unesp

UNIVERSIDADE ESTADUAL PAULISTA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Reticulados Bem Arredondados e Reticulados Semi-Estáveis no $\mathbb{R}^2$

Maria Paula Almeida Cavalcante Dias

INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

RIO CLARO
2018

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Reticulados Bem Arredondados e Reticulados Semi-Estáveis no $\mathbb{R}^2$

Maria Paula Almeida Cavalcante Dias

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

Orientadora
Profa. Dra. Carina Alves Severo

Rio Claro
2018

D541r

Dias, Maria Paula Almeida Cavalcante
Reticulados Bem Arredondados e Reticulados Semi-Estáveis no R^2 / Maria Paula Almeida Cavalcante Dias. -- Rio Claro, 2018
89 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro
Orientadora: Carina Alves Severo

1. Matemática. 2. Teoria dos Números Algébricos. 3. Extensões de Corpos. 4. Teoria dos Reticulados. 5. Anéis (Álgebra). I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Maria Paula Almeida Cavalcante Dias

Reticulados Bem Arredondados e Reticulados Semi-Estáveis no $\mathbb{R}^2$

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves Severo
Orientadora

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - UNESP (Rio Claro)

Prof. Dr. João Eloir Strapasson
Faculdade de Ciências Aplicadas (FCA) - UNICAMP (Limeira)

Rio Claro, 17 de dezembro de 2018

Ao Felipe e à minha família.

Agradecimentos

Ao concluir este trabalho, agradeço:

À minha orientadora, Profa. Dra. Carina Alves Severo, pela sua disponibilidade, atenção, amizade, por toda a sua ajuda e colaboração em todas as etapas da dissertação.

Aos membros da banca, Profa. Dra. Marta Cilene Gadotti (UNESP – Rio Claro) e Prof. Dr. João Eloir Strapasson (UNICAMP – Limeira), pela atenção, disponibilidade e ensinamentos.

Aos professores do curso, pela partilha do conhecimento, pela paciência e pelos ensinamentos para a vida.

À Profa. Dra. Eliris Cristina Rizziolli (UNESP – Rio Claro) e à Profa. Dra. Selene Maria Coelho Loibel (UNESP – Rio Claro), em especial, sempre animadas e dispostas a ajudar, tenho vocês como inspiração.

Aos funcionários do Programa de Pós-Graduação da UNESP, que sempre foram muito atenciosos a todas as dúvidas.

Aos meus amigos, pelas horas de risos e estudos.

Ao Felipe, que sempre me apoiou e me deu forças para seguir em frente.

Aos meus pais e irmãs, que apesar das dificuldades que encontrei, sempre estiveram ao meu lado me apoiando para que eu pudesse concluir essa importante etapa da minha vida.

Enfim, agradeço a todas as pessoas que contribuíram para esta realização.

A mente que se abre a uma nova ideia,
jamais voltará ao seu tamanho original.
Albert Einstein

Resumo

O objetivo deste trabalho é apresentar algumas características relacionadas à teoria de reticulados. Restringimos ao estudo dos reticulados obtidos via corpos quadráticos no $\mathbb{R}^2$. Estudamos, de maneira sucinta, alguns conceitos básicos de álgebra e álgebra linear. Abordamos alguns resultados sobre corpos quadráticos, resultados sobre reticulados e reticulados algébricos. Focamos em duas características relacionadas a reticulados: reticulados *bem arredondados* e reticulados *semi-estáveis.*

Palavras-chave: Corpos Quadráticos, Reticulados Algébricos, Reticulados Bem Arredondados, Reticulados Semi-Estáveis.

Abstract

The aim of this work is to present the study of some characteristics relatedo to theory of lattices. We restrict to the study of lattices obtained via quadratic fields in $\mathbb{R}^2$. We present, in a succinct way, some basic concepts of algebra and linear algebra. We approach some results on quadratic fields, results on lattices and algebraic lattices. We focus in two characteristics related to lattices: *well-rounded* lattices and *semi-stable* lattices.

Keywords: Quadratic Fields, Algebraic Lattices, Well Rounded Lattices, Semi-Stable Lattices.

Lista de Figuras

3.1 Região fundamental 40
3.2 Representação geométrica do reticulado do Exemplo 3.9 41
3.3 Representação geométrica dos reticulados do Exemplo 3.19 43
3.4 Representação geométrica do reticulado Λ do Exemplo 3.21 44
3.5 Representação geométrica do reticulado algébrico do Exemplo 3.30 gerado pela base $\{(1,0),(0,\sqrt{2})\}$. 46
3.6 Representação geométrica do reticulado algébrico do Exemplo 3.32 gerado pela base $\left\{(1,1),\left(\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2}\right)\right\}$. 48
3.7 Representação geométrica do reticulado algébrico do Exemplo 3.33 gerado pela base $\left\{(1,0),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$. 48

4.1 Representação geométrica do reticulado do Exemplo 4.5. 52

Lista de Tabelas

4.1 Exemplos de ideais em corpos quadráticos imaginários $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ que dão origem a reticulados *WR*. 62
4.2 Exemplos de ideais em corpos quadráticos reais $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ que dão origem a reticulados *WR*. 62

Sumário

Introdução **21**

1 Preliminares sobre Teoria Algébrica dos Números **23**
1.1 Extensões de corpos e elemento algébrico 23
1.2 Traço e norma 28
1.3 Base integral e discriminante 30

2 Corpos quadráticos **33**
2.1 Caracterização dos corpos quadráticos 33
2.2 Anel do inteiros algébricos e base integral de um corpo quadrático . . . 33
2.3 Discriminante de um corpo quadrático 36

3 Reticulados **39**
3.1 Definições 39
3.2 Reticulados algébricos 45

4 Reticulados bem arredondados **51**
4.1 Definições iniciais 51
4.2 Reticulados $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondados em $\mathbb{R}^2$ 53
4.3 Construção de uma família infinita de reticulados bem arredondados . . 57

5 Semi-estabilidade de reticulados algébricos no $\mathbb{R}^2$ **65**
5.1 Relação entre reticulados bem arredondados e semi-estáveis no $\mathbb{R}^2$ . . . 65
5.2 Reticulados algébricos semi-estáveis no $\mathbb{R}^2$ 67

6 Considerações finais **71**

Referências **73**

7 Tópicos de Álgebra e Álgebra Linear **75**
7.1 Tópicos de Álgebra Linear 75
7.2 Tópicos de Álgebra 80

Índice Remissivo **87**

Introdução

Entende-se por reticulado um subconjunto discreto do $\mathbb{R}^n$. Esse conjunto é geometricamente organizado. Existem diversas questões que envolvem o estudo de reticulados.

O problema de empacotamento esférico é um dos grandes problemas até hoje sem solução. Empacotar esferas significa saber a melhor forma de dispor esferas de mesmo raio num determinado espaço, onde as esferas podem se tocar nos bordos. O empacotamento perfeito seria aquele onde o espaço seria ocupado na totalidade (ou é deixado o mínimo de espaço entre as esferas). No nosso caso estaremos dando ênfase ao empacotamento reticulado, ou seja, empacotamentos onde o centro das esferas é um reticulado. A densidade de empacotamento é a medida mais importante para medir a qualidade de um reticulado.

Um outro problema semelhante ao empacotamento de esferas é o número de contato. Configurações esféricas que dão bons números de contato sempre vem de reticulados bem arredondados.

Reticulados bem arredondados são importantes por várias razões. Muitos reticulados importantes na matemática e na física são bem arredondados. Por exemplo, o reticulado hexagonal e o reticulado $\mathbb{Z}^2$, em $\mathbb{R}^2$, e o reticulado cúbico, em $\mathbb{R}^3$, são bem arredondados, assim como o reticulado hipercúbico e o reticulado A_4, em $\mathbb{R}^4$, que são importantes em quase cristalografia[1] (quasicrystallography). Exemplos de reticulados bem arredondados em alta dimensão são o reticulado de Leech, os reticulados Barnes-Wall e o reticulado Coxeter-Todd.

Os reticulados bem arredondados também são importantes na teoria da redução, pois eles são exatamente aqueles reticulados para os quais todos os mínimos sucessivos são iguais [20].

Uma das técnicas de gerar reticulados e avaliar sua densidade de empacotamento é através da aplicação de determinados homomorfismos em elementos do anel dos inteiros ou ideais no anel dos inteiros contidos num corpos de números $\mathbb{K}$ de grau n. Os reticulados gerados por este método são conhecidos como reticulados algébricos.

A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ com os elementos de $\mathbb{K}$. Desta forma, podemos utilizar algumas propriedades do corpo $\mathbb{K}$, que possuem uma estrutura algébrica mais rica, no estudo de tais reticulados. Com isso, o estudo de parâmetros relacionados a probabilidade de erro e que do ponto de vista geométrico são difíceis de se calcular, podem ser traduzidos num contexto algébrico.

Reticulados algébricos são objetos importantes na teoria dos números e na geometria discreta, que tem sido extensivamente estudados em uma série de artigos de Eva Bayer-

[1] quase cristalografia: sólido com um espectro de difração essencialmente discreto.

Fluckiger e seus co-autores de 1990 a 2000 (ver, por exemplo, [3, 4, 5]).

Nesse contexto, surge a seguinte pergunta: Quais reticulados algébricos são bem arredondados? Motivados por essa questão e pela importância dos reticulados bem arredondados, estudamos reticulados bem arredondados no plano, tendo como texto base o artigo [12] , em que é mostrado que existe uma infinidade de corpos quadráticos contendo ideais que produzem reticulados bem arredondados no plano.

Outra questão que vem sendo analisada em [13] é o estudo de reticulados algébricos que são semi-estáveis. Veremos que todos os reticulados bem arredondados de posto total em $\mathbb{R}^2$ são semi-estáveis.

Diante do exposto este trabalho está delineado como segue.

No Capítulo 1, apresentamos resultados preliminares necessários para o entendimento dos demais capítulos.

No Capítulo 2, apresentamos os principais resultados sobre corpos quadráticos.

No Capítulo 3, abordamos a teoria de reticulados e reticulados algébricos.

No Capítulo 4, apresentamos a teoria de reticulados bem arredondados, juntamente com definições e propriedades.

No Capítulo 5, abordamos alguns resultados sobre reticulados semi-estáveis.

Todas as figuras deste trabalho são de autoria própria, ou foram confeccionadas utilizando o pacote *tikzpicture* do editor LaTeX, ou feitas no software *Mathematica*®.

1 Preliminares sobre Teoria Algébrica dos Números

Faremos aqui um breve estudo sobre Teoria Algébrica dos Números. Abordaremos extensões de corpos e elemento algébrico, traço e norma, base integral e discriminante. Este capítulo será essencial para o desenvolvimento da teoria dos demais capítulos. Optamos por não realizar todas as demonstrações dos resultados pois algumas delas são extensas e sairíam do escopo do trabalho. As referências aqui utilizadas foram [1], [10], [22] e [28].

1.1 Extensões de corpos e elemento algébrico

Definição 1.1. *Sejam $\mathbb{F}$ e $\mathbb{K}$ corpos. Dizemos que $\mathbb{K}$ é uma **extensão** de $\mathbb{F}$ se $\mathbb{F} \subset \mathbb{K}$. Notação: $\mathbb{K}/\mathbb{F}$.*

Exemplo 1.2. $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é uma extensão de $\mathbb{Q}$.

Observação 1.3. Seja $\mathbb{K}$ uma extensão de $\mathbb{F}$. Como $\mathbb{K}$ e $\mathbb{F}$ são corpos, as condições da Definição 7.1 são satisfeitas, sendo assim, $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{F}$. Portanto, existe uma base de $\mathbb{K}$ sobre $\mathbb{F}$. Para mais detalhes, consulte [17].

Definição 1.4. *Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos.*

*(i) A dimensão do espaço vetorial $\mathbb{K}$ sobre $\mathbb{F}$ é o número de elementos da base de $\mathbb{K}$ sobre $\mathbb{F}$, chamada de **grau da extensão** de $\mathbb{K}$ sobre $\mathbb{F}$ e denotada por $[\mathbb{K} : \mathbb{F}]$.*

(ii) Dizemos que $\mathbb{K}$ é uma extensão finita de $\mathbb{F}$ se $[\mathbb{K} : \mathbb{F}]$ é finito. Caso contrário, $\mathbb{K}$ é uma extensão infinita.

Exemplo 1.5. O grau da extensão do corpo $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ sobre $\mathbb{Q}$ é 2, pois $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

Definição 1.6. *Um **corpo de números** $\mathbb{F}$ é uma extensão finita de $\mathbb{Q}$.*

Exemplo 1.7. Vimos no Exemplo 1.5 que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Logo, $\mathbb{Q}(\sqrt{2})$ é uma extensão finita de $\mathbb{Q}$ e portanto, é um corpo de números.

Teorema 1.8. *(Teorema da multiplicatividade dos graus) Se $\mathbb{F}$, $\mathbb{K}$ e $\mathbb{L}$ são corpos tais que $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{F}]$ é finita, então $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}]$.*

Demonstração. Suponha que $[\mathbb{L} : \mathbb{K}] = m$ e $[\mathbb{K} : \mathbb{F}] = n$. Se $B_1 = \{\alpha_1, \ldots, \alpha_m\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $B_2 = \{\beta_1, \ldots, \beta_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$, vamos mostrar que $B = \{\alpha_i\beta_j, i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ é uma base de $\mathbb{L}/\mathbb{F}$:

(i) O conjunto gerado por B, $[B]$, é $\mathbb{L}$.

Para todo i, j, de fato, se $\alpha \in \mathbb{L}$, então existem $a_1, a_2, \cdots, a_m \in \mathbb{K}$ tais que $\alpha = \sum_{i=1}^{m} a_i\alpha_i$, já que B_1 gera $\mathbb{L}$. Por outro lado, como $a_i \in \mathbb{K}$, então existem $b_{i1}, b_{i2}, \cdots, b_{in} \in \mathbb{F}$ tais que $a_i = \sum_{j=1}^{n} b_{ij}\beta_j$, já que B_2 gera $\mathbb{K}$. Logo, $\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\beta_j\alpha_i$, e assim $\mathbb{L} \subset [B]$. Como $[B] \subset \mathbb{L}$, segue que $[B] = \mathbb{L}$.

(ii) B é linearmente independente sobre $\mathbb{F}$.

Para todo i, j, de fato, suponha que $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j = 0$, então $\sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha_i = 0$. Como B_1 é linearmente independente sobre $\mathbb{K}$, segue que $\sum_{j=1}^{n} b_{ij}\beta_j = 0$, para todo i, e como B_2 é linearmente independente sobre $\mathbb{F}$, segue que $b_{ij} = 0$, para todo j.

Assim, B é uma base de $\mathbb{L}/\mathbb{F}$ com mn elementos. Portanto, $[\mathbb{L} : \mathbb{F}] = mn = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. □

Exemplo 1.9. Vejamos como encontrar o grau da extensão do corpo $\mathbb{Q}\left(\sqrt{11}, \sqrt{17}\right) := \{a + b\sqrt{11} + c\sqrt{17} + d\sqrt{11}\sqrt{17}\} = \{a + b\sqrt{11} + c\sqrt{17} + d\sqrt{187}\}$ sobre $\mathbb{Q}$.

Podemos verificar que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{11}) \subset \mathbb{Q}(\sqrt{11}, \sqrt{17})$. Sendo assim, vamos utilizar o Teorema 1.8 para determinar $\left[\mathbb{Q}\left(\sqrt{11}, \sqrt{17}\right) : \mathbb{Q}\right]$.

(i) $\{1, \sqrt{11}\}$ é uma base de $\mathbb{Q}(\sqrt{11})$ sobre $\mathbb{Q}$. De fato,

(ii) $\{1, \sqrt{11}\}$ gera $\mathbb{Q}(\sqrt{11})$ sobre $\mathbb{Q}$. Como $\mathbb{Q}(\sqrt{11}) = \{\alpha + \beta\sqrt{11} : \alpha, \beta \in \mathbb{Q}\}$, então, se $x \in \mathbb{Q}(\sqrt{11})$ segue que $x = \alpha 1 + \beta\sqrt{11}$, com $\alpha, \beta \in \mathbb{Q}$, ou seja, x é combinação linear de $\{1, \sqrt{11}\}$.

(iii) $\{1, \sqrt{11}\}$ é linearmente independente sobre $\mathbb{Q}$. Suponha que $\alpha 1 + \beta\sqrt{11} = 0$, com $\alpha, \beta, \in \mathbb{Q}$. Se $\beta \neq 0$, então $\sqrt{11} = \dfrac{-\alpha}{\beta}$, o que é um absurdo pois $\sqrt{11}$ é irracional. Portanto, $\beta = 0$, e assim, $\alpha 1 + 0\sqrt{11} = 0$, ou seja, $\alpha = 0$. Dessa forma, $\{1, \sqrt{11}\}$ é uma base de $\mathbb{Q}(\sqrt{11})$ sobre $\mathbb{Q}$. Logo, $[\mathbb{Q}(\sqrt{11}) : \mathbb{Q}] = 2$.

(iv) $\{1, \sqrt{17}\}$ é uma base de $\mathbb{Q}(\sqrt{11}, \sqrt{17})$ sobre $\mathbb{Q}(\sqrt{11})$. De fato,

- $\{1, \sqrt{17}\}$ gera $\mathbb{Q}(\sqrt{11}, \sqrt{17})$ sobre $\mathbb{Q}(\sqrt{11})$. Sabemos que $\mathbb{Q}(\sqrt{11}, \sqrt{17}) = \{\alpha + \beta\sqrt{17} : \alpha, \beta \in \mathbb{Q}(\sqrt{11})\}$. Assim, se $x \in \mathbb{Q}(\sqrt{11}, \sqrt{17})$ então $x = \alpha 1 + \beta\sqrt{17}$, com $\alpha, \beta \in \mathbb{Q}(\sqrt{11})$, ou seja, x é combinação linear de $\{1, \sqrt{17}\}$.
- $\{1, \sqrt{17}\}$ é linearmente independente sobre $\mathbb{Q}(\sqrt{11})$. Suponha que $\alpha 1 + \beta\sqrt{17} = 0$, com $\alpha, \beta, \in \mathbb{Q}(\sqrt{11})$. Assim, podemos reescrever a igualdade como $(p + q\sqrt{11}) + (r + s\sqrt{11})\sqrt{17} = 0$, com $p, q, r\, e\, s \in \mathbb{Q}$. Se $\beta = (r + s\sqrt{11}) \neq 0$, então

$$\sqrt{17} = \frac{-(p + q\sqrt{11})}{r + s\sqrt{11}} = \frac{-(p + q\sqrt{11})}{r + s\sqrt{11}} \cdot \frac{r - s\sqrt{11}}{r - s\sqrt{11}}$$

$$= \frac{-(pr - ps\sqrt{11} + qr\sqrt{11} - 11qs)}{r^2 - 11s^2} = \frac{-pr + 11qs + (ps - qr)\sqrt{11}}{r^2 - 11s^2}$$
$$= \frac{-pr + 11qs}{r^2 - 11s^2} + \frac{(ps - qr)\sqrt{11}}{r^2 - 11s^2} = a + b\sqrt{11},\ a, b \in \mathbb{Q}.$$

Assim, $(\sqrt{17})^2 = (a + b\sqrt{11})^2$, ou seja, $17 = a^2 + 2ab\sqrt{11} + 11b^2$. Logo $17 - a^2 - 11b^2 = 2ab\sqrt{11}$, isto é, $\frac{17 - a^2 - 11b^2}{2ab} = \sqrt{11}$, o que é absurdo pois $\sqrt{11}$ é irracional. Portanto, $r + s\sqrt{11} = \beta = 0$, e assim, $(p + q\sqrt{11}) + (0 + 0\sqrt{17}) = 0$, ou seja $(p + q\sqrt{11}) = \alpha = 0$. Dessa forma, $\{1, \sqrt{17}\}$ é uma base de $\mathbb{Q}(\sqrt{11}, \sqrt{17})$ sobre $\mathbb{Q}(\sqrt{11})$. Logo $[\mathbb{Q}(\sqrt{11}, \sqrt{17}) : \mathbb{Q}(\sqrt{11})] = 2$.

Pelo Teorema 1.8, segue que

$$[\mathbb{Q}(\sqrt{11}, \sqrt{17}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{11}, \sqrt{17}) : \mathbb{Q}(\sqrt{11})][\mathbb{Q}(\sqrt{11}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

e $\{1, \sqrt{11}, \sqrt{17}, \sqrt{187}\}$ é uma base de $\mathbb{Q}(\sqrt{11}, \sqrt{17})$ sobre $\mathbb{Q}$.

Definição 1.10. *Sejam $\mathbb{F} \subset \mathbb{K}$ corpos. Um elemento $\alpha \in \mathbb{K}$ é chamado de **algébrico** sobre $\mathbb{F}$ se existe $f(x) \in \mathbb{F}[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso o polinômio $f(x)$ não exista, α é dito **transcendente**.*

Exemplo 1.11. O elemento $\sqrt{7} \in \mathbb{Q}(\sqrt{7})$ é algébrico sobre $\mathbb{Q}$ pois existe $f(x) = x^2 - 7 \in \mathbb{Q}[x] - \{0\}$ tal que $f(\sqrt{7}) = 0$.

Exemplo 1.12. O número π não é algébrico sobre $\mathbb{Z}$, pois não existe um polinômio em $\mathbb{Z}[x]$ de modo que π seja raiz. Assim, π é transcendente sobre $\mathbb{Z}$.

Proposição 1.13. *Sejam $\mathbb{F} \subset \mathbb{K}$ corpos. Assim, $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$ se, e somente se existe um único polinômio irredutível e mônico de menor grau $f(x) \in \mathbb{F}[x]$ tal que $f(\alpha) = 0$.*

Demonstração. Se $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$, então existe um polinômio $h(x) = a_0 + \cdots + a_n x^n \in \mathbb{F}[x] - \{0\}$, com $n \in \mathbb{N}$ e $a_n \neq 0$, tal que $h(\alpha) = 0$. Tomando $\tilde{h}(x) = a_n^{-1} h(x) \in \mathbb{F}[x]$, temos que $\tilde{h}(x) \in \mathbb{F}[x]$ é um polinômio mônico tal que $\tilde{h}(\alpha) = 0$.

Observe que se $\tilde{h}(x)$ é redutível, então podemos escrevê-lo como $h_1(x) \cdot h_2(x) \cdots h_n(x)$, em que n é o grau do polinômio, de modo que $h_1(x), h_2(x), \cdots, h_n(x)$ sejam irredutíveis. Assim, se α é raiz de $\tilde{h}(x)$ segue que α é raiz de algum $h_1(x), h_2(x), \cdots, h_n(x)$ irredutível.

Para provar a unicidade, suponhamos que existam $f(x)$ e $g(x) \in \mathbb{F}[x]$ irredutíveis e mônicos de menor grau n tal que $f(\alpha) = g(\alpha) = 0$, com $f(x) \neq g(x)$. Como $f(x)$ e $g(x)$ são os polinômios mônicos de menor grau n, segue que o grau da diferença $p(x) = f(x) - g(x)$ deve ser menor ou igual a $n - 1$, isto é, $0 \leq \partial(p(x)) \leq n - 1$. Como $f(\alpha) = g(\alpha) = 0$, então $p(\alpha) = 0$. Portanto, encontramos um polinômio com grau menor que n que também tem α como raiz, o que é um absurdo, pois $f(x)$ e $g(x)$ são os polinômios de menor grau tal que $f(\alpha) = g(\alpha) = 0$. Logo, $f(x) = g(x)$. □

Definição 1.14. *Sejam $\mathbb{F} \subset \mathbb{K}$ corpos e $\alpha \in \mathbb{K}$. O polinômio irredutível e mônico de menor grau $f(x)$, tal que, $f(\alpha) = 0$ é chamado de **polinômio minimal** de α sobre $\mathbb{F}$ e é denotado por $min_{\mathbb{F}}\alpha$.*

Exemplo 1.15. Seja a extensão $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ sobre $\mathbb{Q}$. Como a extensão é de grau 2, pois $\{1, \sqrt{7}\}$ é uma base de $\mathbb{Q}(\sqrt{7})$ sobre $\mathbb{Q}$, então o polinômio minimal de $\sqrt{7}$ é da forma $x^2 + \alpha x + \beta$. Logo,

(i) com α e $\beta \in \mathbb{Q} - \{0\}$, temos

$$\begin{aligned}(\sqrt{7})^2 + \alpha\sqrt{7} + \beta &= 0\\ 7 + \alpha\sqrt{7} + \beta &= 0\\ \sqrt{7} &= \frac{-\beta - 7}{\alpha}\end{aligned}$$

o que é impossível, pois $\sqrt{7}$ é irracional.

(ii) com $\alpha \in \mathbb{Q}$ e $\beta = 0$, temos

$$\begin{aligned}(\sqrt{7})^2 + \alpha\sqrt{7} &= 0\\ 7 + \alpha\sqrt{7} &= 0\\ \sqrt{7} &= \frac{-7}{\alpha}\end{aligned}$$

o que é impossível, pois $\sqrt{7}$ é irracional.

(iii) com $\beta \in \mathbb{Q}$ e $\alpha = 0$, temos

$$\begin{aligned}(\sqrt{7})^2 + \beta &= 0\\ 7 - \beta &= 0\\ \beta &= 0.\end{aligned}$$

Portanto, o polinômio minimal de $\sqrt{7}$ sobre $\mathbb{Q}(\sqrt{7})$ é $x^2 - 7$.

Definição 1.16. *Uma extensão $\mathbb{K}$ sobre $\mathbb{F}$ é **algébrica** se todo $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$.*

Exemplo 1.17. Vamos verificar que a extensão $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$ é algébrica. De fato, se $\alpha \in \mathbb{Q}(\sqrt{3})$, então $\alpha = a + b\sqrt{3}$, com $a, b \in \mathbb{Q}$. Temos que

$$\begin{aligned}\alpha &= a + b\sqrt{3}\\ &\Rightarrow \alpha - a = b\sqrt{3}\\ &\Rightarrow (\alpha - a)^2 = 3b^2\\ &\Rightarrow \alpha^2 - 2a\alpha + a^2 - 3b^2 = 0.\end{aligned}$$

Assim, o elemento α é raiz do polinômio $f(x) = x^2 - 2ax + (a^2 - 3b^2) \in \mathbb{Q}[x]$. Portanto, α é algébrico sobre $\mathbb{Q}$, para todo $\alpha \in \mathbb{Q}[x]$. Sendo assim, a extensão $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ é algébrica.

Definição 1.18. *Dizemos que $\alpha \in \mathbb{C}$ é **inteiro algébrico** se existe $f(x) \in \mathbb{Z}[x] - \{0\}$, mônico, tal que $f(\alpha) = 0$. Seja $\mathbb{F}$ um corpo tal que $\mathbb{Q} \subset \mathbb{F}$, o conjunto $\mathcal{O}_\mathbb{F} = \{\alpha \in \mathbb{F} \mid \alpha$ é inteiro algébrico$\}$ é um anel, chamado de **anel dos inteiros algébricos de** $\mathbb{F}$.*

Em outras palavras, se $\alpha \in \mathcal{O}_\mathbb{F}$, então α é raiz de um polinômio com coeficientes inteiros.

Exemplo 1.19. Se $\mathbb{F} = \mathbb{Q}$, então $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.

De fato, se $\alpha \in \mathcal{O}_{\mathbb{F}}$, então $\alpha \in \mathbb{Q}$ e assim $\alpha = \dfrac{a}{b}$ onde a, $b \in \mathbb{Z}$ e $mdc(a, b) = 1$, com $b \neq 0$. Como α é inteiro algébrico, existe

$$f(x) = a_0 + \sum_{j=1}^{n} a_j x^j \in \mathbb{Z}[x],$$

com $a_n = 1$, tal que $f(\alpha) = 0$.

Se $n = 1$, então $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$ pois $a_0 + \alpha \in \mathbb{Z}$ e $a_0 \in \mathbb{Z}$.

Se $n > 1$, então $\sum_{j=1}^{n} a_j \alpha^j \in \mathbb{Z}$ e assim

$$\sum_{j=1}^{n} a_j x^j = \sum_{j=1}^{n} \frac{a_j a^j b^{n-j}}{b^n} \in \mathbb{Z}.$$

Portanto, b^n divide $\sum_{j=1}^{n} a_j a^j b^{n-j}$. Como $n > 1$, b divide $\sum_{j=1}^{n} a_j a^j b^{n-j}$ e assim $b \mid a^n$. Mas $mdc(a, b) = 1$ e portanto $b = 1$ e $\alpha \in \mathbb{Z}$. Logo, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$.

Exemplo 1.20. O elemento $\alpha = \sqrt{2} + \sqrt{5} \in \mathbb{R}$ é inteiro algébrico, pois é raiz do polinômio $x^4 - 14x^2 + 9 \in \mathbb{Z}[x]$.

Na Seção 2 veremos como caracterizar o conjunto $\mathcal{O}_{\mathbb{F}}$ a partir de um corpo quadrático $\mathbb{F}$.

As demonstrações dos próximos resultados (Teorema 1.21 e Proposição 1.23) podem ser encontradas na referência [22].

Teorema 1.21. *Se $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$, com $[\mathbb{K} : \mathbb{F}] < \infty$, então existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(\theta)$. O elemento θ é chamado* ***elemento primitivo****.*

Exemplo 1.22. O elemento primitivo de $\mathbb{Q}(\sqrt{3})$ é $\sqrt{3}$.

Proposição 1.23. *Se $\mathbb{K} = \mathbb{F}(\theta)$, então $[\mathbb{K} : \mathbb{F}] = \partial(min_{\mathbb{F}}\theta)$.*

Exemplo 1.24. Se $\mathbb{F} = \mathbb{Q}(\sqrt{23})$, então $[\mathbb{F} : \mathbb{Q}] = 2$, pois o grau do polinômio $min_{\mathbb{Q}}(\sqrt{23}) = x^2 - 23$ é 2.

Definição 1.25. *Se $\mathbb{K} = \mathbb{F}(\theta)$ e $\partial(min_{\mathbb{F}}\theta) = n$, então $\mathbb{F}(\theta) = \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}; a_i \in \mathbb{F},$ para qualquer $i = 0, 1, \cdots, n-1\}$.*

Exemplo 1.26. $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

Exemplo 1.27. $\mathbb{Q}(\sqrt[4]{3}) = \{a + b\sqrt{3} + c(\sqrt[4]{3})^2 + d(\sqrt[4]{3})^3 \mid a, b, c, d \in \mathbb{Q}\}$.

Definição 1.28. *Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos. Se σ é um isomorfismo de $\mathbb{K} = \mathbb{F}(\alpha)$ então $\sigma(\alpha)$ é chamado de* ***conjugado*** *de α sobre $\mathbb{F}$.*

Teorema 1.29. *Se $\mathbb{F} = \mathbb{Q}(\theta)$ é uma extensão de $\mathbb{Q}$ de grau n, então existem exatamente n monomorfismos distintos $\{\sigma_1, ..., \sigma_n\}$ de $\mathbb{F}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$. Tais monomorfismos são dados por $\sigma_i(\theta) = \theta_i$, em que $\{\theta_1, ..., \theta_n\}$ são as raízes de $min_{\mathbb{Q}}\theta$ em $\mathbb{C}$.*

A demonstração do Teorema 1.29 pode ser encontrada na referência [22].

Observação 1.30. Quando dizemos que um monomorfismo *fixa* $\mathbb{Q}$, estamos nos referindo a um monomorfismo σ que leva um elemento $q \in \mathbb{Q}$ ao mesmo $q \in \mathbb{Q}$, isto é, $\sigma(q) = q$. Os elementos de $\mathbb{Q}$ não mudam, ou seja, *ficam fixos.*

Exemplo 1.31. Considere a extensão $\mathbb{Q}(\sqrt[3]{7})$. Pela Definição 1.25,

$$\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7})^2 \mid a, b, c \in \mathbb{Q}\}.$$

Portanto, a extensão é de grau 3 sobre $\mathbb{Q}$ e o polinômio minimal de $\sqrt[3]{7}$ sobre $\mathbb{Q}$ é $min_{\mathbb{Q}}\sqrt[3]{7} = x^3 - 7$.

Como a raiz de $min_{\mathbb{Q}}\sqrt[3]{7}$ é $\sqrt[3]{7}$, segue que se $z = \sqrt[3]{7}$ então $z^3 = 7$ e a forma polar de z é $\sqrt[3]{7}(cos\ 0 + i\ sen\ 0)$. Portanto, pela 2ª Fórmula de *Moivre* [24], a raiz cúbica de 7, é dada por

$$z_k = \sqrt[3]{7}\left(cos\ \frac{0 + 2k\pi}{3} + i\ sen\ \frac{0 + 2k\pi}{3} \right), \text{ com } k \in \mathbb{N}.$$

Assim, as raízes são:

$$\begin{cases} \text{se } k = 0 \Rightarrow \sqrt[3]{7}\left(cos\ 0 + i\ sen\ 0 \right) \\ \text{se } k = 1 \Rightarrow \sqrt[3]{7}\left(cos\ \frac{2\pi}{3} + i\ sen\ \frac{2\pi}{3} \right) \\ \text{se } k = 2 \Rightarrow \sqrt[3]{7}\left(cos\ \frac{4\pi}{3} + i\ sen\ \frac{4\pi}{3} \right) \end{cases}.$$

Como $\left(cos\ \frac{4\pi}{3} + i\ sen\ \frac{4\pi}{3} \right)^2 = cos\ \frac{2\pi}{3} + i\ sen\ \frac{2\pi}{3}$, o conjunto solução da equação $x^3 - 7$ é $\{\sqrt[3]{7},\ \omega\sqrt[3]{7},\ \omega^2\sqrt[3]{7}\}$, em que $\omega = cos\ \frac{2\pi}{3} + i\ sen\ \frac{2\pi}{3}$.

Assim, como os elementos de $\mathbb{Q}$ ficam fixos, existem 3 monomorfismos:

$$\sigma_1 \ : \ \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}, \text{ em que } \sigma_1(\sqrt[3]{7}) = \sqrt[3]{7}$$

$$\sigma_2 \ : \ \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}, \text{ em que } \sigma_2(\sqrt[3]{7}) = \omega\sqrt[3]{7}$$

$$\sigma_3 \ : \ \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}, \text{ em que } \sigma_3(\sqrt[3]{7}) = \omega^2\sqrt[3]{7}.$$

Definição 1.32. *Sejam $\mathbb{F}$ um corpo de números de grau n e $\{\sigma_1, ..., \sigma_n\}$ os n $\mathbb{Q}$-monomorfismos distintos de $\mathbb{F}$ em $\mathbb{C}$. Dizemos que o monomorfismo σ_i é* ***real*** *se $\sigma_i(\mathbb{F}) \subset \mathbb{R}$, caso contrário, dizemos que σ_i é* ***imaginário****. Além disso, se todos os $\sigma_i's$, para $i = 1, ..., n$, são reais, dizemos que o corpo $\mathbb{F}$ é* ***totalmente real*** *e, se todos os $\sigma_i's$, para $i = 1, ..., n$, são imaginários, dizemos que $\mathbb{F}$ é* ***totalmente imaginário****.*

1.2 Traço e norma

Vamos introduzir alguns conceitos que serão cruciais para o desenvolvimento da teoria de base integral e discriminante que será abordada na Subseção 1.3.

As referências aqui utilizadas foram [1], [10] e [22].

Definição 1.33. *Seja $\mathbb{F}$ um corpo de números de grau n e seja σ_i para $i = 1, 2, ..., n$ os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. Para cada elemento $\alpha \in \mathbb{F}$,*

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha),$$

é chamado de ***traço*** *de α sobre $\mathbb{F}$. Também*

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha),$$

é chamado de ***norma*** *de α sobre $\mathbb{F}$.*

Exemplo 1.34. Sejam $\mathbb{F} = \mathbb{Q}(\sqrt{19})$, $\alpha = 1 + \sqrt{19}$ e $\beta = \dfrac{3 + \sqrt{19}}{2}$. Como o polinômio minimal de $\sqrt{19}$ é dado por $x^2 - 19$, suas raízes são $\sqrt{19}$ e $-\sqrt{19}$, então, os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são

$$\begin{array}{rccc} \sigma_1: & \mathbb{Q}(\sqrt{19}) & \to & \mathbb{C} \\ & \sqrt{19} & \mapsto & \sqrt{19} \end{array} \qquad \begin{array}{rccc} \sigma_2: & \mathbb{Q}(\sqrt{19}) & \to & \mathbb{C} \\ & \sqrt{19} & \mapsto & -\sqrt{19} \end{array}$$

e os elementos de $\mathbb{Q}$ ficam fixos.

Segue que

$$\begin{aligned} N_{\mathbb{F}/\mathbb{Q}}(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha) = (1 + \sqrt{19})(1 - \sqrt{19}) = -18; \\ N_{\mathbb{F}/\mathbb{Q}}(\beta) &= \sigma_1(\beta)\sigma_2(\beta) = \left(\frac{3 + \sqrt{19}}{2}\right)\left(\frac{3 - \sqrt{19}}{2}\right) = \frac{-5}{2}; \\ Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) = (1 + \sqrt{19}) + (1 - \sqrt{19}) = 2; \\ Tr_{\mathbb{F}/\mathbb{Q}}(\beta) &= \sigma_1(\beta) + \sigma_2(\beta) = \frac{3 + \sqrt{19}}{2} + \frac{3 - \sqrt{19}}{2} = 3. \end{aligned}$$

E também, temos

$$\begin{aligned} N_{\mathbb{F}/\mathbb{Q}}(\alpha\beta) &= N_{\mathbb{F}/\mathbb{Q}}\left((1+\sqrt{19})\left(\frac{3+\sqrt{19}}{2}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}(11+2\sqrt{19}) \\ &= (11+2\sqrt{19})(11-2\sqrt{19}) = 11^2 - 4.19 \\ &= 121 - 76 = 45 = (-18)\cdot\frac{-5}{2} \\ &= N_{\mathbb{F}/\mathbb{Q}}(\alpha)N_{\mathbb{F}/\mathbb{Q}}(\beta). \end{aligned}$$

$$\begin{aligned} Tr_{\mathbb{F}/\mathbb{Q}}(\alpha+\beta) &= Tr_{\mathbb{F}/\mathbb{Q}}\left((1+\sqrt{19})+\left(\frac{3+\sqrt{19}}{2}\right)\right) = Tr_{\mathbb{F}/\mathbb{Q}}\left(\frac{5+3\sqrt{19}}{2}\right) \\ &= \left(\frac{5+3\sqrt{19}}{2}\right)+\left(\frac{5-3\sqrt{19}}{2}\right) = 5 = 2+3 \\ &= Tr_{\mathbb{F}/\mathbb{Q}}(\alpha)+Tr_{\mathbb{F}/\mathbb{Q}}(\beta). \end{aligned}$$

Este exemplo ilustra algumas propriedades de traço e norma apresentadas a seguir.

Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, em que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $\alpha, \alpha' \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:

(i) $Tr_{\mathbb{L}/\mathbb{K}}(\alpha+\alpha') = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\alpha')$;

(ii) $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}/\mathbb{K}}(\alpha)$;

(iii) $Tr_{\mathbb{L}/\mathbb{K}}(a) = [\mathbb{L}:\mathbb{K}]a$;

(iv) $N_{\mathbb{L}/\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$;

(v) $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}/\mathbb{K}}(\alpha)$;

(vi) $N_{\mathbb{L}/\mathbb{K}}(\alpha\alpha') = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\alpha')$.

As demonstrações dessas propriedades podem ser encontrada na referência [22].

1.3 Base integral e discriminante

Apresentamos os conceitos de base integral e discriminante que serão importantes para a construção de reticulados no Capítulo 3. Diferente das outras subseções, aqui não apresentamos exemplos. Para um melhor entendimento, os conceitos introduzidos, aqui, para quaisquer corpos de números, são exemplificados no Capítulo 2, por meio de corpos quadráticos.

As referências utilizadas foram [1], [10] e [22].

Definição 1.35. *Seja $\mathcal{O}_{\mathbb{F}}$ o anel de inteiros algébricos de um corpo de números $\mathbb{F}$. Uma base de $\mathcal{O}_{\mathbb{F}}$ sobre $\mathbb{Z}$, ou simplesmente, uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{F}}$, é chamada de uma* ***base integral*** *para $\mathcal{O}_{\mathbb{F}}$.*

Observação 1.36. Se tomarmos uma base de $\mathcal{O}_{\mathbb{F}}$ sobre $\mathbb{Q}$, teremos uma $\mathbb{Q}$-base.

Teorema 1.37. *Todo corpo de números $\mathbb{F}$ possui uma base integral.*

A demonstração do teorema anterior pode ser encontrada na referência [28].

Definição 1.38. *Sejam $\mathbb{F} = \mathbb{Q}(\alpha)$ um corpo de números com $[\mathbb{F} : \mathbb{Q}] = n$, $\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ uma $\mathbb{Q}$-base para $\mathbb{F}$ e σ_i para $i = 1, \ldots, n$ os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. O **discriminante** de $\mathbb{F}$, é definido por*

$$\mathcal{D}_{\mathbb{F}} := (det(\sigma_j(\alpha_i)))^2,$$

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

O próximo teorema fornece um critério para sabermos quando uma base é integral.

Teorema 1.39. *Se o conjunto $\mathcal{B} \subset \mathcal{O}_{\mathbb{F}}$ é uma base de $\mathcal{O}_{\mathbb{F}}$ e $\mathcal{D}_{\mathbb{F}}$ é livre de quadrados, então $\mathcal{B}$ é uma base integral para $\mathcal{O}_{\mathbb{F}}$.*

A demonstração do Teorema 1.39 pode ser encontrada na referência [22].

Observação 1.40. Como vemos na referência [22], o valor do discriminante associado a uma base integral de um corpo independe das bases tomadas.

2 Corpos quadráticos

Os corpos quadráticos são o principal objeto de estudo do Capítulo 3 e do Capítulo 4. O objetivo aqui é caracterizar seu anel dos inteiros algébricos, base integral e discriminante, a fim de construir reticulados no $\mathbb{R}^n$, com veremos no Capítulo 3.

As referências aqui utilizadas foram [1], [10], [22] e [28].

2.1 Caracterização dos corpos quadráticos

Definição 2.1. *Uma extensão de corpos de grau 2 sobre o corpo $\mathbb{Q}$ é chamada de* ***corpo quadrático****.*

Proposição 2.2. *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados.*

Demonstração. Sejam $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo quadrático, ou seja, um corpo de números de grau 2, e $f(x) = x^2 + ax + b$, com a, $b \in \mathbb{Q}$, o polinômio minimal de $\theta \in \mathbb{F}$.

Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$, segue que $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$ são as raízes de $f(x)$. Como $\pm(2\theta + a) = \sqrt{a^2 - 4b}$, segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Por outro lado, $a^2 - 4b$ é um número racional que pode ser escrito como $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com u, $v \in \mathbb{Z}$, $mdc(u, v) = 1$, e de forma que u e v não sejam quadrados perfeitos simultaneamente, pois caso contrário, teremos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Escrevendo $uv = k^2 d$, com k, $d \in \mathbb{Z}$, e d um inteiro livre de quadrados, então, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2 d}) = \mathbb{Q}(\sqrt{d})$. □

A Proposição 2.2 nos diz que todo corpo quadrático $\mathbb{F}$ é da forma $\mathbb{Q}(\sqrt{d})$, em que d é um inteiro livre de quadrados e $\{1, \sqrt{d}\}$ é uma base do espaço vetorial $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

Definição 2.3. *Se $d > 0$, a extensão $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ é dita* ***real*** *e se $d < 0$, a extensão $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ é dita* ***imaginária****.*

2.2 Anel do inteiros algébricos e base integral de um corpo quadrático

Conforme mencionado anteriormente, exemplificamos aqui os conceitos apresentados na Seção 1.3.

A seguir, vamos caracterizar o anel dos inteiros algébricos de um corpo quadrático $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados e seu discriminante.

Teorema 2.4. *Se $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com d um inteiro livre de quadrados, então o anel dos inteiros algébricos $\mathcal{O}_\mathbb{F}$ de $\mathbb{Q}(\sqrt{d})$ é dado por:*

(i) $\mathcal{O}_\mathbb{F} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right), \text{com } a, b \in \mathbb{Z}\right\}$ *se $d \equiv 1\ (mod\ 4)$, e uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{F}$ é dada por $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$;*

(ii) $\mathcal{O}_\mathbb{F} = \mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d}, \text{ com } a, b \in \mathbb{Z}\}$ *se $d \equiv 2$ ou $d \equiv 3\ (mod\ 4)$, e uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{F}$ é dada por $\{1, \sqrt{d}\}$.*

Demonstração. O conjunto dos inteiros algébricos é não vazio, pois, de imediato, os números inteiros são inteiros algébricos.

Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com a, $b \in \mathbb{Q}$, um inteiro algébrico. Então, existe um polinômio com coeficientes inteiros de modo que α é raiz deste polinômio.

Vamos analisar duas situações:

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

- Se $b \neq 0$, então o polinômio minimal $min_\mathbb{Q}\alpha$ de α sobre $\mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

$$\begin{aligned} \alpha &= a + b\sqrt{d} \\ \alpha - a &= b\sqrt{d} \\ (\alpha - a)^2 &= b^2 d \\ \alpha^2 - 2a\alpha + a^2 &= b^2 d \\ \alpha^2 - 2a\alpha + (a^2 - b^2 d) &= 0. \end{aligned}$$

  Logo $min_\mathbb{Q}\alpha = x^2 - 2ax + a^2 - db^2$. Como α é um 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 $\frac{w}{y}$, com w, y inteiros primos entre si e $y \neq 0$ (se $2b \in \mathbb{R} - \mathbb{Q}$, é claro que $d(2b)^2 \notin \mathbb{Z}$). Como $d(2b)^2 \in \mathbb{Z}$, segue que $d\left(\frac{w}{y}\right)^2 \in \mathbb{Z}$ e portanto ou $y^2 \mid w^2$ ou $y^2 \mid d$. O primeiro caso é impossível, pois $y \nmid w$. Logo, $y^2 \mid d$ e assim, $d = y^2 k$, para algum k inteiro, o que também é um absurdo, pois d é livre de quadrados, por hipótese. Portanto, $2b \in \mathbb{Z}$.

Concluímos que se $\alpha = \{a + b\sqrt{d}, \text{ com } a, b \in \mathbb{Q}\}$ é algébrico, então $2a$ e $2b$ são números inteiros. Portanto, podemos escrever:

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

Temos também que $(2a)^2 - d(2b)^2 \in 4\mathbb{Z}$, pois

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

Substituindo a por $\frac{u}{2}$ e b por $\dfrac{v}{2}$, segue que $u^2 - dv^2 \in 4\mathbb{Z}$. Então $4 \mid u^2 - dv^2$ ou, equivalentemente,

$$u^2 - dv^2 \equiv 0 \ (mod\ 4). \tag{2.1}$$

Agora, vamos determinar em quais condições a equivalência anterior é válida:

(i) Se u e v são ímpares, temos que a e $b \in \mathbb{Q} - \mathbb{Z}$, já que $a = \dfrac{u}{2}$ e $b = \dfrac{v}{2}$. Então, para todo $k_1, k_2 \in \mathbb{Z}$,

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

Neste caso, a equivalência (2.1) é válida se, e somente se, $d \equiv 1 \ (mod\ 4)$.

(ii) Se u e v são pares, temos que a e $b \in \mathbb{Z}$, já que $a = \dfrac{u}{2}$ e $b = \dfrac{v}{2}$. Então, para todo $k_1, k_2 \in \mathbb{Z}$,

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

Neste caso, a equivalência (2.1) é válida se, e somente se, $d \equiv 2 \ (mod\ 4)$ ou $d \equiv 3 \ (mod\ 4)$.

(iii) Se u é ímpar e v é par, então, para todo $k_1, k_2 \in \mathbb{Z}$,

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

Neste caso, a equivalência (2.1) não é válida.

(iv) Se u é par e v é ímpar, então, para todo $k_1, k_2 \in \mathbb{Z}$,

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

já que $d \not\equiv 0 \ (mod\ 4)$, pois d é livre de quadrados. Mais uma vez, a equivalência (2.1) não é válida.

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

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

já que $\dfrac{u-v}{2}$ e $v \in \mathbb{Z}$ (note que se u e v são ímpares, então $u - v$ é par). Portanto, $\mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$.

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

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

pois $d \equiv 1(mod\,4)$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{F}}$, pois os coeficientes do polinômio minimal de α, $min_{\mathbb{Q}}\alpha = x^2 - (2a+b)x + a^2 + ab + \frac{(1-d)b^2}{4}$, estão em $\mathbb{Z}$. Portanto, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Do item (ii) concluímos que se $d \equiv 2$ ou $3\ (mod\ 4)$, o anel $\mathcal{O}_{\mathbb{F}}$ dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ é da forma $\alpha = a + b\sqrt{d}$ com a e $b \in \mathbb{Z}$. Sendo assim, $\alpha \in \mathbb{Z}[\sqrt{d}]$ e, então, $\mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}[\sqrt{d}]$.

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, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{F}}$. Portanto, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\sqrt{d}]$. □

2.3 Discriminante de um corpo quadrático

Proposição 2.5. *Seja d um inteiro livre de quadrados, o discriminante de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ é dado por:*

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

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

Demonstração. Pelo Teorema 1.29, os monomorfismos de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$, com $d \in \mathbb{Z}$ um inteiro livre de quadrados, são

$$\sigma_1(\sqrt{d}) = \sqrt{d} \text{ e } \sigma_2(\sqrt{d}) = -\sqrt{d},$$

segue que o discriminante de um corpo quadrático é obtido do seguinte modo:

(i) Para $d \equiv 1\ (mod\,4)$, temos que uma base integral de $\mathbb{Q}(\sqrt{d})$ é $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$, então, pela Definição 1.38, o discriminante de $\mathbb{Q}(\sqrt{d})$ é

$$\mathcal{D}_{\mathbb{F}} = \mathcal{D}_{\mathbb{F}/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right)^2 =$$

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

(ii) Para $d \equiv 2\ (mod\ 4)$ ou $d \equiv 3\ (mod\ 4)$, temos que uma base integral de $\mathbb{Q}(\sqrt{d})$ é $\{1, \sqrt{d}\}$, então, usando a Definição 1.38, o discriminante de $\mathbb{Q}(\sqrt{d})$ é

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

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

□

Exemplo 2.6. Dado $\mathbb{F} = \mathbb{Q}(\sqrt{5})$, o discriminante de $\mathbb{F}$ é 5, já que $5 \equiv 1 \ (mod\ 4)$. De fato, pelo Teorema 2.4 temos que $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathcal{O}_{\mathbb{F}}$ e os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$. Portanto, de acordo com a Proposição 2.5, o discriminante é dado por

$$\begin{aligned}
\mathcal{D}_{\mathbb{F}} &= \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}\right)^2 \\
&= \left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right)^2 = 5,
\end{aligned}$$

que é livre de quadrados. Observe que todas as hipóteses do Teorema 1.39 são satisfeitas.

3 Reticulados

Neste capítulo, apresentamos os principais conceitos da Teoria de Reticulados. Também vamos expor aqui como construir reticulados no $\mathbb{R}^n$ via corpos de números, especialmente via corpos quadráticos. Dessa forma, podemos identificar os pontos do reticulado no $\mathbb{R}^n$ como os elementos de um corpo de números. A partir daí, podemos estudar esses resultados em diversos contextos e aplicações, conforme veremos neste capítulo e no Capítulo 4.

As referências aqui utilizadas foram [1], [8], [11], [28] e [22].

3.1 Definições

Nesta seção, apresentamos a definição de reticulados e outras definições importantes como a região fundamental, matriz de Gram e volume da região fundamental. A partir de agora os reticulados serão a base de todo o contexto apresentado.

Definição 3.1. *Sejam $\{v_1, v_2, ..., v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$, com $m \leq n$. O conjunto de pontos*

$$\Lambda := \left\{ \mathbf{x} = \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z} \right\},$$

*é chamado **reticulado** de dimensão ou posto m e $\{v_1, v_2, ..., v_m\}$ é chamado de **base do reticulado**.*

Equivalentemente, entende-se por reticulado um subconjunto discreto aditivo do $\mathbb{R}^n$, ou seja, pontos isolados. Como veremos, esse conjunto é geometricamente organizado.

Definição 3.2. *O paralelepípedo formado pelos pontos*

$$\theta_1 v_1 + \cdots + \theta_m v_m, \ 0 \leq \theta_i < 1,$$

é chamado um **paralelepípedo fundamental** *ou* **região fundamental** *do reticulado.*

Exemplo 3.3. $\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na Figura 3.3 a seguir.

Definição 3.4. *Seja $\{v_1, \ldots, v_m\}$ uma base do reticulado Λ. Se $v_i = (v_{i1}, \ldots, v_{in})$, com $i = 1, \cdots, m$, a matriz*

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

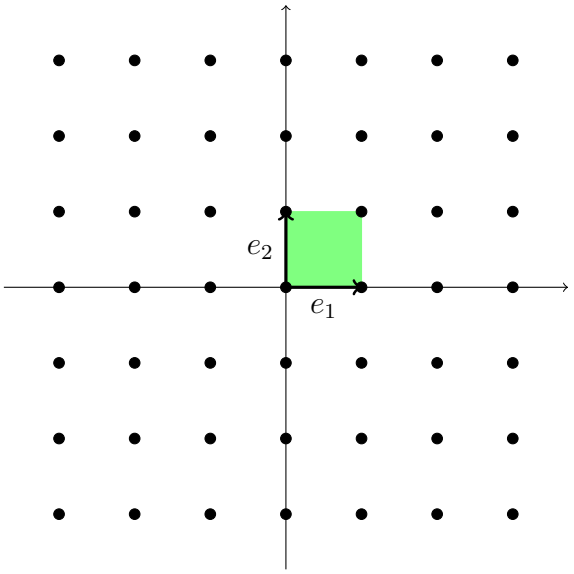

Figura 3.1: Região fundamental

é chamada uma ***matriz geradora*** *para o reticulado. A matriz* $G = M^t M$ *é chamada uma* ***matriz de Gram*** *para o reticulado, em que* t *denota a transposição.*

Observação 3.5. De acordo com a Definição 3.4, o reticulado Λ é formado pelos pontos

$$\Lambda = \{\mathbf{x} = \{M\lambda \mid \lambda \in \mathbb{Z}^m\},$$

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

Definição 3.6. *Para reticulados de posto máximo, isto é,* $m = n$*, a raiz quadrada do determinante do reticulado é o volume do paralelepípedo fundamental, também chamado* ***volume do reticulado****, e denotado por* $\mathcal{V}ol(\Lambda)$.

Definição 3.7. *O* ***determinante do reticulado*** Λ *é definido como sendo o determinante da matriz de Gram,*

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

Observação 3.8. De acordo com a Definição 3.6 e a Definição 3.7, se $m = n$ o volume de Λ é dado por $\mathcal{V}ol(\Lambda) = |det(M)|$.

Exemplo 3.9. Seja o reticulado Λ em $\mathbb{Z}^2$ com base $\{(2,0),(1,4)\}$, representado na Figura 3.2. Uma matriz M geradora para Λ é $M = \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix}$ e de acordo com a Definição 3.4, sua matriz de Gram G é $G = \begin{pmatrix} 4 & 2 \\ 2 & 17 \end{pmatrix}$.
O determinante de Λ é $det(\Lambda) = det(G) = 68 - 4 = 64$, e o volume de Λ é $\mathcal{V}ol(\Lambda) = |det(M)| = |8 - 0| = 8$.

Definição 3.10. *Dizemos que um reticulado tem* ***posto máximo*** *ou* ***posto completo*** *se* $m = n$*, e neste caso* M *é uma matriz quadrada. Assim,*

$$det(\Lambda) = (det(M))^2.$$

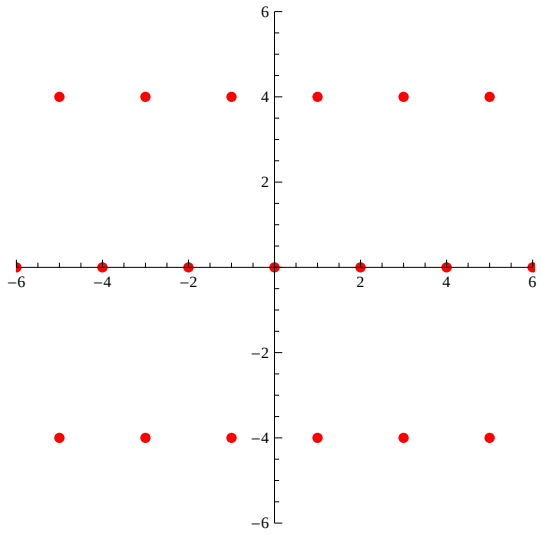

Figura 3.2: Representação geométrica do reticulado do Exemplo 3.9

Exemplo 3.11. Do Exemplo 3.9 temos que Λ tem posto completo e portanto,

$$det(\Lambda) = (det(M))^2 = (8-0)^2 = 64.$$

Neste trabalho vamos considerar reticulados de posto completo.

Definição 3.12. *A **norma mínima** de um reticulado Λ é dada por*

$$|\Lambda| := min\{\|\mathbf{x}\| : \mathbf{x} \in \Lambda,\, \mathbf{x} \neq 0\},$$

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

Observe que é sempre possível definir a norma mínima de um reticulado uma vez que Λ é não vazio e é um conjunto discreto. Dessa forma, pode-se definir o conjunto das distâncias entre os pontos do reticulado e a origem, e esse conjunto terá elemento mínimo, conforme a referência [19].

Exemplo 3.13. Do Exemplo 3.9 temos que a norma mínima do reticulado é 2, já que os vetores com norma mínima são $(2,0)$ e $(-2,0)$.

Definição 3.14. *Um **empacotamento esférico**, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Definição 3.15. *Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, definimos a **densidade de empacotamento** de Λ como*

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

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

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

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

Para mais detalhes sobre o assunto, consulte a Referência [8].

O objetivo do empacotamento esférico é encontrar uma maneira de arranjar esferas de mesmo raio de forma que o espaço do $\mathbb{R}^n$ coberto por elas seja o maior possível.

Observação 3.16. Note que:

(i) Tomaremos o raio das esferas do empacotamento como a metade de η.

(ii) Quando o conjunto dos centros da esferas do empacotamento forma um reticulado, chamamos esse empacotamento de *empacotamento reticulado*.

Exemplo 3.17. Seja o reticulado $\mathbb{Z}^2$ com base $\{(1,0),(1,3)\}$. Temos que o raio das esferas é $\rho = \frac{1}{2}$ e que $\mathcal{V}ol(\mathcal{B}(1)) = 1 \cdot \pi = \pi$. O volume do reticulado é dado por $\mid det(M) \mid = 3 - 1 = 2$. Logo, a densidade de empacotamento é

$$\frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)} = \frac{\pi \cdot (\frac{1}{2})^2}{2} = \frac{\pi}{8} \cong 39,3\%.$$

Isso quer dizer que as esferas (círculos, neste caso) ocupam $39,3\%$ do $\mathbb{R}^2$.

A densidade de centro desse reticulado é $\frac{1}{8}$.

Os empacotamentos reticulados de maior densidade são conhecidos nas dimensões 1 a 8 e 24. Para maiores informações, consulte a Referência [8].

Definição 3.18. *Seja B uma matriz $n \times n$ com coeficientes em $\mathbb{Z}$. Um* ***sub-reticulado*** *Λ' de Λ é dado por*

$$\Lambda' = \{\mathbf{x} = MB\lambda \mid \lambda \in \mathbb{Z}^n\},$$

em que M é a matriz geradora de Λ.

Exemplo 3.19. Considere o reticulado

$$\Lambda = \mathbb{Z}^2 = \left\{\mathbf{x} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \mid \lambda_1,\, \lambda_2 \in \mathbb{Z}\right\}.$$

Se tomarmos um reticulado

$$\Lambda' = \left\{\mathbf{x} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & -5 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \mid \lambda_1,\, \lambda_2 \in \mathbb{Z}\right\},$$

temos que Λ é um sub-reticulado de $\mathbb{Z}^2$.

Em outras palavras, quando um reticulado Λ' é sub-reticulado de Λ, temos que Λ' é um subconjunto de Λ que também é um reticulado. Na Figura 3.3 apresentamos à esquerda a representação geométrica de $\Lambda^{'}$ e à direita a representação geométrica de Λ.

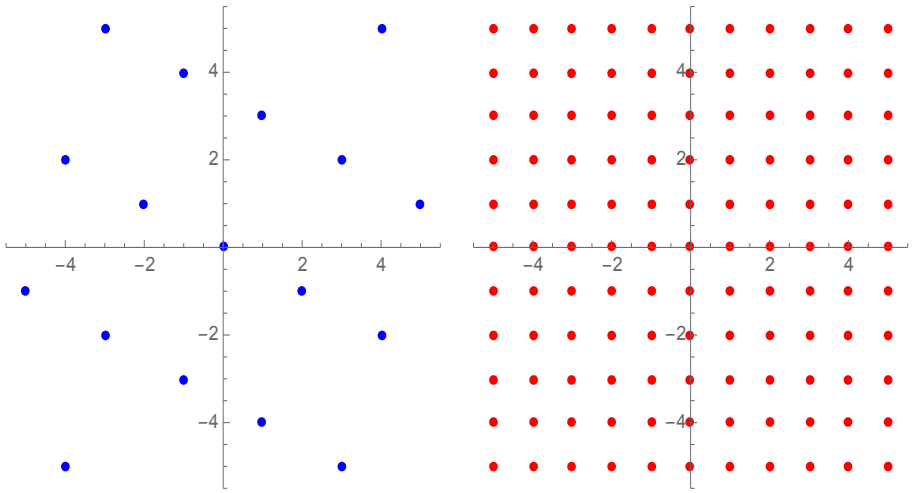

Figura 3.3: Representação geométrica dos reticulados do Exemplo 3.19

Definição 3.20. *Dado um reticulado Λ, um reticulado* ***escalonado*** *Λ' pode ser obtido multiplicando todos os vetores do reticulado por uma constante, isto é,*

$$\Lambda' = c\Lambda,\ c \in \mathbb{R}.$$

Ainda, Λ' é um sub-reticulado de Λ quando $c \in \mathbb{Z}$.

Exemplo 3.21. Considere o reticulado

$$\Lambda = \left\{ \mathbf{x} = \begin{pmatrix} 1 & 0 & 7 \\ 2 & -1 & 1 \\ -3 & 0 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \mid \lambda_1,\ \lambda_2,\ \lambda_3 \in \mathbb{Z} \right\}.$$

Se tomarmos

$$\Lambda' = \left\{ \mathbf{x} = c \begin{pmatrix} 1 & 0 & 7 \\ 2 & -1 & 1 \\ -3 & 0 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \mid \lambda_1,\ \lambda_2,\ \lambda_3 \in \mathbb{Z} \text{ e } c \in \mathbb{R} \right\},$$

temos que Λ' é um reticulado escalonado.

Se $c \in \mathbb{Z}$, temos que Λ' é um reticulado escalonado e um sub-reticulado de Λ.

Na Figura 3.4 apresentamos a representação geométrica de Λ.

Definição 3.22. *Dois reticulados $\Lambda_1,\ \Lambda_2 \subset \mathbb{R}^n$ de posto n são ditos* ***semelhantes*** *ou* ***equivalentes*** *se existe uma matriz ortogonal A, de ordem n com entradas em $\mathbb{R}$, e uma constante real α tal que $\Lambda_1 = \alpha A \Lambda_2$.*

Exemplo 3.23. Os reticulados

$$\Lambda_1 = \left\{ \begin{pmatrix} 6 & 3 \\ 0 & 12 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \mid \lambda_1,\ \lambda_2 \in \mathbb{Z} \right\} \text{ e}$$

$$\Lambda_2 = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} \lambda_3 \\ \lambda_4 \end{pmatrix} \mid \lambda_3, \lambda_4 \in \mathbb{Z} \right\}$$

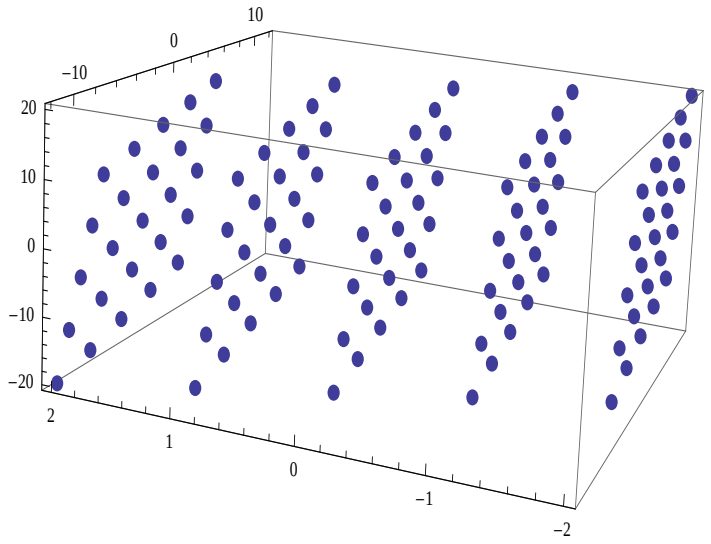

Figura 3.4: Representação geométrica do reticulado Λ do Exemplo 3.21

do $\mathbb{R}^2$ são semelhantes, pois

$$\begin{pmatrix} 6 & 3 \\ 0 & 12 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix}.$$

Em outras palavras, reticulados semelhantes têm a mesma configuração mas não a mesma escala.

Observação 3.24. Note que:

1. Se Λ' é um reticulado escalonado $\Lambda' = c\Lambda$, então Λ' também é semelhante a Λ fazendo $\Lambda' = cI\Lambda$, sendo I a matriz identidade.

2. Se Λ' é um sub-reticulado de Λ, então Λ' e Λ são semelhantes. De fato, se M é a matriz geradora de Λ e MB a matriz geradora de Λ', basta fazer $\alpha = 1$ para obter $\Lambda' = \alpha MB\Lambda$.

3. A semelhança entre Λ_1 e Λ_2 é uma relação de equivalência, que denotamos por $\sim$, isto é, $\Lambda_1 \sim \Lambda_2$. De fato, a semelhança de reticulados segue das condições da Definição 7.36 de relação de equivalência, pois, dados Λ_1, $\Lambda_2 \subseteq \mathbb{R}^n$,

   (i) $\Lambda_1 \sim \Lambda_1$, já que $\Lambda_1 = 1 \cdot I \cdot \Lambda_1$, em que I é a matriz identidade de $M_n(\mathbb{R})$.

   (ii) Se $\Lambda_1 \sim \Lambda_2$ então $\Lambda_2 \sim \Lambda_1$.
   De fato, se $\Lambda_1 = \alpha A\Lambda_2$, com $\alpha \in \mathbb{R}$ e A uma matriz ortogonal de $M_n(\mathbb{R})$, então,

$$\begin{aligned} A^t\Lambda_1 &= \alpha A^t A\Lambda_2 \\ A^t\Lambda_1 &= \alpha I\Lambda_2 \\ \alpha^{-1}A^t\Lambda_1 &= \Lambda_2, \end{aligned}$$

   sendo I a matriz identidade, $\alpha^{-1} \in \mathbb{R}$ e A^t uma matriz ortogonal. Portanto, $\Lambda_2 \sim \Lambda_1$.

(iii) Se $\Lambda_1 \sim \Lambda_2$ e $\Lambda_2 \sim \Lambda_3$, então $\Lambda_1 \sim \Lambda_3$.
De fato, se $\Lambda_1 = \alpha A\Lambda_2$ e $\Lambda_2 = \beta B\Lambda_3$, com $\alpha, \beta \in \mathbb{R}$ e A, B matrizes ortogonais de $M_n(\mathbb{R})$, então

$$\begin{aligned} A^t\Lambda_1 &= \alpha A^t A\Lambda_2 \\ A^t\Lambda_1 &= \alpha I\Lambda_2 \\ \alpha^{-1}A^t\Lambda_1 &= \Lambda_2. \end{aligned}$$

Como $\Lambda_2 = \beta B\Lambda_3$,

$$\begin{aligned} \alpha^{-1}A^t\Lambda_1 &= \beta B\Lambda_3 \\ A^t\Lambda_1 &= (\alpha\beta)B\Lambda_3 \\ AA^t\Lambda_1 &= (\alpha\beta)AB\Lambda_3 \\ I\Lambda_1 &= (\alpha\beta)AB\Lambda_3 \\ \Lambda_1 &= (\alpha\beta)AB\Lambda_3, \end{aligned}$$

sendo I a matriz identidade, $\alpha\beta \in \mathbb{R}$ e AB uma matriz ortogonal, já que a multiplicação de matrizes ortogonais também é ortogonal. Portanto, $\Lambda_1 \sim \Lambda_3$.

As classes de equivalência dos reticulados sob esta relação em $\mathbb{R}^n$ são chamadas de *classes de semelhanças.*

3.2 Reticulados algébricos

Nesta seção apresentamos como construir reticulados algébricos no $\mathbb{R}^n$. Reticulados algébricos são reticulados obtidos via o anel dos inteiros algébricos de um corpo de números ou via um ideal no anel dos inteiros algébricos de um corpo de números. Esse tipo de reticulado é construído através da imagem de um homomorfismo específico.

Definição 3.25. *Sejam $\sigma_1, \cdots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de um corpo de números $\mathbb{K}$ de grau n, e vamos ordenar os σ_i's de modo que, para todo $x \in \mathbb{K}$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, e $\sigma_{j+r_2}(x)$ é o conjugado complexo de $\sigma_j(x)$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Note que $r_1 + 2r_2 = n$. Chamamos de* ***homomorfismo canônico*** *ou* ***homomorfismo de Minkowski*** *$\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por*

$$\sigma(x) := (\sigma_1(x), \cdots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \cdots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

em que $\Re$ e $\Im$ denotam as partes real e imaginária, respectivamente.

Observação 3.26. Note que r_1 é o número de monomorfismos reais e $2r_2$ é o número de monomorfismos complexos.

Exemplo 3.27. Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$, e $\{\sigma_1, \sigma_2\}$ o conjunto dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, em que σ_1 é a aplicação identidade e $\sigma_2(\sqrt{-2}) = -\sqrt{-2}$. Neste caso, $r_1 = 0$ e $r_2 = 1$. Para $x = a + b\sqrt{-2} \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos $\sigma(a + b\sqrt{-2}) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b\sqrt{2})$.

Uma das aplicações do homomorfismo canônico é a geração de reticulados $\mathbb{R}^n$, como apresentamos no teorema a seguir.

Teorema 3.28. *Se $\{w_1, \cdots, w_n\}$ é uma base integral para $\mathcal{O}_\mathbb{K}$ e $\sigma : \mathbb{K} \to \mathbb{C}$ o homomorfismo canônico, então os n vetores $v_i = \sigma(w_i) \in \mathbb{R}^n$, $i = 1, \cdots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado* ***reticulado algébrico****.*

A demonstração do teorema anterior pode ser encontrada na Referência [28].

Em outras palavras, um reticulado algébrico é um reticulado gerado pelas imagens dos vetores de uma de suas bases integrais via homomorfismo canônico.

Partindo do que foi dito no Teorema 3.28, apresentamos a definição a seguir.

Definição 3.29. *Se $\{w_1, \cdots, w_n\}$ é uma base integral de $\mathcal{O}_\mathbb{K}$, o anel dos inteiros algébricos de $\mathbb{K}$, a matriz geradora do reticulado algébrico $\Lambda \subset \mathbb{R}^n$ é dada por*

$$\begin{pmatrix} \sigma_1(w_1) & \sigma_1(w_2) & \cdots & \sigma_1(w_n) \\ \vdots & \ddots & \vdots & \\ \sigma_{r_1}(w_1) & \sigma_{r_1}(w_2) & \cdots & \sigma_{r_1}(w_n) \\ \Re\sigma_{r_1+1}(w_1) & \Re\sigma_{r_1+1}(w_2) & \cdots & \Re\sigma_{r_1+1}(w_n) \\ \Im\sigma_{r_1+r_2}(w_1) & \Im\sigma_{r_1+r_2}(w_2) & \cdots & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}.$$

Exemplo 3.30. Seja o corpo quadrático $\mathbb{K}$ do Exemplo 3.27. Sabemos que $-2 \equiv 2 \ (mod\ 4)$ e, pelo Teorema 2.4, $\mathcal{O}_\mathbb{F} = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}, \text{ com } a, b \in \mathbb{Z}\}$ e uma base integral para $\mathcal{O}_\mathbb{F}$ é $\{1, \sqrt{-2}\}$.
Para $\mathbf{x} = a + b\sqrt{-2} \in \mathbb{K}$, temos que $\sigma(\mathbf{x}) = (a, b\sqrt{2})$, logo

$$\sigma(1) = (1, 0)$$

$$\sigma(\sqrt{-2}) = (0, \sqrt{2}).$$

Assim, os vetores geradores desse reticulado são $(1, 0)$ e $(0, \sqrt{2})$.

Por outro lado, a matriz geradora do reticulado gerado pelas imagens de $\{1, \sqrt{-2}\}$ é

$$\begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(\sqrt{-2}) \\ \Im\sigma_1(1) & \Im\sigma_1(\sqrt{-2}) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix},$$

e a Figura 3.5 apresenta a sua representação geométrica.

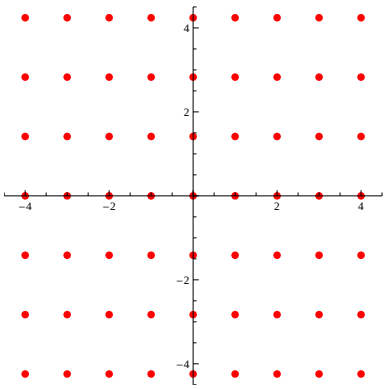

Figura 3.5: Representação geométrica do reticulado algébrico do Exemplo 3.30 gerado pela base $\{(1, 0), (0, \sqrt{2})\}$.

Proposição 3.31. *Sejam $\mathbb{K}$ um corpo de números de grau n, σ o homomorfismo canônico e I um ideal não nulo de $\mathcal{O}_\mathbb{K}$. Os conjuntos $\sigma(\mathcal{O}_\mathbb{K})$ e $\sigma(\mathcal{I})$ são reticulados algébricos, com volumes*

$$\mathcal{V}ol(\sigma(\mathcal{O}_\mathbb{K})) = 2^{-r_2}|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}},$$
$$\mathcal{V}ol(\sigma(\mathcal{I})) = \mathcal{V}ol(\sigma(\mathcal{O}_\mathbb{K}))\mathcal{N}(\mathcal{I}).$$

em que $\mathcal{N}(\mathcal{I})$ indica a norma de I.

A demonstração da Proposição 3.31 pode ser encontrada na Referência [25].

Denotaremos o reticulado $\sigma(\mathcal{O}_\mathbb{K})$ por $\Lambda_\mathbb{K}$ e o reticulado $\sigma(\mathcal{I})$ por $\Lambda_\mathbb{K}(\mathcal{I})$.

Exemplo 3.32. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Pelo Teorema 2.4, o anel dos inteiros algébricos é dado por $\mathcal{O}_\mathbb{K} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ e uma base integral para $\mathcal{O}_\mathbb{K}$ é $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$.

Os dois monomorfismos são $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$. Neste caso, $r_1 = 2$ e $r_2 = 0$, assim para $x = a + b\sqrt{5} \in \mathbb{K}$, temos que o homomorfismo canônico é dado por $\sigma(x) = (\sigma_1(x), \sigma_2(x)) = (a + b\sqrt{5}, a - b\sqrt{5})$. Calculando o homomorfismo canônico nos elementos da base integral, temos

$$\sigma(1) = (\sigma_1(1), \sigma_2(1)) = (1, 1);$$
$$\sigma\left(\frac{1+\sqrt{5}}{2}\right) = \left(\sigma_1\left(\frac{1+\sqrt{5}}{2}\right), \sigma_2\left(\frac{1+\sqrt{5}}{2}\right)\right) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right).$$

Pela Proposição 3.31, $\Lambda_\mathbb{K}$ é um reticulado no $\mathbb{R}^2$ gerado pelos pontos $(1, 1)$ e $\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$.
Além disso, a matriz geradora do reticulado $\Lambda_\mathbb{K}$ é

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}.$$

Como o discriminante de $\mathbb{K}$ é 5, conforme vimos no Exemplo 2.6, o volume de $\Lambda_\mathbb{K}$ é $\mathcal{V}ol(\sigma(\Lambda_\mathbb{K})) = 2^{-0}|5|^{\frac{1}{2}} = \sqrt{5}$.
A Figura 3.6 mostra a forma do reticulado $\Lambda_\mathbb{K}$.

Exemplo 3.33. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Pelo Teorema 2.4, o anel dos inteiros algébricos é dado por $\mathcal{O}_\mathbb{K} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ e uma base integral para $\mathcal{O}_\mathbb{K}$ é $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$.

Os dois monomorfismos são $\sigma_1(\sqrt{-3}) = \sqrt{-3}$, $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$. Neste caso, $r_1 = 0$ e $r_2 = 1$, assim, para $x = a + b\sqrt{-3} \in \mathbb{K}$ temos que o homomorfismo canônico é dado por

$$\sigma(x) = (\Re\sigma_1(x), \Im\sigma_1(x)).$$

Calculando o homomorfismo canônico nos elementos da base integral, temos

$$\sigma(1) = (\Re\sigma_1(1), \Im\sigma_1(1)) = (1, 0);$$

$$\sigma\left(\frac{1+\sqrt{-3}}{2}\right) = \left(\Re\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right), \Im\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right)\right) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right).$$

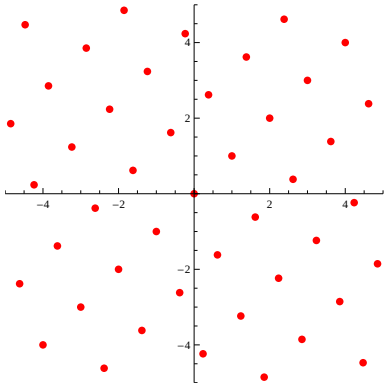

Figura 3.6: Representação geométrica do reticulado algébrico do Exemplo 3.32 gerado pela base $\left\{(1,1), \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)\right\}$.

Pela Proposição 3.31, $\Lambda_{\mathbb{K}}$ é um reticulado no $\mathbb{R}^2$ gerado pelos pontos $(1,0)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. Além disso, a matriz geradora do reticulado $\Lambda_{\mathbb{K}}$ é

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

O volume de $\Lambda_{\mathbb{K}}$ é

$$\mathcal{V}ol(\Lambda_{\mathbb{K}}) \quad = \quad 2^{-1}|-3|^{\frac{1}{2}} = \frac{\sqrt{3}}{2}.$$

A Figura 3.7 mostra a forma do reticulado $\Lambda_{\mathbb{K}}$.

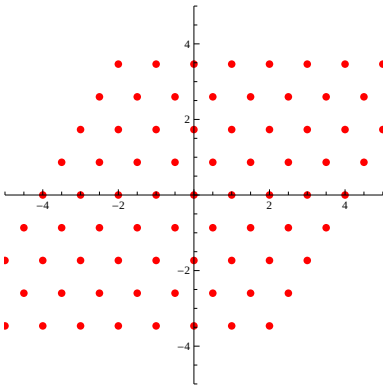

Figura 3.7: Representação geométrica do reticulado algébrico do Exemplo 3.33 gerado pela base $\left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$.

Observação 3.34. Note que:

(i) É possível verificar que com essa estrutura algébrica obtém-se o *reticulado hexagonal*, que na literatura é denotado por A_2, e possui volume igual a $\frac{\sqrt{3}}{2}$ e densidade de centro igual a $\frac{1}{\sqrt{12}}$. Esse tipo de reticulado recebe esse nome pois podemos formar hexágonos regulares com os pontos do reticulado, conforme a Figura 3.7. É importante lembrar que todos os reticulados semelhantes a A_2 também são hexagonais. Para maiores detalhes, consulte [8].

(ii) Observe que nos exemplos anteriores poderíamos ter calculado o volume do reticulado a partir de sua matriz geradora, como na Definição 3.4.

(iii) Como citamos anteriormente, um reticulado algébrico é um reticulado gerado pelas imagens dos vetores de uma de suas bases integrais via homomorfismo canônico. Tais reticulados podem ser obtidos de maneira mais geral, considerando ideais de $\mathcal{O}_{\mathbb{K}}$ ou considerando ideais em $\mathcal{O}_{\mathbb{L}}$, em que $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$.

Um reticulado algébrico $\Lambda^{'}$ construído a partir de um ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{L}}$ fornece um sub-reticulado do reticulado algébrico Λ construído a partir de $\mathcal{O}_{\mathbb{L}}$. Se $\mathcal{I} = \alpha\mathcal{O}_{\mathbb{L}}$, então a matriz geradora M é dada por

$$\begin{pmatrix} \sigma_1(\alpha w_1) & \sigma_1(\alpha w_2) & \cdots & \sigma_1(\alpha w_n) \\ \vdots & \ddots & \vdots & \\ \sigma_{r_1}(\alpha w_1) & \sigma_{r_1}(\alpha w_2) & \cdots & \sigma_{r_1}(\alpha w_n) \\ \Re\sigma_{r_1+1}(\alpha w_1) & \Re\sigma_{r_1+1}(\alpha w_2) & \cdots & \Re\sigma_{r_1+1}(\alpha w_n) \\ \Im\sigma_{r_1+r_2}(\alpha w_1) & \Im\sigma_{r_1+r_2}(\alpha w_2) & \cdots & \Im\sigma_{r_1+r_2}(\alpha w_n) \end{pmatrix}.$$

4 Reticulados bem arredondados

Neste capítulo, investigamos em quais condições reticulados algébricos em $\mathbb{R}^2$ são *bem arredondados*, do inglês, *well rounded*.

Tal investigação é importante para o estudo de empacotamentos esféricos, problemas referentes ao número de contato (do inglês, *kissing number*) e outras propriedades de reticulados que são interessantes na aplicação prática.

Como este é um tema de estudo recente, existem poucas referências relacionadas à ele. Para o seu desenvolvimento, as referências utilizadas foram [6], [12], [14] e [28].

4.1 Definições iniciais

A fim de facilitar a leitura do texto, toda vez que nos referirmos aos reticulados bem arredondados, usaremos a sigla *WR* (Well-Rounded).

Definição 4.1. *Seja Λ um reticulado de posto completo em $\mathbb{R}^d$, com $d \geq 2$. O **conjunto dos vetores mínimos** de Λ é definido por*

$$S(\Lambda) := \{\mathbf{x} \in \Lambda : \|\mathbf{x}\| = |\Lambda|\},$$

onde $|\Lambda| = min\{\|\mathbf{x}\| : \mathbf{x} \in \Lambda, \mathbf{x} \neq 0\}$ (ver Definição 3.12).

Definição 4.2. *Seja Λ um reticulado de posto completo em $\mathbb{R}^d$, com $d \geq 2$. Dizemos que Λ é um **reticulado WR** se $S(\Lambda)$ gera $\mathbb{R}^d$.*

Observação 4.3. A propriedade *WR* é preservada com relação à semelhança. Em outras palavras, se dois reticulados de posto completo Λ_1, $\Lambda_2 \subset \mathbb{R}^n$ são semelhantes e Λ_1 é *WR* então Λ_2 também é *WR*.

Lembremos da Seção 3.2 que $\Lambda_{\mathbb{K}}(\mathcal{I}) = \sigma(\mathcal{I})$ denota o reticulado em $\mathbb{R}^2$ obtido via o ideal $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ e $\Lambda_{\mathbb{K}} = \sigma(\mathcal{O}_{\mathbb{K}})$, em que $\sigma : \mathbb{K} \to \mathbb{R}^2$ é o homomorfismo canônico dado na Definição 3.25.

Observação 4.4. Dado $x \in \Lambda$, $x \neq 0$, a fim de facilitar os cálculos consideramos $||\mathbf{x}||^2$ ao invés de $||\mathbf{x}||$, pois o resultado não se altera.

Exemplo 4.5. Seja $\mathbb{K} = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. De acordo com a Proposição 2.4, como $-1 \not\equiv 1 \ (mod\ 4)$, então $\{1, i\}$ é uma base integral de $\Lambda_{\mathbb{K}}$. Além disso, é claro que $\mathbb{K}$ é totalmente imaginário já que $r_1 = 0$.

Para todo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

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

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

Daí,

$$\|\mathbf{x}\|^2 = x_1^2 + x_2^2,$$

que assume o menor valor, não nulo, quando $x_1 = \pm 1$ e $x_2 = 0$ ou quando $x_1 = 0$ e $x_2 = \pm 1$. Portanto,

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

Claramente, $S(\Lambda_{\mathbb{K}})$ gera $\mathbb{R}^2$, o que é suficiente para concluir que $\Lambda_{\mathbb{K}}$ é bem arredondado.

Observação 4.6. O resultado encontrado no Exemplo 4.5 era intuitivamente esperado. Tal afirmação pode ser verificada a partir da Figura 4.1 a seguir, no plano cartesiano, que descreve os pontos de $\Lambda_{\mathbb{K}}$ em uma parcela da região próxima à origem de $\mathbb{R}^2$.

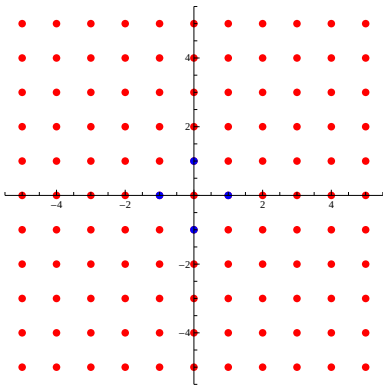

Figura 4.1: Representação geométrica do reticulado do Exemplo 4.5.

Os pontos em azul são os de menor distância até a origem (exceto ela mesma), o que é equivalente a afirmar que são os elementos de $S(\Lambda_{\mathbb{K}})$, o que de fato acontece, como verificado no Exemplo 4.5 .

Exemplo 4.7. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}$. De acordo com a Proposição 2.4, o conjunto $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$ é base integral de $\Lambda_{\mathbb{K}}$, uma vez que $-3 \equiv 1 \ (mod\ 4)$. Além disso, sabemos que $\mathbb{K}$ é totalmente imaginário, já que $r_1 = 0$.

Para todo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

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

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

Daí,

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

que assume o menor valor, não nulo, quando $x_1 = \pm 1$ e $x_2 = 0$, $x_1 = 0$ e $x_2 = \pm 1$, $x_1 = 1$ e $x_2 = -1$ ou $x_1 = -1$ e $x_2 = 1$. Portanto,

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

Novamente, é claro que $S(\Lambda_{\mathbb{K}})$ gera $\mathbb{R}^2$, ou seja, $\Lambda_{\mathbb{K}}$ é bem arredondado.

Para dimensão 2, os únicos reticulados obtidos via o anel dos inteiros de um corpo de números que são *WR* são $\Lambda_{\mathbb{Q}(i)}$ e $\Lambda_{\mathbb{Q}(\sqrt{-3})}$. Mostraremos tal resultado na próxima seção.

Além disso, todos os sub-reticulados de $\Lambda_{\mathbb{Q}(i)}$ e $\Lambda_{\mathbb{Q}(\sqrt{-3})}$, obtidos a partir de ideais em $\mathcal{O}_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(i)$ e $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$, também são *WR*. Isto é uma consequência direta do fato de que sub-reticulados de $\Lambda_{\mathbb{Q}(i)}$ e $\Lambda_{\mathbb{Q}(\sqrt{-3})}$ são semelhantes à $\Lambda_{\mathbb{Q}(i)}$ e $\Lambda_{\mathbb{Q}(\sqrt{-3})}$ (ver 3.24).

No entanto, a unicidade observada acima se refere a reticulados em $\mathbb{R}^2$ obtidos via o anel dos inteiros de um corpo de números. Para o caso dos reticulados em $\mathbb{R}^2$, obtidos via um ideal fracionário no anel dos inteiros de um corpo de números, mostraremos no Teorema 4.13 que existem infinitos corpos quadráticos $\mathbb{K}$ cujo anel dos inteiros algébricos contém um ideal $\mathcal{I}$ com a propriedade de que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*. Apesar disso, é relevante observar que existem corpos quadráticos cujo anel dos inteiros algébricos não contém nenhum ideal de modo que o reticulado correspondente seja *WR*.

4.2 Reticulados $\Lambda_{\mathbb{K}}(\mathcal{I})$ bem arredondados em $\mathbb{R}^2$

Nesta seção investigamos em que condições reticulados em $\mathbb{R}^2$ do tipo $\Lambda_{\mathbb{K}}(\mathcal{I})$, onde $\mathbb{K}$ é um corpo quadrático e $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, são *WR*.

Iniciamos este estudo apresentando uma propriedade geral sobre reticulados *WR* e que será necessária para os resultados que apresentamos adiante.

Lema 4.8. *Um reticulado de posto completo $\Lambda \subset \mathbb{R}^2$ contém $2, 4,$ ou 6 vetores mínimos e é WR se, e somente se, $\mid S(\Lambda) \mid = 4, 6$. Além disso, $\mid S(\Lambda) \mid = 6$ se, e somente se, Λ é semelhante a $\Lambda_{\mathbb{Q}(\sqrt{-3})}$, o reticulado hexagonal.*

Demonstração. Seja $\mathbf{x} \in S(\Lambda)$. É claro que $\|\mathbf{x}\|^2 = \|-\mathbf{x}\|^2$, e então $-\mathbf{x} \in S(\Lambda)$. Sabemos que, se dois vetores distintos de $S(\Lambda)$ são linearmente dependentes, então são opostos entre si. Assim, $S(\Lambda)$ tem um número par de elementos e contém dois vetores linearmente independentes se, e somente se, $|S(\Lambda)| \geq 4$.

Suponha que o ângulo θ entre dois vetores distintos $\mathbf{x}, \mathbf{y} \in S(\Lambda)$ seja tal que $\theta < \frac{\pi}{3}$. Então, pela lei dos cossenos,

$$\|\mathbf{x} - \mathbf{y}\|^2 = \|\mathbf{x}\|^2 - 2\|\mathbf{x}\|\|\mathbf{y}\|\cos\theta + \|\mathbf{y}\|^2 < \|\mathbf{x}\|^2 - \|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2.$$

Como $\|\mathbf{x}\| = \|\mathbf{y}\|$, pois $\mathbf{x}$ e $\mathbf{y} \in S(\Lambda)$, da desigualdade acima segue que

$$\|\mathbf{x} - \mathbf{y}\|^2 < \|\mathbf{x}\|^2 = \|\mathbf{y}\|^2,$$

o que é um absurdo, já que encontramos um vetor $\mathbf{x} - \mathbf{y} \in \Lambda$, com $\mathbf{x} - \mathbf{y} \neq 0$, com norma menor que $\|\mathbf{x}\| = \|\mathbf{y}\|$. Sendo assim, o ângulo entre os vetores de $S(\Lambda)$ deve ser maior ou igual a $\dfrac{\pi}{3}$.

Pela definição de $S(\Lambda)$, seus vetores estão compreendidos na circunferência de centro na origem e raio $|\Lambda|$. Então, $|S(\Lambda)|$ é tal que

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

Segue da desigualdade anterior que $\mid S(\Lambda) \mid \leq 6$. Então $\mid S(\Lambda) \mid = 2,\ 4$ ou 6.

Se $|\ S(\Lambda)\ | = 2$, então Λ não é *WR*, pois 2 vetores linearmente dependentes não geram $\Lambda \subset \mathbb{R}^2$. Portanto Λ é *WR* se, e somente se, $|S(\Lambda)| = 4$ ou 6.

Agora vamos mostrar que se $|\ S(\Lambda)\ | = 6$ então $\Lambda \sim \Lambda_{\mathbb{Q}(\sqrt{-3})}$.

Observe que se $|\ S(\Lambda)\ | = 6$, o ângulo formado por dois vetores quaisquer $\mathbf{x}, \mathbf{y} \in S(\Lambda)$ deve ser, necessariamente, $\frac{\pi}{3}$, pois, se houvesse dois vetores cujo ângulo entre eles fosse maior, haveria também um par de vetores com ângulo entre eles menor que $\frac{\pi}{3}$, o que é um absurdo.

Como o ângulo entre $\mathbf{x}$ e $\mathbf{y}$ é $\frac{\pi}{3}$ e Λ tem posto igual a 2, então $\mathbf{x}$ e $\mathbf{y}$ são linearmente independentes e, consequentemente, estes dois vetores formam uma base de Λ, segue que $\Lambda \sim \Lambda_{\mathbb{Q}(\sqrt{-3})}$. Fazendo rotação e dilatação dos vetores, obtemos o reticulado hexagonal.

Por outro lado, se $\Lambda \sim \Lambda_{\mathbb{Q}(\sqrt{-3})}$, então $|S(\Lambda)| = |S(\Lambda_{\mathbb{Q}(\sqrt{-3})})| = 6$. □

Observação 4.9. Para reticulados com quatro vetores mínimos, existem infinitas classes de semelhanças distintas de reticulados *WR* em $\mathbb{R}^2$.

De fato, isto é intuitivamente esperado, já que, se $\mathbf{x} \in S(\Lambda)$, então $-\mathbf{x} \in S(\Lambda)$. Tais pontos formam um ângulo π entre si, e o arco formado por eles contém uma infinidade de pontos. Cada ponto $\mathbf{y}$ dessa infinidade obviamente se comporta como um vetor em $\mathbb{R}^2$, e seu oposto $-\mathbf{y}$ também tem um ponto correspondente pertencente à mesma circunferência. É demonstrável que a infinidade de possibilidades para $\mathbf{y}$ se mantém se aplicarmos a restrição de que quaisquer dois pontos de $\{-\mathbf{x}, \mathbf{x}, -\mathbf{y}, \mathbf{y}\}$ formem um ângulo maior ou igual a $\frac{\pi}{3}$, como vemos na Figura 4.9. Para isso, basta que y faça um ângulo θ_1 com x de modo que $\frac{\pi}{3} \leq \theta_1 \leq \frac{2\pi}{3}$. Daí, se θ_2 é o ângulo entre $\mathbf{y}$ e $-\mathbf{x}$, então $\theta_2 = \pi - \theta_1 \geq \pi - \frac{2\pi}{3} = \frac{\pi}{3}$. Assim, existem infinitas configurações de quatro pontos numa circunferência de centro na origem que possam eventualmente ser representadas por reticulados de quatro vetores mínimos. É de se esperar então que existam infinitas famílias de reticulados com $|S(\Lambda)| = 4$. Para maiores detalhes, consulte [14].

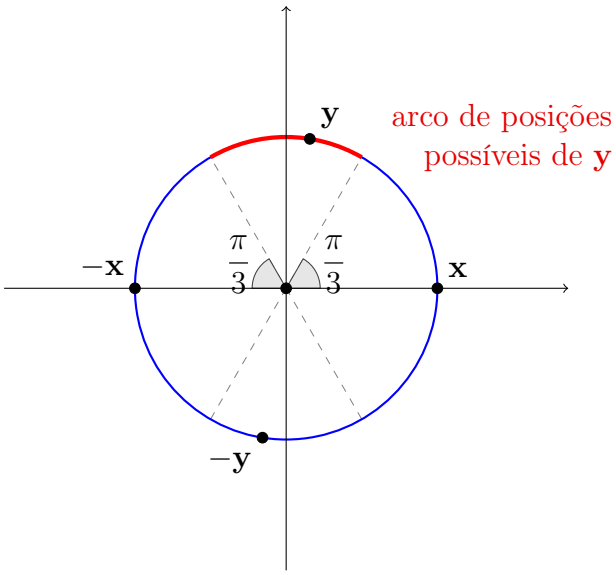

Figura 4.9: Representação de ângulo entre dois vetores

A proposição a seguir mostra que apenas os reticulados algébricos $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$ são *WR*.

Proposição 4.10. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, $d \neq 1$. Então $\Lambda_{\mathbb{K}}$ é WR se, e somente se, $d = -1$ ou $d = -3$.*

Demonstração. Seja $x \in \Lambda_{\mathbb{K}}$.

(i) 1º caso: $d \not\equiv 1 \ (mod\ 4)$, $d > 0$.

Neste caso, para qualquer elemento não nulo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

$$\mathbf{x} = \begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2\sqrt{d} \\ x_1 - x_2\sqrt{d} \end{pmatrix},$$

onde x_1, $x_2 \in \mathbb{Z}$. Daí,

$$\|\mathbf{x}\|^2 = (x_1 + x_2\sqrt{d})^2 + (x_1 - x_2\sqrt{d})^2 = 2(x_1^2 + dx_2^2) \geq 2 \ ,$$

que assume menor valor quando $x_1 = \pm 1$ e $x_2 = 0$, logo $S(\Lambda_{\mathbb{K}}) = \{(1,1), (-1,-1)\}$. Portanto, $\Lambda_{\mathbb{K}}$ não pode ser *WR*.

(ii) 2º caso: $d \not\equiv 1 \ (mod\ 4)$, $d < 0$

Neste caso, para qualquer elemento não nulo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

$$\mathbf{x} = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(\sqrt{d}) \\ \Im\sigma_1(1) & \Im\sigma_1(\sqrt{d}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|d|} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2\sqrt{|d|} \end{pmatrix},$$

onde x_1, $x_2 \in \mathbb{Z}$. Daí,

$$\|\mathbf{x}\|^2 = x_1^2 + |d|x_2^2 \geq 1 \ ,$$

que assume o menor valor quando $x_1 = \pm 1$ e $x_2 = 0$, a menos que $d = -1$. Nesse caso, $x_1 = 0$ e $x_2 = \pm 1$ são também soluções. Portanto, $\Lambda_{\mathbb{K}}$ é *WR* se, e somente se, $d = -1$. Se este é o caso, $S(\Lambda_{\mathbb{K}}) = \{(1,0), (0,1), (-1,0), (0,-1)\}$.

(iii) 3º caso: $d \equiv 1 \ (mod\ 4)$, $d > 0$ (então $d \geq 5$)

Neste caso, para qualquer elemento não nulo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

$$\mathbf{x} = \begin{pmatrix} \sigma_1(1) & \sigma_1(\frac{1+\sqrt{d}}{2}) \\ \sigma_2(1) & \sigma_2(\frac{1+\sqrt{d}}{2}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{2x_1+x_2}{2} + \frac{x_2\sqrt{d}}{2} \\ \frac{2x_1+x_2}{2} - \frac{x_2\sqrt{d}}{2} \end{pmatrix},$$

onde x_1, $x_2 \in \mathbb{Z}$. Daí,

$$\|\mathbf{x}\|^2 = \frac{1}{2}(4x_1^2 + (d+1)x_2^2 + 4x_1x_2) \geq 2 \ ,$$

que assume menor valor quando $x_1 = \pm 1$ e $x_2 = 0$. Logo, $S(\Lambda_{\mathbb{K}}) = \{(1,1), (-1,-1)\}$, o que significa que $\Lambda_{\mathbb{K}}$ não pode ser *WR*.

(iv) 4º caso: $d \equiv 1 \ (mod\ 4)$, $d < 0$ (então $d \leq -3$)

Neste caso, para qualquer elemento não nulo $\mathbf{x} \in \Lambda_{\mathbb{K}}$,

$$\mathbf{x} = \begin{pmatrix} \Re\sigma_1(1) & \Re\sigma_1(\frac{1+\sqrt{d}}{2}) \\ \Im\sigma_1(1) & \Im\sigma_1(\frac{1+\sqrt{d}}{2}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|d|}}{2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{2x_1+x_2}{2} \\ \frac{x_2\sqrt{|d|}}{2} \end{pmatrix},$$

onde x_1, $x_2 \in \mathbb{Z}$. Daí,

$$\|\mathbf{x}\|^2 = x_1^2 + x_1x_2 + \frac{(|d|+1)x_2^2}{4} \geq 1 \ ,$$

que assume o menor valor quando $x_1 = \pm 1$ e $x_2 = 0$, a menos que $d = -3$. Nesse caso, o menor valor é obtido quando $x_1 = 0$ e $x_2 = \pm 1$, quando $x_1 = 1$ e $x_2 = -1$ ou quando $x_1 = -1$ e $x_2 = 1$. Portanto, $\Lambda_{\mathbb{K}}$ é *WR* se, e somente se, $d = -3$. Se este é o caso,

$$S(\Lambda_{\mathbb{K}}) = \{(1,0), (-1,0), (\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}), (\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2}), (-\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}), (-\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2})\},$$

o que conclui a demonstração.

□

O próximo resultado diz respeito à semelhança de reticulados.

Lema 4.11. *Seja $\mathbb{K}$ um corpo quadrático totalmente imaginário. Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ e $J = \alpha\mathcal{I}$ é um ideal fracionário, com $\alpha \in \mathbb{K}^*$, então $\Lambda_{\mathbb{K}}(J) \sim \Lambda_{\mathbb{K}}$.*

Demonstração. Por hipótese, existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{I} = \gamma\mathcal{O}_{\mathbb{K}}$. Pela mesma justificativa, $J = \alpha\gamma\mathcal{O}_{\mathbb{K}}$. Observe que $\alpha\gamma \in \mathbb{C}$. Daí, $\exists\, r, \gamma \in \mathbb{R}$ tais que $\alpha\gamma = r\mathbf{e}^{i\theta}$. Como J é fracionário, faz sentido aplicar o homomorfismo canônico em J para se obter um reticulado. Dado um elemento $\beta = s\mathbf{e}^{i\varphi} \in \mathbb{C}$, $\alpha\gamma$ gera uma rotação e dilatação quando multiplicado por β. Assim,

$$\alpha\gamma\beta = rs\mathbf{e}^{i(\theta+\varphi)}.$$

Como $\Lambda_{\mathbb{K}} = \sigma(\mathcal{O}_{\mathbb{K}})$, essa é a ação de $\alpha\gamma$ no reticulado. Portanto, $\Lambda_{\mathbb{K}}(J) = \sigma(\alpha\gamma\mathcal{O}_{\mathbb{K}})$ é obtido via dilatação e rotação de $\Lambda_{\mathbb{K}}$. Segue que, $\Lambda_{\mathbb{K}} \sim \Lambda_{\mathbb{K}}(J)$. □

Corolário 4.12. *Sejam $\mathbb{K}$ um corpo quadrático tal que $\mathbb{K} = \mathbb{Q}(i)$ ou $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ e $\mathcal{I} \subset \mathbb{K}$ um ideal fracionário não nulo. Então $\Lambda_{\mathbb{K}}(\mathcal{I})$ é WR. Por outro lado, se $\mathbb{K}$ é um corpo quadrático totalmente imaginário tal que $\mathbb{K} \neq \mathbb{Q}(i)$ e $\mathbb{K} \neq \mathbb{Q}(\sqrt{-3})$, e $\mathcal{I} \subset \mathbb{K}$ é ideal não nulo fracionário e principal, então $\Lambda_{\mathbb{K}}(\mathcal{I})$ não é WR.*

Demonstração. Como $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$ são corpos, segue que são também anéis principais. Escreva $\mathbb{K}$ como um desses corpos e seja $\mathcal{I}$ ideal fracionário de $\mathbb{K}$. Assim, $\mathcal{I}$ é ideal principal de $\mathbb{K}$. Daí, $\exists\, \alpha \in \mathbb{K}$ tal que

$$\mathcal{I} = \alpha\mathbb{K} = \left\{\alpha\tfrac{x_1}{x_2} \,:\, x_1, x_2 \in \mathcal{O}_{\mathbb{K}},\, x_2 \neq 0\right\},$$

ou seja, $I = \dfrac{\alpha}{x_2}\mathcal{O}_{\mathbb{K}}$, para algum $x_2 \in \mathcal{O}_{\mathbb{K}}$. Escrevendo $\dfrac{\alpha}{x_2} = \alpha' \in \mathbb{K}$, segue que $\mathcal{I} = \alpha'\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{I}$ é além disso fracionário, segue do Lema 4.11 que $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Lambda_{\mathbb{K}}$. Pela Proposição 4.10, $\Lambda_{\mathbb{K}}$ é *WR*. Como a semelhança entre reticulados preserva a propriedade *WR*, conclui-se a primeira parte da demonstração.

Por outro lado, se $\mathbb{K} \neq \mathbb{Q}(i)$ e $\mathbb{K} \neq \mathbb{Q}(\sqrt{-3})$, pela Proposição 4.10, $\Lambda_{\mathbb{K}}$ não é *WR*.

Se $\mathcal{I}$ é um ideal fracionário principal de $\mathbb{K}$, temos, analogamente ao caso anterior, que $\exists\, \alpha' \in \mathbb{K}$ tal que $\mathcal{I} = \alpha'\mathcal{O}_{\mathbb{K}}$. Daí, pelo Lema 4.11, $\Lambda_{\mathbb{K}}(\mathcal{I}) \sim \Lambda_{\mathbb{K}}$ e, portanto, $\Lambda_{\mathbb{K}}(\mathcal{I})$ não é *WR*.

□

O resultado anterior é importante por apresentar um critério para que reticulados $\Lambda_{\mathbb{K}}(\mathcal{I})$, $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$, em que $\mathbb{K}$ é um corpo quadrático imaginário diferente de $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{-3})$, não sejam *WR*, e também por garantir que, nesses corpos, todo ideal fracionário não nulo gera (mediante o homomorfismo canônico) um reticulado *WR*.

4.3 Construção de uma família infinita de reticulados bem arredondados

Prosseguimos a investigação com a construção de uma família infinita de corpos quadráticos contendo ideais que, mediante o homomorfismo canônico, geram reticulados *WR*. Tal construção é feita a partir de uma escolha conveniente de uma base integral para um ideal em qualquer corpo quadrático.

Em [6], foram provadas as condições apresentadas a seguir. Tais condições serão imprescindíveis para as demonstrações dos Teoremas 4.13 e 4.14.

Sejam $d \in \mathbb{Z}$ livre de quadrados e $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Pelo Teorema 2.4, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\delta]$, onde

$$\delta = \begin{cases} -\sqrt{d}, & \text{se } d \not\equiv 1 \ (mod\ 4) \\ \dfrac{1-\sqrt{d}}{2}, & \text{se } d \equiv 1 \ (mod\ 4). \end{cases} \tag{4.1}$$

Novamente, sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e $\mathcal{I}$ um ideal de $\mathcal{O}_{\mathbb{K}}$.

Existem únicos $a, b, g \in \mathbb{Z}$ com

$$0 < g \leq b < a, \qquad g \mid a \quad e \quad g \mid b \tag{4.2}$$

tais que

$$\mathcal{I} = \mathcal{I}(a, b, g) = \{ax + (b + g\delta)y : x, y \in \mathbb{Z}\}. \tag{4.3}$$

Tal base integral $\{a, b + g\delta\}$ é única para cada ideal $\mathcal{I}$ e é chamada a *base canônica* para $\mathcal{I}$.

Observe que isso não significa diretamente que

$$\mathcal{I} = \langle a, b + g\delta \rangle \ , \tag{4.4}$$

já que, apesar de terem a mesma base, os coeficientes de $\langle a, b + g\delta \rangle$ pertencem a $\mathcal{O}_{\mathbb{K}}$. No entanto, se $a, b, g \in \mathbb{Z}$ também satisfazem a condição

$$\mathcal{N}(b + g\delta) = kga, \text{ para algum inteiro } k \in \mathbb{Z}, \tag{4.5}$$

então vale a igualdade (4.4).

Os dois próximos teoremas fornecem infinitas possibilidades de ideais em $\mathcal{O}_{\mathbb{K}}$, inclusive dando sua caracterização.

Teorema 4.13. *Existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $-d \equiv 1$ $(mod\ 4)$ tais que o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja WR.*

Demonstração. Seja $t \in \mathbb{Z}$, $t > 0$ ímpar e defina

$$g = 1, \ b = \frac{t-1}{2}, \ a = 2b + 2 = t + 1 \text{ e}$$

$$d = (t + 2)(3t + 2) = 3t^2 + 8t + 4.$$

Podemos observar que $a, b, g \in \mathbb{Z}$ satisfazem (4.2), $\forall t \in \mathbb{Z}$.

Além disso, $d \equiv 3 \ (mod\ 4)$, pois como t é ímpar, existe $k \in \mathbb{Z}$ tal que $t = 2k + 1$, em que

$$d = 3(2k+1)^2 + 8(2k+1) + 4 = 3(4k^2 + 4k + 1) + 8(2k+1) + 4. \tag{4.6}$$

Fazendo a congruência módulo 4 em (4.6), temos que

$$\begin{aligned} d &\equiv 3(4k^2 + 4k + 1) \ (mod\ 4) \\ d &\equiv (12k^2 + 12k + 3) \ (mod\ 4) \\ d &\equiv 3 \ (mod\ 4) \ , \end{aligned}$$

o que é equivalente dizer que $-d \equiv 1 \ (mod\ 4)$.

Afirmamos que existem infinitos $t \in \mathbb{Z}$ ímpares tais que d é livre de quadrados. De fato, se $\mathbb{P}$ é o conjunto de números primos ímpares, então $\mathbb{P} \subset \{t + 2 : t \in \mathbb{Z}, 2 \nmid t\}$. Agora, escolhendo $t \in \mathbb{Z}$ de modo que $p = t + 2 \in \mathbb{P}$ e substituindo em (4.6), segue que

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

Pelo Teorema Fundamental da Aritmética, $\exists\, \alpha_1, \alpha_2, ..., \alpha_r, p_1, p_2, ..., p_r, r \in \mathbb{Z}_+^*$ tais que

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

com p_i primo, $\forall i \in \{1, 2, ..., r\}$.

Daí, por definição, para que d seja livre de quadrados, é necessário que $\forall i \in \{1, 2, ..., r\}$, $\alpha_i = 1$ e que $p \neq p_i$. Observe que, se $p \mid 3p - 4$, então $\exists\, k \in \mathbb{Z}$ tal que $4 = p(3 - k)$, em que $p \mid 4$, o que é absurdo, pois $p \in \mathbb{P}$. Portanto, $p \nmid 3p - 4$, ou seja

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

Isso significa que $p \neq p_i$, $\forall i \in \{1, 2, ..., r\}$. Assim, para que $p(3p - 4)$ seja livre de quadrados, basta que $\alpha_i = 1$, $\forall i \in \{1, 2, ..., r\}$, ou seja, que $3p - 4$ também o seja.

Existem infinitos primos p tais que $3p - 4$ é livre de quadrados. Para maiores detalhes, consulte [28]. Assim, existem infinitos primos p tais que d seja livre de quadrados. Para cada uma dessas infinitas possibilidades, $\exists\, t \in \mathbb{Z}$ ímpar tal que $t = p - 2$.

Portanto, existem infinitos $t \in \mathbb{Z}$ ímpares com d livre de quadrados. Para cada t dessa forma, defina $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ e

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

Como $\mathcal{N}(b + g\delta) = \sigma_1(b + g\delta)\sigma_2(b + g\delta) = \left(\frac{t-\sqrt{-d}}{2}\right)\left(\frac{t+\sqrt{-d}}{2}\right) = \frac{t^2+d}{4} = (t+1)^2 = a^2 = a^2 g$, segue que a condição (4.5) é satisfeita, o que significa que $\left\{t + 1, \frac{1-\sqrt{-d}}{2}\right\}$ é base canônica de $\mathcal{I}$. Assim, a matriz geradora de $\Lambda_{\mathbb{K}}(\mathcal{I})$ é dada por

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

Daí, dado $\mathbf{x} \in \Lambda_{\mathbb{K}}(\mathcal{I})$, $\exists\, x_1, x_2 \in \mathbb{Z}$ tais que

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

Assim,

$$\begin{aligned} \|\mathbf{x}\|^2 &= (t+1)^2 x_1^2 + t(t+1)x_1x_2 + \frac{1}{4}(t^2+d)x_2^2,\ d = 3t^2+8t+4 \\ &= a^2x_1^2 + a(a-1)x_1x_2 + a^2x_2^2,\ a = t+1. \end{aligned}$$

Observe que, $\forall x_1, x_2 \in \mathbb{Z}$, com $n \neq 0$, tem-se que

i) $\|\mathbf{x}\|^2 = a^2$ quando $(x_1, x_2) = (\pm 1, 0) = (0, \pm 1)$,

ii) $\|\mathbf{x}\|^2 = 3a^2 - a$ quando $(x_1, x_2) = (1, 1) = (-1, -1)$,

iii) $\|\mathbf{x}\|^2 = a^2 + a$ quando $(x_1, x_2) = (1, -1) = (-1, 1)$,

iv) $\|\mathbf{x}\|^2 > a^2 + a,\ 3a^2 - a,\ a^2$ quando $(x_1, x_2) \neq (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$.

Como $a = t + 1 > 0$, temos que $\|\mathbf{x}\|^2$ assume menor valor em a^2, isto é, quando $x_1 = \pm 1$ e $x_2 = 0$ ou quando $x_1 = 0$ e $x_2 = \pm 1$. Logo,

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

e com isso $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*.

Portanto, existem infinitos corpos quadráticos totalmente imaginários tais que existe pelo menos um ideal I de $\mathcal{O}_{\mathbb{K}}$ tal que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*. □

Observe que a condição $-d \equiv 1\ (mod\ 4)$ não é necessária para a demonstração do teorema, e sim um resultado que é identificado no processo de demonstração.

Teorema 4.14. *Existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $d \equiv 1\ (mod\ 4)$ tais que o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja WR.*

Demonstração. Seja $t \in \mathbb{Z}$, $t > 0$ ímpar e defina

$$g = 1,\ b = \frac{t+1}{2},\ a = 2b + 1 = t + 2 \text{ e}$$

$$d = (t+2)(t-2) = t^2 - 4.$$

Novamente, $a, b, g \in \mathbb{Z}$ satisfazem (4.2), $\forall t \in \mathbb{Z}$.

Além disso, $d \equiv 1\ (mod\ 4)$, pois como t é ímpar, existe $k \in \mathbb{Z}$ tal que $t = 2k + 1$, em que

$$d = (2k+1)^2 - 4 = 4(k^2 + k - 1) + 1, \tag{4.7}$$

e portanto $d \equiv 1\ (mod\ 4)$.

Além disso, $t^2 - 4 = 4(k^2 + k - 1) + 1$, portanto $d \equiv 1\ (mod\ 4)$.

Afirmamos que existem infinitos $t \in \mathbb{Z}$ ímpares tais que d é livre de quadrados. De fato, se $\mathbb{P}$ é o conjunto de números primos ímpares, então $\mathbb{P} \subset \{t+2 : t \in \mathbb{Z}, 2 \nmid t\}$. Agora, escolhendo $t \in \mathbb{Z}$ de modo que $p = t+2 \in \mathbb{P}$ e substituindo em (4.7), segue que

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

Pelo Teorema Fundamental da Aritmética, $\exists\, \alpha_1, \alpha_2, ..., \alpha_r, p_1, p_2, ..., p_r, r \in \mathbb{Z}_+^*$ tais que

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

com p_i primo, $\forall i \in \{1, 2, ..., r\}$.

Daí, por definição, para que d seja livre de quadrados é necessário que, $\alpha_i = 1$ e $p \neq p_i$, $\forall i \in \{1, 2, ..., r\}$. Obviamente, $p \nmid p-4$, pois $p > p-4$. Daí,

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

Isso significa que $p \neq p_i$, $\forall i \in \{1, 2, ..., r\}$. Assim, para que $p(p-4)$ seja livre de quadrados, basta que $\alpha_i = 1$, $\forall i \in \{1, 2, ..., r\}$, ou seja, que $p-4$ também o seja. O fato de que existem infinitos primos p tais que $p-4$ é livre de quadrados novamente segue de [28]. Assim, existem infinitos primos p tais que d é livre de quadrados. Para cada uma dessas infinitas possibilidades, $\exists\, t \in \mathbb{Z}$ ímpar tal que $t = p-2$.

Portanto, existem infinitos $t \in \mathbb{Z}$ ímpares com d livre de quadrados. Para cada t dessa forma, defina $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e

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

Como $\mathcal{N}(b+g\delta) = \sigma_1(b+g\delta)\sigma_2(b+g\delta) = \left(\frac{t+2-\sqrt{d}}{2}\right)\left(\frac{t+2-\sqrt{d}}{2}\right) = \dfrac{t^2+4t+4-d}{4} = t+2 = a = ag$, então a condição (4.5) é satisfeita, o que significa que $\left\{t+2, \frac{t+2-\sqrt{d}}{2}\right\}$ é base canônica de I. Assim, a matriz geradora de $\Lambda_{\mathbb{K}}(\mathcal{I})$ é dada por

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

Daí, dado $\mathbf{x} \in \Lambda_{\mathbb{K}}(\mathcal{I})$, $\exists\, m, n \in \mathbb{Z}$ tais que

$$\mathbf{x} = A \begin{pmatrix} m \\ n \end{pmatrix}.$$

Para facilitar a análise fazemos uma mudança de base de modo que $\exists\, x_1, x_2 \in \mathbb{Z}$ tais que

$$\mathbf{x} = \underbrace{\begin{pmatrix} \frac{t+2+\sqrt{d}}{2} & \frac{t+2-\sqrt{d}}{2} \\ \frac{t+2-\sqrt{d}}{2} & \frac{t+2+\sqrt{d}}{2} \end{pmatrix}}_{B} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\left(\sqrt{d}+t+2\right)x_1 + \frac{1}{2}\left(-\sqrt{d}+t+2\right)x_2 \\ \frac{1}{2}\left(-\sqrt{d}+t+2\right)x_1 + \frac{1}{2}\left(\sqrt{d}+t+2\right)x_2 \end{pmatrix}.$$

$$\begin{aligned}\|\mathbf{x}\|^2 &= t(t+2)x_1^2 + 4(t+2)x_1x_2 + t(t+2)x_2^2,\ d = t^2-4\\ &= a(a-2)x_1^2 + 4ax_1x_2 + a(a-2)x_2^2,\ a = t+2.\end{aligned}$$

Observe que, $\forall x_1, x_2 \in \mathbb{Z}$, com $n \neq 0$, tem-se que

i) $\|\mathbf{x}\|^2 = a(a-2)$ quando $(x_1, x_2) = (\pm 1, 0) = (0, \pm 1)$,

ii) $\|\mathbf{x}\|^2 = 2a(a-2) + 4a$ quando $(x_1, x_2) = (1, 1) = (-1, -1)$,

iii) $\|\mathbf{x}\|^2 = 2a(a-2) - 4a$ quando $(x_1, x_2) = (1, -1) = (-1, 1)$,

iv) $\|\mathbf{x}\|^2 > a(a-2), 2a(a-2)+4a, 2a(a-2)-4a$ quando $(x_1, x_2) \neq (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$.

Temos que $2a(a-2) - 4a > a(a-2) \Leftrightarrow a^2 - 6a > 0$ que é satisfeita quando $a < 0$ ou $a > 6$. Como $a = t+2 > 0$, segue que $\|\mathbf{x}\|^2$ assume menor valor em $a(a-2)$ quando $a \geq 7$ e $x_1 = \pm 1$ e $x_2 = 0$ ou quando $a \geq 7$ e $x_1 = 0$ e $x_2 = \pm 1$.

Convém observar que $a = t+2$ e portanto a restrição para a não afeta a infinidade de possibilidades de t ímpar (mostrada acima). Logo,

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

e com isso $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*.

Portanto, existem infinitos corpos quadráticos totalmente reais tais que existe pelo menos um ideal $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$ tal que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*, o que conclui a demonstração. □

Observação 4.15. Pelo Teorema 4.13, tomando $t = 1$, temos que, se $I = \langle 2, \frac{1-\sqrt{-15}}{2} \rangle$, então $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*.

Graficamente,

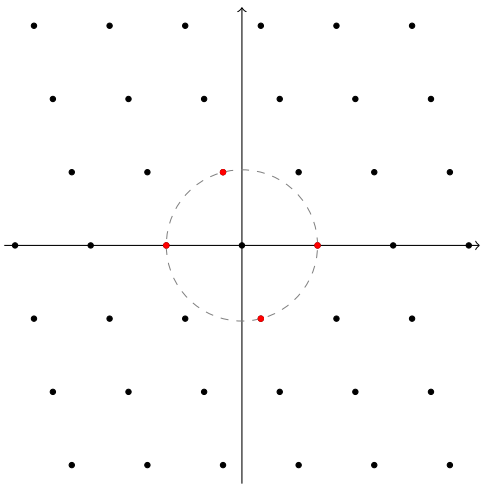

Figura 4.15: Representação de $\Lambda_{\mathbb{K}}(\mathcal{I})$ com $I = \langle 2, \frac{1-\sqrt{-15}}{2} \rangle$

Por outro lado, certamente existem ideais com outras caracterizações que não as encontradas aqui mas que dão origem a reticulados *WR*. A caracterização encontrada foi relevante para mostrar a infinidade dos ideais que satisfazem a condição de que originam reticulados *WR*, mas não representa sua totalidade.

Na Tabela 4.1 e na Tabela 4.2, apresentamos alguns exemplos de ideais I em corpos quadráticos $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ com $-d \equiv 1\ (mod\ 4)$ e $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com $d \equiv 1\ (mod\ 4)$, respectivamente, de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é *WR*, como discutido no Teorema 4.13 e Teorema

4.14. Para cada um dos ideais, apresentamos o ideal em termos da base canônica e escrevemos explicitamente os elementos de I que resultam nos vetores mínimos em $\Lambda_{\mathbb{K}}(\mathcal{I})$ com relação ao mergulho σ (nós os chamamos de *elementos mínimos*).

Note que essas famílias consistem apenas de alguns ideais para os quais a forma quadrática Q, ou corresponde a única escolha da base como em (4.3) ou é obtida a partir dela por um mudança de base, é reduzida e simétrica. Podem haver, é claro, muitos outros exemplos, assim como outras situações mais complicadas quando a forma não é reduzida, mas é equivalente a uma forma simétrica reduzida, nesse caso o reticulado em questão é, mais uma vez, *WR*. Em outras palavras, existem, provavelmente, muito mais reticulados *WR* que vêm de ideais em corpos quadráticos reais e imaginários do que os que demonstramos no Teorema 4.13 e no Teorema 4.14

Tabela 4.1: Exemplos de ideais em corpos quadráticos imaginários $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ que dão origem a reticulados *WR*.

$-d$	Ideal $I \subset \mathcal{O}_{\mathbb{K}}$	Elementos mínimos
-15	$\left\langle\ 2, \dfrac{1-\sqrt{-15}}{2}\ \right\rangle$	$\pm 2, \pm\dfrac{1-\sqrt{-15}}{2}$
-55	$\left\langle\ 4, \dfrac{3-\sqrt{-55}}{2}\ \right\rangle$	$\pm 4, \pm\dfrac{3-\sqrt{-55}}{2}$
-119	$\left\langle\ 6, \dfrac{5-\sqrt{119}}{2}\ \right\rangle$	$\pm 6, \pm\dfrac{5-\sqrt{119}}{2}$
-207	$\left\langle\ 8, \dfrac{7-\sqrt{207}}{2}\ \right\rangle$	$\pm 8, \pm\dfrac{7-\sqrt{207}}{2}$

Tabela 4.2: Exemplos de ideais em corpos quadráticos reais $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ que dão origem a reticulados *WR*.

d	Ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$	Elementos mínimos
21	$\left\langle\ 7, \dfrac{7-\sqrt{21}}{2}\ \right\rangle$	$\pm\dfrac{7\pm\sqrt{21}}{2}$
165	$\left\langle\ 15, \dfrac{15-\sqrt{165}}{2}\ \right\rangle$	$\pm\dfrac{15\pm\sqrt{165}}{2}$
285	$\left\langle\ 19, \dfrac{19-\sqrt{285}}{2}\ \right\rangle$	$\pm\dfrac{19\pm\sqrt{285}}{2}$
957	$\left\langle\ 33, \dfrac{33-\sqrt{957}}{2}\ \right\rangle$	$\pm\dfrac{33\pm\sqrt{957}}{2}$

Por fim, se tomássemos valores arbitrários para a variável t dentro das condições dos Teoremas 4.13 ou 4.14, observaríamos que os reticulados correspondentes sempre têm quatro vetores mínimos. Esse fato inspira o próximo resultado.

Proposição 4.16. *Sejam $d \in \mathbb{Z}$ livre de quadrados, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ e $\mathcal{I}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Se $d \neq \pm 3$ então $\mid S(\Lambda_{\mathbb{K}}(\mathcal{I})) \mid \leq 4$.*

Demonstração. Mostraremos tal resultado pela contra-positiva.

Se $\mid S(\Lambda_{\mathbb{K}}(\mathcal{I})) \mid > 4$, então $\mid S(\Lambda_{\mathbb{K}}(\mathcal{I})) \mid = 6$. Se este é o caso, então, pelo Lema 4.8, $S(\Lambda_{\mathbb{K}}(\mathcal{I})) \sim \Lambda_{\mathbb{Q}(\sqrt{-3})}$. Daí, $\exists\ \mathbf{x}, \mathbf{y} \in S(\Lambda_{\mathbb{K}}(\mathcal{I}))$ tais que, se θ é o ângulo entre $\mathbf{x}$ e $\mathbf{y}$, $\theta = \dfrac{\pi}{3}$. Isso significa que um desses vetores, digamos $\mathbf{y}$, é obtido via uma rotação de $\dfrac{\pi}{3}$ do outro vetor, $\mathbf{x} = (x_{11} + x_{12}\sqrt{|d|}, x_{21} + x_{22}\sqrt{|d|})$, com $x_{ij} \in \mathbb{Q}$, $\forall i, j = 1, 2$. Daí,

$$\mathbf{y} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \mathbf{x} \in \mathbb{Q}(\sqrt{|d|}) \times \mathbb{Q}(\sqrt{|d|}),$$

o que implica que $\sqrt{3} \in \mathbb{Q}(\sqrt{|d|})$, e portanto $d = \pm 3$. □

Concluímos então o capítulo com os principais resultados para reticulados *WR* em $\mathbb{R}^2$. Para reticulados $\Lambda_{\mathbb{K}}$ em $\mathbb{R}^d$, com $d > 2$, a propriedade que os caracteriza como *WR,* só acontece nos casos em que $\mathbb{K}$ é ciclotômico, [12].

5 Semi-estabilidade de reticulados algébricos no $\mathbb{R}^2$

Neste capítulo, apresentamos resultados sobre a estabilidade e semi-estabilidade de reticulados no plano. Através de uma conexão com o Capítulo 4, investigamos de forma introdutória em que condições reticulados algébricos construídos via ideais no anel dos inteiros de um corpo quadrático são semi-estáveis.

Estabilidade e bem arredondamento são propriedades independentes para reticulados de posto maior do que 2, isto é, reticulados *WR* podem ser instáveis e reticulados estáveis não precisam ser *WR*. Por outro lado, veremos que reticulados *WR* no plano formam um subconjunto próprio de reticulados estáveis.

A noção de semi-estabilidade foi introduzida originalmente por Stuhler [27] no contexto da teoria da redução e posteriormente usada por Grayson [16] no estudo de subgrupos aritméticos de grupos algébricos semi-simples. A semi-estabilidade heuristicamente significa que os mínimos sucessivos não estão muito longe um do outro.

Encontrar um vetor cujo comprimento é igual a um certo mínimo sucessivo é necessário em uma variedade de aplicações. Por exemplo, em comunicações [23] e criptografia [21], em que frequentemente é preciso resolver o problema do vetor mais curto de um reticulado.

Em [2], o autor observa que, enquanto reticulados semi-estáveis tem sido investigados em vários contextos aritméticos e geométricos, eles ainda não foram seriamente estudados no âmbito da teoria de reticulados. A principal referência utilizada para o desenvolvimento deste capítulo é [13].

5.1 Relação entre reticulados bem arredondados e semi-estáveis no $\mathbb{R}^2$

Definição 5.1. *Seja Λ um reticulado de posto $n \geq 2$. Para cada $1 \leq i \leq n$, o* ***mínimo sucessivo*** *de Λ é definido como os números reais que tem como característica*

$$\lambda_1 \leq \cdots \leq \lambda_n, \tag{5.1}$$

tal que

$$\lambda_i = min\{\lambda \in \mathbb{R}, \lambda > 0 : dim_{\mathbb{R}}\{\boldsymbol{x} \in \Lambda : \ ||\boldsymbol{x}|| \leq \lambda\} \geq i\}.$$

Em outras palavras, o i-ésimo mínimo sucessivo λ_i, $i = 1, \cdots, n$ é o menor número λ tal que a bola com centro na origem e raio λ contém i vetores do reticulado linearmente independentes.

Note que Λ é bem arredondado se houver igualdade em (5.1) e que o primeiro mínimo sucessivo é o menor comprimento dos elementos não nulos de Λ, ou seja,

$$\lambda_1 = \min\{||\mathbf{x}||:\ \mathbf{x} \in \Lambda; \mathbf{x} \neq 0\}.$$

Vetores linearmente independentes $x_1, \cdots, x_n \in \Lambda$ tais que $||x_i|| = \lambda_i$ são chamados de vetores correspondentes ao i-ésimo mínimo sucessivo. Eles não necessariamente formam uma base para Λ.

Definição 5.2. *Um reticulado Λ é chamado **semi-estável** se para cada sub-reticulado $\Omega \subset \Lambda$,*

$$\det(\Lambda)^{\frac{1}{posto(\Lambda)}} \leq \det(\Omega)^{\frac{1}{posto(\Omega)}}. \tag{5.2}$$

*Se o reticulado não é semi-estável, dizemos que ele é **instável**.*

Por exemplo, quando $posto(\Lambda) = 2$ temos que $posto(\Omega) = 1$. Logo, $\Omega =< z >_{\mathbb{Z}}$, $z \in \mathbb{Z}$ e portanto, $\det(\Omega) = ||z|| \geq \lambda_1$.

Desse modo, a inequação (5.2) pode ser reescrita como

$$\lambda_1 \geq \det(\Lambda)^{\frac{1}{2}}. \tag{5.3}$$

O Lema a seguir trata da semi-estabilidade e instabilidade de reticulados.

Lema 5.3. *Todos os reticulados WR de posto total em $\mathbb{R}^2$ são semi-estáveis e, para cada $n \geq 3$, existe uma infinidade de reticulados WR instáveis de posto n em $\mathbb{R}^n$.*

Demonstração. Primeiro suponha que $\Lambda \subset \mathbb{R}^2$ é bem arredondado. Então existe uma base $\{v_1, v_2\}$ para Λ consistindo de vetores correspondendo aos mínimos sucessivos, isto é,

$$\lambda_1 = ||v_1|| = ||v_2|| = \lambda_2.$$

Se θ é o ângulo entre estes vetores, então

$$\det(\Lambda) = ||v_1||||v_2||\operatorname{sen}\theta = \lambda_1^2 \operatorname{sen}\theta \leq \lambda_1^2,$$

e assim Λ é semi-estável por (5.3). Isto mostra que todos os reticulados *WR* em $\mathbb{R}^2$ são semi-estáveis.

Agora, suponha $n \geq 3$ e sejam $e_1, \cdots, e_n$ vetores da base canônica de $\mathbb{R}^n$. Vamos construir uma família de exemplos de reticulados *WR* de posto n em $\mathbb{R}^n$, que são instáveis. A partir dessa construção, é imediato que muitos outros exemplos são possíveis.

Seja $\theta \in [\frac{\pi}{3}, \frac{\pi}{2})$ e seja

$$\mathbf{x}_\theta = \cos\theta e_1 + \operatorname{sen}\theta e_2,$$

e defina

$$\Lambda_\theta = \langle e_1, \mathbf{x}_\theta, e_3, \cdots, e_n \rangle_{\mathbb{Z}}.$$

É imediato que Λ_θ é bem arredondado com

$$\lambda_1 = \cdots = \lambda_n = 1,$$

onde $e_1, \mathbf{x}_\theta, e_3, \cdots, e_n$ são vetores correspondendo ao mínimo sucessivo.

Considere um sub-reticulado $\Omega_\theta =< e_1, \mathbf{x}_\theta >_{\mathbb{Z}} \subset \Lambda$ de posto 2, e note que

$$\det(\Lambda_\theta)^{1/n} = (\operatorname{sen}\theta)^{1/n} > (\operatorname{sen}\theta)^{1/2} = \det(\Omega_\theta)^{1/2},$$

pois $\frac{\sqrt{3}}{2} \leq \operatorname{sen}\theta < 1$. Portanto, Λ_θ é instável.

□

5.2 Reticulados algébricos semi-estáveis no $\mathbb{R}^2$

Tendo em vista o Lema 5.3, é interessante entender quais reticulados algébricos construídos via corpos quadráticos $\mathbb{K}$ são semi-estáveis.

Seja um reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I}) \subset \mathbb{R}^n$, onde $n = r_1 + 2r_2$, r_1 é o número de mergulhos reais, r_2 o número de pares de mergulhos complexos conjugados de $\mathbb{K}$ e $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$.

Se $\mathbb{K}$ é totalmente real, isto é, $r_2 = 0$ temos que

$$|\Lambda_K(\mathcal{I})|^2 \geq \frac{1}{r_1}|\mathcal{N}(\mathcal{I})|^{\frac{1}{r_1}}. \tag{5.4}$$

Se $\mathbb{K}$ é totalmente complexo, isto é, $r_1 = 0$ temos que

$$|\Lambda_K(\mathcal{I})|^2 \geq \frac{1}{r_2}|\mathcal{N}(\mathcal{I})|^{\frac{1}{r_2}}. \tag{5.5}$$

Podemos conectar o mínimo sucessivo de um reticulado algébrico e a norma do ideal $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$.

De [3] temos que

$$\det(\Lambda_{\mathbb{K}}(\mathcal{I})) = 2^{-r_2}|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}\mathcal{N}(\mathcal{I}), \tag{5.6}$$

onde $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$.

Uma consequência de (5.6) é que todos os reticulados algébricos vindo de corpos de números quadráticos imaginários são semi-estáveis, conforme veremos no Teorema 5.4.

Da Definição 3.12 temos que $|\Lambda| = \lambda_1$. Assim, ao considerarmos reticulados algébricos $\Lambda_{\mathbb{K}}(\mathcal{I})$ denotaremos $|\Lambda_{\mathbb{K}}(\mathcal{I})|$ por $\lambda_1(\Lambda_{\mathbb{K}}(\mathcal{I}))$, que corresponde ao mínimo sucessivo do reticulado $\Lambda_{\mathbb{K}}(\mathcal{I})$.

Teorema 5.4. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ um corpo de números quadrático imaginário e $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ um ideal. O reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável.*

Demonstração. Como $\mathbb{K}$ é um corpo quadrático imaginário, $r_1 = 0$ e $r_2 = 1$. Combinando (5.5) com (5.6), vemos que

$$\lambda_1(\Lambda_{\mathbb{K}}(\mathcal{I})) \geq \frac{\sqrt{2}}{|\mathcal{D}_{\mathbb{K}}|^{1/4}} det(\Lambda_{\mathbb{K}}(\mathcal{I}))^{1/2},$$

e assim,

$$\lambda_1(\Lambda_{\mathbb{K}}(\mathcal{I}))\frac{|\mathcal{D}_{\mathbb{K}}|^{1/4}}{\sqrt{2}} \geq det(\Lambda_{\mathbb{K}}(\mathcal{I}))^{1/2}.$$

Observe que $\dfrac{|\mathcal{D}_{\mathbb{K}}|^{1/4}}{\sqrt{2}} \geq 1 \Leftrightarrow |\mathcal{D}_{\mathbb{K}}| \geq 4$.

Logo, a desigualdade (5.3) é satisfeita quando $|\mathcal{D}_{\mathbb{K}}| \geq 4$. Isto significa que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável quando $|\mathcal{D}_{\mathbb{K}}| \geq 4$, isto é, $-d \neq -3$, d livre de quadrados.

Agora, vamos analisar se $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável quando $|\mathcal{D}_{\mathbb{K}}| < 4$. Pela Proposição 2.5, a única situação com $|\mathcal{D}_{\mathbb{K}}| < 4$ é quando $-d = -3$. Neste caso, todos os reticulados algébricos são *WR*, pelo Corolário 4.12 e, portanto, são semi-estáveis pelo Lema 5.3.

Concluímos assim, que para qualquer valor de d, o reticulado $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável. □

Quando $\mathbb{K}$ é um corpo quadrático real, $r_1 = 2$ e $r_2 = 0$, e combinando (5.4) com (5.6), obtemos

$$\lambda_1(\Lambda_{\mathbb{K}}(\mathcal{I})) \geq \frac{1}{\sqrt{2}|\mathcal{D}_{\mathbb{K}}|^{1/8}} \det(\Lambda_{\mathbb{K}}(\mathcal{I}))^{1/4}.$$

Logo,

$$\lambda_1(\Lambda_{\mathbb{K}}(\mathcal{I}))\sqrt{2}|\mathcal{D}_{\mathbb{K}}|^{1/8} \geq det(\Lambda_{\mathbb{K}}(\mathcal{I}))^{1/4}.$$

Portanto, a situação é mais complicada e exige análise mais detalhada.

Assim, estamos interessados em analisar a semi-estabilidade de reticulados algébricos quando $\mathbb{K}$ é um corpo quadrático totalmente real. Para isso, usaremos a Proposição 5.5, cuja demonstração exige uma sequência de lemas e, portanto, será omitida aqui, podendo ser encontrada em [13].

Considere $d > 1$ um inteiro livre de quadrados. Para cada par de inteiros (a, b) tais que

$$0 < b < a, \ a \mid b^2 - d, \tag{5.7}$$

definimos o reticulado

$$\Lambda(a, b) = \begin{pmatrix} a & b - \sqrt{d} \\ a & b + \sqrt{d} \end{pmatrix} \mathbb{Z}^2. \tag{5.8}$$

Seja

$$S(d) = \{(a, b) \in \mathbb{Z}^2 \mid (a, b) \text{ satisfaz } (5.7)\}.$$

Proposição 5.5. *Para infinitos pares $(a, b) \in S(d)$, o reticulado correspondente $\Lambda(a, b)$ é semi-estável, e para infinitos pares o reticulado é instável. Especificamente, existe uma constante $\gamma > 1$ tal que se*

$$\gamma b \leq a \leq \frac{b^2 + d}{\sqrt{d}}, \tag{5.9}$$

então o reticulado $\Lambda(a, b)$ é semi-estável. Por outro lado, se

$$\frac{b^2 + d}{\sqrt{d}} < a \leq b^2 - d, \tag{5.10}$$

então o reticulado é instável.

Teorema 5.6. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo de números quadrático totalmente real. Então existe uma infinidade de ideais $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que o reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável, assim como, existe uma infinidade de ideais tal que o reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é instável.*

Demonstração. Sejam $a, b, g \geq 0$ satisfazendo (4.2) e (4.5), e o ideal $\mathcal{I} = \mathcal{I}(a, b, g) \subseteq \mathcal{O}_{\mathbb{K}}$ como em (4.3). Então, se $d \not\equiv 1 \, (mod\, 4)$, de (4.1) segue que

$$\Lambda_{\mathbb{K}}(\mathcal{I}) = \begin{pmatrix} \sigma_1(a) & \sigma_1(b - g\sqrt{d}) \\ \sigma_2(a) & \sigma_2(b - g\sqrt{d}) \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} a & b - g\sqrt{d} \\ a & b + g\sqrt{d} \end{pmatrix} \mathbb{Z}^2,$$

e se $d \equiv 1\,(mod\,4)$ de (4.1) segue que

$$\Lambda_{\mathbb{K}}(\mathcal{I}) = \begin{pmatrix} \sigma_1(a) & \sigma_1\left(b - \frac{1-\sqrt{d}}{2}g\right) \\ \sigma_2(a) & \sigma_2\left(b - \frac{1-\sqrt{d}}{2}g\right) \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} a & \frac{2b+1}{2} - \frac{\sqrt{d}}{2} \\ a & \frac{2b+1}{2} + \frac{\sqrt{d}}{2} \end{pmatrix} \mathbb{Z}^2.$$

Sem perda de generalidade assuma que $g = 1$.

Se $d \not\equiv 1\,(mod\,4)$ então

$$\mathcal{I} = \{ax + (b - \sqrt{d})y : \, x, y \in \mathbb{Z}\} \subseteq \mathcal{O}_{\mathbb{K}}.$$

O par (a, b) satisfaz as condições de (5.7) e $\Lambda_{\mathbb{K}}(\mathcal{I}) = \Lambda(a, b)$. Logo, pela Proposição (5.5), segue o resultado.

Agora, se $d \equiv 1\,(mod\,4)$ então

$$\mathcal{I} = \left\{ax + \left(\frac{2b + 1 - \sqrt{d}}{2}\right) y : \, x, y \in \mathbb{Z}\right\} \subseteq \mathcal{O}_{\mathbb{K}},$$

onde

$$b < a,\ a \mid \frac{1}{4}\left((2b+1)^2 - d\right),$$

e

$$\begin{pmatrix} a & \frac{2b+1}{2} - \frac{\sqrt{d}}{2} \\ a & \frac{2b+1}{2} + \frac{\sqrt{d}}{2} \end{pmatrix} \mathbb{Z}^2.$$

Sejam $a_1 = 2a$ e $b_1 = 2b + 1$. Como $b < a$ o par (a_1, b_1) satisfaz as condições de (5.7) e

$$\Lambda(a_1, b_1) = \begin{pmatrix} a_1 & b_1 - \sqrt{d} \\ a_1 & b_1 + \sqrt{d} \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 2a & 2b + 1 - \sqrt{d} \\ 2a & 2b + 1 + \sqrt{d} \end{pmatrix} \mathbb{Z}^2$$

Logo, $\Lambda_{\mathbb{K}}(\mathcal{I}) = \frac{1}{2}\Lambda(a_1, b_1)$. Observe que $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável se, e somente se, $\Lambda(a_1, b_1)$ é semi-estável e portanto, pela Proposição (5.5), segue o resultado.

□

Conforme mencionado, reticulados semi-estáveis tem sido investigados em vários contextos aritméticos e geométricos, porém na teoria de reticulados eles ainda foram pouco estudados. Existem poucas referências sobre esse assunto, e portanto não é de nosso conhecimento que hajam exemplos mais concretos sobre esse tema.

6 Considerações finais

O presente trabalho foi dedicado ao estudo da teoria de reticulados, sendo que o foco foi abordar algumas aplicações dessa teoria.

Primeiramente, apresentamos conceitos e principais resultados sobre corpos quadráticos, tema de grande importância no desenvolvimento deste trabalho, já que usamos tais corpos ao longo de toda a teoria.

Em seguida, desenvolvemos um estudo sobre teoria de reticulados, estudando os principais conceitos e resultados. No entanto, nosso objetivo maior foi o estudo dos dois últimos capítulos, sobre reticulados *WR* e reticulados algébricos semi-estáveis.

Investigamos em quais condições reticulados algébricos são *WR* e uma das principais conclusões de [12] e que neste trabalho apresentamos de forma mais detalhada, é que um reticulado $\Lambda_{\mathbb{K}}$, com $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, é *WR* se, e somente se, $d = -1$ ou $d = -3$ com $d \in \mathbb{Z}$ livre de quadrados e $d \neq 1$.

Vimos também que existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $-d \equiv 1 \ (mod\ 4)$ tais que o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja *WR*. E, analogamente, existem infinitos $d \in \mathbb{Z}$ livres de quadrados, com $d > 1$ e $d \equiv 1 \ (mod\ 4)$ tais que o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ contém pelo menos um ideal $\mathcal{I}$ de modo que $\Lambda_{\mathbb{K}}(\mathcal{I})$ seja *WR*.

Na sequência, apresentamos uma conexão entre reticulados *WR* e *semi-estabilidade* de reticulados. De [13] concluímos que todos os reticulados *WR* de posto total em $\mathbb{R}^2$ são semi-estáveis, mas por outro lado, para cada $n \geq 3$, existe uma infinidade de reticulados *WR* instáveis de posto n em $\mathbb{R}^n$.

Vimos também que se $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ é um corpo de números quadrático imaginário e $\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$ um ideal, o reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável, e que se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo de números quadrático totalmente real, então existe uma infinidade de ideais $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que o reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é semi-estável, assim como, existe uma infinidade de ideais tal que o reticulado algébrico $\Lambda_{\mathbb{K}}(\mathcal{I})$ é instável.

Por fim, vale ressaltar que ainda há muitas aplicações e resultados a serem estudados a partir da teoria apresentada aqui.

Referências

[1] ALVES, C. *Reticulados via Corpos Ciclotômicos.* Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2005.

[2] ANDRÈ, Y. *On nef and semistable hermitian lattices, and their behaviour under tensor product.* Tohoku Math. J. (2), 63(4):629-49, 2011.

[3] BAYER-FLUCKIGER, E. *Lattices and number fields.* Contemporany Mathematics, 241, pages 69–84, 1999.

[4] BAYER-FLUCKIGER, E. *Ideal lattices.* In A panorama of number theory or the view from Baker's garden (Zurich, 1999), pages 168–184. Cambridge Univ. Press, Cambridge, 2002.

[5] BAYER-FLUCKIGER, E., NEBE, G. *On the Euclidean minimum of some real number fields.* J. Theor. Nombres Bordeaux, 17(2):437454, 2005.

[6] BUELL, D.A. *Binary Quadratic Forms.* Springer-Verlag, 1989.

[7] CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. *Álgebra Linear e Aplicações*- 6ed. reform. Atual. São Paulo, 1990.

[8] CONWAY,J.H.; SLOANE N.J.A. *Sphere Packings, Lattices and Groups.* Springer, New York, 1999.

[9] DOMINGUES, H.H.; IEZZI, G. *Álgebra Moderna*- 4ed. reform. Atual. São Paulo, 2003.

[10] ENDLER, O. *Teoria dos Números Algébricos.* IMPA, Rio de Janeiro, 1986.

[11] FLORES, A.L. *Reticulados em Corpos Abelianos.* Dissertação de Doutorado, FEEC - UNICAMP, Campinas, 2000.

[12] FUKSHANSKY, L.; PETERSEN K. *On Well-Rounded Ideal Lattices.* Journal of Number Theory, vol. 8, n. 1, 189–206, 2012.

[13] FUKSHANSKY, L. *Stability of Ideal Lattices from Quadratic Number Fields.*, arXiv:1402.2738v2 [math.NT], 2015.

[14] FUKSHANSKY, L. *On similarity classes of well-rounded sublattices of* $\mathbb{Z}^2$. Journal of Number Theory, vol. 129, n. 10, 2530–2556, 2009.

[15] GONÇALVES, A. *Introdução à Álgebra.* IMPA. Rio de Janeiro, 2003.

[16] GRAYSON, D. R. *Reduction theory using semistability.* Comment. Math. Helv., 59(4):600-634, 1984.

[17] HERSTEIN, I.N. *Topics in Algebra.*- 2ed. John Wiley & Sons. Nova Jersey, 1975.

[18] HOFFMAN, K.; KUNZE, R. *Álgebra Linear*, traduzido por Adalberto P. Bergamasco. Polígono. São Paulo, 1970.

[19] LIMA, E. L. *Análise Real - Vol 1: Funções de uma variável.* IMPA, Rio de Janeiro, 2007.

[20] LU, P., STEINHARDT, P. *Decagonal and quasicrystalline tilings in Medieval Islamic architecture.* Science 315: 1106-1110, 2007.

[21] MICCIANCIO, D.; GOLDWASSER, S. *Complexity of Lattice Problems: a cryptographic perspective*, ser. The Kluwer International Series in Engineering and Computer Science. Boston, Massachusetts: Kluwer Academic Publishers, vol. 671, 2002.

[22] MOLLIN, R. A. *Algebraic Number Theory.* CRC Press, University of Calgary, Alberta, Canada, 2011.

[23] MOW, W.H. *Maximum likelihood sequence estimation from the lattice viewpoint.* IEEE Trans. Inf. Theory, vol. 40, no. 5, pp. 1594-1600, 1994.

[24] NETO, A. L. *Funções de uma variável complexa.* Rio de Janeiro: IMPA, 2005.

[25] SAMUEL, P. *Algebraic Theory of Numbers.* Hermana, Paris, 1967.

[26] STEINBRUCH, A.; WINTERLE, P. *Álgebre Linear* Pearson. São Paulo, 1995.

[27] STUHLER U. *Eine Bemerkung zur Reduktionstheorie quadratischer Formen.* Arch. Math. (Basel), 27(6):604-610, 1976.

[28] STEWART, I.; TALL,D. *Algebric Number Theory.* Chapman & Hall, New York,1987.

7 Tópicos de Álgebra e Álgebra Linear

Apresentamos alguns tópicos de Álgebra e Álgebra Linear que julgamos necessários para um melhor entendimento deste trabalho.

7.1 Tópicos de Álgebra Linear

As referências aqui utilizadas foram [7], [18] e [26].

Definição 7.1. *Dizemos que um conjunto $\mathbb{V}$ não vazio é um* ***espaço vetorial*** *sobre o corpo $\mathbb{F}$ se existir:*

(i) uma regra (ou operação), dita adição de vetores, que associa a cada par de vetores u, v em $\mathbb{V}$ um vetor $u+v$ em $\mathbb{V}$, de maneira que, para todo $u, v, w \in \mathbb{V}$,

1. $u + v = v + u$;
2. $u + (v + w) = (u + v) + w$;
3. *existe um único* 0 *de* $\mathbb{V}$, *chamado vetor nulo, de forma que* $u + 0 = u$;
4. *para cada* u *de* $\mathbb{V}$ *existe um único vetor* $-u$ *em* $\mathbb{V}$ *tal que* $u + (-u) = 0$.

(ii) uma regra (ou operação), dita multiplicação escalar, que associa a cada α em $\mathbb{F}$ e cada vetor u em $\mathbb{V}$ um vetor αu em $\mathbb{V}$, denominado o produto de α por u de maneira que, para todo $u, v \in \mathbb{V}$ e $\alpha, \beta, \gamma \in \mathbb{F}$,

1. $1u = u$;
2. $(\alpha\beta)u = \alpha(\beta u)$;
3. $\alpha(u + v) = \alpha u + \alpha v$;
4. $(\alpha + \beta)u = \alpha u + \beta u$.

Exemplo 7.2. O corpo $\mathbb{R}^2$ é um espaço vetorial sobre $\mathbb{R}$ com as operações de adição e multiplicação usuais.

Exemplo 7.3. O espaço das matrizes $m \times n$ com entradas em um corpo $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{F}$.

Exemplo 7.4. O espaço das funções polinomiais com coeficientes e variável em um corpo $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{F}$.

Definição 7.5. *Seja $\mathbb{F} \subset \mathbb{R}^n$ um espaço vetorial. Dado um vetor $u = (x_1, ..., x_m) \in \mathbb{F}$, com $m \leq n$, indica-se por $\|u\|$ e chama-se* ***norma euclidiana de u*** *o número real positivo dado por $\|u\| := \sqrt{\sum_{i=1}^{m} x_i^2}$.*

Exemplo 7.6. O vetor $u = \left(2, -4, -\frac{1}{2} \right) \in \mathbb{R}^3$ tem norma

$$\sqrt{2^2 + (-4)^2 + \left(-\frac{1}{2} \right)^2} = \sqrt{\frac{81}{4}} = \frac{9}{2}.$$

Em outras palavras, a norma euclidiana de u corresponde ao comprimento de u.

Definição 7.7. *Seja $\mathbb{V}$ um espaço vetorial sobre $\mathbb{F}$. Um subconjunto S de $\mathbb{V}$ é dito* ***linearmente dependente****, LD, se existem vetores distintos $u_1, u_2, ..., u_n$ em S e escalares $\alpha_1, \alpha_2, ..., \alpha_n$ em $\mathbb{F}$, não todos nulos, tais que*

$$\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0.$$

Um conjunto que não é linearmente dependente é dito ***linearmente independente****, LI.*

Exemplo 7.8. O conjunto de vetores $\{1, t + 2, 2t + 4\}$ do espaço $\mathbb{P}_4$ das funções polinomiais de grau menor ou igual a 4 sobre $\mathbb{R}$, é linearmente dependente, pois $2t + 4 = 0 \cdot 1 + 2 \cdot (t + 2)$.

Exemplo 7.9. O conjunto $S = \{(2, 0, 3), (1, 0, 0), (0, 1, 5)\}$ do espaço $\mathbb{R}^3$ é linearmente independente, pois

$$\alpha(2, 0, 3) + \beta(1, 0, 0) + \gamma(0, 1, 5) = (0, 0, 0), \text{ com } \alpha, \beta \text{ e } \gamma \in \mathbb{R}$$

se

$$\begin{cases} 2\alpha + \beta = 0 \\ \gamma = 0 \\ 3\alpha + 5\gamma = 0 \end{cases}$$

As três igualdades anteriores são satisfeitas se, e somente se, $\alpha = 0, \beta = 0$ e $\gamma = 0$.

Definição 7.10. *O conjunto $W \subset \mathbb{V}$ é um* ***subespaço vetorial*** *de $\mathbb{V}$ se W é também um espaço vetorial sobre $\mathbb{R}$ com as operações herdadas de $\mathbb{V}$.*

Teorema 7.11. *Seja $\mathbb{V}$ um espaço vetorial sobre $\mathbb{R}$. O subconjunto W de $\mathbb{V}$ é um subespaço vetorial de $\mathbb{V}$ sobre $\mathbb{R}$ se*

(i) $0 \in W$;

(ii) $\forall\ u,\ v \in W,\ u + v \in W$;

(iii) $\forall\ \alpha \in \mathbb{R}$ *e* $\forall\ u \in W,\ \alpha u \in W$.

Demonstração. De fato,

(i) se $0 \in W$, então W é não vazio e vale a condição 3 do item (i) da Definição 7.1.

(ii) se para todo $u, v \in W$ temos $u + v \in W$, então as condições 1 e 2 do item (i) da Definição 7.1 são satisfeitas pelo fato de W ser subconjunto não vazio de $\mathbb{V}$.

(iii) se $\forall\ \alpha \in \mathbb{R}$ e $\forall\ u \in W,\ \alpha u \in W$, então as condições 1, 2, 3 e 4 do item (ii) da Definição 7.1 são satisfeitas.

Se, ainda $u \in W$ e $\alpha = -1$ então $\alpha u = -u \in W$. Assim, a condição 4 do item (i) da Definição 7.1 também é válida.

Portanto, W é subespaço vetorial de $\mathbb{V}$. □

Definição 7.12. *O subespaço $[S]$ de um espaço vetorial $\mathbb{V}$ é definido por*

$$[S] := \{\alpha_1 u_1 + \cdots + \alpha_n u_n \mid \alpha_1, \cdots, \alpha_n \in \mathbb{R}\}$$

*com $S = \{u_1, \cdots, u_n\} \subset \mathbb{V}$ e $n \in \mathbb{N}$, recebe o nome de **subespaço gerado por** S. Cada elemento de $[S]$ é uma combinação linear de S.*

Dizemos que os vetores $u_1, \cdots, u_n$ da definição anterior geram $[S]$ ou então que são um sistema de geradores de $[S]$.

Definição 7.13. *Um espaço vetorial $\mathbb{V}$ é **finitamente gerado** se existe um conjunto S, finito, com $S \subset \mathbb{V}$, de maneira que $\mathbb{V} = [S]$.*

Observação 7.14. Também usamos a notação $\langle S \rangle_{\mathbb{R}}$ para indicar o conjunto gerado por S sobre $\mathbb{R}$.

Exemplo 7.15. Seja $S = \{(0, 2),\ (1, -1)\}$. O conjunto gerado por S é dado por

$$\alpha(0, 2) + \beta(1, -1) = (\beta,\ 2\alpha - \beta).$$

Portanto, $[S] = \{(\beta,\ 2\alpha - \beta) \mid \alpha,\ \beta \in \mathbb{R}\}$.

Definição 7.16. *Seja $\mathbb{V}$ um espaço vetorial. Uma **base** de $\mathbb{V}$ é um conjunto linearmente independente de vetores em $\mathbb{V}$ que gera $\mathbb{V}$.*

Definição 7.17. *Um espaço vetorial $\mathbb{V}$ é de **dimensão finita** sobre $\mathbb{R}$ se for finitamente gerado e, neste caso, o número de elementos da base é finito. A dimensão de $\mathbb{V}$ sobre $\mathbb{R}$ é definida como o número de elementos de uma base de $\mathbb{V}$ sobre $\mathbb{R}$. Notação: $dim_{\mathbb{R}} V$.*

Exemplo 7.18. O conjunto S do Exemplo 7.9 é uma base do $\mathbb{R}^3$, pois é linearmente independente e gera o $\mathbb{R}^3$.

De fato, qualquer vetor (x, y, z) do $\mathbb{R}^3$ pode ser escrito como combinação linear dos vetores $(2, 0, 3), (1, 0, 0)$ e $(0, 1, 5)$, isto é,

$$(x, y, z) = \alpha(2, 0, 3) + \beta(1, 0, 0) + \gamma(0, 1, 5)$$

$$\Leftrightarrow \begin{cases} x = 2\alpha + \beta \\ y = \gamma \\ z = 3\alpha + 5\gamma. \end{cases}$$

Ou seja, basta tomarmos $\alpha = \dfrac{z - 5y}{3}, \beta = \dfrac{3x - 2z + 10y}{3}$ e $\gamma = y$, para todo x, y e $z \in \mathbb{R}$. Portanto $dim_{\mathbb{R}} S = 3$.

Definição 7.19. *Chamamos de* ***produto interno*** *no espaço vetorial* $\mathbb{V}$ *uma função de* $\mathbb{V}\times\mathbb{V}$ *em* $\mathbb{R}$ *que associa todo par de vetores* $(u,v)\in\mathbb{V}\times\mathbb{V}$ *um número real, indicado por* $\langle u,v\rangle$*, tal que os seguintes axiomas sejam verificados, para todo* $u,v,w\in\mathbb{V}$ *e* $\alpha\in\mathbb{R}$*,*

(i) $\langle u,v\rangle=\langle v,u\rangle$*;*

(ii) $\langle u,v+w\rangle=\langle u,v\rangle+\langle u,w\rangle$*;*

(iii) $\langle \alpha u,v\rangle=\alpha\langle u,v\rangle$*;*

(iv) $\langle u,u\rangle\geq 0$*. E* $\langle u,u\rangle=0$ *se, e somente se* $u=0$*.*

Exemplo 7.20. No espaço vetorial $\mathbb{R}^2$, a função que associa cada par de vetores $u=(x_1,y_1)$ e $v=(x_2,y_2)$ o número real

$$\langle u,v\rangle=3x_1x_2+4y_1y_2$$

é um produto interno.

De fato, para todo $u=(x_1,y_1),v=(x_2,y_2),w=(x_3,y_3)\in\mathbb{V}$ e $\alpha\in\mathbb{R}$,

(i) $\langle u,v\rangle=3x_1x_2+4y_1y_2=3x_2x_1+4y_2y_1=\langle v,u\rangle$;

(ii) $\langle u,v+w\rangle=3x_1(x_2+x_3)+4y_1(y_2+y_3)=(3x_1x_2+4y_1y_2)+(3x_1x_3+4y_1y_3)=\langle u,v\rangle+\langle u,w\rangle$;

(iii) $\langle \alpha u,v\rangle=3(\alpha x_1)x_2+4(\alpha y_1)y_2=\alpha(3x_1x_2+4y_1y_2)=\alpha\langle u,v\rangle$;

(iv) $\langle u,u\rangle=3x_1x_1+4y_1y_1=3x_1^2+4y_1^2\geq 0$ e $\langle u,u\rangle=3x_1^2+4y_1^2=0$ se, e somente se, $x_1=y_1=0$. Isto é, $u=(0,0)$.

Observação 7.21. Espaços vetoriais com produto interno sobre $\mathbb{R}$ são chamados *espaços vetoriais reais* e espaços vetoriais com produto interno sobre $\mathbb{C}$, isto é, espaços vetoriais em que associamos o produto interno a um número complexo, são chamados *espaços vetoriais hermitianos.*

Podemos estender as definições e teoremas de espaços vetoriais reais para espaços vetoriais hermitianos.

Definição 7.22. *Sejam* $\mathbb{V}$ *e* $\mathbb{W}$ *espaços vetoriais sobre* $\mathbb{R}$*. Uma aplicação* $T:\mathbb{V}\to\mathbb{W}$ *é chamada* ***transformação linear*** *de* $\mathbb{V}$ *em* $\mathbb{W}$ *se, e somente se,*

(i) $T(v_1+v_2)=T(v_1)+T(v_2),\ \forall\ v_1,\ v_2\in\mathbb{V}$*, e*

(ii) $T(\alpha v)=\alpha T(v),\ \forall\ v\in\mathbb{V}$ *e* $\alpha\in\mathbb{R}$*.*

Exemplo 7.23. Seja a aplicação $T:\mathbb{R}^3\to\mathbb{R}^2$ definida por $T(x,y,z)=(-y,\ x-2z)$. T é uma transformação linear. De fato, para todo $v_1=(x_1,\ y_1,\ z_1)$, $v_2=(x_2,\ y_2,\ z_2)$ $\in\mathbb{R}^3$ temos que

(i) $T((x_1,\ y_1,\ z_1)+(x_2,\ y_2,\ z_2))=(-y_1-y_2,\ x_1+x_2-2\cdot z_1-2\cdot z_2)=(-y_1,x_1-2z_1)+(-y_2,x_2-2z_2)=T(v_1)+T(v_2)$;

(ii) $T(\alpha v_1)=(-\alpha y_1,\ \alpha x_1-2\alpha z_1)=\alpha T(v_1)$.

A imagem do vetor $v = (-1,\ 2,\ 0)$ é

$$T(-1,\ 2,\ 0) = (-2,\ -1 - 2 \cdot 0) = (-2,\ -1).$$

Definição 7.24. *Sejam A e B bases dos espaços vetoriais $\mathbb{V}$ e $\mathbb{W}$, respectivamente, e uma transformação linear T de $\mathbb{V}$ em $\mathbb{W}$. Temos a igualdade, para todo $v \in \mathbb{V}$,*

$$[T(v)]_B = [T]_B^A\ [v]_A,$$

em que:

- *$[T(v)]_B$ denota a matriz coluna das componentes do vetor imagem de v por T em termos da base B de $\mathbb{W}$;*
- *$[v]_A$ denota a matriz coluna de componentes de v em termos da base A de $\mathbb{V}$;*
- *$[T]_B^A$ denota a matriz das imagens dos vetores de A em termos da base B em coluna.*

A matriz $[T]_B^A$ é chamada ***matriz da transformação linear T em relação às bases A e B****.*

Exemplo 7.25. Seja T a transformação linear do Exemplo 7.23. Vamos definir a matriz da transformação linear em relação às bases $A = \{(1,1,1),(0,1,1),(0,0,1)\}$ e $B = \{(1,0),(0,2)\}$ de $\mathbb{R}^3$ e $\mathbb{R}^2$, respectivamente. Escrevendo as imagens dos vetores da base A em termos da base B, temos

$$T(1,1,1) = (-1,-1) = \left(-1, -\frac{1}{2}\right)_B$$
$$T(0,1,1) = (-1,-2) = (-1,-1)_B$$
$$T(0,0,1) = (0,-2) = (0,-1)_B.$$

Então, a matriz da transformação linear T em relação às bases A e B, pela Definição 7.24, é

$$[T]_B^A = \begin{bmatrix} -1 & -1 & 0 \\ -\frac{1}{2} & -1 & -1 \end{bmatrix}.$$

Agora, para calcular a imagem de um vetor pela transformação T e escrevê-lo em termos de uma base B, fazemos apenas a multiplicação das matrizes. Como exemplo, tomemos o vetor $(0,0,2)$ e apliquemos a transformação T. Obtemos

$$[T(v)]_B = \begin{bmatrix} -1 & -1 & 0 \\ -\frac{1}{2} & -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ -2 \end{bmatrix}_B.$$

Portanto, $T(0,0,2) = (0,-2)_B$.

As definições a seguir tratarão de transformações lineares em $\mathbb{R}^2$.

Definição 7.26. *A rotação do plano em torno da origem, que faz cada ponto descrever um ângulo θ, determina uma transformação linear $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ cuja matriz canônica (isto é, em termos das bases canônicas) é*

$$[T_\theta] = \begin{bmatrix} cos\ \theta & -sen\ \theta \\ sen\ \theta & \cos\ \theta \end{bmatrix}.$$

Essa matriz é chamada ***matriz de rotação*** *de um ângulo θ.*

Exemplo 7.27. Vamos determinar a imagem do vetor $(4, 2)$ pela rotação de $\dfrac{\pi}{2}$. Basta fazer

$$\begin{bmatrix} cos\ \frac{\pi}{2} & -sen\ \frac{\pi}{2} \\ sen\ \frac{\pi}{2} & \cos\ \frac{\pi}{2} \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{bmatrix} -2 \\ 4 \end{bmatrix}.$$

Definição 7.28. *Uma* ***dilatação ou contração*** *na direção um vetor (x, y) em $\mathbb{R}^2$ é definida por*

$$\begin{array}{rcl} T : \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x, y) & \mapsto & \alpha(x, y),\ \alpha \in \mathbb{R}, \end{array}$$

em que:

(i) T dilata o vetor se $|\alpha| > 1$,

(ii) T contrai o vetor se $|\alpha| < 1$.

Se $\alpha < 0$, T troca o sentido do vetor. Analogamente, podemos definir uma dilação ou contração na direção do eixo x ou do eixo y por $T : \mathbb{R}^2 \to \mathbb{R}^2$, onde $T(\alpha(x, y)) = (\alpha x, y)$, $\alpha > 0$ ou $T(\alpha(x, y)) = (x, \alpha y)$, $\alpha > 0$, respectivamente.

Exemplo 7.29. Sejam as transformações lineares $T_1 : \mathbb{R}^2 \to \mathbb{R}^2$ dada por $T_1(x, y) = (3x, y)$ e $T_2 : \mathbb{R}^2 \to \mathbb{R}^2$ dada por $T_2(x, y) = (-2x, -2y)$. Dizemos que T_1 é uma dilatação do vetor (x, y) e T_2 é uma contração de (x, y). Assim, a imagem de $(1, 2)$ por T_1 é

$$T_1(1, 2) = (3 \cdot 1, 2) = (3, 2),$$

e por T_2 é

$$T_2(1, 2) = (-2 \cdot 1, -2 \cdot 2) = (-2, -4).$$

7.2 Tópicos de Álgebra

As referências aqui utilizadas foram [9], [15] e [17].

Definição 7.30. *Um número inteiro é* ***livre de quadrados*** *se não é divisível pelo quadrado de nenhum número inteiro maior do que* 1.

Exemplo 7.31. O número -14 é um inteiro livre de quadrados, pois seus divisores são $1,\ -1,\ 2,\ -2,\ 7,\ -7,\ 14$ e -14, e nenhum deles é quadrado de algum número inteiro maior do que 1. Já o número 12 não é livre de quadrados, pois um de seu divisores é o número 4 e $4 = 2^2 = (-2)^2$.

Definição 7.32. *Sejam a e b números inteiros quaisquer e m um inteiro estritamente positivo. Diz-se que a é* ***congruente a b módulo m*** *se $m \mid (a-b)$, isto é, se $a-b = mq$ para um conveniente inteiro q. Notação: $a \equiv b \,(mod\, m)$.*

Dizer que a é congruente a b módulo m significa que a e b deixam o mesmo resto quando divididos por m.

Exemplo 7.33. $16 \equiv 9 \,(mod\ 7)$, já que $7 \mid (16-9)$ e, além disso, o resto da divisão de 16 por 7 é 2, e o resto da divisão de 9 por 7 é 2.

Definição 7.34. *Chama-se* ***relação binária*** *de E em F todo subconjunto R de $E \times F$. Logo, R é relação de $E \times F$ se, e somente se, $R \subset E \times F$. Se $E = F$, dizemos que R é uma relação em E. Para indicar que $(a, b) \in R$, usaremos a notação aRb.*

Conforme essa definição, R é o conjunto de pares ordenados (a, b) pertencentes a $E \times F$.

Exemplo 7.35. Se $E = F = \mathbb{Z}$, então $E \times F$ é o conjunto de todos os pares ordenados de números inteiros. Um exemplo de relação de $\mathbb{Z}$ em $\mathbb{Z}$ é:

$$\begin{aligned} R &= \{(x, y) \in \mathbb{Z} \mid x = -y\} \\ &= \{\cdots, (-n, n), \cdots, (-2, 2), (-1, 1), (0, 0), (1, -1), \cdots, (n, -n), \cdots\}. \end{aligned}$$

Definição 7.36. *Uma relação R sobre um conjunto E não vazio é chamada* ***relação de equivalência*** *sobre E se cumpre as seguintes propriedades:*

(i) se $x \in E$, então xRx (reflexiva);

(ii) se $x, y \in E$ e xRy então yRx (simétrica);

(iii) se $x, y, z \in E$, xRy e yRz então xRz (transitiva).

Exemplo 7.37. A relação de igualdade é uma relação de equivalência sobre $\mathbb{R}$, pois

(i) $\forall x \in \mathbb{R},\ x = x$;

(ii) $\forall x, y \in \mathbb{R}$, se $x = y$ então $y = x$;

(iii) $\forall x, y, z \in \mathbb{R}$, se $x = y$ e $y = z$ então $x = z$.

Exemplo 7.38. A relação de congruência módulo m, com $m \in \mathbb{Z}$ e $m > 1$, sobre $\mathbb{Z}$ é uma relação de equivalência, pois:

(i) $\forall x \in \mathbb{Z},\ x \equiv x \,(mod\, m)$, já que $m \mid (x - x) = 0$;

(ii) $\forall x, y \in \mathbb{R}$, se $x \equiv y \,(mod\, m)$ então $y \equiv x \,(mod\, m)$, já que se $m \mid (x - y)$ então $m \mid (y - x)$;

(iii) $\forall x, y, z \in \mathbb{R}$, se $x \equiv y \,(mod\, m)$ e $y \equiv z \,(mod\, m)$ então $x \equiv z \,(mod\, m)$. De fato, se $m \mid (x - y)$ e $m \mid (y - z)$, então

$$x - y = mq_1 \text{ e } y - z = mq_2,$$

para algum $q_1,\ q_2 \in \mathbb{Z}$. Substituindo y por $mq_2 + z$ na primeira igualdade,

$$\begin{aligned} x - (mq_2 + z) &= mq_1 \\ x - mq_2 - z &= mq_1 \\ x - z &= m(q_1 + q_2), com\ q_1,\ q_2 \in \mathbb{Z}. \end{aligned}$$

Sendo assim, $m \mid (x - z)$. Portanto, $x \equiv z\ (mod\, m)$.

Observação 7.39. Ainda podemos citar outras propriedades de congruência módulo m, para todo $a, b, c, d, m \in \mathbb{Z}$, com $m > 0$,

(i) $a \equiv b\ (mod\ m) \Leftrightarrow a \pm c \equiv b \pm c\ (mod\ m)$;

(ii) se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $a + c \equiv b + d\ (mod\ m)$;

(iii) se $a \equiv b\ (mod\ m)$, então $ac \equiv bc\ (mod\ m)$;

(iv) se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $ac \equiv bd\ (mod\ m)$.

As demonstrações dos itens anteriores podem ser encontradas na referência [9].

Definição 7.40. *Seja uma relação R de equivalência sobre E. Dado a, com $a \in E$, chama-se **classe de equivalência** determinada por a, módulo R, o subconjunto $\overline{a}$ de E constituído pelos elementos x tais que xRa, isto é,*

$$\overline{a} := \{x \in E \mid xRa\}.$$

Exemplo 7.41. Vimos no Exemplo 7.38 qe a congruência módulo m é uma relação de equivalência. A classe de equivalência determinada por a é dada por

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\ (mod\, m)\},$$

isto é, $\overline{a}$ é o conjunto de todos os elementos de $\mathbb{Z}$ que deixam o mesmo resto que a na divisão por m. Neste contexto, $\overline{a}$ pode, também, ser chamado de *classe de restos de a.*

A partir de agora, apresentaremos alguns tópicos de álgebra básica.

Definição 7.42. *Um sistema matemático constituído de um conjunto A não vazio e duas operações sobre ele, uma adição e uma multiplicação definidas, respectivamente, por:*

$$\begin{aligned} + : (x, y) &\mapsto x + y \\ \cdot : (x, y) &\mapsto xy \end{aligned}$$

*é chamado **anel**, e representado por $(A, +, \cdot)$, ou simplesmente A, se essas operações atendem as seguintes condições: $\forall a, b, c \in A$,*

(i) A adição em A é associativa, isto é, $(a + b) + c = a + (b + c)$;

(ii) A adição em A é comutativa, ou seja, $a + b = b + a$;

(iii) Existe elemento neutro para a adição em A, portanto $\exists\ 0_A \in A \mid a+0_A = a, \forall a \in A$;

(iv) Existem os simétricos aditivos em A, logo $\forall\ a \in A, \exists\ a' \in A \mid a + a' = 0_A$;

(v) A multiplicação em A é associativa, ou seja, $a(bc) = (ab)c$;

(vi) A multiplicação em A é distributiva (à direita e à esquerda) em relação à adição, ou seja, $a(b+c) = ab + ac$ *e* $(a+b)c = ac + bc$.

Para simplificar a notação, vamos representar 0_A apenas por 0.

Exemplo 7.43. Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com as operações de multiplicação e adição usuais, cujas propriedades cumprem os axiomas da Definição 7.42, são anéis representados, respectivamente, por $(\mathbb{Z}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$; $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.

Exemplo 7.44. Para todo $m > 1$, definimos $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$. Considere as operações:

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \text{ e} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b},\ \forall\, \overline{a}, \overline{b} \in \mathbb{Z}_m. \end{aligned}$$

O conjunto $(\mathbb{Z}_m, +, \cdot)$ das classes de resto módulo m, com as operações acima, é um anel, pois

(i) $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{(b+c)} = \overline{a + (b+c)} = \overline{(a+b) + c}$, já que a adição em $\mathbb{Z}$ é associativa. Então, $\overline{(a+b)+c} = \overline{(a+b)} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}, \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(ii) $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a}$ já que em $\mathbb{Z}$ vale a comutatividade da adição. Logo, $\overline{b+a} = \overline{b} + \overline{a}, \forall\, \overline{a}, \overline{b} \in \mathbb{Z}_m$.

(iii) $\exists\ \overline{0} \in \mathbb{Z}_m \mid \overline{0} + \overline{a} = \overline{a}, \forall\, \overline{a} \in \mathbb{Z}_m$. De fato, pois $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$, e isso ocorre porque 0 e a são elementos de $\mathbb{Z}$, e em $\mathbb{Z}$ o elemento 0 é neutro para a adição. Portanto $\overline{0}$ é o elemento neutro da adição em $\mathbb{Z}_m$.

(iv) $\exists\ \overline{a'} \in \mathbb{Z}_m \mid \overline{a} + \overline{a'} = \overline{0}, \forall\, \overline{a} \in \mathbb{Z}_m$. De fato, $\overline{a} + \overline{a'} = \overline{0} \Rightarrow \overline{a+a'} = \overline{0} \Rightarrow a + a' \equiv 0\ (mod\ m)$, isso quer dizer que $m \mid (a+a') - 0 \Rightarrow a + a' = qm$ para algum $q \in \mathbb{Z}$. Logo, $a' = qm - a$, então $\overline{a'} = \overline{qm - a} \Rightarrow \overline{a'} = \overline{qm} + \overline{(-a)}$, mas $\overline{qm} = \overline{m}$, portanto, $\overline{a'} = \overline{m-a}$ é o simétrico aditivo de $\overline{a}, \forall\, \overline{a} \in \mathbb{Z}_m$.

(v) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{(b \cdot c)} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c}$, já que a multiplicação em $\mathbb{Z}$ é comutativa. Então $\overline{(a \cdot b) \cdot c} = \overline{(a \cdot b)} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}, \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(vi) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a \cdot (b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Definição 7.45. *Seja A um anel. Se a multiplicação em A é comutativa, isto é, se*

$$ab = ba,$$

para quaisquer $a, b \in A$*, então se diz que A é um* ***anel comutativo****.*

Definição 7.46. *Seja A um anel. Se A conta com o elemento neutro para a multiplicação, isto é, se existe um elemento $1 \in A,\ 1 \neq 0$, tal que*

$$a \cdot 1 = 1 \cdot a = a,$$

qualquer que seja $a \in A$, dizemos que 1 é a unidade de A e que A é um ***anel com unidade.***

Definição 7.47. *Seja A um anel comutativo com unidade. Se para esse anel vale a lei do anulamento do produto, ou seja, se*

$$ab = 0 \Leftrightarrow a = 0 \quad ou \quad b = 0$$

com $a, b \in A$, então A é um ***anel de integridade*** *ou* ***domínio****.*

Exemplo 7.48. Todos os anéis numéricos, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, são domínios.

Definição 7.49. *Seja $\mathbb{K}$ um anel comutativo com unidade. Se o conjunto dos elementos de $\mathbb{K}$ que possuem simétrico multiplicativo, ou inverso, for igual a $\mathbb{K}^* = \mathbb{K} - \{0\}$, então $\mathbb{K}$ é um* ***corpo****.*

Exemplo 7.50. Os conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com as suas operações usuais são corpos, pois $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são anéis comutativos com unidade e todos os seus elementos, exceto o zero, têm simétrico multiplicativo.

Definição 7.51. *Seja $\mathbb{K}$ um corpo. Um subconjunto não vazio $\mathbb{L} \subset \mathbb{K}$ é chamado de* ***subcorpo*** *de $\mathbb{K}$ se é fechado para a adição e a multiplicação de $\mathbb{K}$ e se $\mathbb{L}$ também tem uma estrutura de corpo, com as operações de $\mathbb{K}$ restritas aos elementos de $\mathbb{L}$.*

Exemplo 7.52. $\mathbb{Q}$ é subcorpo de $\mathbb{R}$.

Definição 7.53. *Seja $\mathbb{F}$ um anel. Chamamos de* ***polinômio*** *sobre $\mathbb{F}$ em uma indeterminada x a expressão $p(x) = a_0 + a_1x + \ldots + a_nx^n$ em que $a_i \in \mathbb{F}$, para todo $i = 1, \ldots, n$.*

Denotamos por $\mathbb{F}[x]$ o ***conjunto de todos os polinômios*** *sobre $\mathbb{F}$, em uma indeterminada x.*

Exemplo 7.54. O polinômio $-4x^3 - 1 + \sqrt{3}x^2$ é um polinômio sobre $\mathbb{R}$.

Definição 7.55. *Seja $p(x) = a_0 + a_1x + \ldots + a_nx^n$, com $a_n \neq 0$, um polinômio. O número natural n é chamado* ***grau*** *de $p(x)$ e é denotado por $\partial p(x)$. Assim, o termo a_n é chamado* ***coeficiente dominante*** *de $p(x)$. Caso o termo a_n seja 1, então $p(x)$ é um* ***polinômio mônico****.*

Exemplo 7.56. O grau do polinômio $p(x) = -3x^4 + \frac{2}{7}x^2 + 6$ é 4. Como seu coeficiente dominante é -3, $p(x)$ não é mônico.

Exemplo 7.57. O grau do polinômio $q(x) = x^5 - 0,8x^3 + 5x$ é 5. Como seu coeficiente dominante é 1, $q(x)$ é mônico.

Definição 7.58. *Seja $\mathbb{K}$ um corpo e $p(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio em $\mathbb{K}[x]$. Se $u \in \mathbb{K}$, chamamos de* ***valor de p(x) em u*** *a expressão $p(u) = a_0 + a_1u + \ldots + a_nu^n \in \mathbb{K}$. Se $p(u) = 0$, dizemos que u é* ***raiz do polinômio*** *$p(x)$.*

Exemplo 7.59. Seja o polinômio $p(x) = \begin{pmatrix} 1 & 1 \\ 3 & 0 \end{pmatrix} x + \begin{pmatrix} -1 & 3 \\ -2 & -2 \end{pmatrix}$ em $M_2(\mathbb{R})[x]$. O valor de $p(x)$ em $u = \begin{pmatrix} 0 & 2 \\ -1 & 4 \end{pmatrix}$ é

$$p\begin{pmatrix} 0 & 2 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ -1 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 3 \\ -2 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 9 \\ -2 & 4 \end{pmatrix}$$

e a raiz de $p(x)$ é $\begin{pmatrix} \frac{2}{3} & \frac{2}{3} \\ \frac{1}{3} & -\frac{11}{3} \end{pmatrix}$, pois

$$p\begin{pmatrix} \frac{2}{3} & \frac{2}{3} \\ \frac{1}{3} & -\frac{11}{3} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{2}{3} & \frac{2}{3} \\ \frac{1}{3} & -\frac{11}{3} \end{pmatrix} + \begin{pmatrix} -1 & 3 \\ -2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definição 7.60. *Seja $f(x) \in \mathbb{F}[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um **polinômio irredutível** sobre $\mathbb{F}$ se toda vez que $f(x) = g(x)h(x)$, que $g(x), h(x) \in \mathbb{F}[x]$, implicar que ou $g(x) = a$, constante em $\mathbb{F}$, ou $h(x) = b$, constante em $\mathbb{F}$. Se $f(x)$ não for irredutível sobre $\mathbb{F}$, dizemos que $f(x)$ é **redutível** sobre $\mathbb{F}$.*

Exemplo 7.61. O polinômio $x^2 - 17$ é redutível sobre $\mathbb{R}$, pois

$$x^2 - 17 = \left(x - \sqrt{17}\right)\left(x + \sqrt{17}\right)$$

em que cada um dos fatores de x^2-17 pertencem a $\mathbb{R}[x]$ e não são polinômios constantes em $\mathbb{R}$ pois ambos tem grau 1.

Exemplo 7.62. O polinômio $x^2 - 17$ é irredutível sobre $\mathbb{Q}$.

Para mostrar isto suponha o contrário, que $x^2 - 17$ não é irredutível sobre $\mathbb{Q}$. Isto significa que

$$x^2 - 17 = (ax + b)(cx + d)$$

com a, b, c e $d \in \mathbb{Q}$. Os coeficientes a e c devem ser diferentes de 0 (pois caso assumissem esse valor, o polinômio seria irredutível). Como $\sqrt{17}$ é raiz de $x^2 - 17$, substituindo x por $\sqrt{17}$ em ambos os membros da igualdade, obtemos

$$0 = \left(a\sqrt{17} + b\right)\left(c\sqrt{17} + d\right).$$

A igualdade acima nos fornece que ou $a\sqrt{17} + b = 0$ ou $c\sqrt{17} + d = 0$, isto é, ou $\sqrt{17} = \dfrac{-b}{a}$ ou $\sqrt{17} = \dfrac{-d}{c}$, o que é absurdo, pois $\sqrt{17}$ é irracional. Portanto, o polinômio $x^2 - 17$ é irredutível sobre $\mathbb{Q}$.

Definição 7.63. *Seja A um anel comutativo. Um subconjunto $I \subset A$, $\mathcal{I} \neq \emptyset$ será chamado de **ideal** em A se, para qualquer $x, y \in \mathcal{I}$ e para quaisquer $a \in A$, verificarem-se as relações seguintes:*

(i) $x - y \in \mathcal{I}$;

(ii) $ax \in \mathcal{I}$.

Exemplo 7.64. O subconjunto $\mathcal{I} = \{f : \mathbb{R} \to \mathbb{R} \mid f(1) = 0\}$ do conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$, é um ideal de $\mathbb{R}^{\mathbb{R}}$, pois, para todo $f, g \in \mathcal{I}$ e $h \in \mathbb{R}^{\mathbb{R}}$,

(i) $(f-g)(1) = f(1) - g(1) = 0 + 0 = 0$;

(ii) $(hf)(1) = h(1) \cdot f(1) = h(1) \cdot 0 = 0$.

Definição 7.65. *Um ideal $\mathcal{I}$ gerado pelo conjunto unitário $\{a\}$ é chamado* ***ideal principal*** *gerado por a, isto é, $\mathcal{I} =< a >$. Se todos os ideais de um anel comutativo são principais, então esse anel recebe o nome de* ***anel principal****.*

Exemplo 7.66. Seja $n \in \mathbb{Z}$ e seja $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, um ideal em $\mathbb{Z}$. Então $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ é um ideal principal. Na verdade, todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$.

Observação 7.67. O conjunto $\mathbb{Z}$ recebe o nome de *domínio de ideais principais* pois todos os seus ideais são principais.

Definição 7.68. *Se A é um domínio, então o corpo $\mathbb{F}$ consistindo de todos os elementos da forma $\alpha\beta^{-1}$ para $\alpha, \beta \in A$ com $\beta \neq 0$ é chamado de* ***corpo de frações*** *de A.*

Exemplo 7.69. O corpo de frações de $\mathbb{Z}$ é $\mathbb{Q}$.

Definição 7.70. *Suponha que A é um domínio com corpo de frações $\mathbb{F}$. Então um subconjunto não vazio $\mathcal{I}$ de $\mathbb{F}$ é chamado de* ***ideal fracionário*** *se satisfaz as três propriedades:*

(i) $\forall\ \alpha, \beta \in \mathcal{I}, \alpha + \beta \in \mathcal{I}$;

(ii) $\forall\ \alpha \in \mathcal{I}$ *e* $r \in A, r\alpha \in \mathcal{I}$;

(iii) $\exists\ \gamma \in A$ *com* $\gamma \neq 0$ *tal que* $\gamma\mathcal{I} \subseteq A$.

Observação 7.71. Todo ideal de A é também um ideal fracionário, basta tomar $\gamma = 1$.

Exemplo 7.72. Seja o domínio $\mathbb{Z}$, seu corpo de frações $\mathbb{Q}$ e o ideal $\mathcal{I} = \left\{\frac{n}{3} \mid n \in \mathbb{Z}\right\} \subset \mathbb{Q}$. O conjunto $\mathcal{I}$ é um ideal fracionário, pois, para todo α, β e $r \in \mathbb{Z}$:

(i) $\frac{\alpha}{3} + \frac{\beta}{3} = \frac{\alpha + \beta}{3} \in I$;

(ii) $r\frac{\alpha}{3} = \frac{r\alpha}{3} \in I$;

(iii) $\exists\ 3 \in \mathbb{Z}$ tal que $3I = \mathbb{Z}$.

Definição 7.73. *Sejam A e B duas estruturas algébricas. Uma aplicação $f : A \to B$ é um* ***homomorfismo*** *de A em B se*

(i) $f(x + y) = f(x) + f(y)$, *para todo* $x, y \in A$;

(ii) $f(xy) = f(x)f(y)$, *para todo* $x, y \in A$.

Se, além disso, a aplicação f for injetora, dizemos que f é um ***monomorfismo*** *ou* ***mergulho****; se f for sobrejetora, dizemos que f é um* ***epimorfismo****; e se f for bijetora, dizemos que f é um* ***isomorfismo*** *e que A é isomorfo a B.*

Observação 7.74. Note que a aplicação f da Definição 7.73 preserva todas as propriedades estruturais de A em B.

Exemplo 7.75. A aplicação $f : \mathbb{Z} \to \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ definida por

$$f(n) = \begin{cases} \overline{0}, \text{ se } n \text{ é par;} \\ \overline{1}, \text{ se } n \text{ é ímpar.} \end{cases}$$

é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_2$, pois, para todo n_1 e $n_2 \in \mathbb{Z}$,

- se n_1 for ímpar e n_2 for par:

  (i) $f(n_1 + n_2) = \overline{1} = \overline{1} + \overline{0} = f(n_1) + f(n_2)$;
  (ii) $f(n_1 n_2) = \overline{0} = \overline{1} \cdot \overline{0} = f(n_1) \cdot f(n_2)$.

- se n_1 e n_2 forem pares:

  (i) $f(n_1 + n_2) = \overline{0} = \overline{0} + \overline{0} = f(n_1) + f(n_2)$;
  (ii) $f(n_1 n_2) = \overline{0} = \overline{0} \cdot \overline{0} = f(n_1) \cdot f(n_2)$.

- se n_1 e n_2 forem ímpares:

  (i) $f(n_1 + n_2) = \overline{0} = \overline{2} = \overline{1} + \overline{1} = f(n_1) + f(n_2)$;
  (ii) $f(n_1 n_2) = \overline{1} = \overline{1} \cdot \overline{1} = f(n_1) \cdot f(n_2)$.

Exemplo 7.76. Seja o conjunto $A = \{m + n\sqrt{2} \mid m,\ n \in \mathbb{Z}\}$. A aplicação $f : A \to A$ definida por $f(m+n\sqrt{2}) = m-n\sqrt{2}$ é um homomorfismo pois, para todo $m, n, s, t \in \mathbb{Z}$,

(i) $f((m + n\sqrt{2}) + (s + t\sqrt{2})) = f((m + s) + (n + t)\sqrt{2}) = (m + s) - (n + t)\sqrt{2} = (m - n\sqrt{2}) + (s - t\sqrt{2}) = f(m + n\sqrt{2}) + f(s + t\sqrt{2})$;

(ii) $f((m+n\sqrt{2}) \cdot (s+t\sqrt{2})) = f(ms+mt\sqrt{2}+ns\sqrt{2}+2nt) = f((ms+2nt)+((mt+ns)\sqrt{2})) = (ms + 2nt) - (mt + ns)\sqrt{2} = (m - n\sqrt{2}) \cdot (s - t\sqrt{2}) = f(m + n\sqrt{2}) \cdot f(s + t\sqrt{2})$.

Além disso, f é bijetora, pois, para todo $m, n, s, t \in \mathbb{Z}$,

(i) f é injetora. De fato, sejam $m+n\sqrt{2}$ e $s+t\sqrt{2} \in A$. Se $m+n\sqrt{2} \neq s+t\sqrt{2}$, então $f(m+n\sqrt{2}) = m-n\sqrt{2} \neq s-t\sqrt{2} = f(s+t\sqrt{2})$. Assim, f é um monomorfismo;

(ii) f é sobrejetora. De fato, para todo elemento $m + n\sqrt{2}$ de A existe $m - n\sqrt{2}$ em A, de modo que $f(m - n\sqrt{2}) = m + n\sqrt{2}$. Assim, f é um epimorfismo.

Portanto, f é um isomorfismo.

Índice Remissivo

Anel, 82
    com Unidade., 84
    Comutativo, 83
    de Integridade, 84
    dos Inteiros, 26
    Principal, 86

Base, 77
Base Integral, 30

Canônica, 57
Classe
    de Equivalência, 82
    de Restos, 82
Congruente, 81
Conjugado, 27
Contração, 80
Corpo, 84
    de Frações, 86
    de Números, 23
    Quadrático, 33

Densidade
    de Empacotamento, 41
    de Centro, 42
Determinante do Reticulado, 40
Dilação, 80
Dimensão, 77
Discriminante, 31
Domínio, 84

Elemento
    Algébrico, 25
    Primitivo, 27
    Transcendente, 25
Empacotamento Esférico, 41
Epimorfismo, 86
Equivalentes, 43
Extensão
    Algébrica, 26
    de Corpos, 23
    Imaginária, 33
    Real, 33

Finitamente Gerado, 77

Grau, 84
Grau da Extensão, 23

Homomorfismo, 86

Ideal, 85
    Fracionário, 86
    Principal, 86
Instável, 66
Inteiro Algébrico, 26
Isomorfismo, 86

Linearmente
    Dependente, 76
    Independente, 76
Livre de Quadrados, 80

Mínimo
    Sucessivo, 65
Matriz
    de Gram, 40
    de Rotação, 80
    Geradora, 40
Matriz da
    Transformação Linear, 79
Mergulho, 86
Monomorfismo, 86

Norma, 29
Norma Mínima, 41

Polinômio, 84
    Irredutível, 85
    Mônico, 84
    Redutível, 85
Posto Completo, 40
Produto Interno, 78

Região Fundamental, 39
Relação, 81
    de Equivalência, 81

Semelhantes, 43
Semi-Estável, 66
Subcorpo, 84
Subespaço
    Gerado, 77
Subsepaço
    Vetorial, 76

Totalmente
    Imaginário, 28
    Real, 28
Traço, 29
Transformação Linear, 78

Volume do Reticulado, 40