i, 0 \leqslant \alpha_i \leqslant 1\}$ construído a partir destes vetores. Como $\mathcal{P}_\beta$ é fechado e limitado segue que $\mathcal{P}_\beta$ é compacto. Assim, $\mathcal{P}_\beta \cup \Lambda$ é finito, pois Λ é discreto. Se $x \in \Lambda$ então pela maximalidade de r, segue que $\{x, e_1, ..., e_r\}$ é linearmente independente. Logo exitem $\lambda_i \in \mathbb{R}, i = 1, ..., n$, não todos nulos, tal que $x = \sum_{i=1}^{r} \lambda_i e_i$. Para cada $j \in \mathbb{N}$, seja

$$x = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \in \Lambda, \tag{2.1}$$

onde $\lceil k \rceil$ denota o maior inteiro menor ou igual a k. Assim,

$$x_j = j\sum_{i=1}^{r}\lambda_i e_i - \sum_{i=1}^{r}\lceil j\lambda_i\rceil e_i = \sum_{i=1}^{r}(j\lambda_i - \lceil j\lambda_i\rceil)e_i \in \mathcal{P}_\beta \cup \Lambda.$$

Dessa forma, se tomarmos $j = 1$ na 2.1, temos $x_1 = x - \sum_{i=1}^{r}\lceil\lambda_i\rceil e_i$, ou seja, $x = x_1 + \sum_{i=1}^{r}\lceil\lambda_i\rceil e_i$. Assim, como $x_1 \in \mathcal{P}_\beta \cup \Lambda$ e este é finito, segue que Λ é finitamente gerado como $\mathbb{Z}$-módulo. Por outro lado, do fato de $\mathcal{P}_\beta \cup \Lambda$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros j e k, tais que $x_j = x_k$. Da 2.1 segue que, $x_j = x_k \Rightarrow jx - \sum_{i=1}^{r}\lceil j\lambda_i\rceil e_i = kx - \sum_{i=1}^{r}\lceil k\lambda_i\rceil e_i \Rightarrow (j-k)x = \sum_{i=1}^{r}(\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil)e_i \Rightarrow (j-k)\sum_{i=1}^{r}\lambda_i e_i = \sum_{i=1}^{r}(\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil)e_i \Rightarrow (j-k)\lambda_i = \lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil \Rightarrow \lambda_i = \dfrac{\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil}{j-k}$, ou seja, $\lambda_i \in \mathbb{Q}$. Assim, Λ é gerado como $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $e_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideramos o conjunto $d\Lambda$. Temos que $d\Lambda \subset \sum_{i=1}^{r}\mathbb{Z}e_i$. Como $\mathbb{Z}$ é principal, segue que existe uma base $\{f_1, ..., f_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r}\mathbb{Z}$ e inteiros α_i, tal que $\{\alpha_1 f_1, ..., \alpha_2 f_2\}$ gera $d\Lambda$ sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo $d\Lambda$ tem o mesmo posto de Λ e como $\sum_{i=1}^{r}\mathbb{Z}e_i \subset \Lambda$, segue que o posto de $d\Lambda \geqslant r$. Pela maximalidade de r decorre que o posto de $d\Lambda$ é r e os $\alpha_i's$ são não nulos, pois caso contrário $d\Lambda$ não teria posto r. Assim, $f_i's$ são linearmente independentes sobre $\mathbb{R}$, uma vez que $\{e_1, ..., e_r\}$ é linearmente independente sobre $\mathbb{R}$. Portando $d\Lambda$ é gerado por r vetores linearmente independentes sobre $\mathbb{R}$ e consequentemente Λ também é gerado por r vetores linearmente independentes sobre $\mathbb{R}$. ■

Observação 2.1.4. *Segue do Teorema 2.1 que todo conjunto discreto do $\mathbb{R}^n$ é um reticulado.*

Exemplo 2.1.5. *O conjunto $\mathbb{Z}^n$ é um subgrupo discreto de $\mathbb{R}^n$. De fato, $\mathbb{Z}$ é infinito e todos os seus pontos são isolados, isto é, não possuem pontos de acumulação, ver [24].*

Em [20] encontra-se uma condição necessária e suficiente para que o conjunto de pontos seja classificado como reticulado, enunciamos o teorema abaixo cuja demonstração pode ser vista nesta mesma referência.

Teorema 2.1.2. *[20] Dado um subconjunto do $\mathbb{R}^n$ este será um reticulado se, e somente se, for um subgrupo aditivo discreto.*

Observação 2.1.5. *Um subgrupo aditivo de $\mathbb{R}^n$ é discreto se sua interseção com qualquer subconjunto limitado em $\mathbb{R}^n$ é finita. Um reticulado Λ é um subgrupo aditivo discreto*

de $\mathbb{R}^n$, ou equivalentemente, os centros do empacotamento esférico Λ formam um grupo aditivo sob adição de vetores.

2.2 Matriz geradora, matriz de Gram e determinante de um reticulado

Nesta seção apresentaremos os conceitos de matriz geradora, volume da região fundamental, volume do reticulado, matriz de Gram e determinante de um reticulado.

Definição 2.2.1. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\beta = \{v_1, ..., v_n\}$ uma $\mathbb{Z}$-base. A **matriz geradora** de Λ é definida como*

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

onde $v_i = (v_{i1}, ..., v_{in})$, para $i = 1, \cdots, n$.

Definição 2.2.2. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \cdots, v_n\}$ uma $\mathbb{Z}$-base de Λ e $\mathcal{P}_\beta$ uma região fundamental. Definimos o **volume da região fundamental** $\mathcal{P}_\beta$, como o módulo do determinante da matriz geradora M, isto é,*

$$vol(\mathcal{P}_\beta) = \left| det \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix} \right|.$$

Proposição 2.2.1. *[5] O volume de qualquer região fundamental do reticulado Λ é o mesmo.*

Observação 2.2.1. *O módulo do determinante de qualquer matriz geradora de Λ é sempre o mesmo, independente da base β de $\mathcal{P}_\beta$.*

Definição 2.2.3. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\beta = \{v_1, \cdots, v_n\}$ uma $\mathbb{Z}$-base. Definimos o **volume do reticulado** Λ como*

$$vol(\Lambda) = vol(\mathcal{P}_\beta).$$

Observação 2.2.2. *Observe que se β' for outra base para Λ, segue que $vol(\Lambda) = vol(\Lambda')$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma faz sentido definir $vol(\Lambda) = vol(\mathcal{P}_\beta)$.*

Exemplo 2.2.1. *Seja $\beta = \{(1,1,1),(1,2,3),(2,-1,1)\}$ um conjunto linearmente independente e considere o reticulado Λ gerado por β. Uma matriz geradora de Λ é dada por*

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & -1 & 1 \end{pmatrix}.$$

O volume da região fundamental $\mathcal{P}_\beta$ de Λ e como consequência o volume do reticulado Λ é dado por

$$vol(\Lambda) = vol(\mathcal{P}_\beta) = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & -1 & 1 \end{vmatrix} = 5.$$

Definição 2.2.4. *Sejam Λ um reticulado e M sua matriz geradora. Definimos a* ***matriz de Gram*** *de Λ por*

$$G = M \cdot M^t.$$

Observação 2.2.3. *(i) A matriz de Gram é simétrica.*

(ii) A matriz de Gram muda dependendo da base escolhida.

(iii) O determinante das matrizes de Gram de um reticulado Λ é o mesmo e esse só depende do reticulado.

Proposição 2.2.2. *[42] Sejam $\beta = \{v_1,...,v_n\}, \beta' = \{u_1,...,u_n\} \subset \mathbb{R}^n$ duas bases de um reticulado Λ. Se $G = M \cdot M^t$ e $G' = M \cdot M'^t$, onde $M = (v_{ij})$ e $M' = (u_{ij})$, então $det(G) = det(G')$.*

Demonstração: Considere $\beta = \{v_1,...,v_n\}$ e $\beta' = \{u_1,...,u_n\}$ bases de Λ, podemos escrever $u_i = \sum_{j=1}^{n} a_{ij}v_j$, para $i = 1,...,n$ e $a_{ij} \in \mathbb{Z}$. Sejam M e M' as matrizes associadas as bases β e β' respectivamente. Como $|det(M)| = |det(M')|$, segue que

$$det(G) = det(M)\cdot det(M^t) = det(M')^2 = det(M)^2 = det(M')\cdot det(M'^t) = det(G'). \blacksquare$$

Observação 2.2.4. *A Proposição 2.2.2 nos diz que o determinante da matriz de Gram de um reticulado não depende da base escolhida.*

Definição 2.2.5. *O* ***determinante de um reticulado*** *Λ é o mesmo que o determinante de uma matriz de Gram de Λ, e denotamos por $det(\Lambda)$ e este número é o quadrado do volume de uma região fundamental*

$$det(\Lambda) = det(G) = (vol(\mathcal{P}_\beta))^2.$$

Exemplo 2.2.2. *A matriz de Gram do Exemplo 2.2.1 é*

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 2 \\ 6 & 14 & 3 \\ 2 & 3 & 6 \end{pmatrix}.$$

O determinante da matriz de Gram é dado por:

$$det(G) = \begin{vmatrix} 3 & 6 & 2 \\ 6 & 14 & 3 \\ 2 & 3 & 6 \end{vmatrix} = 25.$$

Logo, $det(\Lambda) = det(G) = 25$. *Portanto,* $(vol(\mathcal{P}_\beta))^2 = 5^2 = 25$.

Observação 2.2.5. *Se* $\Lambda \subset \mathbb{R}^n$ *é um reticulado, então* $det(\Lambda) = det(G) = det(M^tM) = det(M^t)(M) = det(vol(\Lambda))^2$.

2.3 Empacotamento no $\mathbb{R}^n$

Um problema geométrico importante é o empacotamento esférico no $\mathbb{R}^2$: procura-se encontrar qual melhor maneira, em termos de densidade, de colocar esferas idênticas juntas preenchendo um espaço. Nesta seção veremos o conceito de empacotamento esférico e algumas propriedades de empacotamento reticulado.

Definição 2.3.1. *Um* ***empacotamento esférico****, ou simplesmente, empacotamento no* $\mathbb{R}^n$*, é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a interseção de quaisquer duas esferas euclidianas tenham no máximo um ponto e que este arranjo de esferas ocupem o maior espaço possível.*

Definição 2.3.2. *Um* ***empacotamento reticulado*** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* Λ *em* $\mathbb{R}^n$.

Definição 2.3.3. *Dado um empacotamento no* $\mathbb{R}^n$*, associado a um reticulado* Λ*, com* $\beta = \{v_1, ..., v_n\}$ *uma* $\mathbb{Z}$*-base, definimos sua* ***densidade de empacotamento*** *como* $\Delta(\Lambda)$ *é a proporção do espaço* $\mathbb{R}^n$ *coberto pela união das esferas, e a expressão para calcular* $\Delta(\Lambda)$ *é dada por*

$$\Delta(\Lambda) = \frac{volume\ da\ região\ coberta\ por\ uma\ esfera}{volume\ da\ região\ fundamental} = \frac{vol(B(0,\rho))}{vol(\Lambda)} = \frac{vol(B(1))\rho^n}{vol(\Lambda)}.$$

Em que $B(0,\rho)$ *denota a esfera de centro na origem e raio* ρ*, onde,*

$$vol(B(1)) = \begin{cases} \dfrac{\pi^{n/2}}{(n/2)!}, & se\ n\ for\ par \\ \dfrac{2^n\pi^{(n-1)/2}((n-1)/2)!}{n!}, & se\ n\ for\ ímpar. \end{cases}$$

Observação 2.3.1. *No estudo de empacotamento pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Estamos interessados no empacotamento associado a um reticulado Λ em que as esferas tenham raio máximo e que esse empacotamento ocupe maior espaço possível no $\mathbb{R}^n$. Para determinarmos o melhor raio, usaremos uma importante definição que relaciona o raio do empacotamento, que é a **norma mínima** de um vetor não nulo do reticulado que tem a mesma distância mínima entre os dois pontos distintos deste.

Definição 2.3.4. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\Lambda_{min} = \{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}$. O número $(\Lambda_{min})^2$ é chamado de **norma mínima**.*

Note que tal valor existe, já que a interseção de Λ com uma esfera compacta de centro na origem e raio $k > 0$ é o conjunto finito. Nestes termos, temos que o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento é $\rho = \dfrac{\Lambda_{min}}{2}$, chamado de **raio de empacotamento**.

Definição 2.3.5. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Definimos a **densidade de centro** de Λ por*

$$\delta(\Lambda) = \frac{\rho^n}{vol(\Lambda)},$$

onde ρ é o raio do empacotamento de Λ e $vol(\Lambda)$ o seu volume.

Observação 2.3.2. *Uma vez que $\Delta(\Lambda) = vol(B(1)) \cdot \dfrac{\rho^n}{vol(\Lambda)}$ e $\delta(\Lambda) = \dfrac{\rho^n}{vol(\Lambda)}$, segue que $\Delta(\Lambda) = vol(B(1)) \cdot \delta(\Lambda)$.*

Faremos uma comparação entre dois reticulados do $\mathbb{R}^2$, comparando a densidade do reticulado $\mathbb{Z}^2$ com o reticulado hexagonal.

Exemplo 2.3.1. *Seja $\Lambda = \mathbb{Z}^2$ um reticulado na base canônica $\beta = \{(1,0),(0,1)\}$ como apresentado na Figura 1. O raio do empacotamento é $\rho = \dfrac{1}{2}$ e $vol(B(1)) = \pi$. Assim, o volume do reticulado, a densidade de centro e a densidade de empacotamento são dados, respectivamente, por*

$$vol(\Lambda) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1,\ \delta(\Lambda) = \frac{(\frac{1}{2})^2}{1} = \frac{1}{4} = 0.25,\ \text{e}\ \Delta(\Lambda) = \pi \cdot \frac{1}{4} = \frac{\pi}{4} \cong 0.7853.$$

Isto quer dizer que as esferas ocupam $78,53\%$ do espaço $\mathbb{R}^2$.

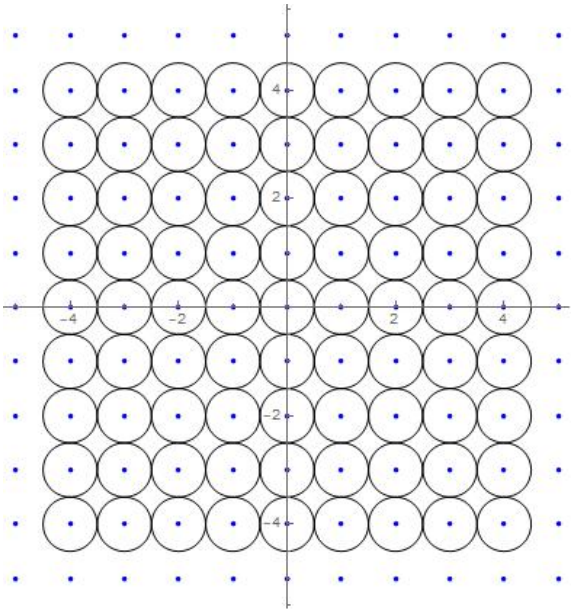


Figura 6 – Empacotamento do reticulado $\Lambda = \mathbb{Z}^2$.
Fonte: Autor.

Exemplo 2.3.2. *Seja Λ_H o reticulado hexagonal como apresentado na Figura 4. Seu raio é $\rho = \frac{1}{2}$ e $vol(B(1)) = \pi$. Assim, o volume do reticulado, a densidade de centro e a densidade do empacotamento são dados, respectivamente, por*

$$vol(\Lambda) = \begin{vmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ 1 & 0 \end{vmatrix} = \frac{\sqrt{3}}{2},\ \delta(\Lambda) = \frac{(\frac{1}{2})^2}{\frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}} \cong 0.2886 \text{ e } \Delta(\Lambda) = \pi \cdot \frac{1}{2\sqrt{3}} = \frac{\pi}{2\sqrt{3}} \cong 0.9069.$$

Isto que dizer que as esferas ocupam 90.69% *do espaço* $\mathbb{R}^2$.

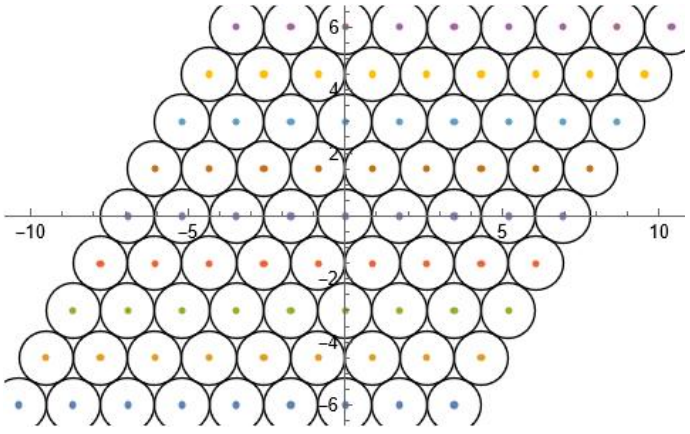


Figura 7 – Empacotamento do reticulado hexagonal.
Fonte: Autor.

A proposição a seguir nos garante que o reticulado hexagonal Λ_H é o reticulado mais denso na dimensão dois, ou seja, o empacotamento apresentado na Figura 7 é o melhor empacotamento na dimensão 2 e, como veremos no Exemplo 2.4.2, este reticulado é equivalente ao reticulado A_2 que será apresentado.

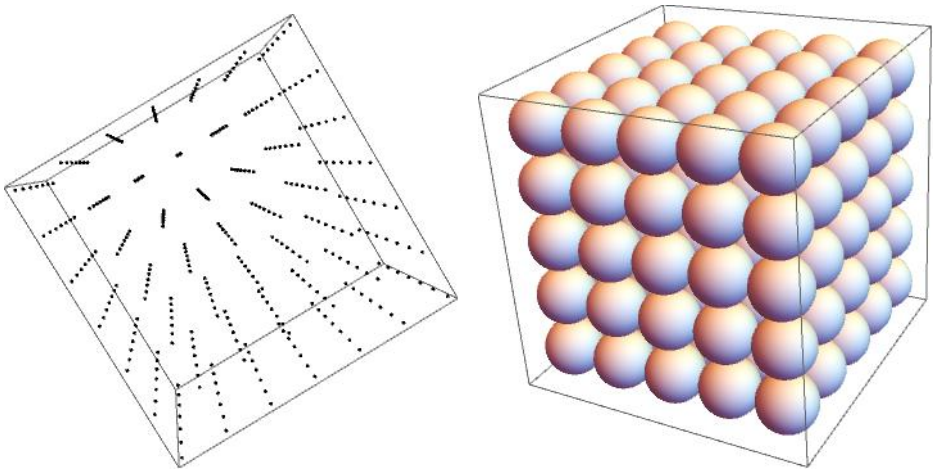
Proposição 2.3.1. *[38] O empacotamento mais denso em $\mathbb{R}^2$ é dado pelo reticulado hexagonal Λ cuja densidade é $\frac{\pi}{2\sqrt{3}} \cong 0.9069$. Além disso, qualquer empacotamento com esta densidade terá por centro dos discos um conjunto que a menos de movimentos rígidos ou dilatação é este reticulado.*

A seguir mostraremos alguns reticulados importantes na dimensão três, sendo: $\mathbb{Z}^3$ (base canônica do $\mathbb{R}^3$), BCC (reticulado de corpo centrado) e o FCC (reticulado de face centrada), comparando as suas densidades de empacotamento.

Exemplo 2.3.3. *Seja $\Lambda_1 = \mathbb{R}^3$ o reticulado com base $\beta_1 = \{(1,0,0),(0,1,0),(0,0,1)\}$. O raio do empacotamento é $\rho = \frac{1}{2}$ e $v(B(1)) = \frac{4\pi}{3}$. Assim, o volume do reticulado, a densidade de centro e a densidade do empacotamento são dados, respectivamente, por*

$$vol(\Lambda_1) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1,\ \delta(\Lambda_1) = \frac{(\frac{1}{2})^3}{1} = \frac{1}{8} = 0.125 \text{ e } \Delta(\Lambda_1) = \frac{4\pi}{3} \cdot \frac{1}{8} = \frac{4\pi}{24} = \frac{\pi}{6} \cong 0.523.$$

Isto quer dizer que as esferas ocupam $52,3\%$ do espaço $\mathbb{R}^3$.



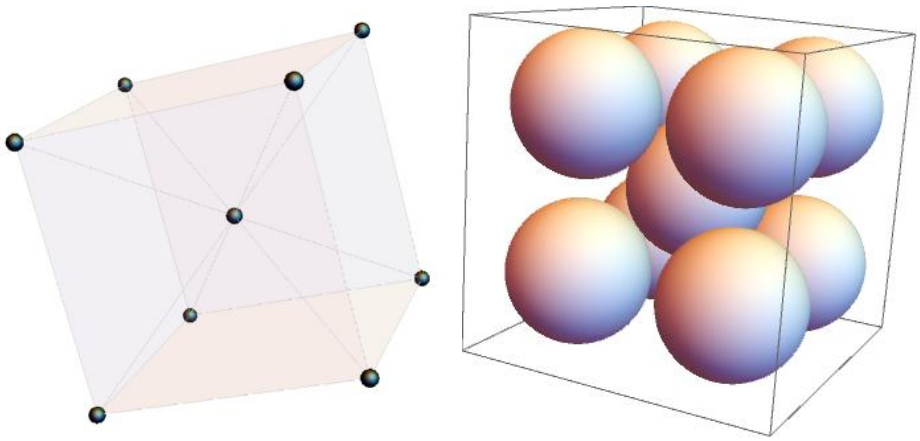
(a) Reticulado $\Lambda_1 = \mathbb{Z}^3$. (b) Empacotamento do $\Lambda_1 = \mathbb{Z}^3$.

Figura 8 – Reticulado $\Lambda_1 = \mathbb{Z}^3$ com seu respectivo empacotamento.
Fonte: Autor.

Exemplo 2.3.4. *Seja Λ_2 o reticulado de corpo centrado (BCC) com base $\beta_2 = \{(2,0,0),(0,2,0),(1,1,1)\}$. O raio de empacotamento é $\rho = \frac{\sqrt{3}}{2}$ e $vol(B(1)) = \frac{4\pi}{3}$. Assim, o volume do reticulado, a densidade de centro e a densidade de empacotamento são dados, respectivamente, por*

$$vol(\Lambda_2) = \begin{vmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 4,\ \delta(\Lambda_2) = \frac{(\frac{\sqrt{3}}{2})^3}{4} = \frac{3\sqrt{3}}{32} \cong 0.162 \text{ e } \Delta(\Lambda_2) = \frac{4\pi}{3} \cdot \frac{3\sqrt{3}}{32} = \frac{\pi\sqrt{3}}{8} \cong 0.680.$$

Isto quer dizer que as esferas ocupam 68% *do espaço* $\mathbb{R}^3$.



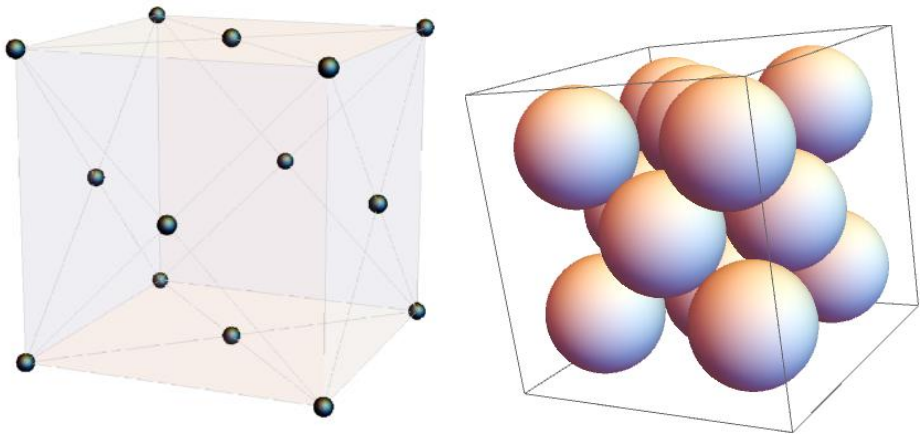
(a) Reticulado Λ_2. (b) Empacotamento do reticulado Λ_2.

Figura 9 – Reticulado e empacotamento do Λ_2.
Fonte: Autor.

Exemplo 2.3.5. *Seja* Λ_3 *o reticulado de face centrada (FCC) com base* $\beta_3 = \{(2,0,0),(1,1,0),(1,0,1)\}$. *O raio de empacotamento é* $\rho = \dfrac{\sqrt{2}}{2}$ *e* $vol(B(1)) = \dfrac{4\pi}{3}$. *Assim, o volume do reticulado, a densidade de centro e a densidade do empacotamento são dados, respectivamente, por*

$$vol(\Lambda_3) = \begin{vmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} = 2,\ \delta(\Lambda_3) = \frac{(\frac{\sqrt{2}}{2})^3}{2} = \frac{\sqrt{2}}{8} \cong 0.1767 \text{ e } \Delta(\Lambda_3) = \frac{4\pi}{3}\cdot\frac{\sqrt{2}}{8} = \frac{\pi\sqrt{2}}{6} \cong 0.7404.$$

Isto quer dizer que as esferas ocupam 74,04% *do espaço do* $\mathbb{R}^3$.



(a) Reticulado Λ_3. (b) Empacotamento do reticulado Λ_3.

Figura 10 – Reticulado e empacotamento do Λ_3.
Fonte: Autor.

A proposição a seguir confirma que o reticulado FCC é o reticulado mais denso na dimensão 3. Veremos na Seção 2.4 que os reticulados A_3 e D_3 apresentam a mesma densidade de centro do FCC.

Proposição 2.3.2. *[17] Dentre todos os arranjos reticulados, a melhor densidade do espaço tridimensional $\mathbb{R}^3$ é dado pelo reticulado FCC.*

Observação 2.3.3. *(i) A demonstração da Proposição 2.3.2 é feita por Gauss em 1831 onde mostra que o reticulado FCC é o mais denso em $\mathbb{R}^3$.*

(ii) A demonstração proposta por Thomas Hales é de alta complexidade computacional e bastante extensa possuindo 250 páginas com mais de 3 Gigabyte de programas de computacionais, ver mais detalhes sobre a história em [38] e para ver a demonstração completa em [18].

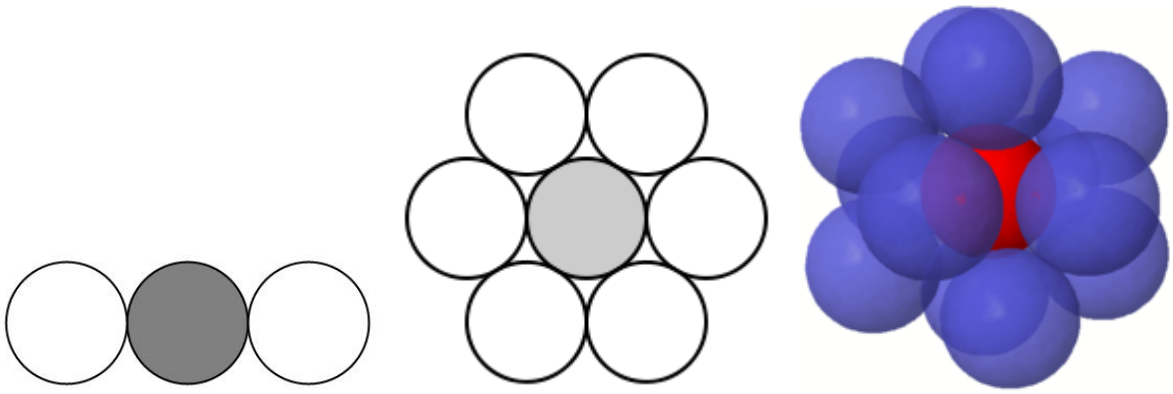
Outra definição importante a ser apresentada é o problema do *k*issing number em empacotamentos esféricos.

Definição 2.3.6. *O **kissing number** é o maior número τ de esferas n-dimensionais de raio ρ que podem tocar simultaneamente uma esfera de mesmo raio.*

Definição 2.3.7. *Dizemos que o **kissing number de um reticulado** Λ é o número de esferas do empacotamento que tocam uma esfera central fixa, denotado por $\tau(\Lambda)$.*

Observação 2.3.4. *Uma maneira de obtermos o kissing number de um reticulado é determinar o número de vetores com norma mínima não nula.*

Mostraremos, as figuras dos kissing numbers das dimensões 1, 2 e 3.



(a) Kissing number: dimensão 1, $\tau(\Lambda) = 2$.

(b) Kissing number: dimensão 2, $\tau(\Lambda_H) = 6$.

(c) Kissing number: dimensão 3, $\tau(\Lambda_{FCC}) = 12$.

Figura 11 – Kissing number dos empacotamentos nas dimensões 1, 2 e 3.
Fonte: Autor.

O problema de encontrar o kissing number do espaço surgiu com debates entre Isaac Newton e David Gregory em 1694. No espaço tridimensional ($\mathbb{R}^3$) Newton acreditava que seriam 12 esferas tocando numa central e Gregory acreditava que seriam 13 esferas. Em 1953, Van der Waerden e Schütte deram a primeira prova detalhada de que Newton estava certo. O kissing number da dimensão 3 é conhecido como o *problema da 13ª esfera.*

Para o cálculo de kissing numbers de reticulados conhecidos é usado métodos e técnicas avançadas que não é foco deste trabalho, para mais detalhes ver [28] e [31], demonstram o kissing number de dimensão três e quatro.

2.4 Alguns reticulados especiais e suas propriedades

Nesta seção veremos exemplos de reticulados bastante explorados na literatura, a saber $\mathbb{Z}^n$, $A_1, A_2, D_3, D_4, D_5, E_6, E_7$ e E_8. Também veremos alguns reticulados introduzidos no século XX com dimensões maiores tais como, K_{12}, Λ_{16} e Λ_{24}. As referências utilizadas nesta seção foram [2], [7], [8], [12] e [14].

2.4.1 Reticulado $\mathbb{Z}^n$

O reticulado n-dimensional $\mathbb{Z}^n$ ou reticulado cúbico é definido como

$$\mathbb{Z}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{Z}, i = 1, ..., n\},$$

e possui matriz geradora $M = I_n$ (matriz identidade de ordem n). Temos que $det(\mathbb{Z}^n) = 1$ e o raio do empacotamento é $\rho = \frac{1}{2}$. Assim, a densidade de centro do $\mathbb{Z}^n$ é dada por

$$\delta(\mathbb{Z}^n) = \frac{\rho^n}{vol(\mathbb{Z}^n)} = 2^{-n}.$$

O kissing number de $\mathbb{Z}^n$ é $\tau(\mathbb{Z}^n) = 2n$.

Exemplo 2.4.1. *Os reticulados de $\mathbb{Z}, \mathbb{Z}^2$ e $\mathbb{Z}^3$ possuem densidade de centro $\delta(\mathbb{Z}) = 0.5$, $\delta(\mathbb{Z}^2) = 0.25$ e $\mathbb{Z}^3 = 0.125$, respectivamente. E seus kissing numbers, $\tau(\mathbb{Z}) = 2$, $\tau(\mathbb{Z}^2) = 4$ e $\tau(\mathbb{Z}^3) = 6$.*

Observação 2.4.1. *(i) Conforme a dimensão de $\mathbb{Z}^n$ aumenta, sua densidade de centro diminui.*

(ii) Qualquer matriz uni-modular gera $\mathbb{Z}^n$. De fato, essa matriz é linearmente independente e seu determinante é ± 1.

O reticulado $\mathbb{Z}^n$ é um importante elemento da base da teoria, já que qualquer outro reticulado é uma transformação linear dele.

2.4.2 Reticulado A_n

O reticulado A_n é um reticulado (n+1)-dimensional, onde $n \geqslant 1$ é definido por

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

Assim, A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$ e possui uma matriz geradora M, dada por

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}.$$

Temos que norma mínima $(\Lambda_{min}(A_n))^2 = 2$, o raio de empacotamento $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é

$$\delta(A_n) = \frac{2^{-\frac{n}{2}}}{\sqrt{n+1}}.$$

O kissing number é dado pela relação $\tau(A_n) = n(n+1)$. O reticulado A_n apresenta densidade de centro ótima para as dimensões 2 e 3.

Exemplo 2.4.2. *O reticulado A_2 é um reticulado bidimensional no $\mathbb{R}^3$, com matriz geradora dada por*

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

distância mínima é $\Lambda_{min}(A_n) = \sqrt{2}$, o raio do empacotamento $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é dada por

$$\delta(A_n) = \frac{2^{-\frac{2}{2}}}{\sqrt{2+1}} = \frac{1}{2\sqrt{3}} \cong 0.28868.$$

E o kissing number é $\tau(A_2) = 2(2+1) = 6$.

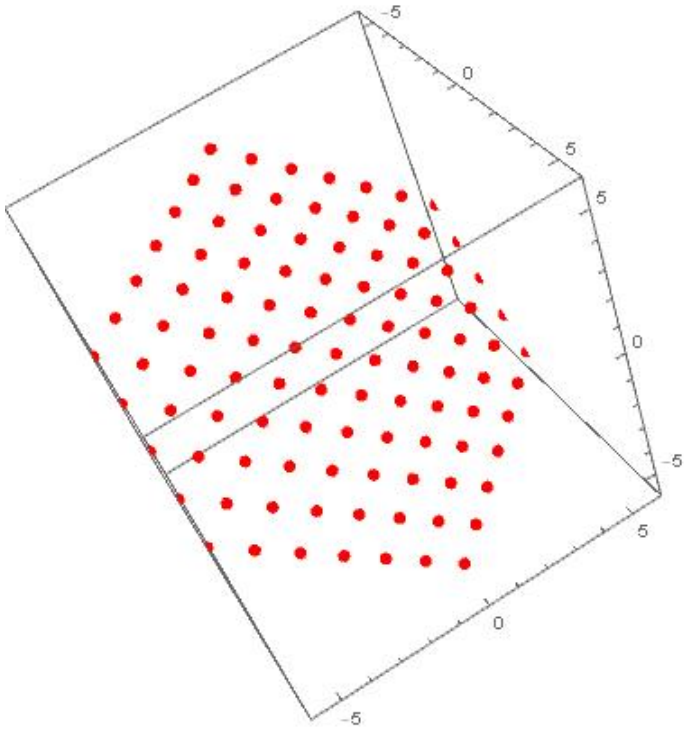


Figura 12 – Reticulado bidimensional A_2
Fonte: Autor.

O reticulado A_2 que é o reticulado mais denso na dimensão 2 é equivalente ao reticulado hexagonal Λ_H apresentado no Exemplo 2.1.3.

2.4.3 Reticulado D_n

O reticulado D_n é n-dimensional, onde $n \geqslant 3$, é dado por

$$D_n = \{(x_1, ..., x_n) \in \mathbb{Z}^n : x_1 + ... + x_n\},$$

é par, e a matriz geradora M de D_n é dada por

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}.$$

O determinante $det(D_n) = 4$, a norma mínima $(\Lambda_{min}(D_n))^2 = 2$, o raio do empacotamento é $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é dada por

$$\delta(D_n) = 2^{-\frac{(n+2)}{2}}.$$

O kissing number é dado por $\tau(D_n) = 2n(n-1)$.

Exemplo 2.4.3. *Este exemplo mostra o arranjo de esferas do empacotamento associado a D_3, este reticulado é formado por todos os pontos $(x_1, x_2, x_3) \in \mathbb{Z}^3$, tal que a soma de suas coordenadas é par. Uma matriz geradora para D_3 é*

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

O determinante $det(D_3) = 4$, a norma mínima $(\Lambda_{min}(D_3))^2 = 2$ o raio do empacotamento é $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é

$$\delta(D_3) = 2^{\frac{-(3+2)}{2}} = 2^{\frac{-5}{2}} = \frac{1}{4\sqrt{2}} \cong 0.17678.$$

Podemos ver esse empacotamento normalmente em bancas de frutas (pirâmide de laranjas).

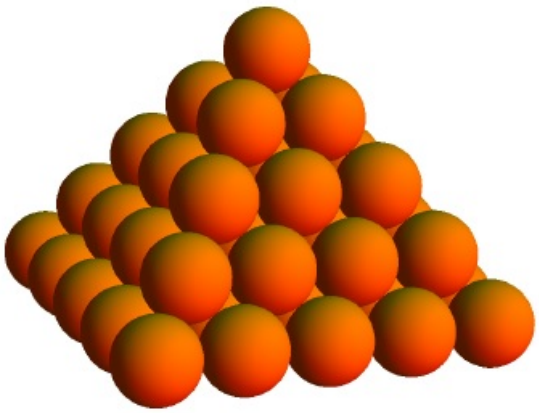


Figura 13 – Empacotamento D_3 laranjas empilhadas.
Fonte: CAMPELLO, A. (2014, p. 3).

O kissing number é $\tau(D_3) = 2 \cdot 3(3-1) = 12$. Este reticulado possui densidade de centro ótima pra dimensão 3.

Exemplo 2.4.4. *O reticulado D_4 é formado por todos os pontos $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ tal que $(x_1 + x_2 + x_3 + x_4)$ é um número par. Assim sua matriz geradora é dada por*

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

O determinante é $det(D_4) = 4$, a norma mínima $(\Lambda_{min}(D_4))^2 = 2$, o raio do empacotamento é $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é

$$\delta(D_4) = 2^{\frac{-(4+2)}{2}} = 2^{-3} = \frac{1}{8} = 0.125.$$

O kissing number $\tau(D_4) = 2 \cdot 4(4-1) = 24$. *O reticulado* D_4 *possui densidade de centro ótimo para a dimensão 4.*

Exemplo 2.4.5. *O reticulado* D_5 *é formado por todos os pontos* $(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$, *tal que a soma* $(x_1 + ... + x_5)$ *é um número par, e sua matriz geradora é*

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

O determinante é $det(D_5) = 4$, *a norma mínima* $(\Lambda_{min}(D_5))^2 = 2$ *o raio do empacotamento é* $\rho = \dfrac{\sqrt{2}}{2}$ *e a densidade de centro é*

$$\delta(D_5) = 2^{\frac{-(5+2)}{2}} = 2^{\frac{-7}{2}} = 2^{\frac{1}{8\sqrt{2}}} \cong 0.08839.$$

O kissing number $\tau(D_5) = 2 \cdot 5(5-1) = 40$. *O reticulado* D_5 *possui densidade de centro ótima para a dimensão 5.*

2.4.4 Reticulado E_8

O reticulado E_8 é um reticulado 8-dimensional definido por

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

Uma matriz geradora para E_8 é dada por

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

O determinante é $det(E_8) = 1$, a norma mínima $(\Lambda_{min}(E_8))^2 = 2$, o raio do empacotamento $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é dado por

$$\delta(E_8) = \frac{(\frac{\sqrt{2}}{2})^8}{1} = \frac{1}{16} \cong 0.0625.$$

O kissing number é $\tau(E_8) = 240$. Este reticulado possui densidade de centro ótima para dimensão 8.

2.4.5 Reticulado E_7

O reticulado E_7 é um reticulado 7-dimensional definido por

$$E_7 = \{(x_1, ..., x_8) \in E_8; \sum_{i=1}^{8} x_i = 0\}.$$

E_7 é um sobre-reticulado de E_8. Uma matriz geradora é dada por

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

O determinante $det(E_7) = 2$, o $vol(E_7) = \sqrt{2}$, a norma mínima $(\Lambda_{min}(E_7))^2 = 2$, o raio do empacotamento é $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é

$$\delta(E_7) = \frac{(\frac{\sqrt{2}}{2})^7}{\sqrt{2}} = \frac{1}{16} \cong 0.0625.$$

O kissing number $\tau(E_7) = 126$. O reticulado E_7 possui densidade de centro ótima para a dimensão 7.

2.4.6 Reticulado E_6

O reticulado E_6 é um reticulado 6-dimensional definido por

$$E_6 = \{(x_1, ..., x_8) \in E_8; xv = 0, \forall v \in V\},$$

onde V é um A_2-sobre-reticulado de E_8. A matriz geradora de E_6 é

$$M = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

O determinante $det(E_6) = 3$, a norma mínima $(\Lambda_{min}(E_6))^2 = 2$, o raio do empacotamento $\rho = \dfrac{\sqrt{2}}{2}$ e a densidade de centro é dada por

$$\delta(E_6) = \frac{(\frac{\sqrt{2}}{2})^6}{\sqrt{3}} = \frac{1}{8\sqrt{3}} \cong 0.07216.$$

O kissing number $\tau(E_6) = 72$. O reticulado E_6 possui densidade de centro ótima para a dimensão 6.

Os próximos reticulados foram introduzidos no século XX, são reticulados de dimensões superiores.

2.4.7 Reticulado de Coxeter-Todd K_{12}

O reticulado k_{12} é um reticulado 12-dimensional sendo descrito pela primeira vez por Coxeter e Todd em 1954. O determinante $det(K_{12}) = 729$, a norma mínima $(\Lambda_{min}(K_{12}))^2 = 4$, o raio do empacotamento é $\rho = 1$ e a densidade de centro é dado por

$$\delta(K_{12}) = \frac{1}{27} \cong 0.03703.$$

O kissing number $\tau(K_{12}) = 756$. Este reticulado possui densidade de centro ótima para a dimensão 12. Uma matriz geradora é dada por

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

2.4.8 Reticulado de Barnes-Wall Λ_{16}

O reticulado Λ_{16} é um reticulado 16-dimensional sendo escrito por Barnes e Wall em 1959. O determinante $det(\Lambda_{16}) = 256$, norma mínima $(\Lambda_{min}(\Lambda_{16}))^2 = 4$, o raio do empacotamento é $\rho = 1$ e a densidade de centro é dado por

$$\delta(\Lambda_{16}) = \frac{1}{16} = 0.0625.$$

O kissing number é $\tau(\Lambda_{16}) = 4320$. O reticulado Λ_{16} possui densidade de centro ótimo para a dimensão 16. Uma matriz geradora para este reticulado é dada por

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

2.4.9 Reticulado de Leech Λ_{24}

O reticulado Λ_{24} é um reticulado 24-dimensional sendo descrito por Leech em 1965. O determinante é $det(\Lambda_{24}) = 1$, a norma mínima $(\Lambda_{min}(\Lambda_{24}))^2 = 4$, o raio do empacotamento é $\rho = 1$ e a densidade de centro é

$$\delta(\Lambda_{24}) = 1.$$

O kissing number $\tau(\Lambda_{24}) = 196560$. O reticulado Λ_{24} possui densidade de centro ótima para a dimensão 24. Uma matriz geradora para este reticulado é dado por

$$M = \frac{1}{\sqrt{8}} \begin{pmatrix}
8 & 4 & 4 & 4 & 4 & 4 & 4 & 2 & 4 & 4 & 4 & 2 & 4 & 2 & 2 & 2 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & 3 \\
0 & 4 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 1 \\
0 & 0 & 4 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 1 \\
0 & 0 & 0 & 4 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

A Tabela 1 abaixo mostra reticulados provados serem os mais densos nas suas respectivas dimensões de 1 a 8 e dimensões 12, 16 e 24.

Reticulado	Dimensão	$\delta(\Lambda)$	$\tau(\Lambda)$
$\mathbb{Z}$	1	0.5	2
$\mathbb{Z}^2$	2	0.25	4
$\mathbb{Z}^3$	3	0.125	6
A_2	2	0.28868	6
D_3	3	0.17678	12
D_4	4	0.125	24
D_5	5	0.08839	40
E_6	6	0.07216	72
E_7	7	0.0625	126
E_8	8	0.625	240
K_{12}	12	0.03703	756
Λ_{16}	16	0.625	4320
Λ_{24}	24	1	196560

Tabela 1 – Melhores valores conhecidos com respeito a densidade de centro e o kissing number para reticulados de dimensões 1 a 8 e dimensão 12, 16 e 24.
Fonte: Autor.

Capítulo 3

Reticulados algébricos

Neste capítulo apresentaremos construções algébricas de reticulados. Na Seção 3.1 apresentaremos o homomorfismo canônico (ou de Minkowski) para a geração de reticulados no $\mathbb{R}^n$ recorrendo a ideais do anel de inteiros de um corpo de números. Na Seção 3.2, a partir do homomorfismo canônico (ou de Minkowski), definiremos uma perturbação do homomorfismo canônico σ_α e na Seção 3.3 apresentaremos a perturbação do homomorfismo canônico $\sigma_{2\alpha}$. Os reticulados construídos a partir do homomorfismo canônico e de suas perturbações serão chamados de **reticulados algébricos**. As principais referências pesquisadas neste capítulo foram [6], [14], [35] e [36].

3.1 Reticulados algébricos via homomorfismo canônico

Seja $\mathbb{K}$ um corpo de números de grau n, pelo Teorema 1.2.4, existem n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}, (i = 1, ..., n)$, que fixam $\mathbb{Q}$. Considerando $\phi : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Assim, para todo $i = 1, ..., n$, temos que $\phi \circ \sigma_i = \sigma_{\mathbb{K}}$ para algum $1 \leqslant \mathbb{K} \leqslant n$ e, $\sigma_i = \sigma_k$ se, e somente se, $\sigma_i(\mathbb{K} \subseteq \mathbb{R})$. Desta forma, podemos ordenar os monomorfismos $\sigma_1, ..., \sigma_n$ de tal forma que até um determinado índice r_1 tenhamos $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ $(1 \leqslant i \leqslant r_1)$ ou seja, de modo que os monomorfismos $\sigma_1, ..., \sigma_{r_1}$ sejam reais e, os demais monomorfismos serão todos imaginários. Como os monomorfismos imaginários aparecem sempre aos pares, temos que o número $n - r_1$ é par e, assim podemos escrever $n - r_1 = 2r_2$, ou seja $n = r_1 + 2r_2$.

A partir desta construção, definiremos a seguir um homomorfismo que chamamos de homomorfismo canônico ou homomorfismo de Minkowski.

Definição 3.1.1. *Seja $x \in \mathbb{K}$. O homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por*

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

*é um homomorfismo inteiro de anéis, chamado de **homomorfismo canônico** ou **homomorfismo de Minkowski**, onde $\Re(y)$ e $\Im(y)$ representa as partes reais e imaginárias de um número complexo y, respectivamente.*

Exemplo 3.1.1. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$ um corpo ciclotômico em que os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são todos dados por $\{\sigma_1, \sigma_2\}$, onde $\sigma_i(\zeta_3) = \zeta_3^i$, para $(i = 1, 2)$. Como $\sigma_i(\mathbb{K}) \nsubseteq \mathbb{R}$ para todo $i = 1, 2$. Temos que $\mathbb{K}$ é totalmente imaginário, implica que $r_1 = 0$ e $r_2 = 1$. Se $x = a + b\zeta_3 = a + b\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}\right) = a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i \in \mathbb{K}$, onde $a, b \in \mathbb{Z}$, temos que a imagem do homomorfismo canônico é*

$$\begin{aligned}
\sigma_{\mathbb{K}}(x) &= (\Re\sigma_1(x), \Im\sigma_1(x)) \\
&= \left(\Re\left(\sigma_1\left(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right)\right), \Im\left(\sigma_1\left(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right)\right)\right) \\
&= \left(\Re\left(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right), \Im\left(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right)\right) \\
&= \left(a - \frac{b}{2}, \frac{b\sqrt{3}}{2}\right) \\
&= a\,(1, 0) + b\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right).
\end{aligned}$$

Exemplo 3.1.2. *Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ e $\{\sigma_1, \sigma_2\}$ o conjunto de $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde $\sigma_1(\sqrt{7}) = \sqrt{7}$ e $\sigma_2(\sqrt{7}) = -\sqrt{7}$, com $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 2$ e $r_2 = 0$, ou seja, o corpo $\mathbb{K}$ é totalmente real. Para $x = a + b\sqrt{7} \in \mathbb{K}$, temos que a imagem do homomorfismo canônico nos elementos da base integral é dado por*

$$\begin{aligned}
\sigma_{\mathbb{K}}(x) &= (\sigma_1(x), \sigma_2(x)) \\
&= ((\sigma_1(a + b\sqrt{7})), (\sigma_1(a + b\sqrt{7}))) \\
&= ((a + b\sqrt{7}), (a - b\sqrt{7})) \\
&= (a + b\sqrt{7}, a - b\sqrt{7}) \\
&= a(1, 1) + b(\sqrt{7}, -\sqrt{7}).
\end{aligned}$$

O reticulado gerado pelos vetores $v_1 = (1, 1)$ e $v_2 = (\sqrt{7}, -\sqrt{7})$, com a região fundamental descrita na figura abaixo

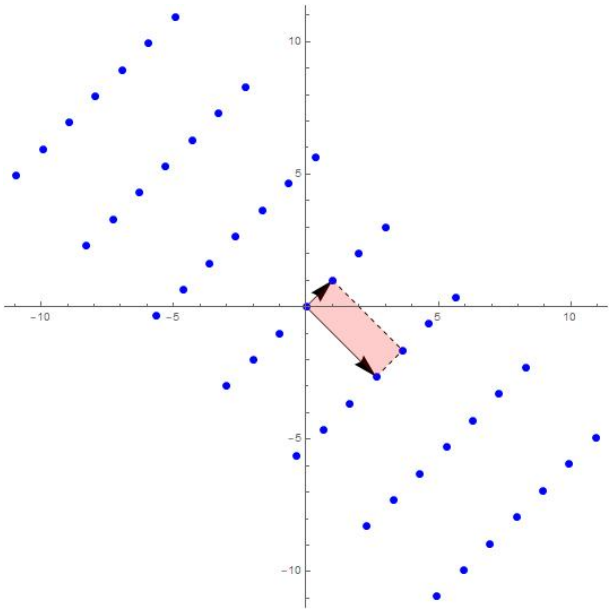


Figura 14 – Reticulado algébrico gerado pelos vetores $v_1 = (1, 1)$ e $v_2 = (\sqrt{7}, -\sqrt{7})$.
Fonte: Autor.

Nos resultados a seguir veremos como obter reticulados utilizando homomorfismos canônicos e também uma fórmula para calcular a densidade de centro destes reticulados. Uma das aplicações destes homomorfismos é geração de reticulados no $\mathbb{R}^n$, por propriedades herdadas de $\mathbb{K}$ e da teoria algébrica dos números.

Teorema 3.1.1. *[35] Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ o homomorfismo de Minkowski. Se $M \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_j\}_{1 \leqslant j \leqslant n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, com base $\{\sigma_{\mathbb{K}}(x_1), ..., \sigma_{\mathbb{K}}(x_n)\}$ e o volume*

$$vol(\sigma_{\mathbb{K}}(M)) = det(\sigma_{\mathbb{K}}(M))^{\frac{1}{2}} = 2^{-r_2} |det(\sigma_j(x_j))_{j,\mathbb{K}=1}^{n}|,$$

onde r_2 é o número de pares de homomorfismos imaginários.

Corolário 3.1.1. *[35] Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$, $\mathbb{I}_{\mathbb{K}}$ é o anel dos inteiros e $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{U})$ são reticulados, com volumes dados respectivamente por*

$$vol(\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})) = 2^{-r_2} \cdot |\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} \text{ e } vol(\sigma_{\mathbb{K}}(\mathcal{U})) = vol(\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})) \cdot \mathcal{N}(\mathcal{U}),$$

onde r_2 é o número de homomorfismos imaginários de $\mathbb{K}$ e $\mathcal{N}(\mathcal{U})$ é a norma do ideal $\mathcal{U}$.

Se $\{x_1, ..., x_n\}$ é uma $\mathbb{Z}$-base de $M \subset \mathbb{K}$, então a matriz geradora do reticulado

$\sigma_{\mathbb{K}}(M) = \left\{ \sum_{i=1}^{n} \sigma_{\mathbb{K}}; a_i \in \mathbb{Z} \right\}$ é dado por

$$M = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_{r_1}(x_1) & \Re\sigma_{r_1+1}(x_1) & \Im\sigma_{r_1+1}(x_1) & \cdots & \Re\sigma_{r_1+r_2}(x_1) & \Im\sigma_{r_1+r_2}(x_1) \\ \sigma_1(x_2) & \cdots & \sigma_{r_1}(x_2) & \Re\sigma_{r_1+1}(x_2) & \Im\sigma_{r_1+1}(x_2) & \cdots & \Re\sigma_{r_1+r_2}(x_2) & \Im\sigma_{r_1+r_2}(x_2) \\ \sigma_1(x_3) & \cdots & \sigma_{r_1}(x_3) & \Re\sigma_{r_1+1}(x_3) & \Im\sigma_{r_1+1}(x_3) & \cdots & \Re\sigma_{r_1+r_2}(x_3) & \Im\sigma_{r_1+r_2}(x_3) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(x_n) & \cdots & \sigma_{r_1}(x_n) & \Re\sigma_{r_1+1}(x_n) & \Im\sigma_{r_1+1}(x_n) & \cdots & \Re\sigma_{r_1+r_2}(x_n) & \Im\sigma_{r_1+r_2}(x_n) \end{pmatrix}.$$

Exemplo 3.1.3. *Considere o corpo quadrático* $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. *Pela Definição 1.3.13, temos que* $d = -3 < 0$, *então a extensão* $\mathbb{Q}(\sqrt{-3})$ *é totalmente imaginária e assim,* $r_1 = 0$ *e* $r_2 = 1$. *Temos pelo Teorema 1.3.9 que o anel dos inteiros de* $\mathbb{K}$ *é* $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ *e* $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$ *é uma base integral de* $\mathbb{K}$. *Dado* $x = a + b\left(\frac{1+\sqrt{-3}}{2}\right)$, *temos que a imagem do homomorfismo canônico* $\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}}) \subset \mathbb{R}^2$ *é dado por*

$$\begin{aligned} \sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}}) &= \left(\Re\sigma_1\left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right), \Im\sigma_1\left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right)\right) \\ &= \left(\Re\left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right), \Im\left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right)\right) \\ &= \Re\left(a + \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right), \Im\left(a + \frac{b}{2} + \frac{b\sqrt{3}}{2}i\right) \\ &= \left(a + \frac{b}{2}, \frac{b\sqrt{3}}{2}\right) \\ &= a(1,0) + b\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \end{aligned}$$

é um reticulado gerado pelos vetores $v_1 = (1,0)$ *e* $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. *Pelo Teorema 3.1.1, volume do reticulado* $\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})$ *é*

$$\begin{aligned} vol(\sigma_{\mathbb{K}}(\mathbb{I})) &= 2^{-1}\left|det\left[\begin{pmatrix} \sigma_1(1) & \sigma_1(1) \\ \sigma_2\left(\frac{1+\sqrt{-3}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{-3}}{2}\right) \end{pmatrix}\right]^2\right|^{\frac{1}{2}} \\ &= \frac{1}{2}\left|det\left[\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{-3}}{2} & \frac{1-\sqrt{-3}}{2} \end{pmatrix}\right]^2\right|^{\frac{1}{2}} \\ &= \frac{1}{2}\left|\left[\frac{1-\sqrt{-3}}{2} - \frac{1+\sqrt{-3}}{2}\right]^2\right|^{\frac{1}{2}} \\ &= \frac{1}{2}\left|\left(-\sqrt{-3}\right)^2\right|^{\frac{1}{2}} \\ &= \frac{\sqrt{3}}{2}. \end{aligned}$$

Observe que o reticulado $\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})$ apresenta os mesmos geradores v_1 e v_2 e o mesmo volume que o reticulado hexagonal. A matriz geradora desse reticulado é

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

Exemplo 3.1.4. *Seja o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, onde $i^2 = -1$. Pelo Teorema 1.3.9 temos que seu anel dos inteiros é $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[i]$ com $\mathbb{Z}$-base $\{1, i\}$. Como $\mathbb{K}$ é totalmente imaginário pela Definição 1.3.13, $d = -1 < 0$, segue que $r_1 = 0$ e $r_2 = 1$. Seja $\mathcal{U}$ um ideal principal de $\mathbb{Z}[i]$, gerado por $(1 - 2i)$ de norma $\mathcal{N}(\mathcal{U}) = 5$. Assim, dado $x \in \mathcal{U}$, temos que $x = (1 - 2i)(a + bi)$, onde $a, b \in \mathbb{Z}$, ou seja, $x = (2b + a)(b - 2a)i$, logo a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathcal{U}) \subset \mathbb{R}^2$ é dada por*

$$\begin{aligned} \sigma_{\mathbb{K}}(\mathcal{U}) &= (\Re(\sigma_1((2b + a) + (b - 2a)i)), \Im(\sigma_1((2b + a) + (b - 2a)i)) \\ &= (\Re((2b + a) + (b - 2a)i), \Im((2b + a) + (b - 2a)i) \\ &= (2b + a, b - 2a) \\ &= a(1, -2) + b(2, 1), \end{aligned}$$

é um reticulado gerado pelos vetores $v_1 = (1, -2)$ e $v_2 = (2, 1)$, com a região fundamental descrita na figura abaixo

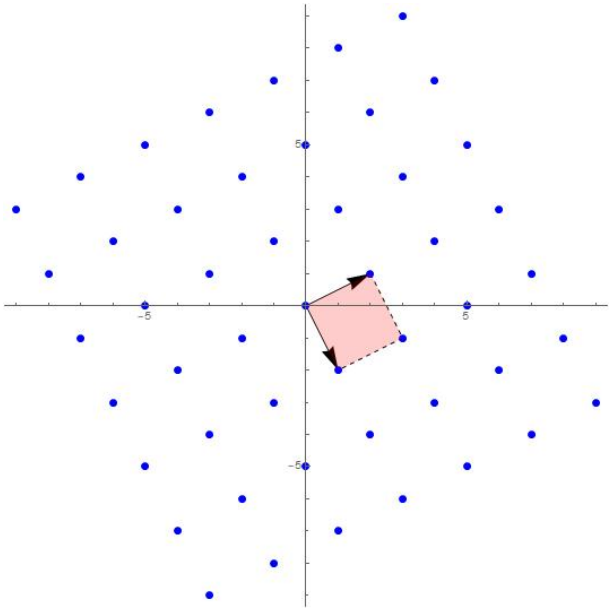


Figura 15 – Reticulado algébrico gerado pelos vetores $v_1 = (1, -2)$ e $v_2 = (2, 1)$.
Fonte: Autor.

O volume do reticulado é dado por

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

Portanto,

$$vol(\sigma_{\mathbb{K}}(\mathcal{U})) = vol(\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})) \cdot \mathcal{N}(\mathcal{U}) = 1 \cdot 5 = 5.$$

E, a matriz geradora do reticulado é

$$M = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}.$$

Exemplo 3.1.5. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$ corpo ciclotômico e seu anel dos inteiros é $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$. Como sabemos $\mathbb{K}$ é totalmente imaginário, implica que $r_1 = 0$ e $r_2 = 1$, temos que a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})$ é dada pelo Exemplo 3.1.1 gerado pelos vetores $v_1 = (1, 0)$ e $v_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, com região fundamental descrita na figura abaixo:*

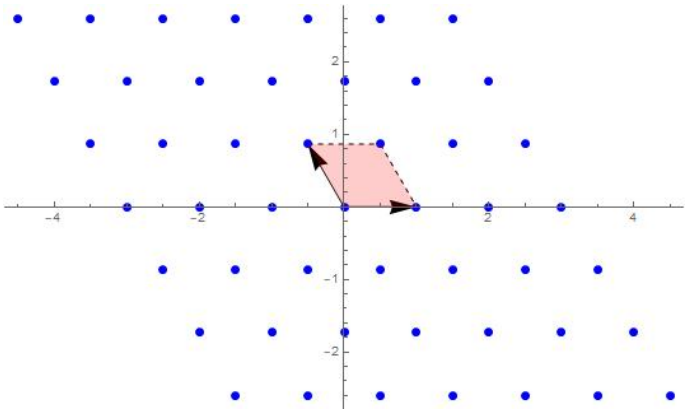


Figura 16 – Reticulado algébrico gerado pelos vetores $v_1 = (1, 0)$ e $v_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.
Fonte: Autor.

O volume do reticulado será

$$\begin{aligned} vol(\sigma_{\mathbb{K}}(\mathbb{I}_{\mathbb{K}})) &= 2^{-1} \left| det \left[\begin{pmatrix} \sigma_1(1) & \sigma_(1) \\ \sigma_2(\zeta_3) & \sigma_2(\zeta_3) \end{pmatrix} \right]^2 \right|^{\frac{1}{2}} \\ &= \frac{1}{2} \left| det \left[\begin{pmatrix} 1 & 1 \\ -\frac{1}{2} - \frac{\sqrt{3}}{2}i & -\frac{1}{2} + \frac{\sqrt{3}}{2}i \end{pmatrix} \right]^2 \right|^{\frac{1}{2}} \\ &= \frac{\sqrt{3}}{2}. \end{aligned}$$

E, a matriz geradora do reticulado é dada por

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

Podemos obter uma expressão para o cálculo da densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{U})$ a partir da expressão dada pela Definição 2.3.5.

Proposição 3.1.1. *[35] Se $\mathbb{K}$ é um corpo de números de grau n, $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$, $\mathbb{I}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K}$, $\mathcal{U}$ um ideal não nulo de $\mathbb{K}$ e r_2 a metade do número de monomorfismo imaginário, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{U})$ é dado por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{U}))^n}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})}, \tag{3.1}$$

onde $\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2} min\{|\sigma_{\mathbb{K}}(x)|, x \in \mathcal{U}, x \neq 0\}$.

O objetivo é melhorar um pouco mais a Equação 3.1, para isso iniciamos com a seguinte proposição.

Proposição 3.1.2. *[35] Se $\mathbb{K}$ é um corpo de números de grau n e $x \in \mathbb{K}$, então*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}} \cdot Tr(x\overline{x}),$$

onde

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

Demonstração: Seja $\sigma_1, ..., \sigma_n$ os n monomorfismos de $\mathbb{K}$ de tal forma que $r_1 + 2r_2 = n$, onde r_1 são os monomorfismos reais e r_2 a metade dos monomorfismos imaginários. Assim, para $x \in \mathbb{K}$ temos pelo homomorfismo canônico que

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

como $\sigma_{\mathbb{K}}(x) \subset \mathbb{R}^n$, segue que

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

Observe que

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

para $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. Assim,

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

Se $r_1 = 0$, ou seja, $\mathbb{K}$ for totalmente imaginário, então

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

e uma vez que $\overline{\sigma}$ é a conjugação complexa, temos que $\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, ..., r_2$. Logo

$$2|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + ... + \sigma_{r_1}(x\overline{x})\sigma_{r_1+1}(x\overline{x}) + ... + \sigma_{r_2+r_2}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}),$$

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

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

Agora, se $r_2 = 0$, ou seja, $\mathbb{K}$ for totalmente real, teremos

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

e como $\sigma_j(x) = (\overline{\sigma} \circ \sigma_j)(x) = (\sigma_j \overline{x})$, segue que

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

Logo,

$$|\sigma_{\mathbb{K}}|^2 = \sigma_1(x\overline{x}) + ... + \sigma_{r_1}(x\overline{x}) = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = 1 \cdot Tr(x\overline{x}),$$

o que conclui a demonstração. ■

Observação 3.1.1. *Pela Proposição 3.1.2, temos que*

$$\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2}\ min\{|\sigma_{\mathbb{K}}(x)|, x \in \mathcal{U}, x \neq 0\},$$

pode ser escrito do seguinte forma

$$\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2} min\{\sqrt{c_{\mathbb{K}} \cdot Tr(x\overline{x})}, x \in \mathcal{U},\ x \neq 0\},$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, & se \quad \mathbb{K}\ for\ totalmente\ real \\ \frac{1}{2}, & se \quad \mathbb{K}\ for\ totalmente\ imaginário. \end{cases}$$

Proposição 3.1.3. *[36] Seja $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário. Se $\mathbb{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$ e $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{U})$ é dado por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2^n |\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}} \cdot \frac{t^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})}, \tag{3.2}$$

onde, $t = min\{Tr(x\overline{x}); x \in \mathcal{U}, x \neq 0\}$ e $\mathcal{N}(\mathcal{U})$ é a norma do ideal de $\mathcal{U}$.

Demonstração: Suponhamos que $\mathbb{K}$ seja um corpo totalmente real. Assim, $r_2 = 0$ e pela Observação 3.1.1, temos que

$$\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2} min\{\sqrt{Tr(x\overline{x})}, x \in \mathcal{U}, x \neq 0\}.$$

E, como $t = min\{Tr(x\overline{x}), x \in \mathcal{U}, x \neq o\}$ segue que

$$\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2}\sqrt{t}.$$

Assim, pela Equação 3.1, tem-se que

$$\delta(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{2^0(\frac{1}{2}\sqrt{t})^n}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{2^{-n}(\sqrt{t})^n}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{1}{2^n|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}} \cdot \frac{t^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})}.$$

Agora, suponhamos que $\mathbb{K}$ seja um corpo totalmente imaginário. Pela Observação 3.1.1 temos,

$$\rho(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2} min\left\{\sqrt{\frac{1}{2} \cdot Tr(x\overline{x})}, x \in \mathcal{U}, x \neq 0\right\} = \frac{1}{2} \cdot \sqrt{\frac{1}{2}t}.$$

Além disso, como $r_1 = 0$ e $n = r_1 + 2r_2 \Rightarrow r_2 = \frac{n}{2}$. Assim, pela Equação 3.1, temos

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

Portanto, se $\mathbb{K}$ for um corpo totalmente real ou totalmente imaginário, temos que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{U})$ será a mesma. ■

A seguir apresentamos um exemplo para o cálculo da densidade de centro de um reticulado construído a partir do homomorfismo canônico.

Exemplo 3.1.6. *Seja o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$. Pelo Teorema 1.3.9 temos que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \ | a, b \in \mathbb{Z}\}$ é o anel dos inteiros de $\mathbb{K}$ com base integral $\{1, \sqrt{-5}\}$. E pela Proposição 1.3.14, o discriminante é $\mathcal{D}_{\mathbb{K}} = -20$, tomando um ideal $\mathcal{U} = \mathbb{I}_{\mathbb{K}}$, então pela Proposição 1.3.7 temos $\mathcal{N}(\mathcal{U}) = 1$. Assim, se $x \in \mathbb{I}_{\mathbb{K}}$, então $x = a + b\sqrt{-5}$ e $x\overline{x} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + b^2$. Logo, $Tr(x\overline{x}) = 2(a^2 + b^2)$ e então $t = 2$ quando $a=1$ e $b=0$. Assim,*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{U})) = \frac{1}{2^2 \cdot |-20|^{\frac{1}{2}}} \cdot \frac{2^{\frac{2}{2}}}{1} = \frac{2}{4\sqrt{20}} = \frac{1}{2\sqrt{20}} \cong 0.11.$$

Embora o homomorfismo de Minkowski seja o método mais conhecido para construção de reticulados provenientes de corpo de números, outros homomorfismos obtidos como perturbações do canônico começaram a ser estudados visando obter reticulados algébricos mais densos. Nas seções seguintes apresentamos as perturbações σ_α e $\sigma_{2\alpha}$.

3.2 Reticulados algébricos via perturbação σ_α

Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os homomorfismos de $\mathbb{K}$ em $\mathbb{C}$, ordenados de modo que σ_i é real para $i = 1, ..., r_1$ e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_j+j}}$ para $j = 1, ..., r_2$ onde r_2 representa a metade dos homomorfismos imaginários e $r_1 + 2r_2 = n$. Nessa seção apresentaremos a perturbação σ_α do homomorfismo canônico, temos que esta perturbação também irá gerar reticulados no $\mathbb{R}^n$, e partir dessa perturbação iremos obter reticulados rotacionados nas dimensões $2, 4$ e 8. Para apresentar esta perturbação, iniciamos com a definição de elemento totalmente positivo.

Definição 3.2.1. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Um elemento $\alpha \in \mathbb{K}$ tal que $\sigma_i(\alpha) \in \mathbb{R}^+$, $\alpha_i = \sigma_i(\alpha)$, para todo $i = 1, ..., r_1 + r_2$ é chamado de* ***totalmente positivo****.*

Definição 3.2.2. *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $\alpha \in \mathbb{K}$ um elemento totalmente real e totalmente positivo. O homomorfismo $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^n$ dado por*

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x)), ..., \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))),$$

é chamado de ***perturbação do homomorfismo canônico*** *ou* ***homomorfismo torcido****, onde as notações $\Re(x)$ e $\Im(x)$ representam a parte real e imaginária do número complexo x, respectivamente.*

O próximo Teorema 3.2.1 caracteriza o volume do reticulado obtido através da perturbação σ_α do homomorfismo canônico.

Teorema 3.2.1. *[14] Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo. Se $M \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, ..., x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, com volume dado por*

$$vol(\sigma_\alpha(M)) = b_\alpha \left| det_{1 \leqslant j,\ \mathbb{K} \leqslant n}(\sigma_j(x_{\mathbb{K}})) \right|,$$

onde

$$b_\alpha = \begin{cases} (\mathcal{N}(\alpha))^{\frac{1}{2}}, & se \quad \mathbb{K} \text{ for totalmente real} \\ 2^{-\frac{n}{2}} \cdot (\mathcal{N}(\alpha))^{\frac{1}{2}}, & se \quad \mathbb{K} \text{ for totalmente imaginário,} \end{cases}$$

e $\mathcal{N}(\alpha)$ é a norma do elemento $\alpha \in \mathbb{K}$.

Seja $\{x_1, x_2, ..., x_n\}$ uma $\mathbb{Z}$-base de $\mathcal{U}$. O reticulado $\sigma_\alpha(\mathcal{U})$ tem matriz geradora dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_1) & \cdots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_1) \\ \sqrt{\alpha_1}\sigma_1(x_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_2) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_2) & \cdots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_2) \\ \sqrt{\alpha_1}\sigma_1(x_3) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_3) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_3) & \cdots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_3) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sqrt{\alpha_1}\sigma_1(x_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) & \sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_n) & \cdots & \sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_n) \end{pmatrix}.$$

Exemplo 3.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ um corpo quadrático. O elemento $\alpha = 5 + 2\sqrt{5} \in \mathbb{K}$ é totalmente real e totalmente positivo. Sendo assim, a perturbação σ_α está bem definida, dada por*

$$\begin{aligned} \sigma_\alpha : \mathbb{K} &\to \mathbb{R}^2 \\ a + b\sqrt{5} &\mapsto ((\sqrt{5+2\sqrt{5}})(a+b\sqrt{5}), (\sqrt{5-2\sqrt{5}})(a-b\sqrt{5})). \end{aligned}$$

Pelo Teorema 1.3.9, temos que $5 \equiv 1 (mod\ 4)$, então $\mathbb{I}_\mathbb{K} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, onde $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral e pelo Teorema 3.2.1 $\sigma_\alpha(\mathbb{I}_\mathbb{K})$ é um reticulado em $\mathbb{R}^2$. Pelo reticulado σ_α ser totalmente real temos que $b_\alpha = \mathcal{N}(\sqrt{5+2\sqrt{5}})^{\frac{1}{2}} = (\sqrt{5+2\sqrt{5}})(\sqrt{5-2\sqrt{5}}) = (5+2\sqrt{5})(5-2\sqrt{5}) = 5$ e os monomorfismos são $\sigma_1 : \frac{1+\sqrt{5}}{2} \mapsto \frac{1+\sqrt{5}}{2}$ e $\sigma_2 : \frac{1+\sqrt{5}}{2} \mapsto \frac{1-\sqrt{5}}{2}$, então o volume do reticulado é

$$vol(\sigma_\alpha(\mathbb{I}_\mathbb{K})) = (5)^{\frac{1}{2}} \cdot \left| det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix} \right| = 5^{\frac{1}{2}} \cdot \sqrt{5} = 5.$$

Corolário 3.2.1. *[14] Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathcal{D}_\mathbb{K}$ é o discriminante de $\mathbb{K}$, $\mathbb{I}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$ e $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_\mathbb{K}$, então $\sigma_\alpha(\mathbb{I}_\mathbb{K})$ e $\sigma_\alpha(\mathcal{U})$ são reticulados, com respectivos volumes*

$$vol(\sigma_\alpha(\mathbb{I}_\mathbb{K})) = b_\alpha \left|\mathcal{D}_\mathbb{K}\right|^{\frac{1}{2}} \qquad e \qquad vol(\sigma_\alpha(\mathcal{U})) = b_\alpha \left|\mathcal{D}_\mathbb{K}\right|^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U}),$$

onde $\mathcal{N}(\alpha)$ é a norma do elemento α, $\mathcal{N}(\mathcal{U})$ é a norma do ideal $\mathcal{U}$ e b_α é como no Teorema 3.2.1.

Exemplo 3.2.2. *Do Exemplo 3.2.1, temos que $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ é um corpo quadrático e $\alpha = 5 + 2\sqrt{5} \in \mathbb{K}$, totalmente real e totalmente positivo. Pela Proposição 1.3.14 o discriminante é $\mathcal{D}_\mathbb{K} = 5$. Como $\mathbb{K}$ é totalmente real, temos que $b_\alpha = (\mathcal{N}(\alpha))^{\frac{1}{2}} = 5^{\frac{1}{2}}$. O volume é dado pelo Corolário 3.2.1,*

$$vol(\sigma_\alpha(\mathbb{I}_\mathbb{K})) = b_\alpha \left|\mathcal{D}_\mathbb{K}\right|^{\frac{1}{2}} = 5^{\frac{1}{2}} \cdot |5|^{\frac{1}{2}} = 5,$$

como no Exemplo 3.2.1.

Proposição 3.2.1. *[14] Se $\mathbb{K}$ é um corpo de números de grau n cujo discriminante é $\mathcal{D}_\mathbb{K}$ e $\mathcal{U}$ um ideal não nulo do anel dos inteiros $\mathbb{I}_\mathbb{K}$, então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{U})$ é dado por*

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{(\rho(\sigma_\alpha(\mathcal{U})))^n}{b_\alpha \cdot \sqrt{|\mathcal{D}_\mathbb{K}|} \cdot \mathcal{N}(\mathcal{U})}, \tag{3.3}$$

onde $\rho(\sigma_\alpha(\mathcal{U})) = \frac{1}{2} min\{|\sigma_\alpha(x)|, x \in \mathcal{U}, x \neq 0\}$.

O nosso objetivo é melhorar a expressão do Corolário 3.2.1, que determina a densidade de centro do reticulado $\sigma_\alpha(\mathcal{U})$, para isto usaremos a Proposição 3.2.2 e a Observação 3.2.1 que veremos a seguir.

Proposição 3.2.2. *[36] Se $\mathbb{K}$ é um corpo de números de grau n, $x \in \mathbb{K}$ e $\alpha \in \mathbb{K}$ totalmente positivo, então*

$$|\sigma_\alpha(x)|^2 = c_\alpha \cdot Tr(\alpha x \overline{x}),$$

onde

$$c_\alpha = \begin{cases} 1, & se \quad \mathbb{K} \text{ for totalmente real} \\ \frac{1}{2}, & se \quad \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Observação 3.2.1. *Pela Proposição 3.2.2 temos que*

$$\rho(\sigma_\alpha(\mathcal{U})) = \frac{1}{2} min\left\{|\sigma_\alpha(x)|, x \in \mathcal{U}, x \neq 0\right\},$$

pode ser escrito da seguinte forma

$$\rho(\sigma_\alpha(\mathcal{U})) = \frac{1}{2} min\{\sqrt{c_\alpha Tr(\alpha x \overline{x})}, x \in \mathcal{U}, x \neq 0\}.$$

Na próxima Proposição 3.2.3 veremos que a densidade de centro do reticulado $\sigma_\alpha(\mathcal{U})$ será a mesma se $\mathbb{K}$ for totalmente real ou totalmente imaginário.

Proposição 3.2.3. *[14] Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathbb{I}_\mathbb{K}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_\mathbb{K}$ o discriminante de $\mathbb{K}$ e $\mathcal{U}$ é um ideal não nulo de $\mathbb{K}$, então a densidade de centro do reticulado $\sigma_\alpha(\mathcal{U})$ é dado por*

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{1}{2^n \left(\mathcal{N}(\alpha) |\mathcal{D}_\mathbb{K}|\right)^{\frac{n}{2}}} \cdot \frac{t_\alpha^{\frac{1}{2}}}{\mathcal{N}(\mathcal{U})}, \tag{3.4}$$

onde o $t_\alpha = min\{Tr(\alpha x \overline{x}), x \in \mathcal{U}, x \neq 0\}$, $\mathcal{N}(\alpha)$ é a norma do elemento α.

Demonstração: Suponhamos que $\mathbb{K}$ seja um corpo totalmente real, então temos que $r_2 = 0$, $b_\alpha = (\mathcal{N}(\alpha))^{\frac{1}{2}}$ e pela Observação 3.2.1 temos,

$$\rho(\sigma_\alpha(\mathcal{U})) = \frac{1}{2} min\{\sqrt{1 \cdot Tr(\alpha x \overline{x})}, x \in \mathcal{U}, x \neq 0\}.$$

E, como $t_\alpha = min\{Tr(\alpha x \overline{x}), x \in \mathcal{U}, x \neq 0\}$, segue que $\rho_\alpha(\mathcal{U})) = \frac{1}{2}\sqrt{t_\alpha}$. Assim pela 3.2.1, temos

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{(\frac{1}{2}\sqrt{t_\alpha})^n}{(\mathcal{N}(\alpha))^{\frac{1}{2}} \cdot |\mathcal{D}_\mathbb{K}|^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{2^{-n}(\sqrt{t_\alpha})^n}{(\mathcal{N}(\alpha) \cdot |\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{1}{2^n (\mathcal{N}(\alpha) \cdot |\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})}.$$

Agora, suponhamos que $\mathbb{K}$ seja um corpo totalmente imaginário. Pela Observação 3.2.1, temos que

$$\rho(\sigma_\alpha(\mathcal{U})) = \frac{1}{2} min\left\{\sqrt{\frac{1}{2} Tr(\alpha x \overline{x})}, x \in \mathcal{U}, x \neq 0\right\} = \frac{1}{2}\sqrt{\frac{1}{2} t_\alpha}.$$

Além disso, $b_\alpha = 2^{-\frac{n}{2}} \cdot (\mathcal{N}(\alpha))^{\frac{1}{2}}$ e, como $r_1 = 0$ e $r_1 + 2r_2 = n$ segue que $r_2 = \frac{n}{2}$. Assim, pela Equação 3.2.1, temos

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{(\frac{1}{2}\sqrt{\frac{1}{2}t_\alpha})^n}{2^{-\frac{n}{2}}(\mathcal{N}(\alpha))^{\frac{1}{2}}|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathcal{U})} = \frac{2^{-n}2^{-\frac{n}{2}}(\sqrt{t_\alpha})^n}{2^{-\frac{n}{2}}(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathcal{U})} = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})}.$$

Portanto, se $\mathbb{K}$ for um corpo totalmente real ou totalmente imaginário temos que a densidade de centro do reticulado $\sigma_\alpha(\mathcal{U})$ é a mesma dada por

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{1}{2^n\left(\mathcal{N}(\alpha)\,|\mathcal{D}_\mathbb{K}|\right)^{\frac{n}{2}}} \cdot \frac{t_\alpha^{\frac{1}{2}}}{\mathcal{N}(\mathcal{U})}.$$

■

A seguir, apresentaremos um exemplo do cálculo da densidade de centro utilizando a perturbação σ_α e, comparando com a mesma construção sem perturbação, ou seja, utilizando o homomorfismo canônico, percebemos que com a perturbação σ_α temos uma densidade melhor.

Exemplo 3.2.3. *Sejam o corpo $\mathbb{K} = \mathbb{Q}(\zeta_4)$, $\mathcal{U} = (1-\zeta_4)\mathbb{I}_\mathbb{K}$ um ideal de $\mathbb{I}_\mathbb{K} = \mathbb{Z}[\zeta_4]$, a base integral $\{1, \zeta_4\}$ dada pelo Teorema 1.3.11 e $\alpha = 3$. Pelo Teorema 1.3.10 temos $[\mathbb{K} : \mathbb{Q}] = 2$. Pelo Teorema 1.3.13 temos que $\mathcal{D}_\mathbb{K} = 4$ e pela Definição 1.3.7 temos que $\mathcal{N}(\alpha) = 9$. Pela Proposição 1.3.18 temos que os monomorfismos são $\sigma_i(\zeta_4) = \zeta_4^1$, com $i = 1, 3$. A norma do ideal $\mathcal{U}$ é $\mathcal{N}(\mathcal{U}) = 2$. Dado $x \in \mathcal{U}$, podemos escrever $x = (1-\zeta_4)\cdot(a_0 + a_1\zeta_4)$ onde $a_0, a_1 \in \mathbb{Z}$. Assim, $Tr(x\overline{x}) = 2(a_0^2 + a_1^2)$ e $Tr(\alpha x\overline{x}) = 12(a_0^2 + a_1^2)$. Portanto, $t = min\{Tr(x\overline{x}); x \in \mathcal{U}, x \neq 0\} = 2$ e $t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, x \neq 0\} = 12$, e as densidades de centro são dadas por*

- *Com perturbação*

$$\delta(\sigma_\alpha(\mathcal{U})) = \frac{1}{2^n(\mathcal{N}(\alpha)\cdot|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = 0.25.$$

- *Sem perturbação*

$$\delta(\sigma_\mathbb{K}(\mathcal{U})) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = 0.125.$$

3.3 Reticulados algébricos via perturbação $\sigma_{2\alpha}$

Apresentaremos nesta seção a perturbação $\sigma_{2\alpha}$ do homomorfismo canônico. Obteremos reticulados no $\mathbb{R}^n$ a partir desta perturbação. Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, ordenados de modo que σ_i é real para $i = 1, ..., r_1$ e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, ..., r_2$, onde r_2 representa metade dos homomorfismos imaginários.

Definição 3.3.1. *Seja $\alpha \in \mathbb{K}$ totalmente positivo. A* ***perturbação*** $\sigma_{2\alpha} : \mathbb{K} \to \mathbb{R}^n$ *do* ***homomorfismo canônico*** *é definida como*

$$\sigma_{2\alpha}(x) = \left(\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x)), ..., \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))\right),$$

onde as notações $\Re(x)$ e $\Im(x)$ representam a parte real e imaginária do número complexo x, respectivamente.

Teorema 3.3.1. *[6] Seja $\mathbb{K}$ um corpo número de grau n. Se $M \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, ..., x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{2\alpha}(M)$ é um reticulado no $\mathbb{R}^n$ com volume dado por*

$$vol(\sigma_{2\alpha}(M)) = (\mathcal{N}(\alpha))^{\frac{1}{2}} \cdot |det_{1\leqslant j,\mathbb{K}\leqslant n}(\sigma_j(x_{\mathbb{K}}))|,$$

onde $\mathcal{N}(\alpha)$ é a norma do elemento α.

Corolário 3.3.1. *[6] Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$. Se $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$, $\mathbb{I}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$, então $\sigma_{2\alpha}(\mathbb{I}_{\mathbb{K}})$ e $\sigma_{2\alpha(\mathcal{U})}$ são reticulados com respectivos volumes,*

$$vol(\sigma_{2\alpha}(\mathbb{I}_{\mathbb{K}})) = (\mathcal{N}(\alpha)\,|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}} \quad e \quad vol(\sigma_{2\alpha}(\mathcal{U})) = (\mathcal{N}(\alpha)\,|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U}),$$

onde $\mathcal{N}(\alpha)$ é a norma do elemento α e $\mathcal{N}(\mathcal{U})$ é a norma do ideal $\mathcal{U}$.

Seja $\{x_1, x_2, ..., x_n\}$ uma $\mathbb{Z}$-base de $\mathcal{U}$. O reticulado $\sigma_{2\alpha}(\mathcal{U})$ tem matriz geradora dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_1) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_1) \\ \sqrt{\alpha_1}\sigma_1(x_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_2) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_2) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_2) \\ \sqrt{\alpha_1}\sigma_1(x_3) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_3) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_3) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_3) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sqrt{\alpha_1}\sigma_1(x_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x_n) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x_n) \end{pmatrix}.$$

Exemplo 3.3.1. *Do Exemplo 3.2.2, temos que $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ é um corpo quadrático e $\alpha = 5 + 2\sqrt{5} \in \mathbb{K}$ totalmente real e totalmente positivo. Pela Proposição 1.3.14 o discriminante $\mathcal{D}_{\mathbb{K}} = 5$. A norma de α é $\mathcal{N}(\alpha) = 5$. O volume do reticulado é dado pelo Corolário 3.3.1,*

$$vol(\sigma_{2\alpha}(\mathbb{I}_{\mathbb{K}})) = (\mathcal{N}(\alpha) \cdot |\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}} = (5 \cdot 5)^{\frac{1}{2}} = 5.$$

Corolário 3.3.2. *[14] Se $\mathbb{K}$ um corpo de números de grau n, $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$, $\mathbb{I}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$, $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$ e $\mathcal{N}(\mathcal{U})$ a norma do ideal $\mathcal{U}$, então a densidade de centro do reticulado $\sigma_{2\alpha}(\mathcal{U})$ é dada por*

$$\delta(\sigma_{2\alpha}(\mathcal{U})) = \frac{(\rho(\sigma_{2\alpha}(\mathcal{U})))^n}{(|\mathcal{D}_{\mathbb{K}}|\,\mathcal{N}(\alpha))^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})}, \tag{3.5}$$

onde ρ é o raio do empacotamento do reticulado dado por

$$\rho(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2} min\{|\sigma_{2\alpha}(x)|, x \in \mathcal{U}, x \neq 0\}.$$

O nosso objetivo é melhorar a Equação 3.5, e para isso usaremos a Proposição 3.3.1 e a Observação 3.3.1 que veremos a seguir.

Proposição 3.3.1. *[14] Se $\mathbb{K}$ é um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo, então*

$$|\sigma_{2\alpha}(x)|^2 = Tr(\alpha x\overline{x}),$$

onde $\overline{x}$ é o conjugado complexo do $x \in \mathbb{K}$.

Demonstração: Sejam $\sigma_1, ..., \sigma_n$ os n monomorfismos de $\mathbb{K}$ de tal forma que $r_1 + 2r_2 = n$, onde r_1 são os monomorfismos reais e r_2 a metade dos monomorfismos imaginários. Assim, para cada $x \in \mathbb{K}$ temos pela perturbação $\sigma_{2\alpha}$ do homomorfismo canônico que

$$\sigma_{2\alpha}(x) = \left(\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1}}\Re\sigma_{r_1+1}(x), ..., \sqrt{2\sigma_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x)\right).$$

Como $\sigma_{2\alpha}(x) \in \mathbb{R}^n$, segue que

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

Observe que $[\Re(\sigma_j(x))]^2 + [\Im(\sigma_j(x))]^2 = \sigma_j(x) \cdot \overline{\sigma_j(x)} = \sigma_j(x\overline{x})$, para $r_{1+1} \leqslant j \leqslant r_1 + r_2$. Assim,

$$|\sigma_{2\alpha}(x)|^2 = \alpha_1(\sigma_1(x))^2 + ... + \alpha_{r_1}(\sigma_{r_1}(x))^2 + 2\alpha_{r_1+1}\sigma_{r_1+1}(x\overline{x}) + + ... + 2\alpha_{r_1+r_2}\sigma_{r_1+r_2}(x\overline{x}).$$

Se $r_1 = 0$ ou seja, $\mathbb{K}$ for totalmente imaginário, então

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

pois sendo $\overline{\sigma}$ a conjugação complexa, temos que $\sigma_{r_2+j}(\alpha x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(\alpha x\overline{x}) = \sigma_j(\alpha x\overline{x})$, para $j = 1, ..., r_2$. Logo,

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

e como os $\sigma_i(\alpha x\overline{x})$ são os conjugados de $(\alpha x\overline{x})$, segue que $|\sigma_{2\alpha}(x)|^2 = \frac{1}{2}Tr(\alpha x\overline{x})$. Se $r_2 = 0$, ou seja, $\mathbb{K}$ totalmente real, teremos $|\sigma_{2\alpha}(x)|^2 = \alpha_1(\sigma_1(x))^2 + ... + \alpha_{r_1}(\sigma_{r_1}(x))^2$, e como $\sigma_j(x) = (\overline{\sigma} \circ \sigma_j)(x) = \sigma_j(\overline{x})$, segue que $\sigma_j(x\overline{x}) = \sigma_j(x)\sigma_j(\overline{x}) = \sigma_j(x)\sigma_j(x) = (\sigma_j(x))^2$.

Logo,

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

O que conclui a demonstração. ■

Observação 3.3.1. *Pelo Corolário 3.3.2 e pela Proposição 3.3.1, temos que*

$$\rho(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2}min\{|\sigma_{2\alpha}(x)|, x \in \mathcal{U}, x \neq 0\},$$

pode ser escrito da seguinte forma:

$$\rho(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2}min\{\sqrt{Tr(\alpha x\overline{x})}, x \in \mathcal{U}, x \neq 0\}.$$

Na próxima Proposição 3.3.2 veremos que a densidade de centro de reticulados $\sigma_{2\alpha}(\mathcal{U})$ será a mesma independente se $\mathbb{K}$ for totalmente real ou totalmente imaginário.

Proposição 3.3.2. *[6] Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathbb{I}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$ e $\mathcal{U}$ um ideal não nulo de $\mathbb{I}_{\mathbb{K}}$, então a densidade de centro do reticulado $\sigma_{2\alpha}(\mathcal{U})$ é dada por*

$$\delta(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}}} \cdot \frac{t_{2\alpha}^{n/2}}{\mathcal{N}(\mathcal{U})}, \tag{3.6}$$

Demonstração: Pela Observação 3.3.1 temos,

$$\rho(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2}min\{\sqrt{Tr(\alpha x\overline{x})}, x \in \mathcal{U}, x \neq 0\}.$$

E, como $t_{2\alpha} = min\{Tr(\alpha x\overline{x}), x \in \mathcal{U}, x \neq 0\}$, segue que $\rho(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2}\sqrt{t_{2\alpha}}$. Assim, pela 3.5, temos

$$\delta(\sigma_{2\alpha}(\mathcal{U})) = \frac{(\frac{1}{2}\sqrt{t_{2\alpha}})^n}{(|\mathcal{D}_{\mathbb{K}}| \cdot \mathcal{N}(\alpha))^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{2^{-n}\sqrt{t_{2\alpha}})^n}{(|\mathcal{D}_{\mathbb{K}}| \cdot \mathcal{N}(\alpha))^{\frac{1}{2}} \cdot \mathcal{N}(\mathcal{U})} = \frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}} \cdot \frac{t_{2\alpha}^{n/2}}{\mathcal{N}(\mathcal{U})}.$$

Portanto, $\mathbb{K}$ é um corpo totalmente real ou totalmente imaginário, temos que a densidade de centro do reticulado $\sigma_{2\alpha}(\mathcal{U})$ é a mesma. ■

A seguir, cederemos um exemplo de cálculo da densidade de centro usando a perturbação $\sigma_{2\alpha}$.

Exemplo 3.3.2. *Sejam o corpo ciclotômico* $\mathbb{K} = \mathbb{Q}(\zeta_6)$, $\mathcal{U} = \mathbb{I}_{\mathbb{K}}$, *um ideal de* $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_6]$ *e, uma base integral* $\{1, \zeta_6\}$ *dada pelo Teorema 1.3.11 e* $\alpha = 2$. *Pelo Teorema 1.3.10 temos que* $[\mathbb{K} : \mathbb{Q}] = 2$. *Pelo Teorema 1.3.13 temos que o discriminante é* $\mathcal{D}_{\mathbb{K}} = 3$ *e a norma de* α *é* $\mathcal{N}(\alpha) = 4$ *dada pela Definição 1.3.7. Pela Proposição 1.3.18 temos que* $\sigma_i(\zeta) = \zeta^i$, *com* $i = 1, 5$. *A norma do ideal* $\mathcal{U}$ *é* $\mathcal{N}(\mathcal{U}) = 1$. *Dado* $x \in \mathcal{U}$, *podemos escrever* $x = (1 - \zeta_6) \cdot (a_0 + a_1\zeta_6)$ *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 4(a_0^2 + a_0a_1 + a_1^2)$ *e* $Tr(x\overline{x}) = 2(a_0^2 + a_0a_1 + a_1^2)$. *Portanto* $t_{2\alpha} = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, x \neq 0\} = 4$ *e* $t = min\{Tr(x\overline{x}); x \in \mathcal{U}, x \neq 0)\} = 2$, *com* $a_0 = 0$ *e* $a_1 = 1$. *Portanto, a densidade de centro do reticulado é*

$$\delta(\sigma_{2\alpha}(\mathcal{U})) = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}}} \cdot \frac{t^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = 0.28868.$$

Capítulo 4

Construção de reticulados algébricos em dimensão $2, 4$ e 8.

Neste capítulo apresentamos uma construção de reticulados algébricos nas dimensões $2, 4$ e 8 que possuem densidade de centro ótima para estas dimensões, ou seja, coincidem com a densidade de centro dos reticulados A_2, D_4 e E_8, que como sabemos, são os reticulados mais densos nas dimensões 2, 4 e 8, respectivamente.

A construção apresentada será realizada da seguinte forma. Consideramos um corpo ciclotômico $\mathbb{K}$ de grau n. Neste trabalho $n = 2, 4$ ou 8. Pelos resultados apresentados no Capítulo 1, podemos obter o seu anel dos inteiros $\mathbb{I}_{\mathbb{K}}$, uma base integral, seus monomorfismos e calcular seu discriminante. Daí, aplicando a perturbação σ_α do homomorfismo canônico, sabemos pelo Capítulo 3 que, a imagem deste homomorfismo aplicada em um ideal dos anéis dos inteiros é um reticulado algébrico no $\mathbb{R}^n$. Além disso, temos uma expressão que calcula a densidade de centro deste reticulado. Assim, se queremos obter reticulados que possuam a mesma densidade de centro dos reticulados mais densos A_2, D_4 e E_8, basta igualarmos a expressão da densidade de centro ao valor desejado e obter os valores convenientes para os parâmetros que ainda necessitam ser calculados na expressão. Esta estratégia de construção de reticulados algébricos densos foi utilizada em [3]. Neste trabalho, utilizamos esta técnica com corpos de números diferentes dos utilizados no artigo citado e obtemos novos exemplos de reticulados algébricos densos nessas dimensões.

4.1 Dimensão 2

Nessa seção, o objetivo será construir reticulados algébricos na dimensão 2 com densidade de centro ótima. Para tal construção, precisamos de um corpo de números de grau $n = 2$. Dessa forma usaremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_3)$ que possui dimensão 2, pois pela Observação 1.3.12 temos que $\varphi(3) = 2$. Temos através do Teorema 1.3.10 que

$[\mathbb{K} : \mathbb{Q}] = 2$ e, do Teorema 1.3.11 que o anel dos inteiros deste corpo é dado por $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ e uma base integral $\{1, \zeta_3\}$. Pela Proposição 1.3.19 o discriminante $\mathcal{D}_{\mathbb{K}} = -3$, e pela Proposição 1.3.18 temos que os monomorfismos são $\sigma_i(\zeta_3) = \zeta_i$, com $i = 1, 2$. Queremos encontrar reticulados cujas densidade de centro seja a mesma do reticulado A_2, ou seja, $\frac{1}{2\sqrt{3}}$, utilizando a perturbação σ_α do homomorfismo canônico, que para a dimensão 2 é dado por

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), (\sqrt{\sigma_2(\alpha)}\sigma_2(x)),$$

com $\sigma_i(\alpha) > 0, \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2$.

A ideia é substituir os valores obtidos e usar a Equação 3.4 que expressa a densidade de centro para reticulados algébricos obtidos a partir da perturbação σ_α do homomorfismo canônico. Como já temos $n = 2$ e $\mathcal{D}_{\mathbb{K}} = -3$, vamos igualar a fórmula da densidade de centro apresentada na Proposição 3.2.3 com $\frac{1}{2\sqrt{3}}$ obtemos,

$$t_\alpha - 2 \cdot \mathcal{N}(\mathcal{U}) \cdot \mathcal{N}(\alpha) = 0, \tag{4.1}$$

ou seja, precisamos encontrar valores convenientes de $\alpha, \mathcal{U}$ e t_α que tornem a Equação 4.1 verdadeira. Fazendo o uso do Software Mathematica obtemos uma lista de combinações para $t_\alpha, \mathcal{N}(\mathcal{U})$ e $\mathcal{N}(\alpha)$, que satisfazem a Equação 4.1 e, na Tabela 2 apresentamos algumas dessas combinações.

$\mathcal{N}(\mathcal{U})$	$\mathcal{N}(\alpha)$	t_α
1	1	2
3	4	24
9	5	90
13	6	156

Tabela 2 – Alguns valores de t_α, $\mathcal{N}(\mathcal{U})$ e $\mathcal{N}(\alpha)$ que satisfazem a Equação 4.1.
Fonte: Autor.

Temos que um ideal principal de $\mathbb{I}_{\mathbb{K}}$ é da seguinte forma $\mathcal{U} =< a_0 + a_1\zeta_3 >$, assim, a norma desse ideal é dado pela expressão

$$\mathcal{N}(\mathcal{U}) = \mathcal{N}(< a_0 + a_1\zeta_3 >) = |\mathcal{N}(a_0 + a_1\zeta_3)| = \prod_{i=1,2} \sigma_i(a_0 + a_1\zeta_3) = a_0^2 - a_0a_1 + a_1^2. \tag{4.2}$$

Igualando a Equação 4.2 aos valores de $\mathcal{N}(\mathcal{U})$ obtidos na Tabela 2, alguns ideais $\mathcal{U}$ de $\mathcal{I}_{\mathbb{K}}$ que satisfazem a Equação 4.2 são dados na Tabela 3.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$
1	$\pm(1\mathbb{I}_{\mathbb{K}}), \quad \pm(\zeta_3\mathbb{I}_{\mathbb{K}}), \quad \pm(1+\zeta_3)\mathbb{I}_{\mathbb{K}}$
3	$\pm(1+2\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(2+\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(-1+\zeta_3)\mathbb{I}_{\mathbb{K}}$
9	$\pm(3\mathbb{I}_{\mathbb{K}}), \quad \pm(3\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(3+3\zeta_3)\mathbb{I}_{\mathbb{K}}$
13	$\pm(1-3\zeta)\mathbb{I}_{\mathbb{K}}, \pm(4+3\zeta_3)\mathbb{I}_{\mathbb{K}}, \pm(3+4\zeta_3)\mathbb{I}_{\mathbb{K}}$

Tabela 3 – Alguns ideais $\mathcal{U}$ de $\mathbb{I}_{\mathbb{K}}$ que satisfazem a Equação 4.2.
Fonte: Autor.

Como estamos trabalhando com a perturbação σ_α do homomorfismo canônico, o elemento α tem que satisfazer as condições $\sigma_i(\alpha) > 0, \sigma_i(\alpha) \in \mathbb{R}$. No corpo $\mathbb{K} = \mathbb{Q}(\zeta_3)$, temos que estas condições irão ocorrer somente quando $\alpha \in \mathbb{N}$. Assim, $\sigma_i(\alpha) = \alpha$, com $i = 1, 2$ e, portanto

$$\mathcal{N}(\alpha) = \prod_{i=1,2} \sigma_i(\alpha) = \alpha^2. \tag{4.3}$$

Novamente, igualando a Equação 4.3 aos valores de α obtidos na Tabela 2, temos na Tabela 4 alguns valores para $\mathbb{N}(\alpha)$.

α	$\mathcal{N}(\alpha)$
1	1
3	9
5	25

Tabela 4 – Alguns valores de α que satisfazem a Equação 4.3.
Fonte: Autor.

A partir dos valores das Tabelas 2, 3 e 4 apresentamos na Tabela 5 combinações de α e $\mathcal{U}$ para termos t_α desejado. A partir dos dados fornecidos na Tabela 5 teremos possibilidade de obter reticulados com densidade de centro ótima para a dimensão 2.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$	$\mathcal{N}(\alpha)$	α	t_α
1	$\pm(1\mathbb{I}_{\mathbb{K}}), \quad \pm(\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(1+\zeta_3)\mathbb{I}_{\mathbb{K}}$	1	1	2
3	$\pm(1+2\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(2+\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(-1+\zeta_3)\mathbb{I}_{\mathbb{K}}$	16	4	24
9	$\pm(3\mathbb{I}_{\mathbb{K}}), \quad \pm(3\zeta_3)\mathbb{I}_{\mathbb{K}}, \quad \pm(3+3\zeta_3)\mathbb{I}_{\mathbb{K}}$	25	5	90
13	$\pm(1-3\zeta)\mathbb{I}_{\mathbb{K}}, \pm(4+3\zeta_3)\mathbb{I}_{\mathbb{K}}, \pm(3+4\zeta_3)\mathbb{I}_{\mathbb{K}}$	36	6	156

Tabela 5 – Parâmetros que satisfazem a Equação 4.1.
Fonte: Autor.

A seguir ilustramos alguns exemplos de reticulados algébricos ótimos utilizando os dados da Tabela 5.

Exemplo 4.1.1. *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_3)$, $\mathcal{U} = (\zeta_3)\mathbb{I}_{\mathbb{K}}$ *um ideal de* $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ *e* $\alpha = 1 \in \mathbb{I}_{\mathbb{K}}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_K = -3$, $\mathcal{N}(\mathcal{U}) = 1$ *e* $\mathcal{N}(\alpha) = 1$. *Dado* $x \in \mathcal{U}$,

podemos escrever $x = (\zeta_3)\cdot(a_0+a_1\zeta_3)$, *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 2a_0^2 - 2a_0a_1 + 2a_1^2$ *e, então* $t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, \quad x \neq 0\} = 2$, *com* $a_0 = -1$ *e* $a_1 = -1$. *Portanto, a densidade de centro do reticulado* $\Gamma_1 = \sigma_\alpha(\mathcal{U})$ *é dada por*

$$\delta(\Gamma_1) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\cdot\mathcal{N}(\alpha))^{\frac{1}{2}}}\cdot\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{2\sqrt{3}} \cong 0.28868,$$

que é a mesma densidade de centro do reticulado A_2.

Exemplo 4.1.2. *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_3)$, $\mathcal{U} = (-1+\zeta_3)\mathbb{I}_\mathbb{K}$ *um ideal de* $\mathbb{I}_\mathbb{K} = \mathbb{Z}[\zeta_3]$ *e* $\alpha = 4 \in \mathbb{I}_\mathbb{K}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_K = -3$, $\mathcal{N}(\mathcal{U}) = 3$ *e* $\mathcal{N}(\alpha) = 16$. *Dado* $x \in \mathcal{U}$, *podemos escrever* $x = (1+\zeta_3)\cdot(a_0 + a_1\zeta_3)$, *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 24a_0^2 - 24a_0a_1 + 24a_1^2$ *e, então* $t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, \quad x \neq 0\} = 24$, *com* $a_0 = 1$ *e* $a_1 = 0$. *Portanto, a densidade de centro do reticulado* $\Gamma_2 = \sigma_\alpha(\mathcal{U})$ *é dada por*

$$\delta(\Gamma_2) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\cdot\mathcal{N}(\alpha))^{\frac{1}{2}}}\cdot\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{2\sqrt{3}} \cong 0.28868,$$

que é a mesma densidade de centro do reticulado A_2.

Exemplo 4.1.3. *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_3)$, $\mathcal{U} = (3+3\zeta_3)\mathbb{I}_\mathbb{K}$ *um ideal de* $\mathbb{I}_\mathbb{K} = \mathbb{Z}[\zeta_3]$ *e* $\alpha = 5 \in \mathbb{I}_\mathbb{K}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_K = -3$, $\mathcal{N}(\mathcal{U}) = 9$ *e* $\mathcal{N}(\alpha) = 25$. *Dado* $x \in \mathcal{U}$, *podemos escrever* $x = (3+3\zeta_3)\cdot(a_0 + a_1\zeta_3)$, *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 90a_0^2 - 90a_0a_1 + 90a_1^2$ *e, então* $t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, \quad x \neq 0\} = 90$, *com* $a_0 = 0$ *e* $a_1 = 1$. *Portanto, a densidade de centro do reticulado* $\Gamma_3 = \sigma_\alpha(\mathcal{U})$ *é dada por*

$$\delta(\Gamma_3) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\cdot\mathcal{N}(\alpha))^{\frac{1}{2}}}\cdot\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{2\sqrt{3}} \cong 0.28868,$$

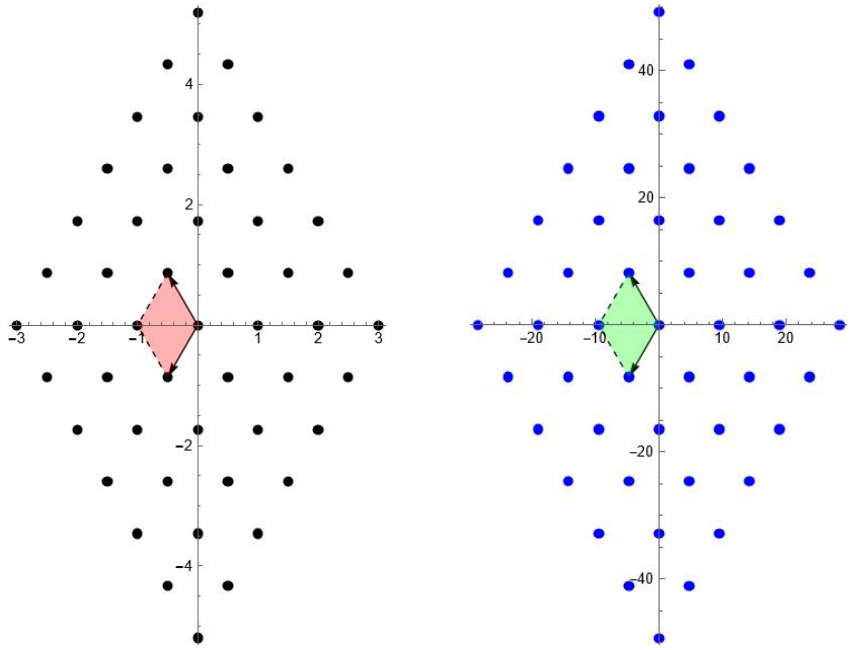
que é a mesma densidade de centro do reticulado A_2.

Observamos que todas as combinações de α, $\mathcal{U}$ e t_α de uma mesma linha da Tabela 5 geram o mesmo reticulado. Por exemplo, construindo os reticulados a partir dos ideais de norma 1 vemos que eles são todos iguais ao reticulado hexagonal, apresentando os mesmos valores do coeficiente $c = 1$ e possuem a mesma matriz de Gram. Já os reticulados construídos a partir dos ideais de norma 9, apresentam os mesmos valores do coeficiente $c = 90$ e também possuem a mesma de matriz de Gram. Além disso, concluímos que os reticulados construídos a partir dos ideais de norma 9 são 3 vezes os reticulados construídos a partir dos ideais de norma 1.

Comparando o reticulado Γ_1 construído no Exemplo 4.1.1 a partir do ideal de norma 1, $(\zeta_3)\mathbb{I}_\mathbb{K}$, com o reticulado construído a partir do ideal de norma 9, $(3\zeta_3)\mathbb{I}_\mathbb{K}$, temos respectivamente as matrizes de Gram

$$G((\zeta_3)\mathbb{I}_\mathbb{K}) = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} \qquad e \qquad G((3\zeta_3)\mathbb{I}_\mathbb{K}) = \begin{pmatrix} 90 & -45 \\ -45 & 90 \end{pmatrix},$$

com respectivos determinantes $det(G((\zeta_3)\mathbb{I}_{\mathbb{K}})) = \frac{3}{4}$ e $det(G((3\zeta_3)\mathbb{I}_{\mathbb{K}})) = 6075$. Na Figura 17 representamos geometricamente os reticulados gerados pelos ideais $(\zeta_3)\mathbb{I}_{\mathbb{K}}$ e $(3\zeta_3)\mathbb{I}_{\mathbb{K}}$.



(a) Reticulado gerado por $(\zeta_3)\mathbb{I}_{\mathbb{K}}$. (b) Reticulado gerado por $(3\zeta_3)\mathbb{I}_{\mathbb{K}}$.

Figura 17 – Comparação reticulados.
Fonte: Autor.

Os reticulados da Figura 17 estão em escalas diferentes, assim para uma análise melhor temos que olhar para o coeficiente $c = 90$ do reticulado gerado a partir do ideal $(3\zeta_3)\mathbb{I}_{\mathbb{K}}$, que indica que sua região fundamental é 90 vezes maior do que a região fundamental do reticulado gerado a partir do ideal $(\zeta_3)\mathbb{I}_{\mathbb{K}}$. A comparação dos reticulados na mesma escala é apresentada na Figura 18.

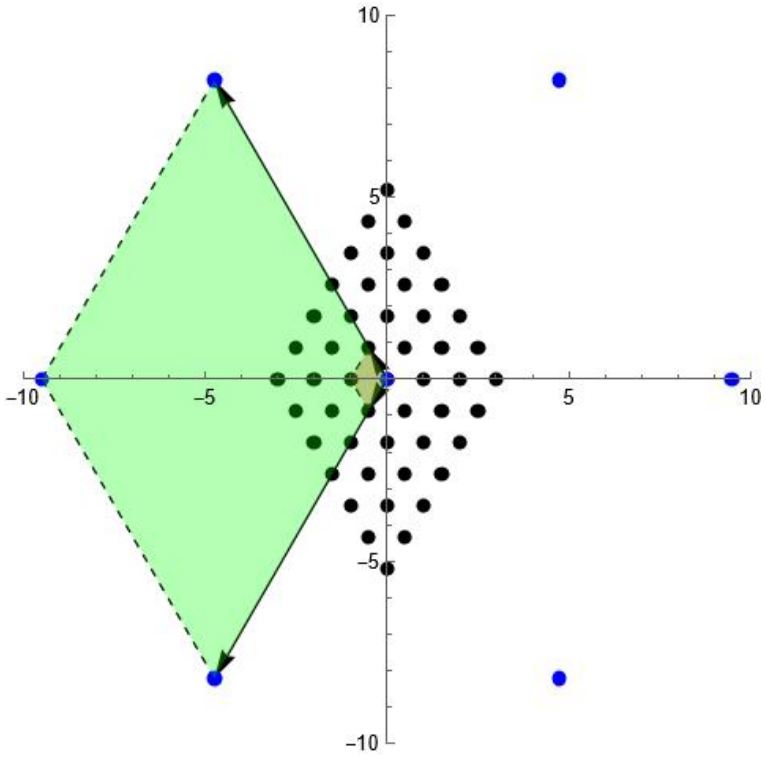


Figura 18 – Comparação entre os reticulados $(\zeta_3)\mathbb{I}_{\mathbb{K}}$ e $(3\zeta_3)\mathbb{I}_{\mathbb{K}}$.

4.2 Dimensão 4

Nessa seção, o objetivo será construir reticulados algébricos na dimensão 4 com densidade de centro ótima. Para tal construção, precisamos de um corpo de números de grau $n = 4$. Dessa forma usaremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_{12})$ que possui dimensão 4, pela Observação 1.3.12 temos que $\varphi(12) = 4$. Temos que através do Teorema 1.3.10 que $[\mathbb{K} : \mathbb{Q}] = 4$ e, do Teorema 1.3.11 que o anel dos inteiros deste corpo é dado por $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{12}]$ e uma base integral $\{1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3\}$. Pela Proposição 1.3.19 o discriminante $\mathcal{D}_{\mathbb{K}} = 144$, e pela Proposição 1.3.18 temos que os monomorfismos são $\sigma_i(\zeta_{12}) = \zeta_{12}^i$, com $i = 1, 5, 7, 11$. Queremos encontrar reticulados cuja densidade de centro seja a mesma do reticulado D_4, ou seja, $\frac{1}{8}$, utilizando a perturbação σ_α do homomorfismo canônico dado por:

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_5(\alpha)}\sigma_5(x), \sqrt{\sigma_7(\alpha)}\sigma_7(x), \sqrt{\sigma_{11}(\alpha)}\sigma_{11}(x)),$$

onde $\sigma_i(\alpha) > 0, \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 5, 7, 11$.

A ideia é substituir os valores obtidos e usar a Equação 3.4 que expressa a densidade de centro para reticulados algébricos obtidos a partir da perturbação σ_α do homomorfismo canônico. Como já temos $n = 4$ e $\mathcal{D}_{\mathbb{K}} = 144$, vamos igualar a fórmula da densidade de centro apresentada na Proposição 3.2.3 com $\frac{1}{8}$, obtemos

$$t_\alpha^2 - 24 \cdot \sqrt{\mathcal{N}(\alpha)} \cdot \mathcal{N}(\mathcal{U}) = 0, \tag{4.4}$$

ou seja, precisamos encontrar valores convenientes de $\alpha, \mathcal{U}$ e t_α que tornem a Equação 4.4 verdadeira. Fazendo o uso do Software Mathematica obtemos uma lista de combinações para $t_\alpha, \mathcal{N}(\mathcal{U})$ e $\mathcal{N}(\alpha)$, que satisfazem a Equação 4.4 e, na Tabela 6 apresentamos dessas combinações.

$\mathcal{N}(\mathcal{U})$	t_α	$\mathcal{N}(\alpha)$
1	12	36
4	24	36
9	36	36
16	48	36
36	72	36

Tabela 6 – Alguns valores de t_α, $\mathcal{N}(\mathcal{U})$ e $\mathcal{N}(\mathcal{U})$ que satisfazem a Equação 4.4.
Fonte: Autor.

Temos que um ideal principal de $\mathbb{I}_\mathbb{K}$ é da seguinte forma $\mathcal{U} =< a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3 >$ assim, a norma desse ideal é dado pela seguinte expressão

$$\begin{aligned}
\mathcal{N}(\mathcal{U}) &= \mathcal{N}(< a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3 >) \\
&= \left|\mathcal{N}(a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3)\right| \\
&= \left|\prod_{i=1,5,7,11} \sigma_i(a_0 + a_1\zeta_{12} + a_2\zeta_{12}^2 + a_3\zeta_{12}^3)\right| \\
&= \prod_{i=1,5,7,11} \sigma_i\left(\sum_{j=1}^{3} a_j\zeta_{12}^j\right). \qquad (4.5)
\end{aligned}$$

Igualando a Equação 4.5 aos valores de $\mathcal{N}(\mathcal{U})$ obtidos na Tabela 6, alguns ideais de $\mathcal{I}_\mathbb{K}$ que satisfazem a Equação 4.5 são os dados na Tabela 7.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$
1	$\pm(-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12})\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12}-\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$
4	$\pm(1-\zeta_{12}-\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(3-3\zeta_{12}-\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1-\zeta_{12}-\zeta_{12}^2)\mathbb{I}_\mathbb{K}$
9	$\pm(2-\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(1-2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(2-3\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(2+3\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$
16	$\pm(-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(2+2\zeta_{12})\mathbb{I}_\mathbb{K}$, $\pm(2+2\zeta_{12}-2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(2\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$
36	$\pm(1+3\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(\zeta_{12}+3\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1-3\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$

Tabela 7 – Alguns ideais de $\mathbb{I}_\mathbb{K}$ que satisfazem a Equação 4.5.
Fonte: Autor.

Para o elemento α, como precisamos ter $\sigma_i(\alpha) \in \mathbb{R}^+$, tomamos α no subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_{12})$, o corpo $\mathbb{L} = \mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$. O anel dos inteiros deste corpo é

$\mathbb{I}_K = \mathbb{Z}[\zeta_{12} + \zeta_{12}^{-1}]$ e, a base integral $\{1, \zeta_{12} + \zeta_{12}^{-1}\}$ dados pelo Teorema 1.3.12. Assim, podemos escrever $\alpha = b_0 + b_1(\zeta_{12} + \zeta_{12}^{-1})$, então a norma desse elemento é dada por

$$\mathcal{N}(\alpha) = \prod_{i=1,5,7,11} \sigma_i(b_0 + b_1(\zeta_{12} + \zeta_{12}^{-1})) = b_0^4 - 6b_0^2b_1^2 + 9b_1^4. \tag{4.6}$$

Utilizando dados das Tabelas 6 e 7, apresentamos na Tabela 8 combinações de α e $\mathcal{U}$ para que tenhamos t_α desejado. A partir dos dados fornecidos na Tabela 8 teremos possibilidade de obter reticulados com densidade de centro ótima para a dimensão 4. Para isso, seja $\gamma_1 = \zeta_{12} + \zeta_{12}^{-1}$.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$	α	$\mathcal{N}(\alpha)$	t_α
1	$\pm(-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12})\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12}-\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$	$3-\gamma$	36	12
4	$\pm(1-\zeta_{12}-\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(3-3\zeta_{12}-\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1-\zeta_{12}-\zeta_{12}^2)\mathbb{I}_\mathbb{K}$	$33+19\gamma$	36	24
9	$\pm(2-\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(1+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(1-2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(2-3\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(2+3\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$	$3+\gamma$	36	36
16	$\pm(-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(2+2\zeta_{12})\mathbb{I}_\mathbb{K}$, $\pm(2+2\zeta_{12}-2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(2\zeta_{12}+2\zeta_{12}^2)\mathbb{I}_\mathbb{K}$	$9-5\gamma$	36	48
36	$\pm(1+3\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$, $\pm(\zeta_{12}+3\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, $\pm(1-3\zeta_{12}+\zeta_{12}^2)\mathbb{I}_\mathbb{K}$	$9-5\gamma$	36	72

Tabela 8 – Parâmetros que satisfazem a Equação 4.4.
Fonte: Autor.

Agora, vamos ilustrar alguns exemplos de reticulados algébricos ótimos utilizando os dados da Tabela 8.

Exemplo 4.2.1. *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{12})$, $\mathcal{U} = (-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$ *um ideal de* $\mathbb{I}_\mathbb{K} = \mathbb{Z}[\zeta_{12}]$ *e,* $\alpha = 3-(\zeta_{12}^2+\zeta_{12}^{-1}) \in \mathbb{I}_\mathbb{K}$. *Temos que* $[\mathbb{K}:\mathbb{Q}] = 4$, $\mathcal{D}_\mathbb{K} = 144$, $\mathcal{N}(\mathcal{U}) = 1$ *e* $\mathcal{N}(\alpha) = 36$. *Dados* $x \in \mathcal{U}$, *podemos escrever* $x = (-1+\zeta_{12}^2+\zeta_{12}^3)\cdot(a_0+a_1\zeta_{12}+a_2\zeta_{12}^2+a_3\zeta_{12}^3)$, *onde* $a_0, a_1, a_2, a_3 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 12(a_0^2+a_0a_1+a_1^2+a_0a_2+a_1a_2+a_2^2+a_0a_3+a_1a_3+a_3^2)$ *e, então o* $t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, \quad x \neq 0\} = 12$, *com* $a_0 = a_1 = a_2 = 0$ *e* $a_3 = -1$. *Portanto, a densidade de centro do reticulado* $\Gamma_4 = \sigma_\alpha(\mathcal{U})$ *é dado por*

$$\delta(\Gamma_4) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\cdot\mathcal{N}(\alpha))^{\frac{1}{2}}}\cdot\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{8} = 0.125,$$

que é a mesma densidade de centro do reticulado D_4.

Exemplo 4.2.2. *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{12})$, $\mathcal{U} = (2-\zeta_{12}^2)\mathbb{I}_\mathbb{K}$ *um ideal de* $\mathbb{I}_\mathbb{K} = \mathbb{Z}[\zeta_{12}]$ *e,* $\alpha = 3+(\zeta_{12}+\zeta_{12}^{-1}) \in \mathbb{I}_\mathbb{K}$. *Temos que* $[\mathbb{K}:\mathbb{Q}] = 4$, $\mathcal{D}_\mathbb{K} = 144$, $\mathcal{N}(\mathcal{U}) = 9$ *e* $\mathcal{N}(\alpha) = 36$. *Dados* $x \in \mathcal{U}$, *podemos escrever* $x = (2-\zeta_{12}^2)\cdot(a_0+a_1\zeta_{12}+a_2\zeta_{12}^2+a_3\zeta_{12}^3)$, *onde* $a_0, a_1, a_2, a_3 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x}) = 36(a_0^2+a_0a_1+a_1^2+a_0a_2+a_1a_2+a_2^2+a_1a_3+a_2a_3+a_3^2)$ *e, então o*

$t_\alpha = min\{Tr(\alpha x\overline{x}); x \in \mathcal{U}, \quad x \neq 0\} = 36$, *com* $a_0 = a_1 = a_3 = 0$ *e* $a_2 = 1$. *Portanto, a densidade de centro do reticulado* $\Gamma_5 = \sigma_\alpha(\mathcal{U})$ *é dado por*

$$\delta(\Gamma_5) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}| \cdot \mathcal{N}(\alpha))^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{8} = 0.125,$$

que é a mesma densidade de centro do reticulado D_4.

Da mesma forma que na dimensão 2, observamos que todas as combinações de α, $\mathcal{U}$ e t_α de mesma linha da Tabela 8 geram o mesmo reticulado. Por exemplo, construindo os reticulados a partir dos ideais de norma 1 vemos que eles apresentam os mesmos valores de coeficiente $c = 3$ e possuem a mesma matriz de Gram. já os reticulados construídos a partir dos ideais de norma 16, apresentam os valores do coeficiente $c = 12$ e também possuem a mesma matriz de Gram. Além disso, concluímos que os reticulados construídos a partir dos ideais de norma 16 são 2 vezes os reticulados construídos a partir dos ideais de norma 1.

Comparando o reticulado construído a partir do ideal de norma 1, $(-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, com o reticulado construído a partir do ideal de norma 16, $(-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}$, temos respectivamente as matrizes de Gram

$$G((-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}) = \begin{pmatrix} 6 & 3 & 3 & 0 \\ 3 & 6 & 3 & 3 \\ 3 & 3 & 6 & 3 \\ 0 & 3 & 3 & 6 \end{pmatrix}$$

$$G((-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K}) = \begin{pmatrix} 24 & -12 & 12 & 0 \\ -12 & 24 & -12 & 12 \\ 12 & -12 & 24 & -12 \\ 0 & 12 & -12 & 24 \end{pmatrix},$$

com seus respectivos determinantes $det(G((-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K})) = 324$ e $det(G((-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K})) = 82944$, ou seja, $det(G((-2+2\zeta_{12}^2+2\zeta_{12}^3)\mathbb{I}_\mathbb{K})) = 4^4 det(G((-1+\zeta_{12}^2+\zeta_{12}^3)\mathbb{I}_\mathbb{K}))$. Na dimensão 4 não podemos visualizar geometricamente os reticulados, mas conseguimos analisar algebricamente que eles são os mesmos reticulados a menos de um fator de escala.

4.3 Dimensão 8

Nessa seção, o objetivo será construir reticulados algébricos na dimensão 8 com densidade de centro ótima. Para tal construção, precisamos de um corpo de números de grau $n = 8$. Dessa forma usaremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ que possui dimensão 8, pela Observação 1.3.12 temos que $\varphi(20) = 8$. Temos através do Teorema 1.3.10 que

$[\mathbb{K} : \mathbb{Q}] = 8$ e, do Teorema 1.3.11 que o anel dos inteiros deste corpo é $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$ e, uma base integral $\{1, \zeta_{20}, \zeta_{20}^2, \zeta_{20}^3, \zeta_{20}^4, \zeta_{20}^5, \zeta_{20}^6, \zeta_{20}^7\}$. Pelo Teorema 1.3.13 o discriminante $\mathcal{D}_{\mathbb{K}} = 2^8 \cdot 5^6$, e pela Proposição 1.3.18 temos os monomorfismos $\sigma_i(\zeta_{20}) = \zeta_{20}^i$, com $i = 1, 3, 7, 9, 11, 13, 17, 19$. Queremos encontrar reticulados cuja densidade de centro seja a mesma do reticulado E_8, ou seja, $\frac{1}{16}$, utilizando a perturbação σ_α do homomorfismo canônico, dado por

$$\begin{aligned}\sigma_\alpha(x) =&(\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_3(\alpha)}\sigma_3(x), \sqrt{\sigma_7(\alpha)}\sigma_7(x), \sqrt{\sigma_9(\alpha)}\sigma_9(x),\\ &\sqrt{\sigma_{11}(\alpha)}\sigma_{11}(x), \sqrt{\sigma_{13}(\alpha)}\sigma_{13}(x), \sqrt{\sigma_{17}(\alpha)}\sigma_{17}(x), \sqrt{\sigma_{19}(\alpha)}\sigma_{19}(x)),\end{aligned}$$

onde $\sigma_i(\alpha) > 0, \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 7, 9, 11, 13, 17, 19$.

A ideia é substituir os valores obtidos e usar a Equação 3.4 que expressa a densidade de centro para reticulados algébricos obtidos a partir da perturbação σ_α do homomorfismo canônico. Como já temos $n = 8$ e $\mathcal{D}_{\mathbb{K}} = 2^8 \cdot 5^6$, vamos igualar a fórmula da densidade de centro apresentada na Proposição 3.2.3 com $\frac{1}{16}$ obtemos

$$t_\alpha^4 - 32000 \cdot \sqrt{\mathcal{N}(\alpha)} \cdot \mathcal{N}(\mathcal{U}) = 0, \tag{4.7}$$

ou seja, precisamos encontrar valores convenientes de $\alpha, \mathcal{U}$ e t_α que tornem a Equação 4.7 verdadeira. Recorrendo ao Software Mathematica obtemos uma lista de combinações par $t_\alpha, \mathcal{N}(\alpha)$ e $\mathcal{N}(\mathcal{U})$ que satisfazem a Equação 4.7 e, na Tabela 9 apresentamos algumas dessas combinações

$\mathcal{N}(\mathcal{U})$	$\mathcal{N}(\alpha)$	t_α
1	25	20
16	25	40
80	1	40
81	25	60
256	25	40

Tabela 9 – Alguns valores de t_α, $\mathcal{N}(\mathcal{U})$ e $\mathcal{N}(\alpha)$.
Fonte: Autor.

Temos que um ideal principal de $\mathbb{I}_{\mathbb{K}}$ é da seguinte forma $\mathcal{U} =< a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7 >$, assim a norma desse ideal é dada pela seguinte expressão

$$\begin{aligned}\mathcal{N}(\mathcal{U}) &= \mathcal{N}(< a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7 >)\\ &= \left|\mathcal{N}(a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7)\right|\\ &= \left|\prod_{i=1,3,7,9,11,13,17,19} \sigma_i(a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7)\right|\\ &= \left|\prod_{i=1,3,7,9,11,13,17,19} \sigma_i\left(\sum_{j=1}^{7} a_i\zeta_{20}^j\right)\right|. \end{aligned}\tag{4.8}$$

Igualando a Equação 4.8 aos valores de $\mathcal{N}(\mathcal{U})$ obtidos na Tabela 9, alguns ideais $\mathcal{U}$ de $\mathcal{I}_{\mathbf{K}}$ que satisfazem a Equação 4.8 são dados na Tabela 10.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$
1	$(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4+\zeta_{20}^5+\zeta_{20}^6),\quad(\zeta_{20}+\zeta_{20}^3+\zeta_{20}^5)$
16	$(2+2\zeta_{20}+\zeta_{20}^2+2\zeta_{20}^4+2\zeta_{20}^5-\zeta_{20}^7),\quad(1+\zeta_{20}-\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^5-\zeta_{20}^7)$
80	$(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6),\quad(\zeta_{20}+\zeta_{20}^2+2\zeta_{20}^4+2\zeta_{20}^6-\zeta_{20}^7)$
81	$(2+2\zeta_{20}+\zeta_{20}^3+2\zeta_{20}^4),\quad\$(2\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^6+2\zeta_{20}^7)$
256	$(2+2\zeta_{20}+2\zeta_{20}^2+2\zeta_{20}^3+2\zeta_{20}^4+2\zeta_{20}^5+2\zeta_{20}^6),\quad(2\zeta_{20}+2\zeta_{20}^3+2\zeta_{20}^5)$

Tabela 10 – Alguns ideais $\mathcal{U}$ de $\mathbb{I}_{\mathbb{K}}$ que satisfazem a Equação 4.8.
Fonte: Autor.

Para o elemento α, como precisamos ter $\sigma_i(\alpha) \in \mathbb{R}^+$, tomamos α no subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, o corpo $\mathbb{L} = \mathbb{Q}(\zeta_{20}+\zeta_{20}^{-1})$, pois este corpo é totalmente real. Temos que o anel dos inteiros deste corpo é $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}+\zeta_{20}^{-1}]$ e, a base integral $\{1, \zeta_{20}+\zeta_{20}^{-1}, \zeta_{20}^2+\zeta_{20}^{-2}, \zeta_{20}^3+\zeta_{20}^{-3}\}$ de $\mathbb{L}$, dados pelo Teorema 1.3.12. Assim, podemos escrever $\alpha = b_0 + b_1(\zeta_{20}+\zeta_{20}^{-1}) + b_2(\zeta_{20}^2+\zeta_{20}^{-2}) + b_3(\zeta_{20}^3+\zeta_{20}^{-3})$, e a norma desse elemento é dado pela seguinte expressão

$$\mathcal{N}(\alpha) = \prod_{i=1,3,7,9,11,13,17,19} \sigma_i\left(b_0 + b_1(\zeta_{20}+\zeta_{20}^{-1}) + b_2(\zeta_{20}^2+\zeta_{20}^{-2}) + b_3(\zeta_{20}^3+\zeta_{20}^{-3})\right). \quad (4.9)$$

Abaixo na Tabela 11, veremos alguns elementos α´s que irão satisfazer a Equação 4.9 e também temos que $\alpha_i = \sigma_i(\alpha) > 0, \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 7, 9, 11, 13, 17, 19$.

$\mathcal{N}(\alpha)$	α
1	$(3-2(\zeta_{20}^2+\zeta_{20}^{-2}))$
25	$(\zeta_{20}^3+\zeta_{20}^{-3})$ $((\zeta_{20}+\zeta_{20}^{-1})+(\zeta_{20}^3+\zeta_{20}^{-3}))$ $(1+2(\zeta_{20}+\zeta_{20}^{-1})+3(\zeta_{20}^2+\zeta_{20}^{-2})+2(\zeta_{20}^3+\zeta_{20}^{-3}))$ $(\zeta_{20}+\zeta_{20}^{-1})$ $(2-(\zeta_{20}+\zeta_{20}^{-1})+(\zeta_{20}^2+\zeta_{20}^{-2}))$ $(2+(\zeta_{20}+\zeta_{20}^{-1})+(\zeta_{20}^2+\zeta_{20}^{-2}))$

Tabela 11 – Alguns valores que satisfazem a Equação 4.9.
Fonte: Autor.

Utilizando dados das Tabelas 10 e 11, apresentamos na Tabela 12 combinações de $\alpha, \mathcal{U}$ para termos t_α desejado, e só então podermos encontrar reticulados com densidade de centro ótimo para a dimensão 8. A partir dos dados fornecidos na Tabela 12 teremos possibilidade de obter reticulados com densidade de centro ótima para a dimensão 8. Para isso, seja $\gamma_1 = \zeta_{20}+\zeta_{20}^{-1}$, $\gamma_2 = \zeta_{20}^2+\zeta_{20}^{-2}$ e $\gamma_3 = \zeta_{20}^3+\zeta_{20}^{-3}$.

$\mathcal{N}(\mathcal{U})$	$\mathcal{U}$	α	$\mathcal{N}(\alpha)$	t_α
1	$(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4+\zeta_{20}^5+\zeta_{20}^6)$ $(\zeta_{20}+\zeta_{20}^3+\zeta_{20}^5)$	γ_3	25	20
16	$(2+2\zeta_{20}+\zeta_{20}^2+2\zeta_{20}^4+2\zeta_{20}^5-\zeta_{20}^7)$ $(1+\zeta_{20}-\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^5-\zeta_{20}^7)$	$\gamma_1+\gamma_3$	25	40
80	$(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6)$ $(\zeta_{20}+\zeta_{20}^2+2\zeta_{20}^4+2\zeta_{20}^6-\zeta_{20}^7)$	$3-2\gamma_2$	1	40
81	$(2+2\zeta_{20}+\zeta_{20}^3+2\zeta_{20}^4)$ $(2\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^6+2\zeta_{20}^7)$	γ_1	25	60
256	$(2+2\zeta_{20}+2\zeta_{20}^2+2\zeta_{20}^3+2\zeta_{20}^4+2\zeta_{20}^5+2\zeta_{20}^6)$ $(2\zeta_{20}+2\zeta_{20}^3+2\zeta_{20}^5)$	$2-\gamma_1+\gamma_2$	25	80

Tabela 12 – Parâmetros que satisfazem a Equação 4.7.
Fonte: Autor.

Observação 4.3.1. *Observe que para a dimensão 8, encontramos menos exemplos de ideais, isso se deve ao custo computacional que ocorre para altas dimensões devido à quantidade elementos na base que aumenta com a dimensão do corpo.*

Agora, vamos ilustrar alguns exemplos de reticulados algébricos ótimos utilizando os dados da Tabela 12.

Exemplo 4.3.1. *Seja o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_{20})$, $\mathcal{U}=(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6)\mathbb{I}_{\mathbb{K}}$ *um ideal de* $\mathbb{I}_{\mathbb{K}}=\mathbb{Z}[\zeta_{20}]$ *e,* $\alpha=3-2(\zeta_{20}^2+\zeta_{20}^{-2})\in\mathbb{I}_K$. *Temos que* $[\mathbb{K}:\mathbb{Q}]=8$, $\mathcal{D}_{\mathbb{K}}=2^8\cdot 5^6$, $\mathcal{N}(\mathcal{U})=80$ *e* $\mathcal{N}(\alpha)=1$. *Dado* $x\in\mathcal{U}$, *podemos escrever* $x=(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6)\cdot(a_0+a_1\zeta_{20}+a_2\zeta_{20}^2+a_3\zeta_{20}^3+a_4\zeta_{20}^4+a_5\zeta_{20}^5+a_6\zeta_{20}^6+a_7\zeta_{20}^7)$, *onde* $a_1,a_2,a_3,...,a_7\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x})=40(a_0^2+a_0a_1-a_0a_2-2a_0a_3-a_0a_4+2a_0a_6+2a_0a_7+a_1^2+a_1a_2-a_1a_3-2a_1a_4-2a_1a_5+2a_1a_7+a_2^2+a_2a_3-a_2a_4-2a_2a_5-2a_2a_6+a_3^2+a_3a_4-a_3a_5-2a_3a_6-2a_3a_7+a_4^2+a_4a_5-a_4a_6-2a_4a_7+a_5^2+a_5a_6-a_5a_7+a_6^2+a_6a_7+a_7^2)$ *e, então o traço mínimo* $t_\alpha=min\{Tr(\alpha x\overline{x});x\in\mathcal{U},x\neq 0\}=40$, *com* $a_3=0,a_0=a_4=a_7=1,a_2=a_5=a_6=-1$ *e* $a_1=-2$. *Portanto, a densidade de centro do reticulado* $\Gamma_6=\sigma_\alpha(\mathcal{U})$ *é dada por*

$$\delta(\Gamma_6)=\frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\cdot\mathcal{N}(\alpha))^{\frac{1}{2}}}\cdot\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})}=\frac{1}{16}\cong 0.06250,$$

que é a mesma densidade de centro do reticulado E_8.

Exemplo 4.3.2. *Seja o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_{20})$, $\mathcal{U}=(2\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^6+2\zeta_{20}^7)\mathbb{I}_{\mathbb{K}}$ *um ideal de* $\mathbb{I}_{\mathbb{K}}=\mathbb{Z}[\zeta_{20}]$ *e,* $\alpha=2+(\zeta_{20}+\zeta_{20}^{-1})+(\zeta_{20}^2+\zeta_{20}^{-2})\in\mathbb{I}_K$. *Temos que* $[\mathbb{K}:\mathbb{Q}]=8,\mathcal{D}_{\mathbb{K}}=2^8\cdot 5^6$, $\mathcal{N}(\mathcal{U})=81$ *e* $\mathcal{N}(\alpha)=25$. *Dado* $x\in\mathcal{U}$, *podemos escrever* $x=(2\zeta_{20}^3+\zeta_{20}^4+2\zeta_{20}^6+2\zeta_{20}^7)\cdot(a_0+a_1\zeta_{20}+a_2\zeta_{20}^2+a_3\zeta_{20}^3+a_4\zeta_{20}^4+a_5\zeta_{20}^5+a_6\zeta_{20}^6+a_7\zeta_{20}^7)$, *onde* $a_1,a_2,a_3,...,a_7\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\overline{x})=60(2a_0^2+5a_0a_1+2a_1^2+4a_0a_2+5a_1a_2+2a_2^2+2a_0a_3+4a_1a_3+5a_2a_3+2a_3^2+2a_0a_4+2a_1a_4+4a_2a_4+5a_3a_4+2a_4^2+2a_1a_5+2a_2a_5+4a_3a_5+5a_4a_5+2a_5^2-2a_0a_6+2a_2a_6+2a_3a_6+4a_4a_6+5a_5a_6+2a_6^2-2a_0a_7-2a_1a_7+2a_3a-7+2a_4a_7+4a_5a_7+5a_6a_7+2a_7^2)$ *e, então o traço mínimo* $t_\alpha=min\{Tr(\alpha x\overline{x});x\in\mathcal{U},x\neq 0\}=60$, *com* $a_0=a_3=a_5=$

$1, a_1 = a_6 = -2, a_7 = a_4 = 0$ *e* $a_2 = -1$. *Portanto, a densidade de centro do reticulado* $\Gamma_7 = \sigma_\alpha(\mathcal{U})$ *é dada por*

$$\delta(\Gamma_7) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}| \cdot \mathcal{N}(\alpha))^{\frac{1}{2}}} \cdot \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathcal{U})} = \frac{1}{16} \cong 0.06250,$$

que é a mesma densidade de centro do reticulado E_8.

Seguindo o mesmo raciocínio das dimensões 2 e 4, observamos que todas as combinações de $\alpha, \mathcal{U}$ e t_α de mesma linha da Tabela 12 geram o mesmo reticulado. Por exemplo, construindo os reticulados a partir dos ideais de norma 1 vemos que eles apresentam os mesmos valores de coeficiente $c = 5$ e possuem a mesma matriz de Gram. Já os reticulados construídos a partir dos ideais de norma 256, apresentam os valores do coeficiente $c = 20$ e também possuem a mesma matriz de Gram. Além disso, concluímos que os reticulados construídos a partir dos ideais de norma 256 são 2 vezes os reticulados construídos a partir dos ideais de norma 1.

Comparando o reticulado construído a partir do ideal de norma 1, $(\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^5)\mathbb{I}_\mathbb{K}$, com o reticulado construído a partir do ideal de norma 256, $(2\zeta_{20} + 2\zeta_{20}^3 + 2\zeta_{20}^5)\mathbb{I}_\mathbb{K}$, temos que os respectivos determinantes das matrizes de Gram são $det(G((\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^5)\mathbb{I}_\mathbb{K}))\mathbb{I}_\mathbb{K})) = 390625$ e $det(G((2\zeta_{20} + 2\zeta_{20}^3 + 2\zeta_{20}^5)\mathbb{I}_\mathbb{K})) = 25600000000$, ou seja, $det(G((2\zeta_{20} + 2\zeta_{20}^3 + 2\zeta_{20}^5)\mathbb{I}_\mathbb{K})) = 4^8 det(G((\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^5)\mathbb{I}_\mathbb{K}))\mathbb{I}_\mathbb{K}))$. Na dimensão 8 não podemos visualizar geometricamente os reticulados, mas conseguimos analisar algebricamente que eles são os mesmos reticulados a menos de um fator de escala.

Capítulo 5

Análises dos reticulados construídos

Neste capítulo vamos analisar os reticulados construídos no Capítulo 4, os quais são versões rotacionadas dos reticulados mais densos nas dimensões 2, 4 e 8, a partir de suas matrizes geradoras e de Gram. Veremos que aplicando o algoritmo LLL na matriz de Gram do reticulado obtemos uma matriz de base reduzida, a qual nos possibilita obter o fator escala que expressa a razão entre os volumes dos reticulados. Estes elementos nos possibilitam diferenciar as rotações obtidas e compará-las proporcionalmente em relação aos reticulados mais densos nas dimensões consideradas.

5.1 Reticulados equivalentes e razão entre reticulados

Nessa seção definiremos reticulados equivalentes e desenvolveremos algumas expressões importantes para analisar os reticulados.

Definição 5.1.1. *Se um reticulado Λ pode ser obtido de outro reticulado Λ' por rotação, reflexão ou escalar, então dizemos que Λ e Λ' são* ***equivalentes****.*

Sejam Λ e Λ' reticulados com matrizes de Gram G e G', respectivamente. Pela Definição 5.1.1, se Λ e Λ' são equivalentes, então

$$G = c \cdot U \cdot G' \cdot B, \tag{5.1}$$

onde c é uma constante não nula positiva, U é uma matriz uni-modular e B uma matriz ortogonal. Assim,

$$det(G) = c^n \cdot det(U) \cdot det(G') \cdot det(B) = c^n \cdot det(G') \Rightarrow det(G) = c^n \cdot det(G'). \tag{5.2}$$

Isolando o fator c^n da Equação 5.2, temos

$$\frac{det(G)}{det(G')} = c^n. \tag{5.3}$$

O algoritmo LLL (Lenstra, Lenstra e Lovász) ou método de redução de base foi originalmente proposto em [23], tal método permite encontrar uma base reduzida constituída por vetores próximos da ortogonalidade para um reticulado. Usando o algoritmo LLL, obtemos uma matriz V e a sua transposta V^t, tal que

$$G' = \frac{1}{c} \cdot V \cdot G \cdot V^t. \tag{5.4}$$

Vimos na Definição 2.2.5 que o volume e o determinante de um reticulado são relacionados da seguinte maneira:

$$vol(\Lambda)^2 = det(\Lambda). \tag{5.5}$$

Tomando $R = \dfrac{vol(\Lambda)}{vol(\Lambda')}$ como a razão entre os volumes dos reticulados Λ e Λ' temos que

$$R^2 = \left(\frac{vol(\Lambda)}{vol(\Lambda')}\right)^2 = \left(\frac{det(\Lambda)}{det(\Lambda')}\right). \tag{5.6}$$

Logo, igualando (5.6) e (5.3), segue que

$$R^2 = \frac{det(G)}{det(G')} = c^n \Rightarrow c^n = R^2. \tag{5.7}$$

Para as dimensões $n = 2, 4$ e 8, temos o seguinte

$$c^2 = \left(\frac{vol(\Lambda)}{vol(\Lambda')}\right)^2 \Rightarrow c = R \tag{5.8}$$

$$c^4 = \left(\frac{vol(\Lambda)}{vol(\Lambda')}\right)^2 \Rightarrow c = \sqrt{R} \tag{5.9}$$

$$c^8 = \left(\frac{vol(\Lambda)}{vol(\Lambda')}\right)^2 \Rightarrow c = \sqrt[4]{R}. \tag{5.10}$$

A partir das relações apresentadas nesta seção, iremos analisar nas seções seguintes os fatores de escala e as respectivas proporções de alguns dos reticulados rotacionados obtidos no Capítulo 4 com relação aos respectivos reticulados mais densos nas dimensões correspondentes. Observamos que para a dimensão 2 é possível analisar os reticulados considerados geometrica e algebricamente, o que facilita a visualização das proporções entre os reticulados rotacionados e o reticulado hexagonal. Já nas dimensões 4 e 8 apresentaremos apenas as análises algébricas. Todos os cálculos foram realizados utilizando o Software Mathemática.

5.2 Comparações entre reticulados rotacionados na dimensão 2 com o reticulado A_2

Vimos na Seção 2.4.2 e no Exemplo 2.4.2 que o reticulado A_2 é o reticulado mais denso na dimensão 2 e vimos também que este é equivalente ao reticulado hexagonal Λ_H apresentado no Exemplo 2.1.3. Geometricamente esses reticulados Λ_H e A_2 podem ser vistos nas Figuras 4 e 12, respectivamente. Neste sentido, apresentamos nesta seção, uma comparação de alguns reticulados rotacionados obtidos na Seção 4.1 com o reticulado hexagonal Λ_H.

Uma matriz geradora M_H e sua correspondente matriz de Gram G_H para o reticulado hexagonal Λ_H são dadas por

$$M_H = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ 1 & 0 \end{pmatrix} \quad e \quad G_H = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}.$$

Temos que o determinante da matriz geradora M_H é dado por $det(M_H) = \frac{\sqrt{3}}{2}$ e o determinante da matriz de Gram G_H é dado por $det(G_H) = \frac{3}{4}$.

No Exemplo 4.1.1 mostramos que o reticulado definido como Γ_1 gerado pelo ideal $\mathcal{U} = \zeta_3\mathbb{I}_{\mathbb{K}}$ em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$, $\mathcal{N}(\mathcal{U}) = 1, \alpha = 1, \mathcal{N}(\alpha) = 1$ e $t_\alpha = 2$, é uma versão rotacionada do reticulado A_2, ou seja, é um reticulado que apresenta a mesma densidade de centro que o reticulado A_2 e analogamente ao reticulado hexagonal Λ_H. Vamos analisar esta versão rotacionada através da construção das matrizes geradora e de Gram deste reticulado. Temos que

$$M_1 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{1}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix} \quad e \quad G_1 = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix},$$

são respectivamente as matrizes geradoras e de gram do reticulado Γ_1 com determinantes $det(M_1) = \frac{\sqrt{3}}{2}$ e $det(G_1) = \frac{3}{4}$, respectivamente. Apresentamos na Figura 19 o reticulado Γ_1 construído a partir da matriz geradora M_1 indicando os vetores que geram este reticulado e delimitando a região fundamental preenchida.

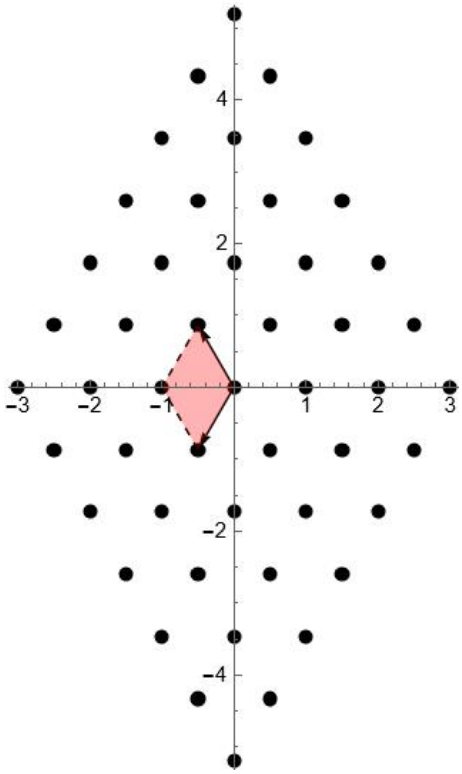


Figura 19 – Reticulado e região fundamental.
Fonte: Autor.

Pela Equação 5.2 temos que

$$det(G_1) = c^2 \cdot det(G_H) \Rightarrow \frac{3}{4} = c^2 \cdot \frac{3}{4} \Rightarrow c = 1.$$

Agora, aplicando o algoritmo LLL na matriz de Gram G_1 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

tal que a Equação 5.4 é satisfeita e nos fornecendo a seguinte matriz

$$G_1' = \frac{1}{c} \cdot V \cdot G_2 \cdot V^t = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix},$$

onde o $det(G_1') = \frac{3}{4} = det(G_H)$. Além disso, como o volume do reticulado Λ_H é dado por $vol(\Lambda_H) = \frac{\sqrt{3}}{2}$ e o volume do reticulado A_2 é $vol(\Gamma_1) = det(M_1) = \frac{\sqrt{3}}{2}$, temos pela Equação 5.8 que a razão

$$R = \frac{vol(\Gamma_1)}{vol(\Lambda_H)} = 1 = c,$$

representa a proporção entre o reticulado Γ_1 e o reticulado hexagonal Λ_H, sendo esta, dada pelo fator de escala $c = 1$. Na Figura 20 apresentamos a comparação destes reticulados onde

podemos observar que a região fundamental do reticulado Γ_1 é igual à região fundamental de Λ_H.

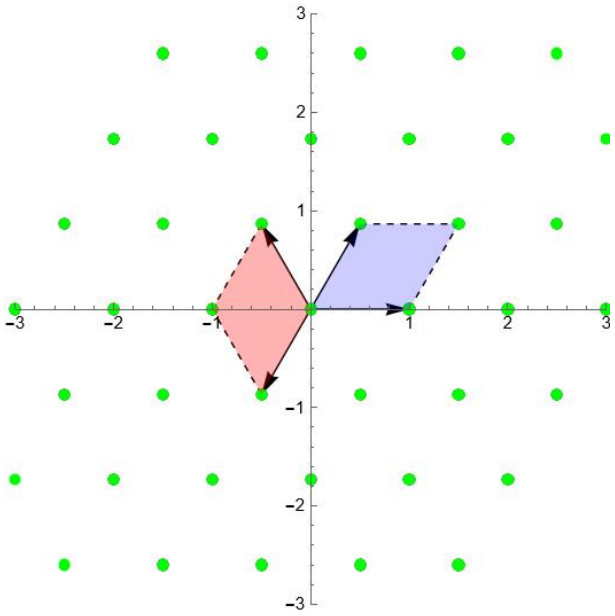


Figura 20 – Comparação entre Γ_1 e Λ_H.
Fonte: Autor.

No Exemplo 4.1.2 mostramos que o reticulado Γ_2 gerado pelo ideal $\mathcal{U} = (-1+\zeta_3)\mathbb{I}_{\mathbb{K}}$ em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$, $\mathcal{N}(\mathcal{U}) = 3, \alpha = 4, \mathcal{N}(\alpha) = 16$ e $t_\alpha = 24$, é também uma versão rotacionada do reticulado A_2. Vamos analisar esta versão rotacionada através da construção das matrizes geradora e de Gram deste reticulado. Temos que

$$M_2 = \begin{pmatrix} -3\sqrt{2} & \sqrt{6} \\ 0 & -2\sqrt{6} \end{pmatrix} \quad e \quad G_2 = \begin{pmatrix} 24 & -12 \\ -12 & 24 \end{pmatrix},$$

são respectivamente as matrizes geradora e de Gram do reticulado Γ_2 com determinante $det(M_2) = 12\sqrt{3}$ e $det(G_2) = 432$, respectivamente. Apresentamos na Figura 21 o reticulado Γ_2 construído a partir da matriz geradora M_2 indicando os vetores que geram este reticulado e delimitando a região fundamental preenchida.

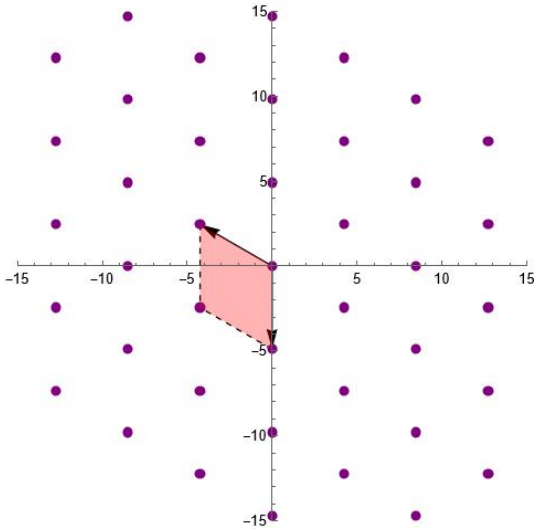


Figura 21 – Reticulado Γ_2 e região fundamental.
Fonte: Autor.

Como $det(G_H) = \frac{3}{4}$, pela Equação 5.2 temos que

$$det(G_2) = c^2 \cdot det(G_H) \Rightarrow 432 = c^2 \cdot \frac{3}{4} \Rightarrow c = 24.$$

Agora, aplicando o algoritmo LLL na matriz de Gram G_2 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

tal que a Equação 5.4 é satisfeita nos fornecendo a seguinte matriz

$$G_2' = \frac{1}{c} \cdot V \cdot G_2 \cdot V^t = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix},$$

onde o $det(G_2') = \frac{3}{4} = det(G_H)$. Além disso, como o volume do reticulado hexagonal é dado por $vol(\Lambda_H) = \frac{\sqrt{3}}{2}$ e o volume do reticulado Γ_2 é $vol(\Gamma_2) = det(M_2) = 12\sqrt{3}$, temos pela Equação 5.8 que a razão

$$R = \frac{vol(\Gamma_2)}{vol(\Lambda_H)} = \frac{12\sqrt{3}}{\frac{\sqrt{3}}{2}} = 24 = c,$$

representa a proporção entre o reticulado Γ_2 e o reticulado hexagonal Λ_H, sendo esta, dada pelo fator de escala $c = 8$. Na Figura 22 apresentamos a comparação destes reticulados onde podemos observar que a região fundamental do reticulado Γ_2 é 24 vezes maior que a região fundamental do reticulado hexagonal Λ_H.

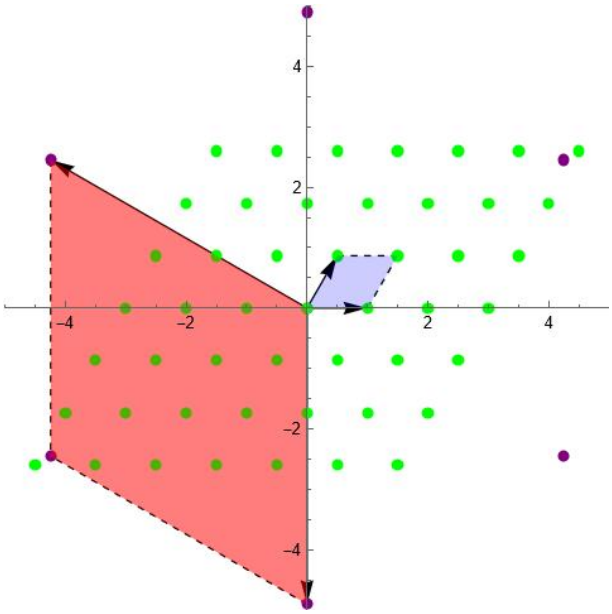


Figura 22 – Comparação entre Γ_2 e Λ_H.
Fonte: Autor.

Por fim, no Exemplo 4.1.3 mostramos que o reticulado Γ_3 gerado pelo ideal $\mathcal{U} = (3+3\zeta_3)\mathbb{I}_{\mathbb{K}}$ em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$, $\mathcal{N}(\mathcal{U}) = 9, \alpha = 5, \mathcal{N}(\alpha) = 25$ e $t_\alpha = 90$, é uma versão rotacionada do reticulado A_2. Vamos analisar este reticulado através da construção de suas matrizes geradora e de Gram. Temos que

$$M_3 = \begin{pmatrix} 3\sqrt{\frac{5}{2}} & 3\sqrt{\frac{15}{2}} \\ -3\sqrt{10} & 0 \end{pmatrix} \quad e \quad G_3 = \begin{pmatrix} 90 & -45 \\ -45 & 90 \end{pmatrix},$$

são respectivamente as matrizes geradora e de Gram do reticulado Γ_3 com determinante $det(M_3) = 45\sqrt{3}$ e $det(G_3) = 6075$, respectivamente. Apresentamos na Figura 23 o reticulado Γ_3 construído a partir da matriz geradora M_2 indicando os vetores que geram este reticulado e delimitando a região fundamental preenchida.

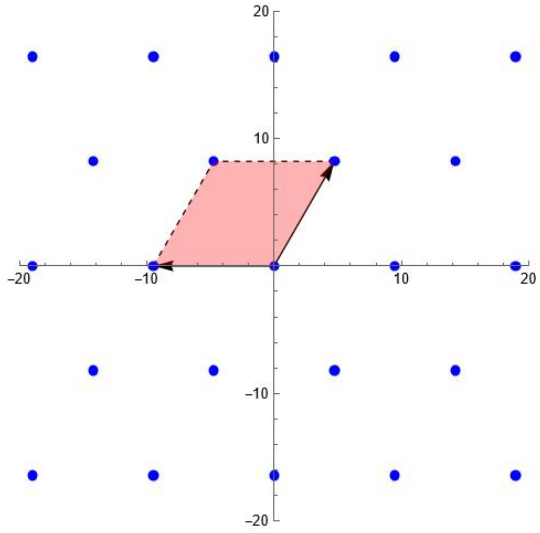


Figura 23 – Reticulado Γ_3 e região fundamental.
Fonte: Autor.

Como $det(G_H) = \frac{3}{4}$, pela Equação 5.2 temos que

$$det(G_2) = c^2 \cdot det(G_H) \Rightarrow 6075 = c^2 \cdot \frac{3}{4} \Rightarrow c = 90.$$

Agora, aplicando o algoritmo LLL na matriz de Gram G_3 obtemos uma matriz reduzida V,

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

tal que a Equação 5.4 é satisfeita nos fornecendo a seguinte matriz

$$G_3' = \frac{1}{c} \cdot V \cdot G_2 \cdot V^t = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix},$$

onde o $det(G_3') = \frac{3}{4} = det(G_H)$. Além disso, como o volume do reticulado hexagonal Λ_H) é dado por $vol(\Lambda_H) = \frac{\sqrt{3}}{2}$ e o volume do reticulado Γ_3 é $vol(\Gamma_3) = det(M_3) = 45\sqrt{3}$, temos pela Equação 5.8 que a razão

$$R = \frac{vol(\Gamma_3)}{vol(\Lambda_H)} = 90 = c,$$

representa a proporção entre o reticulado Γ_3 e o reticulado hexagonal, sendo esta, dada pelo fator escala $c = 90$. Na Figura 24 apresentamos a comparação destes reticulados onde podemos observar que a região fundamental do reticulado Γ_3 é 90 vezes maior que a região fundamental do reticulado hexagonal Λ_H).

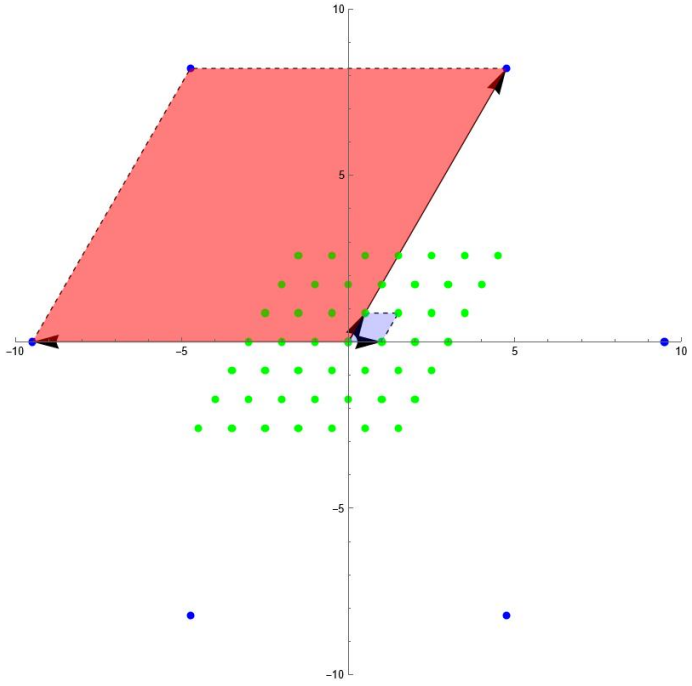


Figura 24 – Comparação entre Γ_3 e Λ_H.
Fonte: Autor.

5.3 Comparações entre reticulados rotacionados na dimensão 4 com o reticulado D_4

Vimos na Seção 2.4.3 e no Exemplo 2.4.4 que o reticulado D_4 é o mais denso na dimensão 4. Apresentamos nesta seção, uma comparação de alguns reticulados rotacionados obtidos na Seção 4.2 com o reticulado D_4.

Uma matriz geradora M_{D_4} e a matriz de Gram G_{D_4} para o reticulado D_4 são dadas por

$$M_{D_4} = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad e \quad G_{D_4} = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Temos que o determinante da matriz geradora M_{D_4} é dado por $det(M_4) = 2$ e o determinante da matriz de Gram G_{D_4} é dado por $det(G_{D_4}) = 4$.

No Exemplo 4.2.1 mostramos que o reticulado Γ_4 gerado pelo ideal $\mathcal{U} = (-1 + \zeta_{12}^2 + \zeta_{12}^3)\mathbb{I}_{\mathbb{K}}$ em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{12}]$, $\mathcal{N}(\mathcal{U}) = 1, \alpha = 3 - (\zeta_{12} + \zeta_{12}^{-1}), \mathcal{N}(\alpha) = 36$ e $t_\alpha = 12$, é uma versão rotacionada do reticulado D_4. Vamos analisar esta versão rotacionada através da construção da matriz geradora e de Gram deste reticulado. Temos que

$$G_4 = \begin{pmatrix} 6 & 3 & 3 & 0 \\ 3 & 6 & 3 & 3 \\ 3 & 3 & 6 & 3 \\ 0 & 3 & 3 & 6 \end{pmatrix},$$

é a matriz de Gram do reticulado Γ_4 com determinante $det(G_4) = 324$ e a matriz geradora M_4 tem determinante $det(M_4) = 18$.

Pela Equação 5.2 temos que

$$det(G_4) = c^4 \cdot det(G_{D_4}) \Rightarrow 324 = c^4 \cdot 4 \Rightarrow c = 3.$$

Agora, aplicando o algoritmo LLL na matriz de Gram G_4 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

tal que, a Equação 5.4 é satisfeita nos fornecendo a seguinte matriz

$$G'_4 = \frac{1}{c} \cdot V \cdot G_4 \cdot V^t = \begin{pmatrix} 2 & 1 & 1 & -1 \\ 1 & 2 & 1 & -1 \\ 1 & 1 & 2 & 0 \\ -1 & -1 & 0 & 2 \end{pmatrix},$$

onde o $det(G'_4) = 4 = det(G_{D_4})$. Além disso, o volume do reticulado D_4 é dado por $vol(D_4) = 2$ e o volume do reticulado Γ_4 é $vol(\Gamma_4) = det(M_4) = 18$, temos que pela Equação 5.9 que a razão

$$R = \sqrt{\frac{vol(\Gamma_4)}{vol(D_4)}} = \sqrt{\frac{18}{2}} = 3 = c,$$

representa a proporção entre o reticulado Γ_4 e o reticulado D_4, sendo esta, dada pelo fator escala $c = 3$, ou seja, a região fundamental do reticulado Γ_4 é 3 vezes maior que a região fundamental do reticulado D_4.

No Exemplo 4.2.2 mostramos que o reticulado Γ_5 gerado pelo ideal $\mathcal{U} = (2 - \zeta_{12}^2)\mathbb{I}_{\mathbb{K}}$, em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{12}]$, $\mathcal{N}(\mathcal{U}) = 9, \alpha = 3 + (\zeta_{12} + \zeta_{12}^{-1}), \mathcal{N}(\alpha) = 36$ e $t_\alpha = 36$, é uma versão rotacionada do reticulado D_4. Vamos analisar esta versão rotacionada através da construção da matriz geradora e de Gram deste reticulado. Temos que

$$G_5 = \begin{pmatrix} 18 & 9 & 9 & 0 \\ 9 & 18 & 9 & 9 \\ 9 & 9 & 18 & 9 \\ 0 & 9 & 9 & 18 \end{pmatrix},$$

é a matriz de Gram do reticulado Γ_5 com determinante é $(G_5) = 26244$ e a matriz geradora M_5 tem determinante $det(M_5) = 162$, respectivamente.

Pela Equação 5.2 temos que

$$det(G_5) = c^4 \cdot det(G_{D_4}) \Rightarrow 26244 = c^4 \cdot 4 \Rightarrow c = 9.$$

Agora, aplicando o Algoritmo LLL na matriz de Gram G_5 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

tal que a Equação 5.4 é satisfeita nos fornecendo a seguinte matriz

$$G'_5 = \frac{1}{c} \cdot V \cdot G_5 \cdot V^t = \begin{pmatrix} 2 & 1 & 1 & -1 \\ 1 & 2 & 1 & -1 \\ 1 & 1 & 2 & 0 \\ -1 & -1 & 0 & 2 \end{pmatrix},$$

onde o $det(G'_5) = 4 = det(G_{D_4})$. Além disso, o volume do reticulado D_4 é dado por $vol(D_4) = 2$ e o volume do reticulado $vol(\Gamma_5) = det(M_5) = 162$, temos que pela Equação 5.9 que a razão

$$R = \sqrt{\frac{vol(\Gamma_5)}{vol(D_4)}} = 9 = c,$$

representa a proporção entre os reticulados Γ_5 e o reticulado D_4, sendo esta, dada pelo fator escala $c = 9$, ou seja, a região fundamental do reticulado do Γ_5 é 9 vezes maior que a região fundamental do reticulado D_4.

5.4 Comparações entre reticulados rotacionados na dimensão 8 com o reticulado E_8

Vimos na Seção 2.4.4 que o reticulado E_8 é o mais denso na dimensão 8. Apresentamos nesta seção, uma comparação de alguns reticulados rotacionados obtidos na Seção 4.3 com o reticulado E_8.

Uma matriz geradora M_{E_8} e a matriz de Gram G_{E_8} para o reticulado E_8 são dadas por

$$M_{E_8} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

e

$$G_{E_8} = \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & 1 \\ -2 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Temos que o determinante da matriz geradora M_{E_8} é dado por $det(M_{E_8}) = 1$ e determinante da matriz de Gram G_{E_8} é dado por $det(G_{E_8}) = 1$.

No Exemplo 4.3.1 mostramos que o reticulado Γ_6 gerado pelo ideal $\mathcal{U} = (1 - \zeta_{20}^2 - \zeta_{20}^3 - \zeta_{20}^4 - \zeta_{20}^6)\mathbb{I}_{\mathbb{K}}$, em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$, $\mathcal{N}(\mathcal{U}) = 80$, $\alpha = 3 - 2(\zeta_{20}^2 + \zeta_{20}^{-2})$, $\mathcal{N}(\alpha) = 1$ e $t_\alpha = 40$, é uma verão rotacionada do reticulado E_8. Vamos analisar esta versão rotacionada através da construção da matriz geradora e de Gram deste reticulado. Temos que

$$G_6 = \begin{pmatrix} 20 & 10 & 10 & 0 & 0 & 0 & 0 & 0 \\ 10 & 20 & 10 & 10 & 0 & 0 & 0 & 0 \\ 10 & 10 & 20 & 10 & 10 & 0 & 0 & 0 \\ 0 & 10 & 10 & 20 & 10 & 10 & 0 & 0 \\ 0 & 0 & 10 & 10 & 20 & 10 & 10 & 0 \\ 0 & 0 & 0 & 10 & 10 & 20 & 10 & 10 \\ 0 & 0 & 0 & 0 & 10 & 10 & 20 & 10 \\ 0 & 0 & 0 & 0 & 0 & 10 & 10 & 20 \end{pmatrix},$$

é a matriz de Gram do reticulado Γ_6 com determinante $det(G_6) = 100000000$ e a matriz geradora M_6 tem determinante $det(M_6) = 10000$.

Pela Equação 5.2 temos que

$$det(G_6) = c^8 \cdot det(G_{E_8}) \Rightarrow 100000000 = c^8 \cdot 1 \Rightarrow c = 10.$$

Agora, aplicando o Algoritmo LLL na matriz de Gram G_6 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 & -1 & 0 & 1 \end{pmatrix},$$

tal que a Equação 5.4 é satisfeita nos fornecendo a seguinte matriz

$$G'_5 = \frac{1}{c} \cdot V \cdot G_5 \cdot V^t = \begin{pmatrix} 2 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 2 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 2 & 1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & -1 & 0 & 2 & -1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 2 & 1 \\ -1 & -1 & 0 & 1 & 0 & -1 & 1 & 2 \end{pmatrix},$$

onde o $det(G'_5) = 1 = det(G_{E_8})$. Além disso, o volume do reticulado E_8 é dado por $vol(E_8) = 1$ e o volume do reticulado Γ_6 é $vol(\Gamma_6) = det(M_6) = 10000$, temos que pela Equação 5.10 que a razão

$$R = \sqrt[4]{\frac{vol(\Gamma_6)}{vol(E_8)}} = 10 = c,$$

representa a proporção entre os reticulados Γ_6 e reticulado E_8, sendo esta, dada pelo fator escala $c = 10$, ou seja, a razão entre a região fundamental do reticulado Γ_6 é 10 vezes maior que a região fundamental do reticulado E_8.

No Exemplo 4.3.2 mostramos que reticulado Γ_7 gerado pelo ideal $\mathcal{U} = (2\zeta_{20}^3 + \zeta_{20}^4 + 2\zeta_{20}^6 + 2\zeta_{20}^7)\mathbb{I}_{\mathbb{K}}$, em que $\mathbb{I}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$, $\mathcal{N}(\mathcal{U}) = 81$, $\alpha = 2 + (\zeta_{20} + \zeta_{20}^{-1}) + (\zeta_{20}^2 + \zeta_{20}^{-2})$, $\mathcal{N}(\alpha) = 25$ e $t_\alpha = 60$, é uma versão rotacionada do reticulado E_8. Vamos analisar esta versão rotacionada através da construção da matriz geradora e de Gram deste reticulado. Temos que

$$G_7 = \begin{pmatrix} 210 & 195 & 165 & 120 & 60 & 0 & -60 & -120 \\ 195 & 210 & 195 & 165 & 120 & 60 & 0 & -60 \\ 165 & 195 & 210 & 195 & 165 & 120 & 60 & 0 \\ 120 & 165 & 195 & 210 & 195 & 165 & 120 & 60 \\ 60 & 120 & 165 & 195 & 210 & 195 & 165 & 120 \\ 0 & 60 & 120 & 165 & 195 & 210 & 195 & 165 \\ -60 & 0 & 60 & 120 & 165 & 195 & 210 & 195 \\ -120 & -60 & 0 & 60 & 120 & 165 & 195 & 210 \end{pmatrix},$$

é a matriz de Gram do reticulado Γ_7 com determinante $det(G_7) = 2562890625$ e a matriz geradora M_7 tem determinante $det(M_7) = 50625$.

Pela Equação 5.2 temos que

$$det(G_7) = c^8 \cdot det(G_{E_8}) \Rightarrow 2562890625 = c^8 \cdot 1 \Rightarrow c = 15.$$

Agora, aplicando o Algoritmo LLL na matriz de Gram G_7 obtemos uma matriz reduzida V,

$$V = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 \\ 2 & -1 & -1 & 0 & 1 & -1 & 0 & 1 \\ -2 & 1 & 2 & -2 & 0 & 0 & 2 & -2 \end{pmatrix},$$

tal que a Equação 5.4 e satisfeita nos fornecendo a seguinte matriz

$$G'_7 = \frac{1}{c} \cdot V \cdot G_7 \cdot V^t = \begin{pmatrix} 2 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ -1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 2 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 2 & 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 1 & 2 & 1 & 1 & -1 \\ -1 & 0 & 1 & 0 & 1 & 2 & 1 & -1 \\ -1 & 0 & 1 & 1 & 1 & 1 & 2 & -1 \\ 1 & 0 & -1 & 0 & -1 & -1 & -1 & 2 \end{pmatrix},$$

onde o $det(G'_7) = 1 = det(G_{E_8})$. Além disso, o volume do reticulado E_8 é dado por $vol(E_8) = 1$ e o volume do reticulado $vol(\Gamma_7) = det(M_7) = 50625$, temos que pela Equação 5.10 que a razão

$$R = \sqrt[4]{\frac{vol(\Gamma_7)}{vol(E_8)}} = 15 = c,$$

representa a proporção entre os reticulados Γ_7 e o reticulado E_8, sendo esta, dada pelo fator escala $c = 15$, ou seja, a razão entre a região fundamental do reticulado Γ_7 é 15 vezes maior que a região fundamental do reticulado E_8.

Conclusão

Neste trabalho, apresentamos uma construção de reticulados algébricos que nos possibilitam obter reticulados com densidade ótima nas dimensões $2, 4$ e 8.

Primeiramente, apresentamos os conceitos e principais resultados sobre álgebra moderna, tais como grupo, anéis, módulos e teoria de Galois. Em seguida, desenvolvemos um estudo sobre teoria algébrica dos números, abordando assuntos relevantes como inteiros algébricos, traço e norma, norma de ideal, discriminante, corpo quadrado e corpo ciclotômico. Na sequência, investigamos os reticulados, estudamos os principais conceitos e resultados, tais como, matriz geradora, matriz de Gram, determinantes e empacotamentos. Além de apresentar algumas famílias de reticulados conhecidas na literatura.

Logo após, o homomorfismo canônico (ou de Minkowski) e suas perturbações σ_α e $\sigma_{2\alpha}$ são apresentados visando de definir os reticulados algébricos no $\mathbb{R}^n$, fazendo uso de ideais do anel de inteiros de um corpo de números. Para reticulados algébricos obtidos a partir do homomorfismo canônico ou de suas perturbações, foi apresentada uma expressão para calcular a densidade de centro desses reticulados. Utilizando estes conceitos, apresentamos uma construção de reticulados algébricos nas dimensões $2, 4$ e 8 que possuem densidade de centro ótima para estas dimensões, ou seja, são versões rotacionadas dos reticulados A_2, D_4 e E_8, os reticulados mais densos nessas dimensões. Esta construção foi baseada na construção proposta em [3], e novos exemplos de reticulados algébricos densos nessas dimensões foram encontrados.

Por fim, analisamos os reticulados construídos no Capítulo 4 a partir de suas matrizes geradoras e de Gram. Aplicando o algoritmo LLL nas matrizes de Gram do reticulados obtemos uma matriz de base reduzida, a qual nos possibilita obter o fator escala que expressa a razão entre os volumes dos reticulados. Estes elementos nos possibilitam diferenciar as rotações obtidas e compará-las proporcionalmente em relação aos reticulados A_2, D_4 e E_8.

Como continuidade deste trabalho, pretendemos estender a construção utilizada e as análises realizadas para outras dimensões 2^n, com $n > 3$, para obter uma família

de reticulados algébricos nestas dimensões que possuam a mesma densidade de centro de reticulados conhecidos nestas dimensões como, por exemplo, a família de reticulados Barness-Wall.

Bibliografia

[1] Edgard de Alencar Filho. ***Elementos de álgebra abstrata***. Nobel, São Paulo, 1979.

[2] Carina Alves e Antônio Aparecido de Andrade. ***Reticulados via corpos ciclotômicos***. Editora UNESP, 2014.

[3] Antônio Aparecido Andrade et al. "**Constructions of algebraic lattices**". Em: *Computational & Applied Mathematics* 29 (2010), pp. 493–505.

[4] Robson Ricardo de Araújo. ***Anéis de inteiros de corpos de números e aplicações***. Universidade Estadual Paulista (UNESP), 2015.

[5] Alan F Beardon. ***The geometry of discrete groups***. Vol. 91. Springer Science & Business Media, 2012.

[6] Cintya Wink de Oliveira Benedito. ***Famílias de reticulados algébricos e reticulados ideais***. Universidade Estadual Paulista (UNESP), 2010.

[7] Antônio Carlos de Andrade Campello Júnior et al. ***Reticulados, projeções e aplicações à teoria da informação***. [sn], 2014.

[8] John Horton Conway e Neil James Alexander Sloane. ***Sphere packings, lattices and groups***. Vol. 290. Springer Science & Business Media, 2013.

[9] Maria Paula Almeida Cavalcante Dias. ***Reticulados bem arredondados e reticulados semi-estáveis no R^2***. Universidade Estadual Paulista (UNESP), 2018.

[10] Hygino H Domingues e Gelson Iezzi. ***Álgebra moderna***. Atual reform. São Paulo, 2003.

[11] David Steven Dummit e Richard M Foote. ***Abstract algebra***. Vol. 3. Wiley Hoboken, 2004.

[12] Emerson Dutra et al. ***Construçoes do reticulado E8 via teoria algébrica dos números, álgebra dos quatérnios e álgebra dos octônios***. [sn], 2016.

[13] Otto Endler. ***Teoria dos números algébricos***. Vol. 15. Instituto de Matemática Pura e Aplicada, CNPq, 1986.

[14] Agnaldo José Ferrari et al. ***Reticulados algébricos: Abordagem matricial e simulações***. [sn], 2012.

[15] Arnaldo Garcia e Yves Lequain. ***Elementos de álgebra***. Instituto de Matemática Pura e Aplicada, 2005.

[16] Adilson Gonçalves. ***Introdução à álgebra***. Impa, 1979.

[17] Thomas Hales e Thomas Callister Hales. ***Dense sphere packings: a blueprint for formal proofs***. Vol. 400. Cambridge University Press, 2012.

[18] Thomas C Hales. ***A proof of the Kepler Conjecture (DCG version)***. Vol. 163. 2004.

[19] Abramo Hefez e Maria Lúcia T Villela. ***Códigos corretores de erros***. Instituto de Matemática Pura e Aplicada, 2008.

[20] J.W.Cassels. ***An introduction to the geometry of numbers***. [S.l.]: Springer Science Business Media, 1997.

[21] Grasiele Cristiane Jorge. ***Reticulados ideais via corpos abelianos***. Universidade Estadual Paulista (UNESP), 2008.

[22] Serge Lang. ***Algebraic number theory***. Vol. 110. Springer Science & Business Media, 2013.

[23] Arjen K Lenstra, Hendrik Willem Lenstra e László Lovász. "**Factoring polynomials with rational coefficients**". Em: *Mathematische annalen* 261.ARTICLE (1982), pp. 515–534.

[24] Elon Lages Lima. ***Analise Real-vol 1,(2a Edição)***. Coleção Matemática Universitária, IMPA, 1989.

[25] Daniel A Marcus e Emanuele Sacco. ***Number fields***. Vol. 2. Springer, 1977.

[26] Richard A Mollin. ***Algebraic number theory***. CRC press, 1999.

[27] Luiz Henrique Jacy Monteiro. ***Elementos de álgebra***. Livro Tecnico e Cientifico, 1978.

[28] Oleg R Musin. ***The kissing problem in three dimensions***. Vol. 35. 3. Springer, 2006, pp. 375–384.

[29] F Oggier. "**Algebraic methods for channel coding. 2005, 125f**". Tese de dout. Tese (Doutorado em Matemática e Informática), École Polytechnique Fédeérale ..., 2005.

[30] José Plínio de Oliveira Santos. ***Introdução à teoria dos números***. Instituto de Matemática Pura e Aplicada, 1998.

[31] Florian Pfender e Günter M Ziegler. ***Kissing numbers, sphere packings, and some unexpected proofs***. 2004.

[32] Cátia Regina de Oliveira Quilles. ***Discriminante de corpos de números***. Universidade Estadual Paulista (UNESP), 2006.

[33] Makson Miller Alves Ribeiro et al. ***Sobre a densidade de empacotamento de reticulados obtidos através da Construção A***. [sn], 2020.

[34] Paulo Ribenboim. ***Algebraic Numbers***. Wiley-Interscience, 1972.

[35] Pierre Samuel. ***Algebraic theory of numbers***. Hermann, 1970.

[36] Plınio Gabriel Sicuti. ***Um estudo sobre reticulados algébricos bem arredondados***. Universidade Estadual Paulista (UNESP), 2020.

[37] Paulo Roberto da Silva. ***Tópicos de teoria dos números algébricos e aplicações em reticulados e equações diofantinas***. Universidade Estadual Paulista (UNESP), 2015.

[38] Juliana Gomes Ferreira de Souza. ***O problema do empacotamento de esferas no espaço n-dimensional***. [sn], 2019.

[39] Márcio Antônio de Souza. ***Introdução à teoria de Galois***. 2017.

[40] Ian Stewart e David Tall. ***Algebraic number theory***. Rel. técn. 1979.

[41] Jonas Szutkoski. "**Fatoração polinomial univariada**". Em: (2014).

[42] Carlos Roberto Lopes Vicente. ***Construções de reticulados algébricos via extensões galoisianas de grau prima***. Universidade Estadual Paulista (UNESP), 2018.

[43] Lawrence C Washington. ***Introduction to cyclotomic fields***. Springer, 1982.