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

Universidade Estadual Paulista

Campus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Famílias de Reticulados Algébricos e Reticulados Ideais

Cintya Wink de Oliveira Benedito

Orientador: Prof. Dr. Antonio Aparecido de Andrade

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

São José do Rio Preto

Fevereiro - 2010

Livros Grátis

http://www.livrosgratis.com.br

Milhares de livros grátis para download.

CINTYA WINK DE OLIVEIRA BENEDITO

Famílias de reticulados algébricos e reticulados ideais

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

Orientador:Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto, 26 de fevereiro de 2010.

Benedito, Cintya Wink de Oliveira.
Famílias de reticulados algébricos e reticulados ideais / Cintya Wink de Oliveira Benedito. - São José do Rio Preto : [s.n.], 2010.
165 f. : il. ; 30 cm.

Orientador: Antonio Aparecido de Andrade
Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra comutativa. 2. Reticulados (Matemática). 3. Teoria dos reticulados. 4. Homomorfismos (Matemática). 5. Homomorfismo canônico.
Funções de. I. Andrade, Antonio Aparecido. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 512.71

Ficha catalográfica elaborada pela Biblioteca do IBILCE
Campus de São José do Rio Preto - UNESP

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
Professor Doutor - IBILCE - UNESP
Orientador

Prof. Dr. Edson Donizete de Carvalho
Professor Doutor - UNESP - Ilha Solteira

Prof. Dr. Jéfferson Luiz Rocha Bastos
Professor Doutor - IBILCE - UNESP

AGRADECIMENTOS

Ao concluir este trabalho agradeço:

Primeiramente à Deus.

Aos meus pais Gaudeley de Oliveira Benedito (in memorian) e Denise Wink, que me deram à vida e em meio a tantas dificuldades, sempre me apoiaram.

Aos meus avós Domingos Benedito (in memorian) e Isolina da Conceição (in memorian), pelo amor, educação e todos os ensinamentos que me fizeram quem eu sou.

Aos demais membros da minha família, que mesmo sem perceber, ao mostrar o orgulho e confiança que depositavam em mim me davam forças para continuar. Em especial as minhas tias Marlene, Vera e Deise.

Ao Clayton, pelo seu amor, sua amizade e por estar comigo em todos os momentos, fazendo com que tudo parecesse mais belo e mais fácil.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, pelos conselhos, pela paciência, pela amizade e por depositar sua confiança em mim diante desse trabalho.

Aos professores do Departamento de Matemática do IBILCE/UNESP - São José do Rio Preto, pelo conhecimento transmitido e pela amizade.

Aos professores da Banca examinadora.

Aos meus colegas de Pós-graduação, pela amizade e agradável convívio. Em especial a minha grande amiga Jucilene e, aos meus amigos Gustavo, Júnior e Eduardo que estiveram comigo desde o ínicio, dividindo comigo todos momentos difíceis e felizes desta caminhada.

À FAPESP, pelo auxílio financeiro, no Processo 2007/06381-5.

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

Uma pessoa é capaz de conseguir qualquer coisa se o seu entusiasmo não tiver limites.
(Charles Schwab)

Resumo

Neste trabalho é feito um estudo sobre famílias de reticulados algébricos e reticulados ideais. Nosso principal objetivo é a construção de reticulados que são versões rotacionadas de reticulados já conhecidos na literatura. Deste modo, apresentamos construções obtidas via polinômios, via perturbações do homomorfismo canônico e, também, construções ciclotômicas a partir do reticulado $\mathbb{Z}^n$.

Palavras-Chave: Reticulados, homomorfismo canônico, reticulados algébricos, reticulados ideais, reticulados rotacionados.

Abstract

This work presents a study of algebraic and families of ideal lattices. Our main goal is the construction of lattices which are rotated versions of known lattices in the literature. In this way, we present constructions obtained via polynomials, via pertubations of the canonical homomorphism, and also cyclotomic construction from the lattice $\mathbb{Z}^n$.

Keywords: Lattices, canonical homomorphism, algebraic lattices, ideal lattices, rotated lattices.

Índice de Símbolos

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

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

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

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

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

$\prod$: produtório

$\sum$: somatório

$\overline{x}$: conjugado complexo de x

$\#B$: cardinalidade do conjunto B

$A = (a_{ij})$: matriz

$\det(A)$: determinante da matriz A

A: anel

$\mathfrak{a}, \mathfrak{p}, \mathfrak{m}, \mathfrak{I}, ...$: ideais

$A/\mathfrak{a}$: anel quociente

$A[x]$: anel de polinômios com coeficientes em A

$\partial(f)$: grau do polinômio f

$Ker(f)$: núcleo da aplicação f

$Im(f)$: imagem da aplicação f

f': derivada de f

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

$[\mathbb{K} : \mathbb{L}]$: grau da extensão $\mathbb{K}/\mathbb{L}$

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

$Tr_{\mathbb{K}/\mathbb{L}}(\alpha)$: traço do elemento $\alpha \in \mathbb{K}$

$\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)$: norma do elemento $\alpha \in \mathbb{K}$

$\mathcal{O}_{\mathbb{K}}$: anel de inteiros de A em $\mathbb{K}$

$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \cdots, \alpha_n)$: discriminante da n-upla $(\alpha_1, \cdots, \alpha_n) \in \mathbb{K}$ e $\mathbb{K}/\mathbb{L}$ extensão

$\mathcal{D}_{\mathbb{K}}$: discriminante da extensão $\mathbb{K}$ sobre $\mathbb{L}$

$\mathcal{N}(\mathfrak{a})$: norma do ideal $\mathfrak{a}$

$\varphi(n)$: função de Euler aplicada a n

$\phi_n(x)$: n-ésimo polinômio ciclotômico

$\Delta(\mathbb{K}/\mathbb{L})^{-1}$: codiferente da extensão $\mathbb{K}$ sobre $\mathbb{L}$

div: diversidade

$d_{p,min}$: distância produto mínima

Sumário

Introdução **14**

1 Conceitos Iniciais **17**

1.1 Conceitos básicos de álgebra 17

1.1.1 Anéis e corpos 17

1.1.2 Módulos 20

1.1.3 Módulos Noetherianos 22

1.2 Teoria de Galois 25

1.3 Teoria algébrica dos números 27

1.3.1 Inteiros algébricos 27

1.3.2 Traço e norma 31

1.3.3 Norma de um ideal 36

1.3.4 Discriminante 38

1.3.5 Anéis de Dedekind 42

1.3.6 Ideais fracionários 43

1.4 Corpos quadráticos e corpos ciclotômicos 45

1.4.1 Corpos quadráticos 46

1.4.2 Corpos ciclotômicos 48

1.5 Codiferente 52

1.6 Conclusão do capítulo 56

2 Aplicação das formas quadráticas aos corpos ciclotômicos **57**

2.1 Aplicações aos corpos $\mathbb{Q}(\zeta_p)$ 57

2.2 Aplicações aos corpos $\mathbb{Q}(\zeta_n)$ 59

2.3 Conclusão do capítulo 65

3 Reticulados **66**

3.1 Definição 66

3.2 Matriz de Gram e o determinante de um reticulado 71

3.3 Empacotamento no $\mathbb{R}^n$ . . . 72
3.4 Diversidade e distância produto mínima . . . 74
3.5 Exemplos de reticulados conhecidos . . . 76
3.5.1 Reticulado n-dimensional A_n . . . 76
3.5.2 Reticulado n-dimensional D_n . . . 78
3.5.3 Reticulado 8-dimensional E_8: . . . 80
3.5.4 Reticulado laminado Λ_n . . . 82
3.6 Conclusão do Capítulo . . . 82

4 Reticulados de dimensões 2 e 3 via polinômios 83
4.1 Reticulados de dimensão 2 via polinômios de grau 2 com raízes reais . . . 83
4.2 Reticulados de dimensão 2 via polinômios de grau 2 com raízes complexas conjugadas . . . 88
4.3 Reticulados de dimensão 3 via polinômios de grau 3 com raízes reais . . . 91
4.4 Conclusão do capítulo . . . 96

5 Reticulados algébricos 97
5.1 Reticulados via o homomorfismo canônico e suas perturbações . . . 97
5.1.1 Homomorfismo canônico . . . 97
5.1.2 Perturbação σ_α . . . 108
5.1.3 Perturbação $\sigma_{2\alpha}$ . . . 115
5.2 Uma construção de reticulados algébricos rotacionados de dimensões 2, 4, 6, 8 e 12 via a perturbação σ_α do homomorfismo canônico . . . 121
5.2.1 Reticulados algébricos rotacionados de dimensão 2 . . . 122
5.2.2 Reticulados algébricos rotacionados de dimensão 4 . . . 124
5.2.3 Reticulados algébricos rotacionados de dimensão 6 . . . 128
5.2.4 Reticulados algébricos rotacionados de dimensão 8 . . . 132
5.2.5 Reticulados algébricos rotacionados de dimensão 12 . . . 135
5.3 Conclusão do capítulo . . . 137

6 Reticulados Ideais 138
6.1 Definição . . . 138
6.2 Reticulados ideais obtidos a partir da perturbação $\sigma_{2\alpha}$ do homomorfismo canônico 140
6.3 Diversidade e distância produto mínima de um reticulado ideal . . . 143
6.4 Construções de $\mathbb{Z}^n$-reticulados rotacionados utilizando reticulados ideais . . . 147
6.4.1 O reticulado $\mathbb{Z}^n$ . . . 147
6.4.2 Construção de $\mathbb{Z}^n$-reticulados rotacionados via o corpo ciclotômico $\mathbb{Q}(\zeta_p)$ 148

6.4.3 Construção de $\mathbb{Z}^n$-reticulados rotacionados via o corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$ 153
6.5 Conclusão do capítulo 159

Conclusão **160**

Referências bibliográficas **162**

Índice Remissivo **164**

Introdução

A Teoria de códigos corretores de erros surgiu com o semanal artigo do matemático Claude A. Shannon, [25]. Quando transmitimos uma informação há uma possibilidade da mensagem recebida ser diferente da mensagem enviada. Assim, esta teoria surgiu desta necessidade de detectar e recuperar a mensagem enviada ao receptor e com isso poder construir códigos com pequena probabilidade de ocorrerem erros.

Um dos bons parâmetros para se encontrar bons códigos corretores de erros está ligado ao problema do empacotamento de esferas, que surgiu a partir do 18º Problema de Hilbert, que é uma forma de dispor esferas no espaço euclidiano de modo a cobrir a maior parte do espaço. Este problema, é denominado de empacotamento esférico e, quando o conjunto de centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ então estes empacotamentos passam a se chamar empacotamentos reticulados.

Pela Teoria de Códigos, ao tomarmos o espaço euclidiano n-dimensional, para n suficientemente grande, se considerarmos os centros das esferas de um mesmo empacotamento reticulado denso como sinais (para valores altos da relação sinal-ruído, SNR), obtemos um código de bloco ótimo para um canal gaussiano branco (AWGN), limitado em faixa. Garantindo pequena probabilidade de erro numa transmissão de dados abaixo de uma certa taxa C, chamada capacidade de canal, como demonstrado por Shannon em [25], o que estabeleceu um importante vínculo entre empacotamento esférico e a Teoria de Códigos.

Assim, podemos observar que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes. A partir desta percepção, passaram a associar o estudo dos códigos aos reticulados e surgiram várias famílias de reticulados. Dentre tais famílias destaca-se a descrita por Herman Minkowski, no final do século XIX e início do século XX, que encontrou na Teoria algébrica dos números ferramentas que viabilizaram o efetivo cálculo da densidade de centro.

Este modelo, descrito por Minkowski, consiste em tomar um corpo de números $\mathbb{K}$ de grau n e o seu anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ e obter um homomorfismo, chamado de homomorfismo

de Minkowski (ou homomorfismo canônico), de modo que a imagem de um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, obtido por este homomorfismo, é um reticulado de posto n em $\mathbb{R}^n$.

A partir do homomorfismo de Minkowski, Bayer em [5] e [4] definiu outros homomorfismos que chamamos de perturbações do homomorfismo canônico. E, destes homomorfismos, podemos também obter reticulados em $\mathbb{R}^n$ e, classificá-los quanto a sua densidade de centro (os quais chamamos de reticulados algébricos) ou sua diversidade e distância produto mínima (os quais chamamos de reticulados ideais).

Deste modo, neste trabalho, apresentamos dois métodos de gerar reticulados no $\mathbb{R}^n$ através das pertubações do homomorfismo canônico. O primeiro método é um aperfeiçoamento do método utilizado por Ferrari em [11], onde apresentou famílias de reticulados de dimensões 2, 4, 6 e 8 com densidade de centro ótima, via o homomorfismo canônico. Assim, nosso objetivo com estas novas versões do homomorfismo canônico, é obter famílias de reticulados de dimensões 2, 4, 6, 8 e 12 com densidade de centro ótima. Também fazendo uso destas perturbações apresentamos uma construção de $\mathbb{Z}^n$-reticulados rotacionados via o anel dos inteiros algébricos dos subcorpos maximais reais dos corpos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_{2^r})$, onde p é um número primo e r um inteiro positivo, construções estas feitas por Oggier em [22] e por Andrade em [2]. Uma das vantagens dos reticulados ideais é que os parâmetros que aparecem como a diversidade e distância produto mínima (parâmetros estes que aparecem em problemas de comunicação móvel) e a forma $\mathbb{Z}^n$ cúbica serve para manter a energia de transmissão constante.

Além destes dois métodos descritos acima, um outro método ainda pouco explorado de obter reticulados que será estudado neste trabalho, é o método apresentado por Souza em [26], que consiste em obter reticulados via polinômios irredutíveis sobre o corpo dos racionais. Via este método, apresentamos construções de reticulados com densidade de centro ótima para dimensões 2 e 3. Um dos motivos para estudarmos este método é que ele mostrou-se eficiente quando tratamos de reticulados com densidade de centro ótima para dimensão ímpar, o que não obtemos através do método algébrico.

Assim, este trabalho foi estruturado da seguinte forma. No Capítulo (1) apresentamos os pré-requisitos que serão utilizados no decorrer deste trabalho. As definições e resultados apresentados neste capítulo servirão de base para os capítulos posteriores. Iniciamos apresentando alguns conceitos algébricos, a teoria de Galois, fazemos um estudo sobre a teoria algébrica dos números, os corpos quadráticos, os corpos ciclotômicos e apresentamos o conceito de codiferente. Para o desenvolvimento deste capítulo foram utilizadas as referências [9], [19], [20], [14], [17], [10], [24], [27], [29] e [13].

No Capítulo (2) fazemos um estudo sobre as formas quadráticas aplicadas aos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_n)$, onde p é um número primo e n um inteiro positivo. Essas formas quadráticas serão de grande importância no cálculo do raio de empacotamento de um reticulado.

Neste capítulo, fizemos uso das referências [18], [23] e [21].

No Capítulo (3) apresentamos o conceito central deste trabalho que são os reticulados. Além de definirmos os reticulados, apresentamos também seus principais parâmetros. Após isto, apresentamos o conceito de empacotamento esférico e algumas famílias de reticulados conhecidos na literatura. Para compor este capítulo utilizamos as referências [8], [15], [11] e [1].

No Capítulo (4) apresentamos uma construção de reticulados de dimensões 2 e 3 via polinômios. A partir desta construção, obtemos versões rotacionados de dimensões 2 e 3 via polinômios de graus 2 e 3. Para este estudo fizemos uso das referências [12], [26] e [28].

No Capítulo (5) definimos o homomorfismo de Minkowski e suas perturbações σ_α e $\sigma_{2\alpha}$ e, mostramos que podemos obter reticulados a partir destes homomorfismos aos quais chamaremos neste trabalho de reticulados algébricos. Até aqui fizemos uso das referências [24], [11], [1], [6] e [5]. Para finalizar este capítulo, apresentamos uma construção de nossa autoria para obtenção de reticulados rotacionados de dimensões 2, 4, 6, 8 e 12, utilizando ideais principais do anel dos inteiros de um corpo de números, via pertubações do homomorfismo canônico. Esta construção foi baseada na construção feita por Ferrari em [11]. Destacamos ainda que estas construções deram origem a [3], que está submetido à revista CAM (Computational and Applied Mathematics).

No Capítulo (6) apresentamos os reticulados ideais e suas propriedades. Mostramos que os reticulados ideais também podem ser obtidos via perturbações do homomorfismo canônico. E, para finalizar, apresentamos uma construção de $\mathbb{Z}^n$-reticulados rotacionados via o anel dos inteiros algébricos dos subcorpos maximais reais dos corpos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_{2^r})$, onde p é um número primo e r um inteiro positivo. Neste capítulo utilizamos as referências [8], [6], [7], [13], [5], [4], [22], [2] e [16].

Capítulo 1

Conceitos Iniciais

Neste capítulo iremos apresentar alguns conceitos e resultados que servirão de base no decorrer deste trabalho. Iniciamos na Seção (1.1) apresentando conceitos primordiais da álgebra que são os conceitos de anéis, corpos e módulos. Após isto, na Seção(1.2) apresentamos alguns conceitos e resultados da teoria de Galois. Na Seção (1.3) desenvolvemos um estudo sobre a teoria algébrica dos números. Muitos dos resultados que serão vistos nesta seção irão nos auxiliar na prova de resultados importantes deste trabalho. Na Seção (1.4) definiremos os corpos quadráticos e os corpos ciclotômicos. O estudo destes corpos será focalizado sobre algumas propriedades e resultados que serão utilizados no decorrer deste trabalho. Para finalizar, na Seção (1.5) apresentamos o conceito de codiferente e de algumas de suas propriedades. Algumas demonstrações neste capítulo serão omitidas mas, assim como em todos os resultados, será colocado a referência que a contém.

1.1 Conceitos básicos de álgebra

Nesta seção apresentamos as definições de grupos, anéis, corpos, ideais, módulos e módulos noetherianos e, algumas de suas principais propriedades. Veremos também alguns resultados clássicos da álgebra.

1.1.1 Anéis e corpos

Definição 1.1.1 *Um conjunto não vazio G e uma operação $*$ sobre G é chamado* **grupo** *se essa operação satisfaz as seguintes propriedades:*

1. *$(a * b) * c = a * (b * c)$, para todo $a, b, c \in G$ (associativa)*
2. *existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$ (existência de elemento neutro)*
3. *para todo $a \in G$ existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$ (existência de simétricos).*

Se além disso a operação $*$ for comutativa, isto é, $a * b = b * a$, para todo $a, b \in G$, o grupo é chamado de **abeliano** ou **comutativo**.

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

1. *$a(bc) = (ab)c$, para todo $a, b, c \in A$ (associativa)*
2. *$a(b + c) = ab + ac$ e $(a + b)c = ac + bc$, para todo $a, b, c \in A$ (distributiva).*

Definição 1.1.3 *Nas condições da Definição (1.1.2) ainda temos que:*

1. *Quando a multiplicação do anel A satisfaz $ab = ba$, para todo $a, b \in A$, dizemos que A é um* **anel comutativo**.
2. *A multiplicação pode admitir um elemento neutro, isto é, existe $1 \in A$ tal que $a1 = 1a = a$, para todo $a \in A$. Neste caso, dizemos que A é um* **anel com unidade**.
3. *Um anel cuja multiplicação é comutativa e que possui unidade é chamado de* **anel comutativo com unidade**.

Definição 1.1.4 *Um subconjunto não vazio B de um anel A é um* **subanel** *de A se B é um anel com as mesmas operações de A porém restritas aos elementos de B.*

Definição 1.1.5 *Seja A um anel comutativo com unidade.*

1. *Dizemos que um elemento $a \in A$ é um* **divisor de zero** *se existe um elemento não nulo $b \in A$ tal que $ab = ba = 0$. Se além disso $a \neq 0$, então dizemos que a é um* **divisor próprio de zero**.
2. *Quando A não possui divisores próprios de zero dizemos que A é um* **domínio de integridade**.

Definição 1.1.6 *Dizemos que um anel comutativo com unidade $\mathbb{K}$, é um* **corpo** *se todo elemento não nulo de $\mathbb{K}$ possui inverso em relação à multiplicação, isto é, para todo $a \in \mathbb{K}/\{0\}$, existe $b \in \mathbb{K}$ tal que $ab = 1$.*

Definição 1.1.7 *Um subconjunto não vazio $\mathbb{L} \subset \mathbb{K}$ é chamado* **subcorpo** *de $\mathbb{K}$ se $\mathbb{L}$ é um corpo com as operações de $\mathbb{K}$ restritas a $\mathbb{L}$.*

Definição 1.1.8 *Seja A um anel comutativo. Um subconjunto $\mathfrak{a} \subset A$, $\mathfrak{a} \neq \emptyset$, é chamado de* **ideal** *em A se, para quaisquer $x, y \in \mathfrak{a}$ e para qualquer $a \in A$, as seguintes condições são satisfeitas:*

1. $x - y \in \mathfrak{a}$
2. $ax \in \mathfrak{a}$.

Definição 1.1.9 *Seja A um anel. Um ideal $\mathfrak{a}$ gerado por um elemento $a \in A$, isto é, $\mathfrak{a} = \langle a \rangle = \{ax \ x \in A\}$, é chamado* **ideal principal** *gerado por a. Se todo ideal do anel A é principal, então dizemos que A é um* **anel principal**. *Em particular, se A é um domínio de integridade onde todo ideal é principal dizemos que A é um* **domínio principal**.

Definição 1.1.10 *Seja A um anel.*

1. *Dizemos que um ideal $\mathfrak{p}$ de A é um* **ideal primo** *se $\mathfrak{p} \neq A$ e se para todo $a, b \in A$ tal que $ab \in \mathfrak{p}$ então $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.*
2. *Diz-se que um ideal $\mathfrak{m}$ é um* **ideal maximal** *se $\mathfrak{m} \neq A$ se os únicos ideais em A que contém $\mathfrak{m}$ são o próprio $\mathfrak{m}$ e A.*

Definição 1.1.11 *Sejam A um anel e $\mathfrak{a}$ um ideal de A.*

1. *Chamamos de* **classe de equivalência** *do elemento $a \in A$ em relação ao ideal $\mathfrak{a}$ o subconjunto $\bar{a} = a + \mathfrak{a} = \{a + x : x \in \mathfrak{a}\}$.*
2. *Dados $a, b \in A$, dizemos que a* **é côngruo a** *b* **módulo** *$\mathfrak{a}$ se $a - b \in \mathfrak{a}$, e denotamos por $a \equiv b (mod\ \mathfrak{a})$.*

Sejam A um anel e $\mathfrak{a}$ um ideal. Considerando $A/\mathfrak{a}$ o conjunto das classes de equivalência dos elementos de A, definimos as seguintes operações de soma e produto entre os seus elementos:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \text{isto é,} \quad (a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + \mathfrak{a};$$

$$\bar{a}\bar{b} = \overline{ab}, \quad \text{isto é,} \quad (a + \mathfrak{a})(b + \mathfrak{a}) = (ab) + \mathfrak{a}.$$

Definição 1.1.12 *Sejam A um anel e $\mathfrak{a}$ um ideal. O conjunto $A/\mathfrak{a}$, munido das duas operações definidas acima, é um anel chamado de* **anel quociente** *de A pelo ideal $\mathfrak{a}$. Os ideais de $A/\mathfrak{a}$ são da forma $\mathfrak{a}'/\mathfrak{a}$ onde $\mathfrak{a}'$ pertence ao conjunto dos ideais de A que contém $\mathfrak{a}$.*

Teorema 1.1.1 *([9]) Sejam A um anel comutativo com identidade e $\mathfrak{a}$ um ideal de A. Então*

1. *$A/\mathfrak{a}$ é um domínio se, e somente se, $\mathfrak{a}$ é um ideal primo;*

2. *$A/\mathfrak{a}$ é um corpo se, e somente se, $\mathfrak{a}$ é um ideal maximal.* ∎

Definição 1.1.13 *Sejam A e B dois anéis com elementos identidades 1_A e 1_B, respectivamente. Uma aplicação $\phi : A \to B$ é um* **homomorfismo de anéis** *de A em B se satisfaz as seguintes condições:*

1. $\phi(x+y) = \phi(x) + \phi(y),\ \forall x, y \in A$;

2. $\phi(xy) = \phi(x)\phi(y),\ \forall x, y \in A$;

3. $\phi(1_A) = 1_B$.

Definição 1.1.14 *Chamamos de* **monomorfismo** *um homomorfismo injetor e de* **isomorfismo** *um homomorfismo bijetor. Os isomorfismos de um anel A sobre si mesmo são chamados de* **automorfismo**.

Teorema 1.1.2 *([9]) Se A e B anéis e $\phi : A \to B$ um homomorfismo, então:*

1. *$Im(\phi)$ é um subanel de B.*

2. *$Ker(\phi)$ é um ideal de A.*

3. *ϕ é injetora se, e somente se, $Ker(\phi) = \{0\}$.*

4. *Os anéis $A/Ker(\phi)$ e $Im(\phi)$ são isomorfos (Teorema do Isomorfismo).* ∎

1.1.2 Módulos

Definição 1.1.15 *Seja A um anel. Um conjunto não vazio M é dito um A-***módulo** *se M é um grupo abeliano com relação à operação $+$ e munido de uma aplicação $\phi : A \times M \to M$, definida por $\phi(a, m) = am$, que satisfaz:*

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

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

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

4. $1m = m$,

para todo $a, b \in A$ e $m, n \in M$.

Definição 1.1.16 *Um subgrupo aditivo N do A-módulo M é chamado A-***submódulo** *de M se para todo $a \in A$ e $n \in N$ então $an \in N$.*

Dado um A-módulo M e um A-submódulo N podemos construir o **módulo quociente** M/N da mesma forma como construímos o anel quociente, onde

$$a(m+N) = am + N$$

para todo $a \in A$ e $m \in M$.

Definição 1.1.17 *Um A-módulo M é chamado* **finitamente gerado** *e denotado por f.g., se existem elementos $x_1, \ldots, x_n \in M$ tais que todo $m \in M$ é da forma $m = a_1x_1 + a_2x_2 + \ldots a_nx_n$ com $a_i \in A,\ i = 1, \ldots, n$. Neste caso, dizemos que $x_1, \ldots, x_n$ formam um sistema de geradores de M.*

Definição 1.1.18 *Sejam A um anel, M um A-módulo $x_1, \ldots, x_n \in M$. Dizemos que $\{x_1, \ldots, x_n\}$ é uma* **base** *de M se $x_1, \ldots, x_n$ formar um sistema de geradores de M e se forem linearmente independentes, ou seja, se existem $a_1, \cdots, _n \in A$ tais que $a_1x_1 + a_2x_2 + \ldots a_nx_n = 0$ então $a_i = 0$, para todo $i = 1, \cdots, n$.*

Definição 1.1.19 *Um A-módulo que possui uma base é chamado de A-***módulo livre***.*

Teorema 1.1.3 *([24]) Se A é um anel principal, M um A-módulo livre de posto n, e $M' \neq 0$ um submódulo de M, então:*

1. *M' é livre de posto $q,\ 0 \leq q \leq n$.*
2. *existe uma base $\{e_1, \ldots, e_n\}$ de M e elementos não nulos $a_1, \ldots, a_q \in A$ tais que $\{a_1e_1, \ldots, a_qe_q\}$ é uma base de M' e tal que a_i divide $a_{i+1},\ 1 \leq i \leq q-1$.* ∎

Definição 1.1.20 *Sejam A um anel e M, N dois A-módulos. Dizemos que uma aplicação $f : M \to N$ é um* **homomorfismo de A-módulos** *se satisfaz as seguintes condições*

1. *$f(x+y) = f(x) + f(y)$*
2. *$f(ax) = af(x)$,*

para todo $x, y \in M$ e $a \in A$. Se além disso, a aplicação f for injetora, dizemos que f é um **monomorfismo de A-módulos** *e, se f for bijetora dizemos que f é um* **isomorfismo de A-módulos***.*

Teorema 1.1.4 *([19]) (Teorema do Isomorfismo de Módulos) Se A é um anel, M, N são dois A-módulos e $f : M \to N$ um homomorfismo de A-módulos, então os módulos $M/Ker(f)$ e $Im(f)$ são isomorfos.* ∎

1.1.3 Módulos Noetherianos

Definição 1.1.21 *Sejam M um A-módulo e $I_1 \subset I_2 \ldots \subset I_n \subset \ldots$ uma sequência crescente de A-submódulos de M. Dizemos que esta é uma* **sequência estacionária** *se existir $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$, para todo $n \geq n_0$.*

Observação 1.1.1 *A definição é análoga para* **sequência decrescente estacionária**

Definição 1.1.22 *Sejam A um anel e M um A-módulo. Dizemos que M é um A-***módulo noetheriano** *se satisfaz uma das seguintes condições:*

1. *Todo conjunto não vazio de A-submódulos de M contém um elemento maximal.*
2. *Toda sequência crescente de A-submódulos de M é estacionária.*
3. *Todo A-submódulo de M é finitamente gerado.*

Dizemos que A é um **anel noetheriano** *se A for um A-módulo noetheriano.*

Proposição 1.1.1 *([19]) Todo anel principal A é noetheriano.*

Demonstração: Considere uma sequência crescente de A-submódulos de M,

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots .$$

Como A é um anel principal segue que todos os ideais de A são principais e como os submódulos de A são exatamente os ideais de A, segue que os submódulos de A são principais. Seja $I = \bigcup_{n \in N} I_n$. Temos que I é um ideal de A pois I_j são ideais de A para todo $j \in \mathbb{N}$. Agora, notemos que $I_n \subset I = \langle a \rangle$, para todo $n \in \mathbb{N}$ e $a \in I_{n_0}$, para algum $n_0 \in \mathbb{N}$, pois $a \in \langle a \rangle = I = \bigcup_{n \in \mathbb{N}} I_n$. Como $a \in I_{n_0}$ e $a \in \langle a \rangle$ segue que $I = \langle a \rangle \subset I_{n_0}$. Portanto, $I = I_{n_0}$. Assim, existe $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$, para todo $\forall n \geq n_0$. ∎

Proposição 1.1.2 *([24]) Se A é um anel, M um A-módulo e N um submódulo de M, então as seguintes condições são equivalentes*

1. *M é um A-módulo noetheriano.*
2. *N e $\dfrac{M}{N}$ são A-módulos noetherianos.*

Demonstração: Suponha que M é noetheriano. Seja $(M_n)_{n \geq 0}$ uma sequência crescente de A-submódulos de N. Assim, $(M_n)_{n \geq 0}$ também é uma sequência crescente de A-submódulos de M. Como M é noetheriano, segue que $(M_n)_{n \geq 0}$ é estacionária. Portanto, N é noetheriano. Para mostrar que $\dfrac{M}{N}$ é noetheriano, consideremos os conjuntos

$$S = \{ \text{ submódulos de M que contém } N\} \text{ e } T = \{ \text{ submódulos de } \frac{M}{N}\}.$$

Temos que a aplicação $\varphi : S \longrightarrow T$ definida por $\varphi(L) = \dfrac{L}{N}$, para $L \in S$, é uma bijeção de S em T. Assim, se $(M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos de $\dfrac{M}{N}$, então $(\varphi^{-1}(M_n))_{n\geq 0}$ também é uma sequência crescente A-submódulos de M. Como M é noetheriano, segue que $(\varphi^{-1}(M_n))_{n\geq 0}$ é estacionária, e portanto $(M_n)_{n\geq 0}$ é estacionária. Assim, $\dfrac{M}{N}$ é noetheriano. Reciprocamente, suponhamos que $\dfrac{M}{N}$ e N são noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de A-submódulos de M. Assim, $(N \cap M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos de N. Como N é noetheriano, segue que $(N \cap M_n)_{n\geq 0}$ é estacionária, ou seja, existe $k \in \mathbb{L}$ tal que

$$M_n \cap N = M_{n+1} \cap N, \ \forall n \geq k \text{ e } \frac{M_n}{N} = \frac{M_{n+1}}{N}, \ \forall n \geq k.$$

Sabemos, que $M_n \subseteq M_{n+1}$, para todo $n \geq k$. Se $x \in M_{n+1}$, então existe $y \in M_n$ tal que $x + M_1 = y + N$. Assim, $x - y \in N \cap M_{n+1} = N \cap M_n$. Logo, $x - y \in M_n$ e como $y \in M_n$ segue que $x \in M_n$. Portanto, $M_n = M_{n+1}$, para todo $n \geq k$ e assim, M é noetheriano. ∎

Corolário 1.1.1 *([24]) Se $M_1, \cdots, M_n$ são A-módulos noetherianos então o produto $M_1 \times \cdots \times M_n$ é um A-módulo noetheriano.*

Demonstração: Faremos a prova por indução sobre n. Para $n = 2$, identificamos $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$ e definimos a função $\varphi : M_1 \times M_2 \longrightarrow M_2$ tal que $\varphi(0, y) = y$. Como φ é um homomorfismo sobrejetor, segue que $\dfrac{M_1 \times M_2}{\ker \varphi} \simeq M_2$, onde $\ker \varphi = M_1 \times \{0\}$. Como M_2 é noetheriano, segue que $\dfrac{M_1 \times M_2}{M_1 \times \{0\}} \simeq M_2$ é noetheriano e pela Proposição (1.1.2), segue que $M_1 \times M_2$ é noetheriano. Suponhamos agora, por hipótese de indução, que $M = M_1 \times \cdots \times M_{n-1}$ é noetheriano. Como M_n é noetheriano, segue do caso $n = 2$, que $M = M_1 \times \cdots \times M_n$ é um A-módulo noetheriano. ∎

Observação 1.1.2 *Do Corolário (1.1.1) concluímos que para qualquer anel noetheriano A, o A-módulo $\underbrace{A \times \cdots \times A}_{n}$ é noetheriano.*

Corolário 1.1.2 *([24]) Se A é um anel noetheriano e M é um A-módulo finitamente gerado, então M é um A-módulo noetheriano.*

Demonstração: Seja $\{e_1, \cdots, e_n\}$ um conjunto de geradores do A-módulo M. Temos que a aplicação $\varphi : A^n \longrightarrow M$ definida por $\varphi(a_1, \cdots, a_n) = a_1e_1 + \cdots + a_ne_n$, é um homomorfismo

sobrejetor. Assim, pelo Teorema do Homomorfismo, temos que $\frac{A^n}{\ker\varphi} \simeq M$. Como A é noetheriano, pelo Corolário (1.1.1), segue que A^n é noetheriano. Pela Proposição (1.1.2), segue que M é um A-módulo noetheriano. ■

Observação 1.1.3 *Vimos no Corolário (1.1.2) que se A for um anel noetheriano, então todo submódulo de qualquer A-módulo finitamente gerado será finitamente gerado. Mas, quando A não for noetheriano isto não ocorre. De fato, considerando o próprio A como A-módulo temos que A possui submódulos (ideais) não finitamente gerados.*

Proposição 1.1.3 *([24]) Se A é um anel, B um subanel de A e $\mathfrak{p}$ um ideal primo de A, então $\mathfrak{p} \cap B$ é um ideal primo de B.*

Demonstração: Consideremos a aplicação $\varphi : B \xrightarrow{i} A \xrightarrow{\pi} A/\mathfrak{p}$, onde i é a inclusão e π é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo, pois π e i são homomorfismo. Além disso, $\ker(\varphi) = \mathfrak{p} \cap B$, já que $\varphi(x) = \pi \circ i(x) = \pi(x) = x + \mathfrak{p}$ e $\varphi(x) = \bar{0}$ se, e somente se, x $\in \mathfrak{p} \cap B$. Portanto, pelo Teorema (1.1.2) (Teorema do Isomorfismo), $B/\mathfrak{p} \cap B \simeq Im(\varphi) \subset A/\mathfrak{p}$. Como $A/\mathfrak{p}$ é um domínio, segue que $B/\mathfrak{p} \cap B$ é um domínio. Portanto, pelo Teorema (1.3.2), $\mathfrak{p} \cap B$ é um ideal primo de B. ■

Proposição 1.1.4 *([24]) Se um ideal primo $\mathfrak{p}$ de um anel A contém um produto $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ de ideais então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$, $i = 1, \cdots, n$.*

Demonstração: Se $\mathfrak{a}_j \not\subseteq \mathfrak{p}$, para todo $j = 1, \cdots, n$, então existe $\alpha_j \in \mathfrak{a}_j$ e $\alpha_j \notin \mathfrak{p}$. Como $\mathfrak{p}$ é primo, segue que $\alpha_1 \cdots \alpha_n \notin \mathfrak{p}$. Mas, $\alpha_1 \cdots \alpha_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}$, o que é um absurdo. Portanto, $\mathfrak{p}$ contém $\mathfrak{a}_j$ para algum $j = 1, \cdots, n$. ■

Proposição 1.1.5 *([24]) Em um anel noetheriano A todo ideal de A contém um produto de ideais primos de A.*

Demonstração: Sejam A um anel noetheriano e F o conjuntos dos ideais de A que não contém um produto de ideais primos. Suponhamos $F \neq \emptyset$. Como A é noetheriano, segue que F tem um elemento maximal $\mathfrak{m}$. Temos que $\mathfrak{m}$ não é um ideal maximal, pois caso contrário, $\mathfrak{m}$ seria primo e assim, $\mathfrak{m} \notin F$. Assim, existem $x, y \in A - \mathfrak{m}$ tal que $xy \in \mathfrak{m}$. Notemos que $\mathfrak{m} \subsetneq \langle x \rangle + \mathfrak{m}$ e $\mathfrak{m} \subsetneq \langle y \rangle + \mathfrak{m}$. Logo, $\langle x \rangle + \mathfrak{m}$ e $\langle y \rangle + \mathfrak{m}$ não pertencem a F. Assim,

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n \subseteq \langle x \rangle + \mathfrak{m} \text{ e } \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n \subseteq \langle y \rangle + \mathfrak{m},$$

onde $\mathfrak{p}_i, \mathfrak{q}_j$ são ideais primos de A, e

$$(\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n)(\mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n) \subseteq (\langle x \rangle + \mathfrak{m})(\langle y \rangle + \mathfrak{m}) \subseteq \mathfrak{m},$$

o que é um absurdo. Portanto, $F = \emptyset$. ∎

Corolário 1.1.3 *([24]) Em um domínio noetheriano, todo ideal não nulo contém um produto de ideais primos não nulos.*

Demonstração: Análoga a Proposição (1.1.5). ∎

1.2 Teoria de Galois

Nesta seção apresentamos alguns conceitos da teoria de Galois. Apesar desta teoria ser muito rica em resultados, aqui serão apresentados apenas os conceitos e resultados que serão utilizados no decorrer deste trabalho. Também por necessitar de um estudo mais aprofundado, muitas das demonstrações nesta seção serão omitidas.

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

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

Observação 1.2.1 *No caso em que $[\mathbb{K} : \mathbb{L}]$ é finito dizemos que $\mathbb{K}$ é uma* **extensão finita** *de $\mathbb{L}$. Temos também que se $\mathbb{L} \subseteq \mathbb{K} \subseteq \mathbb{M}$ então $[\mathbb{M} : \mathbb{L}] = [\mathbb{M} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{L}]$ e que $[\mathbb{K} : \mathbb{L}] = 1$ se, e somente se, $\mathbb{K} = \mathbb{L}$.*

Definição 1.2.3 *Sejam $\mathbb{L} \subseteq \mathbb{K}$ corpos. Um elemento $\alpha \in \mathbb{K}$ é chamado* **algébrico** *sobre $\mathbb{L}$ se existe $f(x) \in \mathbb{L}[x] \backslash \{0\}$ tal que $f(\alpha) = 0$. Se $\alpha \in \mathbb{K}$ não é algébrico sobre $\mathbb{L}$ dizemos que α é* **transcendente** *sobre $\mathbb{L}$.*

Observação 1.2.2 *Temos que se $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{L}$ então existe um único polinômio mônico $p(x)$ de grau mínimo tal que $p(\alpha) = 0$, chamamos este polinômio $p(x)$ de* **polinômio minimal** *de α sobre $\mathbb{L}$.*

Definição 1.2.4 *Um* **corpo de números** *$\mathbb{K}$ é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Se $\dim_{\mathbb{Q}} \mathbb{K} = n$ diz-se que $\mathbb{K}$ é um corpo de números de grau n.*

Teorema 1.2.1 *([27]) Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$ para algum número algébrico α.* ∎

Teorema 1.2.2 *([27]) Se $\mathbb{K} = \mathbb{Q}(\alpha)$ é um corpo de números de grau n, então existem exatamente n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$ tal que, $\sigma_i(\alpha) = \alpha_i$, para todo $i = 1, \cdots, n$, onde $\alpha_1, \cdots, \alpha_n$ são as raízes do polinômio minimal de $\alpha \in \mathbb{K}$.* ∎

Definição 1.2.5 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \cdots, \sigma_n$ os n-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$. Temos que:*

1. *Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ dizemos que σ_i é um* **homomorfismo real**. *Caso contrário dizemos que σ_i é um* **homomorfismo imaginário**.

2. *Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, para todo $i = 1, \cdots, n$, dizemos que $\mathbb{K}$ é um* **corpo totalmente real**. *Se $\sigma_i(\mathbb{K}) \nsubseteq \mathbb{R}$, para todo $i = 1, \cdots, n$, dizemos que $\mathbb{K}$ é um* **corpo totalmente imaginário**.

Definição 1.2.6 *Um corpo de números $\mathbb{K}$ é chamado de CM-corpo se existir um corpo de números totalmente real $\mathbb{F}$ tal que $\mathbb{K}$ é uma extensão quadrática totalmente imaginária de $\mathbb{F}$.*

Teorema 1.2.3 *([20]) Se $\mathbb{L} \subset \mathbb{K}$ é uma extensão de corpos e $\alpha \in \mathbb{K}$, então α é algébrico sobre $\mathbb{K}$ se, e somente se, $\mathbb{L}(\alpha)$ é uma extensão finita de $\mathbb{L}$. Neste caso, $[\mathbb{L}(\alpha) : \mathbb{L}] = \partial p$, onde $p(x)$ é o polinômio minimal de α sobre $\mathbb{L}$, e $\mathbb{L}(\alpha) = \mathbb{L}[\alpha]$.* ■

Definição 1.2.7 *Sejam $\mathbb{L} \subset \mathbb{K}$ uma extensão de corpos e $f \in \mathbb{L}[x]$. Dizemos que $\mathbb{K}$ é o* **corpo de raízes** *de f se $\mathbb{K}$ é o menor corpo contendo $\mathbb{L}$ e todas as raízes de f e denotamos por $\mathbb{K} = \mathbb{L}(R_f)$.*

Definição 1.2.8 *Seja $\mathbb{L}$ um corpo e $f(x) \in \mathbb{L}[x]$ um polinômio não constante. Dizemos que $f(x)$ é* **separável** *se todas as raízes de $f(x)$ são simples no seu corpo de raízes.*

Definição 1.2.9 *Uma extensão finita $\mathbb{K}/\mathbb{L}$ é* **galoisiana** *se $\mathbb{K}$ é o corpo de raízes de $\mathbb{L}$, para algum $f(x) \in \mathbb{L}[x]$ separável.*

Definição 1.2.10 *Sejam $\mathbb{L} \subset \mathbb{K}$ uma extensão e $H \subset Aut(\mathbb{K})$. O corpo*

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

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

Definição 1.2.11 *Seja $\mathbb{L} \subset \mathbb{K}$ uma extensão. O* **grupo de Galois** *de $\mathbb{K}$ sobre $\mathbb{L}$ é dado por:*

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

Definição 1.2.12 *Seja $\mathbb{K}$ um corpo de números.*

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

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

Proposição 1.2.1 *([20]) Se $\phi : \mathbb{K} \to \mathbb{K}$ é uma involução então $\phi \in Gal(\mathbb{K}/\mathbb{Q})$, onde $Gal(\mathbb{K}/\mathbb{Q})$ denota o grupo de galois de $\mathbb{K}$ sobre $\mathbb{Q}$.*

Demonstração: Pela definição de involução segue que ϕ é um homomorfismo e que ϕ fixa $\mathbb{Q}$. Mostremos que ϕ é injetora. Sejam $a, b \in \mathbb{K}$ tal que $\phi(a) = \phi(b)$. Aplicando ϕ na igualdade temos que $\phi(\phi(a)) = \phi(\phi(b))$, mas $\phi^2 = id$ pois ϕ é uma involução. Logo, $a = b$. Para mostrarmos que ϕ é sobrejetora tomemos $y \in \mathbb{K}$. Sabemos que $\phi^2(y) = y$. Assim, se $x = \phi(y)$ então $\phi(x) = \phi(\phi(y)) = \phi^2(y) = y$. Desta forma, temos que ϕ é um isomorfismo que fixa $\mathbb{Q}$. Portanto, $\phi \in Gal(\mathbb{K}/\mathbb{Q})$. ∎

Proposição 1.2.2 *([20]) Se $\mathbb{K}$ é um corpo de números, ϕ uma involução e $\mathbb{F}$ o corpo fixo da involução, então $[\mathbb{K} : \mathbb{F}] \leq 2$.*

Demonstração: Por definição de extensão galoisiana temos que $\mathbb{K}/\mathbb{Q}$ é uma extensão finita e separável. Assim, se H é um subgupo normal de G, onde $G = Gal(\mathbb{K}/\mathbb{Q})$, então o corpo $\mathbb{L}^H$, fixo por H, satisfaz $[\mathbb{K} : \mathbb{L}^H] \leq |H|$. Agora, se tomarmos $H = \{id, \phi\}$ temos que H é um subgrupo de G, pois $\phi^2 = id$. Como $\mathbb{L}^H = \mathbb{F}$ é o corpo fixo por H, segue que $[\mathbb{K} : \mathbb{F}] \leq |H|$. Mas, $|H| = o(\phi) \leq 2$. Logo, $[\mathbb{K} : \mathbb{F}] \leq 2$. ∎

Exemplo 1.2.1 *Sejam $\mathbb{K} = \mathbb{Q}(i)$ um corpo de números de grau 2 e $\phi : \mathbb{K} \to \mathbb{K}$ a conjugação complexa. Temos que ϕ é uma involução, $\mathbb{F} = \{x \in \mathbb{K} | \phi(x) = x\} = \mathbb{Q}$ e $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{Q}] = 2$.*

Observação 1.2.3 *Se $\mathbb{K}$ é um CM-corpo, então a conjugação complexa comuta com todos os $\mathbb{Q}$-homomorfismos $\sigma_1, \cdots, \sigma_n$ de $\mathbb{K}$ em $\mathbb{C}$.*

1.3 Teoria algébrica dos números

Nesta seção serão apresentados conceitos que serão indispensáveis para o desenvolvimento deste trabalho. Definiremos, mostraremos as propriedades e os principais resultados dos inteiros algébricos, traço, norma, norma de um ideal, discriminante, anéis de Dedekind e ideais fracionários.

1.3.1 Inteiros algébricos

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

Teorema 1.3.1 *([24]) Se A é um anel, $B \subset A$ um subanel e $x \in A$, então são equivalentes:*

1. *x é inteiro sobre B.*

2. *O anel $B[x]$ é um $B-$módulo finitamente gerado.*

3. *Existe um subanel C de A tal que C é um $B-$módulo finitamente gerado que contém B e x.*

Demontração: **1) $\Rightarrow$ 2)** Temos por hipótese que x é inteiro sobre B, ou seja, existem $b_0, \ldots, b_{n-1} \in B$, não todos nulos, tal que $x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 = 0$. Assim, podemos escrever $x^n = -(b_{n-1}x^{n-1} + \ldots + b_1x + b_0)$. Seja $M =< 1, x, \ldots, x^{n-1} >$ um A-módulo finitamente gerado, provemos que $B[x] = M$. Temos que $x^n \in M$ pois x^n é uma combinação de $1, x, \ldots, x^{n-1}$. Agora mostremos por indução que $x^j \in M$, $\forall j \in \mathbb{N}$. Temos que para $j \leq n$ o resultado se verifica. Suponhamos por hipótese de indução que $x^j \in M$, ou seja, $x^j = a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ para $a_0, a_1, \ldots, a_{n-1} \in B$. Mostremos então que $x^{j+1} \in M$. De fato:

$$\begin{aligned} x^{j+1} &= x^j \cdot x \\ &= (a_{n-1}x^{n-1} + \ldots + a_1x + a_0)x \\ &= a_{n-1}x^n + \ldots + a_1x^2 + a_0x \\ &= a_{n-1}(-b_{n-1}x^{n-1} - \ldots - a_1x - b_0) + \ldots + a_1x^2 + a_0x \\ &= a_{n-1}b_0 + (a_0 - a_{n-1}b_1)x + \ldots + (a_{n-2} - a_{n-1}b_{n-1})x^{n-1}. \end{aligned}$$

Logo, $x^{j+1} \in M$ e $B[x] \subset M$. Mas, $M \subset B[x]$. Portanto, $B[x] = M$ o que prova que $B[x]$ é uma $B-$módulo finitamente gerado. Para provar que **2) $\Rightarrow$ 3)** basta tomarmos $C = B[x]$ pois $B \subset B[x]$ e $x \in B[x]$. **3) $\Rightarrow$ 1)** Suponhamos que $C =< y_1, \ldots, y_n >$ seja um $B-$módulo finitamente gerado, ou seja, $C = By_1 + \ldots + By_n$. Por hipótese, temos que $x \in C$ então $xy_i \in C$, para todo $i = 1, \ldots, n$. Assim, temos que

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j,$$

para todo $i = 1, \ldots, n$, $a_{ij} \in A$, $1 \leq i,\ j \leq n$, é um sistema linear homogêneo nas variáveis $y_1, \ldots, y_n$, ou seja,

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})y_j = 0, \quad i = 1, \ldots, n$$

onde $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$. Seja $d = det(\delta_{ij}x - a_{ij})$. Pela regra de Cramer temos que $dy_i = 0$, $\forall i$. Consequentemente, $db = 0$, $\forall b \in B$; em particular para $b = 1$ temos $d = 0$. Mas, d é um polinômio mônico na indeterminada x, $d = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, onde $a_i \in A$. Portanto, x é inteiro sobre A. ∎

Proposição 1.3.1 *([24]) Sejam A um anel, $B \subset A$ um subanel e sejam $x_1, \ldots, x_n \in A$. Se $x_1, \ldots, x_n$ são inteiros sobre $B[x_1, \ldots, x_{i-1}]$, para $i = 2, \ldots, n$, então, $B[x_1, \ldots, x_n]$ é um $B-$módulo finitamente gerado.*

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

$$C[x_n] = \sum_{k=1}^{q} Cw_k = \sum_{k=1}^{q} \left(\sum j = 1^{p} Bc_j \right) w_k = \sum_{j,k} Bc_j w_k$$

onde $w_k \in C[x_n]$. Logo, $B[x_1, \ldots, x_n]$ é um $B-$módulo finitamente gerado por $\{c_j w_k\}$ com $1 \leq j \leq p,\ 1 \leq k \leq q$ e portanto $B[x_1, \ldots, x_n]$ é um $B-$módulo finitamente gerado. ∎

Corolário 1.3.1 *([24]) Sejam A um anel, $B \subset A$ um subanel e $x, y \in A$. Se x e y são inteiros sobre B então $x + y,\ x - y$ e xy são inteiros sobre B.*

Demonstração: Temos que $x+y,\ x-y$ e xy pertencem a $B[x, y]$ é um $B-$módulo finitamente gerado. Logo, pelo Teorema (1.3.1) temos que $x + y,\ x - y$ e xy são inteiros sobre B. ∎

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

Proposição 1.3.2 *([24]) Sejam $C \subseteq B \subseteq A$ anéis. Assim, A é inteiro sobre C se, e somente se, A é inteiro sobre B e B é inteiro sobre C.*

Demonstração: Suponhamos que A é inteiro sobre C. Se $\alpha \in A$, então existem $a_0, \ldots, a_{n-1} \in C$, não todos nulos, tal que

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

Como $C \subset B$, segue que $a_i \in B$, para $i = 0, 1, \ldots, n-1$, ou seja, α é inteiro sobre B. Portanto, A é inteiro sobre B. Agora, seja $\alpha \in B$. Como $B \subset A$, segue que $\alpha \in A$ e então por hipótese α é inteiro sobre C. Portanto, B é inteiro sobre C. Reciprocamente, seja $x \in A$. Por hipótese temos que A é inteiro sobre B, assim temos que existem $b_0, b_1, \ldots, b_{n-1} \in B$ tal que $x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0$. Se $R = C[b_0, b_1, \ldots, b_{n-1}]$, então x é inteiro sobre R. Mas, como B é inteiro sobre C segue que $b_i,\ i = 0, \ldots, n-1$, são inteiros sobre C. Pela Proposição (1.3.1) segue que $R[x] = C[b_0, \ldots, b_{n-1}, x]$ é um $C-$módulo finitamente gerado. E, pelo Teorema (1.3.1), segue que x é inteiro sobre C. Portanto, A é inteiro sobre C como queríamos. ∎

Definição 1.3.3 *Sejam $A \subset B$ anéis. O conjunto $\mathcal{O}_B = \{\alpha \in B : \alpha$ é inteiro sobre $A\}$ é chamado de* **anel dos inteiros** *de B em A. Se A é um domínio e $B = \mathbb{K}$ é o seu corpo de frações, dizemos que $\mathcal{O}_B$ é o anel dos inteiros de A em $\mathbb{K}$.*

Definição 1.3.4 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que A é um* **anel integralmente fechado** *em $\mathbb{K}$ se ele contém o anel dos inteiros de A.*

Proposição 1.3.3 *([24]) Todo domínio principal é integralmente fechado.*

Demonstração: Sejam A um domínio principal, $\mathbb{K}$ seu corpo de frações e $x \in \mathbb{K}$ um inteiro sobre A tal que $x = \frac{\alpha}{\beta},\ \alpha, \beta \in A$ e $\text{mdc}(\alpha, \beta) = 1$. Assim, existem $a_0, \ldots, a_{n-1} \in A$ tal que

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Substituindo x por $\frac{\alpha}{\beta}$,

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

ou seja,

$$\alpha^n + \beta(a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha\beta^{n-2} + a_0\beta^{n-1}).$$

Logo, β divide α^n e como $\text{mdc}(\alpha, \beta) = 1$ segue que β divide α, isto é, $\alpha = c\beta$ para algum $c \in A$. Assim, β é uma unidade de A e $\frac{\alpha}{\beta} \in A$. Portanto A é integralmente fechado. ∎

Até agora, vimos os elementos inteiros sobre um anel qualquer. A partir de agora veremos estes elementos sobre um anel específico, o anel dos inteiros $\mathbb{Z}$.

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

Observação 1.3.1 *Como na Definição (1.3.3), se $\mathbb{K}$ é um corpo de números, podemos definir o anel dos inteiros algébricos de $\mathbb{K}$ como o conjunto formado pelos inteiros algébricos de $\mathbb{K}$ e denotamos por $\mathcal{O}_{\mathbb{K}}$.*

Teorema 1.3.2 *([24]) Se α é um número complexo que satisfaz um polinômio mônico cujos coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Demonstração: Seja α raiz de $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, onde a_i é inteiro algébrico para $i = 0, 1, \cdots, n-1$. Temos que α é inteiro sobre $\mathbb{Z}[a_0, \cdots, a_{n-1}]$. Mas, pela Proposição (1.3.1) temos que $\mathbb{Z}[a_0, \cdots, a_{n-1}]$ é um $\mathbb{Z}$-módulo finitamente gerado. Desta forma, novamente pela Proposição (1.3.1) temos que $\mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ é um $\mathbb{Z}$-módulo finitamente gerado. Pelo Teorema (1.3.1), segue que α é inteiro algébrico. ∎

Corolário 1.3.2 *([24]) Se $\mathbb{K}$ é um corpo de números, então $K = \mathbb{Q}(\alpha)$ para algum inteiro algébrico α.* ∎

Proposição 1.3.4 *([24]) Se A é um domínio, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}$ uma extensão finita de $\mathbb{L}$ de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ sobre A, então $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado.*

Demonstração: Seja $\mathbb{M}$ o corpo das frações de $\mathcal{O}_{\mathbb{K}}$. Temos que $\mathbb{L} \subset \mathbb{M} \subset \mathbb{K}$. Seja $x \in \mathbb{M}$ tal que x é inteiro sobre $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre A segue, da demonstração da Proposição (1.3.2), que x é inteiro sobre A. Assim, se $\mathcal{O}_{\mathbb{M}}$ é o conjunto dos elementos de $\mathbb{M}$ que são inteiros sobre $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{O}_{\mathbb{M}} \subset \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{M}}$, temos que $\mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{M}}$, o que implica que $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado. ∎

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

Observação 1.3.2 *Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral $\mathcal{O}_{\mathbb{K}}$ então todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, \cdots, n$.*

1.3.2 Traço e norma

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

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

Observação 1.3.3 *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão de grau n. Se $\alpha, \beta \in \mathbb{K}$ e $x \in \mathbb{L}$, então valem as seguintes propriedades:*

1. $Tr_{\mathbb{K}/\mathbb{L}}(\alpha + \beta) = Tr_{\mathbb{K}/\mathbb{L}}(\alpha) + Tr_{\mathbb{K}/\mathbb{L}}(\beta)$
2. $Tr_{\mathbb{K}/\mathbb{L}}(x\alpha) = xTr_{\mathbb{K}/\mathbb{L}}(\alpha)$
3. $Tr_{\mathbb{K}/\mathbb{L}}(x) = nx$
4. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha\beta) = \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\beta)$
5. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(x\alpha) = x^n\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)$
6. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(x) = x^n$.

Se tivermos $\mathbb{M} \subseteq \mathbb{L} \subseteq \mathbb{K}$ extensões finitas e $\alpha \in \mathbb{K}$ temos ainda que:

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

E, se tivermos $\mathbb{M} \subseteq \mathbb{L} \subseteq \mathbb{K}$ extensões finitas e $\alpha \in \mathbb{L}$ temos também que:

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

Observação 1.3.4 *Denotaremos o traço e a norma simplesmente por $Tr(\alpha)$ e $\mathcal{N}(\alpha)$ quando não houver dúvida quanto a extensão que contém o elemento α.*

Proposição 1.3.5 *([24]) Sejam $\mathbb{L}$ um corpo de característica zero ou um corpo finito, $\mathbb{K}$ um extensão algébrica de grau n de $\mathbb{L}$ e $\alpha \in \mathbb{K}$. Se $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{L}$, então $Tr(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, $\mathcal{N}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$ e $p(x) = (x-\alpha_1)\ldots(x-\alpha_n)$, onde $p(x)$ é um polinômio mônico com coeficientes em $\mathbb{K}$ chamado de polinômio característico.*

Demonstração: Primeiro faremos a demonstração para o caso em que α é um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{L}$, ou seja, $\mathbb{K} = \mathbb{L}[\alpha]$. Se $f(x) = x^n + \cdots + a_1x + a_0$ é o polinômio minimal de α sobre $\mathbb{L}$, então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Temos que a matriz do endomorfismo σ_α com respeito a esta base é dada por

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

Assim, $\det(xI - M)$ é o determinante da matriz

$$xI_n - M = \begin{bmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix}. \tag{1.3.1}$$

Calculando o determinante da matriz (1.3.1), obtemos o polinômio característico em α, que é igual a $f(x)$, o polinômio minimal de α. Sabemos que,

$$p(x) = \det(xI_n - M) = x^n - (Tr(\alpha))x^{n-1} + \cdots + (-1)^n \det(M).$$

Como α é primitivo, segue que

$$p(x) = f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = x^n - \left(\sum_{i=1}^{n}\alpha_i\right)x^{n-1} + \cdots + (-1)^n\left(\prod_{i=1}^{n}\alpha_i\right).$$

Logo, $Tr(\alpha) = \sum_{i=1}^{n}\alpha_i$ e $N(\alpha) = \prod_{i=1}^{n}\alpha_i$. Para o caso geral, seja $r = [\mathbb{K} : \mathbb{L}[\alpha]]$. É suficiente mostrar que o polinômio característico $p(x)$ de α, com relação a $\mathbb{K}$ sobre $\mathbb{L}$, é igual a r-ésima potência do polinômio minimal de α sobre $\mathbb{L}$. Seja $\{y_1, \cdots, y_q\}$ uma base de $\mathbb{L}[\alpha]$ sobre $\mathbb{L}$ e seja $\{z_1, \ldots, z_r\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}[\alpha]$ com $n = qr$. Seja $M = (a_{ih})$ a matriz do endomorfismo de $\mathbb{L}[\alpha]$ sobre $\mathbb{L}$ com relação a base $\{y_1, \ldots, y_q\}$. Assim, $\alpha y_i = \sum_{h=1}^{q}(a_{ih})y_h$ e $\alpha(y_i z_j) = \left(\sum_{h=1}^{q} a_{ih}y_h\right)z_j = \sum_{h=1}^{q} a_{ih}(y_h z_j)$. Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11}y_1z_1 + a_{21}y_2z_1 + \cdots + a_{q1}y_qz_1 \\ \alpha y_2 z_1 = a_{12}y_1z_1 + a_{22}y_2z_1 + \cdots + a_{q2}y_qz_1 \\ \qquad\qquad \vdots \\ \alpha y_q z_1 = a_{1q}y_1z_1 + a_{2q}y_2z_1 + \cdots + a_{qq}y_qz_1. \end{cases}$$

Ordenamos a base $\{y_i z_j\}$ de $\mathbb{K}$ sobre $\mathbb{L}$, de modo que a matriz do endomorfismo seja da seguinte forma

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

isto é, M repete r-vezes na diagonal como blocos na matriz M_1. A matriz $xI_n - M_1$, consiste de r-blocos diagonais, cada um tem a forma $xI_q - M$, e consequentemente, $\det(xI_n - M_1) = \det(xI_q - M)^r$. Assim, $p(x) = det(xI_n - M_1)$ e $det(xI_q - M)$ é o polinômio minimal de α sobre $\mathbb{L}$, de acordo com a primeira parte da demonstração. ∎

Proposição 1.3.6 *([24]) Sejam A um domínio, $\mathbb{L}$ seu corpo de frações (de característica zero) e $\mathbb{K}$ uma extensão finita de $\mathbb{L}$. Se α é um elemento de $\mathbb{K}$ inteiro sobre A, então os coeficientes do polinômio característico $p(x)$ de α relativo a $\mathbb{K}$ e $\mathbb{L}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$, são inteiros sobre A.*

Demonstração: Pela Proposição (1.3.5), temos que $p(x) = (x-\alpha_1)\ldots(x-\alpha_n)$. Os coeficientes de $p(x)$ são somas de produtos de $\alpha_i's$, a menos de sinal. Assim, é suficiente provar que

cada α_i é inteiro sobre A. Mas cada α_i é um conjugado de α sobre $\mathbb{L}$, isto é, existe um isomorfismo $\sigma_i : \mathbb{L}[\alpha] \to \mathbb{L}[\alpha_i]$ tal que $\sigma_i(\alpha) = \alpha_i$. Assim, aplicando σ_i na equação de dependêcia integral de α sobre A, obtemos uma equação de dependêcia integral de α_i sobre A. ∎

Corolário 1.3.3 *([24]) Se A é um anel integralmente fechado então os coeficientes do polinômio característico de $\alpha \in \mathbb{K}$, em particular, $Tr(\alpha)$ e $\mathcal{N}(\alpha)$ são elementos de A.*

Demonstração: Por definição esses coeficientes são elementos do corpos de frações $\mathbb{L}$ de A. Pela Proposição (1.3.6), temos que são inteiros sobre A e como A é integralmente fechado, segue que são elementos de A. ∎

Lema 1.3.1 *([10]) Sejam A um anel integralmente fechado, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos $\mathbb{K}$. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ onde $\det(Tr(\alpha_i\alpha_j)) \neq 0$. Seja $\alpha \in \mathbb{K}$. Se $Tr(\alpha\beta) = 0$ para todo $\beta \in \mathbb{K}$, então $\alpha = 0$.*

Demonstração: Por hipótese $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, se α é um elemento de $\mathbb{K}$ então existem $a_1, \cdots, a_n \in \mathbb{Q}$ tal que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Logo, é suficiente mostrar que se $Tr(\alpha\alpha_j) = 0$, para cada $j = 1, \cdots, n$, então $\alpha = 0$. Assim, para cada $j = 1, \cdots, n$, temos que

$$\begin{aligned} 0 &= Tr(\alpha\alpha_j) = Tr(a_1\alpha_1\alpha_j + \cdots + a_n\alpha_n\alpha_j) \\ &= Tr(a_1\alpha_1\alpha_j) + \cdots + Tr(a_n\alpha_n\alpha_j) \\ &= a_1Tr(\alpha_1\alpha_j) + a_2Tr(\alpha_2\alpha_j) + \cdots + a_nTr(\alpha_n\alpha_j). \end{aligned}$$

Na forma matricial, temos que

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

Como $\det(Tr(\alpha_i\alpha_j)) \neq 0$ segue que $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ∎

Lema 1.3.2 *([10]) A aplicação $\rho : \mathbb{L} \longrightarrow Hom_{\mathbb{Q}}(\mathbb{K}, \mathbb{Q})$ definida por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = Tr(\alpha\beta)$, com $\beta \in \mathbb{K}$, é um isomorfismo.*

Demonstração: Se $\alpha_1, \alpha_2 \in \mathbb{K}$, então

$$\rho(\alpha_1 + \alpha_2)(\beta) = S_{\alpha_1+\alpha_2}(\beta) = Tr((\alpha_1 + \alpha_2)\beta)$$

$$\begin{aligned} &= Tr(\alpha_1\beta) + Tr(\alpha_2\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) \\ &= (\rho(\alpha_1) + \rho(\alpha_2))(\beta) \end{aligned}$$

e

$$\begin{aligned} \rho(a\alpha)(\beta) &= S_{a\alpha}(\beta) = Tr(a\alpha\beta) = aTr(\alpha\beta) \\ &= aS_\alpha(\beta) = a\rho(\alpha)(\beta), \end{aligned}$$

para todo $\beta \in \mathbb{K}$. Logo, ρ é um homomorfismo. Agora, se $\alpha \in \mathbb{K}$ é tal que $\rho(\alpha) = 0$, então, $\rho(\alpha)(\beta)$=$S_\alpha(\beta) = Tr(\alpha\beta) = 0$, para todo $\beta \in \mathbb{K}$. Assim, pelo Lema (1.3.1), segue que $\alpha = 0$ e então ρ é injetora. Finalmente, como $dim_{\mathbb{Q}}\mathbb{K} = dim_{\mathbb{Q}}(Hom_{\mathbb{Q}}(\mathbb{K}, \mathbb{Q}))$ segue que ρ é sobrejetora. Portanto, ρ é um isomorfismo. ∎

Teorema 1.3.3 *([10]) Se A é um anel integralmente fechado, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros algébricos $\mathbb{K}$, então $\mathcal{O}_\mathbb{K}$ é um A-submódulo livre de posto n.*

Demonstração: Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Como toda extensão finita é algébrica, segue que todos os α_i são algébricos sobre $\mathbb{L}$, ou seja, existem $a_{ij} \in A$, $i = 1, \cdots, n$, não todos nulos, tal que

$$a_{in}\alpha_i^n + a_{i(n-1)}\alpha_i^{n-1} + \cdots + a_{i0} = 0.$$

Suponhamos que $a_{in} \neq 0$. Multiplicando a equação acima por a_{in}^{n-1}, temos que $a_{in}\alpha_i$ é inteiro sobre A, pois

$$a_{in}^{n-1}(a_{in}\alpha_i^n + \cdots + a_{i0}) = (a_{in}\alpha_i)^n + a_{i(n-1)}(a_{in}\alpha_i)^{n-1} + \cdots + a_{in}^{n-1}a_{i0} = 0.$$

Tomando $a_{in}\alpha_i = z_i \in \mathcal{O}_\mathbb{K}$, para cada $i = 1, \cdots, n$. Mostraremos que $\{z_1, \cdots, z_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Para isso, suponhamos que $b_1z_1 + \cdots + b_nz_n = 0$, onde $b_i \in A$, para $i = 1, \cdots, n$. Assim, $b_1a_{1n}\alpha_1 + \cdots + b_na_{nn}\alpha_n = 0$. Mas, como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$, segue que $b_ia_{in} = 0$ e portanto $b_i = 0$ para $i = 1, \cdots, n$. Portanto, $\{z_1, \cdots, z_n\}$ é linearmente independente e como possui n elementos segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Lema (1.3.2) existe uma base dual $\{y_1, \cdots, y_n\}$ tal que

$$\rho(z_i)(y_j) = S_{z_i}(y_j) = Tr(z_iy_j) = \delta_{ij} \text{ para } i, j = 1, \cdots, n.$$

Agora, se $\alpha \in \mathcal{O}_\mathbb{L}$ então $\alpha z_i \in \mathcal{O}_\mathbb{L}$, para $i = 1, \cdots, n$. Pelo Corolário (1.3.3) segue que $Tr(\alpha z_i) \in A$, para $i = 1, \cdots, n$. Como $\alpha = c_1y_1 + \cdots + c_ny_n$, com $c_i \in \mathbb{K}$, para $i = 1, \cdots, n$, segue que $Tr(\alpha z_i) = c_i \in A$, para $i = 1, \cdots, n$. Portanto, $\mathcal{O}_\mathbb{K}$ é um submódulo de um A-módulo livre gerado por $\{z_1, \cdots, z_n\}$. ∎

Proposição 1.3.7 *([24]) Seja A um anel noetheriano e integralmente fechado. Se $\mathbb{L}$ é o corpo de frações de A, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de A em $\mathbb{K}$, então $\mathcal{O}_{\mathbb{K}}$ é um A-módulo finitamente gerado e $\mathcal{O}_{\mathbb{K}}$ é um anel noetheriano.*

Demonstração: Pelo Teorema (1.3.3), temos que $\mathcal{O}_{\mathbb{K}}$ é um submódulo de um A-módulo livre de posto n. Pelo Corolário (1.1.2), temos que $\mathcal{O}_{\mathbb{K}}$ é um A-módulo noetheriano e portanto finitamente gerado. Como os ideais de $\mathcal{O}_{\mathbb{K}}$ são A-submódulos de $\mathcal{O}_{\mathbb{K}}$, segue que satisfazem a condição de maximilidade da Definição (1.1.22). Portanto, $\mathcal{O}_{\mathbb{K}}$ é um anel noetheriano. ∎

1.3.3 Norma de um ideal

Definição 1.3.8 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. A* **norma do ideal $\mathfrak{a}$** *é definida como sendo a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$, isto é,*

$$\mathcal{N}(\mathfrak{a}) = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}.$$

Teorema 1.3.4 *([24]) Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Se $\mathfrak{a} = \langle\alpha\rangle$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ então $\mathcal{N}(\mathfrak{a}) = |\mathcal{N}(\alpha)|$.*

Demonstração: Como $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha \neq 0$, segue, pelo Corolário (1.3.3), que $\mathcal{N}(\alpha) \in \mathbb{Z}$. Pelo Teorema (1.3.3), temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\varphi : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\varphi(a) = a\alpha$, onde $\alpha \in \mathcal{O}_{\mathbb{K}}$, é um isomorfismo, segue que $\mathcal{O}_{\mathbb{K}}\alpha$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\mathbb{Z}$ é um anel principal e $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre segue, pelo Teorema (1.1.3), que existe uma $\mathbb{Z}$-base $\{e_1, \ldots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros $c_1, \ldots, c_n$ tal que $\{c_1e_1, \ldots, c_ne_n\}$ é $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}\alpha$. A aplicação $\psi : \mathcal{O}_{\mathbb{K}} \longrightarrow \dfrac{\mathbb{Z}}{c_1\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{c_n\mathbb{Z}}$, definida por $\psi(\sum_{i=1}^{n} a_ie_i) = (\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n})$, é um homomorfismo sobrejetor e $Ker(\psi) = \mathcal{O}_{\mathbb{K}}\alpha$, pois $a \in Ker(\psi)$ se, e somente se, $\psi(a) = \bar{0}$ se, e somente se, $\bar{a_i} = \bar{0}$, para $i = 1, \ldots, n$, se, e somente se, $a_i \in c_i\mathbb{Z}$, se, e somente se, c_i divide a_i se, e somente se, $a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i \in \mathcal{O}_{\mathbb{K}}\alpha$. Assim,

$$\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \simeq \frac{\mathbb{Z}}{c_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{c_n\mathbb{Z}}.$$

Logo $\#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = c_1c_2\ldots c_n$. Seja a aplicação $\mathbb{Z}$-linear $\mu : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\mu(e_i) = c_ie_i$, para $i = 1, \ldots, n$. Logo, $\mu(e_1) = c_1e_1 + 0e_2 + \cdots + 0e_n, \cdots, \mu(e_n) = 0e_1 + \cdots + c_ne_n$ e $\det(\mu) = c_1c_2\ldots c_n$. Por outro lado, temos que $B = \{c_1e_1, \ldots, c_ne_n\}$ e $C = \{\alpha e_1, \ldots, \alpha e_n\}$ são $\mathbb{Z}$-bases de $\mathcal{O}_{\mathbb{K}}\alpha$. Portanto existe um automorfismo $\varphi : \mathcal{O}_{\mathbb{K}}\alpha \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ tal que $\varphi(c_ie_i) = \alpha e_i$, para $i = 1, \ldots, n$. Como a matriz mudança de base é inversível, segue que $\det(\varphi)$ é inversível em $\mathbb{Z}$, isto é, $\det(\varphi) = \pm 1$. Também, $(\varphi\circ\mu)(e_i) = \varphi(\mu(e_i)) = \varphi(c_ie_i) = \alpha e_i$, para $i = 1, \ldots, n$.

Assim, $(\varphi\circ\mu)(a) = \alpha a$, para todo $a \in \mathcal{O}_{\mathbb{K}}$. Finalmente, pela Proposição (1.3.5), temos que $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \det(\varphi\circ\mu) = \det(\varphi)\det(\mu) = \pm 1 c_1 c_2 \dots c_n = \pm \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$. Portanto, $|\mathcal{N}(\alpha)| = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = \mathcal{N}(\mathfrak{a})$. ■

Proposição 1.3.8 *([24]) A norma $\mathcal{N}(\mathfrak{a})$ é finita.*

Demonstração: Se $\alpha \in \mathfrak{a}$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathfrak{a}$. Consideremos a aplicação $\varphi : \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \longrightarrow \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)$ dada por $\varphi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + \mathfrak{a}$. Temos que φ é um homomorfismo sobrejetor e $Ker(\varphi) = \left(\frac{\mathfrak{a}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$. De fato, $x + \mathcal{O}_{\mathbb{K}}\alpha \in Ker(\varphi)$ se, e somente se, $\varphi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + \mathfrak{a} = \bar{0}$ se, e somente se, $x \in \mathfrak{a}$. Desta forma, pelo Teorema (1.1.2), segue que

$$\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \Big/ \left(\frac{\mathfrak{a}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right).$$

Assim, segue que

$$\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) \# \left(\frac{\mathfrak{a}}{\mathcal{O}_{\mathbb{K}}\alpha}\right).$$

Pelo Teorema (1.3.4), temos que $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$ é finito. Portanto, $\mathcal{N}(\mathfrak{a}) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)$ é finito. ■

Lema 1.3.3 *([24]) Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.* ■

Proposição 1.3.9 *([24]) Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então:*

1. *$\mathcal{N}(\mathfrak{a}) = 1$ se, e somente se, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$.*
2. *Se $\mathcal{N}(\mathfrak{a})$ for um número primo então o ideal $\mathfrak{a}$ é primo.*

Demonstração: 1) Temos que $\mathcal{N}(\mathfrak{a}) = 1$ se, e somente se, $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) = 1$ se, e somente se, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$.
2) Suponhamos que $\mathfrak{a}$ não seja um ideal primo. Assim, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$ ou $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2$, onde $\mathfrak{q}_1, \mathfrak{q}_2$ são ideais não nulos distintos de $\mathcal{O}_{\mathbb{K}}$. Se $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$, pelo item (1), temos que $\mathcal{N}(\mathfrak{a}) = 1$, o que é contra a hipótese. Se $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2$ temos, pelo Lema (1.3.3), que $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{q}_1)\mathcal{N}(\mathfrak{q}_2)$ e, como por hipótese, $\mathcal{N}(\mathfrak{a}) = p$, p primo, segue que $\mathcal{N}(\mathfrak{q}_1) = 1$ e $\mathcal{N}(\mathfrak{q}_2) = p$ ou $\mathcal{N}(\mathfrak{q}_1) = p$ e $\mathcal{N}(\mathfrak{q}_2) = 1$. Logo, $\mathfrak{q}_1 = \mathcal{O}_{\mathbb{K}}$ ou $\mathfrak{q}_2 = \mathcal{O}_{\mathbb{K}}$, o que é contra a hipótese. Portanto, $\mathfrak{a}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$. ■

Proposição 1.3.10 *([27]) Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Se $\{w_1, \cdots, w_n\}$ for uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e $\{e_1w_1, \cdots, e_nw_n\}$ for uma $\mathbb{Z}$-base de $\mathfrak{a}$, onde $e_1, \cdots, e_n$ são inteiros não nulos, então $\mathcal{N}(\mathfrak{a}) = |e_1 \cdots e_n|$.*

Demonstração: Consideremos a aplicação:

$$\psi : \mathcal{O}_{\mathbb{K}} \longrightarrow \frac{\mathbb{Z}}{e_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{e_n\mathbb{Z}}$$

$$\sum_{i=1}^{n} a_i w_i \longmapsto (a_1 + e_1\mathbb{Z}, \cdots, a_n + e_n\mathbb{Z}).$$

Temos que ψ é um homomorfismo sobrejetor. Agora, $Ker(\psi) = \mathfrak{a}$. De fato, se $x = \sum_{i=1}^{n} a_i w_i \in Ker(\psi)$, então $\psi(x) = (a_1 + e_1\mathbb{Z}, \cdots, a_n + e_n\mathbb{Z}) = (0 + e_1\mathbb{Z}, \cdots, 0 + e_n\mathbb{Z})$. Logo, segue que $a_i \in e_i\mathbb{Z}$, para todo $i = 1, \cdots, n$ e, assim, existem $b_1, \cdots, b_n \in \mathbb{Z}$ tal que $a_i = e_i b_i$, para todo i, o que implica que $x = \sum_{i=1}^{n} a_i w_i = x = \sum_{i=1}^{n} b_i e_i w_i \in I$. Portanto, $Ker(\psi) \subset \mathfrak{a}$. Analogamente, se $x \in \mathfrak{a}$, então $x = \sum_{i=1}^{n} b_i e_i w_i$; $b_i \in \mathbb{Z}$. Desta forma, $\psi(x) = (b_1 e_1 + e_1\mathbb{Z}, \cdots, b_n e_n + e_n\mathbb{Z}) = (0 + e_1\mathbb{Z}, \cdots, 0 + e_n\mathbb{Z})$, o que mostra que $\mathfrak{a} \subset Ker(\psi)$. Pelo Teorema (1.1.2), temos que $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}} \simeq \frac{\mathbb{Z}}{e_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{e_n\mathbb{Z}}$. Portanto, $\mathcal{N}(\mathfrak{a}) = |\mathcal{O}_{\mathbb{K}}/\mathfrak{a}| = |e_1 \cdots e_n|$. ∎

Proposição 1.3.11 *([27]) Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\phi : \mathbb{K} \to \mathbb{K}$ a conjugação complexa. Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ então $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\phi(\mathfrak{a}))$.*

Demonstração: Consideremos a aplicação:

$$\psi : \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) \longrightarrow \left(\frac{\mathcal{O}_{\mathbb{K}}}{\phi(\mathfrak{a})}\right)$$

$$x + \mathfrak{a} \longmapsto \phi(x) + \phi(\mathfrak{a}).$$

Temos que ψ está bem definida. De fato, primeiro notemos que se $x \in \mathcal{O}_{\mathbb{K}}$, então $\phi(x) \in \mathcal{O}_{\mathbb{K}}$. Agora, se $x+\mathfrak{a} = y+\mathfrak{a}$, então $x-y \in \mathfrak{a}$. Logo, $\phi(x-y) \in \phi(\mathfrak{a})$. Assim, $\phi(x)+\phi(\mathfrak{a}) = \phi(y)+\phi(\mathfrak{a})$. Além disso, ψ é um homomorfismo sobrejetor, pois se $\phi(x) + \phi(\mathfrak{a}) \in \mathcal{O}_{\mathbb{K}}/\phi(\mathfrak{a})$, então existe $x = \phi(\phi(x)) \in \mathcal{O}_{\mathbb{K}}$ tal que $\psi(x + I) = \phi(x) + \phi(\mathfrak{a})$. Notemos também que ψ é injetora, pois se $\phi(x) + \phi(\mathfrak{a}) = \phi(y) + \phi(\mathfrak{a})$, então $\phi(x) - \phi(y) \in \phi(\mathfrak{a})$ e, assim, $x - y \in \mathfrak{a}$. Logo, $x + \mathfrak{a} = y + \mathfrak{a}$. Portanto, ψ é um isomorfismo. Desta forma, temos que $\mathcal{N}(\mathfrak{a}) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\phi(\mathfrak{a})}\right) = \mathcal{N}(\phi(\mathfrak{a}))$. ∎

1.3.4 Discriminante

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

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

Proposição 1.3.12 *([24]) Sejam $B \subseteq A$ anéis. Se $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\} \in A^n$ são tais que $\beta_i = \sum_{j=1}^n a_{ij}\alpha_j$ com $a_{ij} \in B$, então*

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

Demonstração: Consideremos $\beta_p = \sum_{i=1}^n a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^n a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in B$ e $1 \leq p, q \leq n$. Assim,

$$\beta_p\beta_q = \sum_{i=1}^n a_{pi}\alpha_i \sum_{j=1}^n a_{qj}\alpha_j = \sum_{1\leq i,j\leq n} a_{pi}a_{qj}\alpha_i\alpha_j,$$

e então

$$Tr_{A/B}(\beta_p\beta_q) = Tr_{A/B}(\sum_{1\leq i,j\leq n} a_{pi}a_{qj}\alpha_i\alpha_j) = \sum_{1\leq i,j\leq n} a_{pi}a_{qj}Tr_{A/B}(\alpha_i\alpha_j).$$

Na forma matricial, teremos

$$(Tr_{A/B}(\beta_p\beta_q))_{n,p=1}^n = (a_{pi})_{p,i=1}^n (Tr_{A/B}(\alpha_i\alpha_j))_{i,j=1}^n ((a_{qj})_{q,j=1}^n)^t.$$

Aplicando o determinante em ambos os lados segue que

$$\begin{aligned}
\mathcal{D}_{A/B}(\beta_1, \ldots, \beta_n) &= \det(Tr_{A/B}(\beta_p\beta_q)) = \det((a_{pi})(Tr_{A/B}(\alpha_i\alpha_j))(a_{qj})^t) \\
&= \det(a_{pi}) \det(Tr_{A/B}(\alpha_i\alpha_j)) \det((a_{qj})^t) = \det(a_{pi}) \det((a_{qj})^t) \det(Tr_{A/B}(\alpha_i\alpha_j)) \\
&= \det(a_{ij})^2 \mathcal{D}_{A/B}(\alpha_1, \ldots, \alpha_n),
\end{aligned}$$

como queríamos provar. ∎

Observação 1.3.5 *Sejam $B \subseteq A$ anéis. Se $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ são duas bases de A sobre B tais que $\beta_j = \sum_{j=1}^n a_{ij}\alpha_i$ e $\alpha_j = \sum_{j=1}^n b_{ij}\beta_i$, onde $a_{ij}, b_{ij} \in B$, temos pela Proposição (1.3.12) que o discriminante dessas bases são associados em B ou ambas possuem determinantes nulos, ou seja, se (a_{ij}) é a matriz mudança de base $\{\alpha_1, \ldots, \alpha_n\}$ para $\{\beta_1, \ldots, \beta_n\}$, então a matriz inversa $(a_{ij})^{-1}$ tem entradas em A. Portanto,* $\det(a_{ij})$ *e* $\det(a_{ij})^{-1}$ *são unidades em B.*

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

Observação 1.3.6 *Note que o ideal da Definição (1.3.10) independe da base escolhida pois pela Observação (1.3.5) o determinante de quaisquer duas bases são associados e então estes geram o mesmo ideal.*

Lema 1.3.4 *([24])***(Lema de Dedekind)** *Sejam G um grupo e $\mathbb{K}$ um corpo. Se $\sigma_1, \ldots, \sigma_n$ são homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então $\{\sigma_1, \ldots, \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.* ∎

Proposição 1.3.13 *([24]) Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os monomorfismos distintos de $\mathbb{K}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{L}$. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$ então*

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

Demonstração: Por definição, temos que $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n) = \det(Tr(\alpha_i\alpha_j))$. Como o traço $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que

$$\begin{aligned}
\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \ldots, \alpha_n) &= \det(Tr(\alpha_i\alpha_j)) = \det(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) \\
&= \det(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)) = \det(\sigma_k(\alpha_i))\det(\sigma_k(\alpha_j)) \\
&= (\det(\sigma_i(\alpha_j))^2.
\end{aligned}$$

Resta mostrar que $\det(\sigma_i(\alpha_j)) \neq 0$. Suponhamos por absurdo que $\det(\sigma_i(\alpha_j)) = 0$, então as colunas da matriz $(\sigma_k(\alpha_j))_{j,k=1}^n$ são linearmente dependentes. Assim, existem $a_1, \ldots, a_n \in \mathbb{F}$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$ para todo $j = 1, \cdots, n$. Assim, por linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{K}$, o que contradiz o Lema de Dedekind. Portanto, $\det(\sigma_i(\alpha_j))^2 \neq 0$. ∎

Proposição 1.3.14 *([24]) Se $\mathbb{K}/\mathbb{L}$ é uma extensão finita de grau n tal que $\mathbb{K} = \mathbb{L}(\alpha)$ e $f(x)$ o polinômio minimal de α sobre $\mathbb{L}$, então,*

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

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

Demonstração: Se $\alpha_1, \cdots, \alpha_n$ são as raízes de $f(x)$ em alguma extensão de $\mathbb{K}$, então são conjugados de α. Pelo Lema (1.3.13) temos que $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(1, \alpha, \cdots, \alpha^{n-1}) = (\det(\sigma_i(\alpha_j)))^2 = \det(\alpha_j^i)^2$, com $i = 1, \cdots, n$ e $j = 0, \cdots, n-1$. Como $\det(\alpha_j^i)$ é um determinante de Vandermonde segue que

$$\det(\alpha_j^i)^2 = \left[\prod_{1 \leq k < i \leq n} (\alpha_i - \alpha_k)\right]^2$$

$$
\begin{aligned}
&= \prod_{1\leq k<i\leq n}[(\alpha_i-\alpha_k)(\alpha_i-\alpha_k)] \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{1\leq k<i\leq n,\, i\neq k}(\alpha_i-\alpha_k) \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}\left[\prod_{k=1,\, k\neq i}^{n}(\alpha_i-\alpha_k)\right] \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}f'(\alpha_i) \\
&= (-1)^{\frac{1}{2}n(n-1)}\mathcal{N}(f'(\alpha)),
\end{aligned}
$$

como queríamos provar. ∎

Teorema 1.3.5 *([27]) O discriminante de qualquer base de $\mathbb{K}=\mathbb{Q}(\theta)$ é racional e não nulo. Se todos os $\mathbb{K}$-monomorfismos de θ são reais, então o discriminante de qualquer base é positivo.*

Demonstração: Seja $\{1,\alpha,\ldots,\alpha^{n-1}\}$ uma base de $\mathbb{K}=\mathbb{Q}(\theta)$. Se os conjugados de α são $\theta_1,\ldots,\theta_n$, então

$$
\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\alpha) & \ldots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \ldots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \ldots & \sigma_n(\alpha^{n-1}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \theta_1 & \ldots & \theta_1^n \\ 1 & \theta_2 & \ldots & \theta_2^n \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \ldots & \theta_n^n \end{vmatrix}^2 = (det\theta_i^j)^2.
$$

Um determinante da forma $\Delta = det(t_i^j)$ é chamado de determinante de *Vandermonde*, e é dado por $\Delta=\prod_{1\leq i\leq j\leq n}(t_i-t_j)$. Para verificar isto, vamos pensar em tudo como pertencente a $\mathbb{Q}[t_1,\ldots,t_n]$. Então para $t_i=t_j$ o determinante tem duas linhas (ou colunas) múltiplas, logo o determinante tem valor zero. Temos que Δ é divisível por cada (t_i-t_j). Para evitar que se repita algum fator, tomemos $i<j$. Comparando os graus vemos que Δ não tem outros fatores não constantes, comparando os coeficientes de $t_1t_2^2\ldots t_n^n$. Logo

$$
\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1}) = [\prod(\theta_i-\theta_j)]^2.
$$

Logo, $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1})$ é racional desde que θ_i sejam distintos e $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1})\neq 0$. Agora, se $\{\beta_1,\ldots,\beta_n\}$ uma outra base de $\mathbb{K}$, então,

$$
\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1,\ldots,\beta_n) = (detc_{ik})^2\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1}],
$$

para $c_{ik}\in\mathbb{Q}$, com $det(c_{ik})\neq 0$, tal que $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1,\ldots,\beta_n)\neq 0$ e $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1,\ldots,\beta_n)\in\mathbb{Q}$. Logo, se todos os θ_i's são reais, então $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1})$ é um número real positivo. ∎

Lema 1.3.5 *([27]) Se G um grupo abeliano livre de posto n, $\{\alpha_1, \cdots, \alpha_n\}$ uma base de G e (a_{ij}) uma matriz $n \times n$ com entradas inteiras, então $\{\beta_1, \cdots, \beta_n\}$ tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, forma uma base de G se e somente se (a_{ij}) é uma matriz unimodular.* ∎

Teorema 1.3.6 *([27]) Sejam $\mathbb{K}$ um corpo de números de grau n, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\{\alpha_1, \cdots, \alpha_n\} \in \mathcal{O}_{\mathbb{K}}$ uma $\mathbb{Q}$-base de $\mathbb{K}$. Se $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$ é livre de quadrados então $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral.*

Demonstração: Se $\{\beta_1, \cdots, \beta_n\}$ é uma base integral, então existem inteiros $a_{ij} \in \mathbb{Z}$ tal que $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$ e $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = \det(a_{ij})^2 \mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \cdots, \beta_n)$. Mas, para termos o lado esquerdo da igualdade livre de quadrado devemos ter $\det(a_{ij}) = \pm 1$, ou seja, a matriz (a_{ij}) é unimodular. Assim, pelo Lema (1.3.5), segue que $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Z}$ de $\mathcal{O}_{\mathbb{K}}$, ou seja, uma base integral de $\mathbb{K}$. ∎

1.3.5 Anéis de Dedekind

Definição 1.3.11 *Dizemos que um anel A é um* **anel de Dedekind** *se satisfaz as seguintes condições:*

1. *A é integralmente fechado.*
2. *A é noetheriano.*
3. *Todo ideal primo não nulo de A é maximal.*

Teorema 1.3.7 *([24]) Se A é um anel de Dedekind, $\mathbb{L}$ seu corpo de frações, $\mathbb{L} \subseteq \mathbb{K}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre A. Então $\mathcal{O}_{\mathbb{K}}$ é um anel Dedekind.*

Demonstração: Pelas Prposições (1.3.4) e (1.3.7), temos que $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado e noetheriano, respectivamente. Assim, falta mostrar que todo ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ é maximal. Seja $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ um ideal primo não nulo. Como $A \subset \mathcal{O}_{\mathbb{K}}$ segue pela Proposição (1.1.4) que $\mathfrak{p} \cap A$ é um ideal primo de A. Vamos mostrar que $\mathfrak{p} \cap A$ é não nulo. Seja $\alpha \in \mathfrak{p}$ e $\alpha \neq 0$. Como $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$. Assim, existem $a_i \in A$, para $i = 0, \ldots, n-1$, não todos nulos, tal que

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

e que n seja mínimo. Logo, $a_0 \neq 0$, pois caso contrário, obteríamos uma equação de grau menor. Assim,

$$a_0 = \alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \cdots - a_1) \in \alpha\mathcal{O}_{\mathbb{K}} \cap A \subset \mathfrak{p} \cap A.$$

Portanto, $\mathfrak{p} \cap A \neq 0$. Como $\mathfrak{p} \cap A$ é um ideal primo de A e A é Dedekind segue que $\mathfrak{p} \cap A$ é um ideal maximal de A e assim $\dfrac{A}{\mathfrak{p} \cap A}$ é corpo. Seja a aplicação $\varphi : A \xrightarrow{i} \mathcal{O}_B \xrightarrow{\pi} \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}$, onde i é a inclusão e π é a projeção. Como $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre A, segue que $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}$ é inteiro sobre $\dfrac{A}{\mathfrak{p} \cap A}$. Assim,

$$\frac{A}{\mathfrak{p} \cap A} \simeq Im(\varphi) \subset \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}.$$

Logo, como $\dfrac{A}{\mathfrak{p} \cap A}$ é um corpo segue que $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}$ é um corpo. Portanto, $\mathfrak{p}$ é maximal. ∎

Corolário 1.3.4 *([24]) Se $\mathbb{K}$ é um corpo de números de grau n então o anel dos inteiros algébricos de $\mathbb{K}$ é um anel de Dedekind.*

Demonstração: Como $\mathbb{Z}$ um anel de Dedekind, pelo Teorema (1.3.7) segue o resultado. ∎

Observação 1.3.7 *O anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números é um anel de Dedekind, mas nem sempre é principal. De fato, vimos que em $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$, $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2.3$ são duas fatorações distintas do 6, cujas normas são $6, 6, 4$ e 9, respectivamente. Logo, $\mathcal{O}_{\mathbb{K}}$ não é um domínio fatorial. Se o elemento $1+\sqrt{-5}$ possuisse um divisor não trivial então $\mathcal{N}(1-\sqrt{-5}) = 6$ também possuiria um divisor não trivial mas isso é impossível pois a equação $a^2 + 5b^2 = 2$ ou 3 não possui solução inteira. Assim, $1+\sqrt{-5}$ é um elemento primo. Agora, se $\mathcal{O}_{\mathbb{K}}$ fosse principal e como $1+\sqrt{-5}$ divide $6 = 2.3$, teríamos que $1+\sqrt{-5}$ divide 2 ou 3. Tomando as normas obtemos que 6 divide 4 ou 9 o que é um absurdo. Portanto, $\mathcal{O}_{\mathbb{K}}$ não é principal.*

1.3.6 Ideais fracionários

Definição 1.3.12 *Seja $\mathbb{K}$ um corpo de números. Um $\mathcal{O}_{\mathbb{K}}$-módulo $\mathfrak{I}$ de $\mathbb{K}$ é um* **ideal fracionário** *se existe $d \in \mathcal{O}_{\mathbb{K}}$ não nulo tal que $d\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Em particular, os ideais inteiros de A são ideais fracionários com $d = 1$*

Observação 1.3.8 *Segue da Definição 1.3.12 que os elementos de um ideal fracionário $\mathfrak{I}$ tem um denominador comum $d \in A$*

Lema 1.3.6 *([13]) Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$. Se $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$.*

Demonstração: Como $\mathbb{K}$ é um corpo de números de grau n, temos pelo Teorema (1.2.1) que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$ e $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Como $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, segue que $\mathfrak{I}$ é um $\mathbb{Z}$-módulo livre de posto n. Seja $\{\gamma_1, \cdots, \gamma_n\}$ uma

$\mathbb{Z}$-base de $\mathfrak{I}$. Para cada i, temos que $\gamma_i = \sum_{j=0}^{n-1} a_{ij}\alpha^j$ tal que $a_{ij} \in \mathbb{Q}$, para todo $i = 1, \cdots, n$ e $j = 0, 1, \cdots, n-1$. Como $a_{ij} \in \mathbb{Q}$, para todo $i, j = 1, \cdots, n$, segue que $a_{ij} = \frac{b_{ij}}{c_{ij}}$; $b_{ij}, c_{ij} \in \mathbb{Z}$ e $c_{ij} \neq 0$, para todo $i, j = 1, \cdots, n$. Seja $d = mmc\{c_{ij};\ i = 1, \cdots, n,\ j = 0, 1, \cdots, n-1\}$. Temos que $d\gamma_i \in \mathbb{Z}[\alpha]$, para todo $i = 1, \cdots, n$. Como $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, temos que $d\mathfrak{I} = d\sum_{i=1}^{n} \mathbb{Z}\gamma_i = \sum_{i=1}^{n} \mathbb{Z}d\gamma_i \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, como queríamos. ∎

Proposição 1.3.15 *([13]) Se A é um domínio noetheriano, então todo ideal fracionário $\mathfrak{I}$ de A é um A-módulo finitamente gerado.*

Demonstração: Como $\mathfrak{I}$ é um ideal fracionário de A, segue pelo Lema (1.3.6) que existe $d \in A - \{0\}$ tal que $d\mathfrak{I} \subseteq A$. Assim, $\mathfrak{I} \subseteq d^{-1}A$. A aplicação $\varphi : A \to d^{-1}A$, definida por $\varphi(x) = d^{-1}x,\ x \in A$, é um isomorfismo. Assim, A é isomorfo a $d^{-1}A$. Como A é noetheriano, segue que $d^{-1}A$ é noetheriano. Logo, $\mathfrak{I}$ é um A-módulo finitamente gerado. ∎

Proposição 1.3.16 *([24]) Se A é um anel de Dedekind que não é corpo, $\mathbb{K}$ seu corpo de frações e $\mathfrak{m}$ um ideal maximal de A, então o conjunto $\mathfrak{m}' = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$ é um ideal fracionário de A.*

Demonstração: Seja $\mathfrak{m}$ um ideal maximal de A. Como A não é um corpo, segue que $\mathfrak{m} \neq \{0\}$. Consideremos $\mathfrak{n}' = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$. Temos que $\mathfrak{n}'$ é um ideal fracionário, pois $\mathfrak{n}'$ é um A-módulo tal que $\mathfrak{n}' \subseteq \mathbb{K}$ e se $c \in \mathfrak{m}$, $c \neq 0$, então $c\mathfrak{m}' \subseteq A$. ∎

Lema 1.3.7 *([24]) Se A é um anel de Dedekind que não é um corpo e $\mathbb{K}$ o seu corpo de frações, então todo ideal maximal $\mathfrak{m}$ de A é inversível no conjunto dos ideais fracionários de A.*

Demonstração: Considere o ideal fracionário $\mathfrak{n} = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$. Vamos mostrar que $\mathfrak{n}\mathfrak{m} = A$. Pela definição de $\mathfrak{n}$ temos $\mathfrak{n}\mathfrak{m} \subset A$. Por outro lado, $A \subset \mathfrak{n}$, pois $\mathfrak{m}$ é um ideal de A. Assim, $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{m}\mathfrak{n} \subset A$. Como $\mathfrak{m}$ é maximal, segue que $\mathfrak{m} = \mathfrak{n}\mathfrak{m}$ ou $\mathfrak{n}\mathfrak{m} = A$. Suponhamos que $\mathfrak{m} = \mathfrak{n}\mathfrak{m}$ e consideremos $\alpha \in \mathfrak{n}$. Então $\alpha\mathfrak{m} \subset \mathfrak{m}$, $\alpha^2\mathfrak{m} \subset \alpha\mathfrak{m} \subset \mathfrak{m}$ e $\alpha^n\mathfrak{m} \subset \mathfrak{m}$, para todo $n \in \mathbb{N}$. Seja $d \in \mathfrak{m}$, $d \neq 0$. Então, $d\alpha^n \in A$. Portanto, $A[\alpha]$ é um ideal fracionário. Como A é noetheriano, pela Proposição (1.3.15), segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema (1.3.1), segue que α é inteiro sobre A. Sendo A integralmente fechado, segue que $\alpha \in$ A. Assim, $\mathfrak{n} \subset A$ e como $A \subset \mathfrak{n}$ segue que $\mathfrak{n} = A$. Falta mostrar que esta igualdade é impossível. Seja $a \in \mathfrak{m}$. Pela Proposição (1.1.5), temos que $\langle a \rangle = aA \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$, onde os $\mathfrak{p}_i s$ são ideais primos não nulos de A, com n o menor valor possível. Assim, $\mathfrak{m} \supset aA \supset \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$. Pela Proposição (1.1.4), $\mathfrak{m}$ contém um dos $\mathfrak{p}_i$, para algum $i = 1, \ldots, n$. Sem perda de generalidade,

digamos que seja $\mathfrak{p}_1$, isto é, $\mathfrak{m} \supset \mathfrak{p}_1$. Como A é Dedekind, segue que $\mathfrak{m} = \mathfrak{p}_1$, pois $\mathfrak{p}_1$ é maximal. Agora, considere $\mathfrak{q} = \mathfrak{q}_2 \dots \mathfrak{q}_n$. Então $aA \supset \mathfrak{m}\mathfrak{q}$ e $aA \not\supset \mathfrak{q}$, pela minimalidade de n. Assim, existe $b \in \mathfrak{q}$ e $b \notin \langle a \rangle$ tal que $\mathfrak{m}b \subset \langle a \rangle$. Logo, $\frac{b}{a}\mathfrak{m} \subseteq A$ e assim $\frac{b}{a} \in \mathfrak{n}$. Como $b \notin \langle a \rangle$ segue que $\frac{b}{a} \notin A$. Assim, $\mathfrak{n} \neq A$. Portanto, $\mathfrak{m}\mathfrak{n} = A$. ∎

Teorema 1.3.8 *([24]) Se A é um anel de Dedekind que não é um corpo, então*

1. *Todo ideal fracionário $\mathfrak{I}$ não nulo de A é um produto de ideais primos de A, de modo único, isto é, $\mathfrak{I} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$, onde $e_1, \cdots, e_n$ são inteiros positivos.*
2. *O conjunto dos ideais fracionários de A formam um grupo.*

Demonstração: 1) Se $\mathfrak{I}$ é um ideal fracionário de A, então existe $d \in A - \{0\}$ tal que $d\mathfrak{I} \subseteq A$. Notemos que, $\mathfrak{I} = (d\mathfrak{I})(d^{-1}A)$, assim, é suficiente mostrar o resultado para ideais inteiros. Seja F a família dos ideais inteiros de A, não nulos, que não são um produto de ideais primos de A. Suponha que $F \neq \emptyset$. Como A é noetheriano, segue que F tem um elemento maximal $\mathfrak{m}$. Temos que $\mathfrak{m} \neq A$, pois A é o produto da coleção vazia de ideias primos. Assim, $\mathfrak{m} \subseteq \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal maximal de A. Pelo Lema (1.3.7), temos que $\mathfrak{q} = \{x \in \mathbb{K} : x\mathfrak{p} \subset A\}$ é tal que $\mathfrak{p}\mathfrak{q} = A$. Como $\mathfrak{m} \subseteq \mathfrak{p}$ segue que $\mathfrak{m}\mathfrak{q} \subseteq \mathfrak{p}\mathfrak{q} = A$. Além disso, como $A \subset \mathfrak{q}$, segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{m}\mathfrak{q} \subset A$. Temos que $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{q}$, pois se $\mathfrak{m} = \mathfrak{m}\mathfrak{q}$ e se $\alpha \in \mathfrak{q}$, então $\alpha\mathfrak{m} \subset \mathfrak{m}$, $\alpha^2\mathfrak{m} \subset \alpha\mathfrak{m} \subset \mathfrak{m}$ e $\alpha^n\mathfrak{m} \subset \mathfrak{m}$, para todo $n \in \mathbb{N}$. Assim, se $d \in \mathfrak{m} - \{0\}$, então $d\alpha^n \in \mathfrak{m} \subseteq A$. Portanto, $A[\alpha]$ é um ideal fracionário de A. Como A é noetheriano, pela Proposição (1.3.15), segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema (1.3.1), segue que α é inteiro sobre A, e sendo A integralmente fechado, segue que $\alpha \in A$. Portanto, $\mathfrak{q} \subset A$ e assim $\mathfrak{q} = A$. Mas isto é impossível, pois se $\mathfrak{q} = A$, então $\mathfrak{p} = \mathfrak{p}A = \mathfrak{p}\mathfrak{q} = A$, o que é um absurdo, pois $\mathfrak{p}$ é um ideal primo. Pela maximalidade de $\mathfrak{m}$ e como $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{q}$ temos que $\mathfrak{m}\mathfrak{q} \notin F$, ou seja, $\mathfrak{m}\mathfrak{q} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, onde $\mathfrak{p}_i, i = 1, \cdots, n$, são ideais primos de A. Multiplicando por $\mathfrak{p}$ ambos os lados, temos que $\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_n\mathfrak{p}$, o que é um absurdo, pois $\mathfrak{m} \in F$. Portanto, $F = \emptyset$.
2) Pelo Lema (1.3.7), temos que todo ideal $\mathfrak{m}$ de A é inversível. Além disso, A é o elemento neutro e a multiplicação de ideais é associativa. ∎

1.4 Corpos quadráticos e corpos ciclotômicos

Como vimos na Definição 1.2.4, um corpo de números é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Nesta seção veremos duas classes importantes desses corpos, a classe dos corpos quadráticos e a classe dos corpos ciclotômicos. Estas classes de corpos desempenham um papel muito importante na teoria algébrica dos números uma vez que é possível encontrar o anel dos inteiros algébricos destes corpos e também podemos obter uma expressão para calcular o seu discriminante.

1.4.1 Corpos quadráticos

Definição 1.4.1 *Um corpo quadrático é um corpo de números de grau* 2.

Proposição 1.4.1 *([27]) Um corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$*, onde* d *é um inteiro livre de quadrados.*

Demonstração: Pelo Teorema (1.2.1) temos que $\mathbb{K} = \mathbb{Q}(\alpha)$, para algum $\alpha \in \mathbb{K}$. Seja $f(x) = x^2 + bx + c, \text{com } b, c \in \mathbb{Q}$, o polinômio minimal de $\alpha \in \mathbb{K}$. Sabemos que este polinômio tem grau 2 pois $\mathbb{K}$ é um corpo quadrático e então $[\mathbb{K} : \mathbb{Q}] = 2$. Resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$ temos que $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Assim, $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4c})$. Como $b^2 - 4c$ é um número racional, segue que $b^2 - 4c = \dfrac{r}{s} = \dfrac{rs}{s^2} \in \mathbb{Q}$, com $r, s \in \mathbb{Z}$. Portanto

$$\mathbb{Q}(x) = \mathbb{Q}\left(\sqrt{\frac{rs}{s^2}}\right) = \mathbb{Q}(\sqrt{rs}).$$

Suponhamos que $rs = k^2 d$, com $k, d \in \mathbb{Z}$, e d livre de quadrados. Logo, $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{rs}) = \mathbb{Q}(\sqrt{k^2 d}) = \mathbb{Q}(\sqrt{d})$. ∎

Observação 1.4.1 *Se* $\sqrt{d}$ *é raiz do polinômio irredutível* $f(x) = x^2 - d$ *sobre* $\mathbb{Q}$*, então o grupo de Galois de* K *sobre* $\mathbb{Q}$ *possui dois automorfismos dados por*

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$$

e

$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d},$$

com $a, b \in \mathbb{Q}$*. Deste modo, temos*

$$\sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = 2a \in \mathbb{Q}$$

e

$$\sigma_1(a + b\sqrt{d})\sigma_2(a + b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}.$$

Proposição 1.4.2 *([27]) Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*, com* d *livre de quadrados, um corpo quadrático. Se um elemento* $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *é um inteiro algébrico, então* $2a$ *e* $a^2 - db^2$ *são números inteiros.*

Demonstração: Se $\alpha \in \mathbb{K}$ é um inteiro algébrico, então existem $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Assim, considerando σ um automorfismo de $\mathbb{K}$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$, ou seja, $\sigma(\alpha)$ também é

um inteiro algébrico de $\mathbb{K}$. Do Corolário (1.3.1), temos que $\alpha+\sigma(\alpha)$ e $\alpha\sigma(\alpha)$ também são inteiros algébricos de $\mathbb{K}$. Além disso, temos que se $\alpha = a+b\sqrt{d}$, com $a, b \in \mathbb{Q}$, então $\alpha+\sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é integralmente fechado (Proposição (1.3.3)) segue que $2a$ e $a^2 - db^2$ são números inteiros. ∎

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

Teorema 1.4.1 *([27]) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, tal que $d \not\equiv 0(mod\ 4)$.*

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

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

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ um inteiro algébrico. Pela Proposição 1.4.2, tomemos $a = u/2$, $b = v/2$ com $u, v \in \mathbb{Z}$ e temos que $u^2 - dv^2 \in 4\mathbb{Z}$.

1. Se $d \equiv 2$ ou $3(mod\ 4)$, temos que u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1(mod\ 4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$ segue que $u^2 \equiv dv^2 \equiv d(mod\ 4)$, ou seja, $d \equiv 0(mod\ 4)$ ou $d \equiv 1(mod\ 4)$, o que é um absurdo. Portanto, concluimos que v é par, isto é, $v^2 \equiv 0(mod\ 4)$ e assim, $u^2 \equiv dv^2 \equiv 0(mod\ 4)$ o que implica que u é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ então $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois pela Proposição (1.4.2), temos que $2a$, $a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

2. Se $d \equiv 1(mod\ 4)$, já que $u^2 - dv^2 \in 4\mathbb{Z}$, então u e v têm a mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a, b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u-v)/2 + v\left((1+\sqrt{d})/2\right) \in \mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right]$, ou seja, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right]$. Por outro lado, se $\alpha = a+b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right]$ com $a, b \in \mathbb{Z}$, temos que $2a+b \in \mathbb{Z}$ e $(a+b/2)^2 - d\,(b/2)^2 = a^2 + ab + (1-d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1(mod\ 4)$. Logo, $\mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right] \subset \mathcal{O}_{\mathbb{K}}$, pois os coeficientes do polinômio minimal de α, $m(x) = x^2 - (2a+b)x + a^2 + ab + (1-d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{(1+\sqrt{d})}{2}\right] = \mathcal{O}_{\mathbb{K}}$. ∎

Proposição 1.4.3 *([27]) Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático, onde d é um inteiro livre de quadrados, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por:*

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

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

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

1. Se $d \equiv 1(mod\ 4)$ então

$$D_{\mathbb{K}} = D\left(1, \tfrac{1+\sqrt{d}}{2}\right) = \left[\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right]^2 =$$
$$= \left[\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right]^2 = d,$$

2. Se $d \equiv 2$ *ou* $3(mod\ 4)$ então

$$D_{\mathbb{K}} = D\left(1, \sqrt{d}\right) = \left[\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right]^2 =$$
$$= \left[\det\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right]^2 = 4d.$$

■

1.4.2 Corpos ciclotômicos

Definição 1.4.2 *Seja n um inteiro positivo.*

1. *Dizemos que ζ_n é uma* **raiz n-ésima primitiva da unidade** *se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$.*

2. *Um* **corpo ciclotômico** *é um corpo da forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade.*

3. *O polinômio $\phi_n(x) = \prod_{j=1,\, mdc(j,n)=1}^{n} (x - \zeta_n^j)$ é chamado de* $n-$**ésimo polinômio ciclotômico**.

Proposição 1.4.4 *([27]) Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

Demonstração: Sendo $f(x) = x^n - 1$, temos que as raízes de $f(x)$ são $1, \omega, \omega^2, \cdots, \omega^{n-1}$. Logo, podemos escrever $x^n - 1 = (x-1)(x-\omega)\cdots(x-\omega^{n-1})$. Analisando os períodos de

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

Observação 1.4.2 *Como consequência da Proposição 1.4.4 segue que*

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d<n} \phi_d(x)}. \tag{1.4.2}$$

Assim,

1. *Quando $n = p$, onde p é um número primo, segue que*

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1,$$

   que é chamado de **p-ésimo polinômio ciclotômico**.

2. *Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, segue que*

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1,$$

   que é chamado de **$\mathbf{p^r}$-ésimo polinômio ciclotômico**.

Teorema 1.4.2 *([14]) Se n é um inteiro positivo, ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ o corpo ciclotômico correspondente, então $[\mathbb{K} : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler.*

Demonstração: Seja $f(x)$ o polinômio minimal de ζ_n sobre $\mathbb{Q}$. Logo, $x^n - 1 = f(x)h(x)$, com $h(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss, temos que $f(x), h(x) \in \mathbb{Z}[x]$. Se p é um número primo tal que $p \nmid n$, então, ζ_n^p é uma raiz n-ésima primitiva da unidade. Logo, $(\zeta_n^p)^n - 1 = f(\zeta_n^p)h(\zeta_n^p)$, ou seja, $0 = f(\zeta_n^p)h(\zeta_n^p)$. Assim, se ζ_n^p não for raiz de $f(x)$, então ζ_n^p é raiz de $h(x)$ e, portanto, ζ_n é raiz de $h(x^p)$. Pela forma que tomamos $f(x)$, segue que $f(x) \mid h(x^p)$. Pelo Lema de Gauss, segue que $h(x^p) = f(x)g(x)$, com $g(x) \in \mathbb{Z}[x]$. Como consequência do Teorema de Fermat, segue que $a^p \equiv a(mod\ p)$, e assim, $h(x^p) \equiv h(x)^p(mod\ p)$. Portanto, $f(x)g(x) \equiv h(x)^p(mod\ p)$ o que é equivalente a $h(x)^p \equiv f(x)g(x)(mod\ p)$. Logo, $\bar{h}(\zeta_n)^p = \bar{0}$, pois ζ_n é raiz de $f(x)$. E recursivamente, chegamos que $\bar{h}(\zeta_n) = 0$. Portanto $\bar{f}$ e $\bar{h}$ tem uma raiz em comum. Assim, $x^n - \bar{1} = \bar{f}(x)\bar{h}(x)$ tem uma raiz múltipla. Logo, $nx^{n-1} = \bar{0}$ e assim, para qualquer $\lambda \in \mathbb{Z}_p$, temos que $n\lambda^{n-1} = \bar{0}$. Como a característica de $\mathbb{Z}_p$ é p, segue que $p \mid n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto, ζ_n^p é raiz de $f(x)$, $\forall p \nmid n$ e $mdc(p, n) = 1$. Logo $\partial(f(x)) \geq \partial(\phi_n(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x) \mid \phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$. Portanto, $\partial(\phi_n(x)) = \partial(f(x)) = \varphi(n)$. ∎

Corolário 1.4.1 *([13]) Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico, onde ζ_n é uma raiz n-ésima primitiva da unidade. Se $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, então $[\mathbb{K} : \mathbb{L}] = 2$.*

Demonstração: Seja $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{L}[x]$. Temos que $f(\zeta_n) = 0$. Além disso, como $\zeta_n \notin \mathbb{L}$, segue que f é irredutível sobre $\mathbb{L}$. Logo, $f = min_{\mathbb{L}}\zeta_n$. Desta forma, $[\mathbb{K} : \mathbb{L}] = \partial(f) = 2$. ∎

Proposição 1.4.5 *([13]) Os homomorfismos de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{C}$ são dados por*

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

Demostração: Segue do Teorema (1.2.2). ∎

Observação 1.4.3 *Segue da Proposição (1.4.5) que $\mathbb{K}/\mathbb{Q}$, onde $\mathbb{K} = \mathbb{Q}(\zeta_n)$, é uma extensão de Galois, pois $[\mathbb{K} : \mathbb{Q}] = \varphi(n) = |\mathbb{Z}_n{}^*|$. Além disso, $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_i;\ mdc(i,n) = 1$ e $\sigma_i(\zeta_n) = \zeta_n^i\}$.*

Teorema 1.4.3 *([29]) Se n é um inteiro positivo, ζ_n uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ o corpo ciclotômico correspondente, então*

1. *o anel $\mathcal{O}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{\varphi(n)-1}\}$ é uma base integral de $\mathbb{K}$;*

2. *$\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é seu anel dos inteiros e $\{1, \zeta_n + \zeta_n^{-1}, \cdots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-(\frac{\varphi(n)}{2}-1)}\}$ é uma base integral do subcorpo $\mathbb{L}$.* ∎

Proposição 1.4.6 *([27]) Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raiz p-ésima da unidade e p um número primo ímpar, então o discriminante de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é dado por*

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

Demonstração: Sejam p um número primo e ζ_p uma raiz p-ésima da unidade. Vimos, pelo Teorema (1.4.3), que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base integral de $\mathbb{Z}[\zeta_p]$. Pela Proposição 1.3.14 temos que

$$\mathcal{D}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} \mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\phi_p'(\zeta_p)).$$

Assim, precisamos mostrar que $\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\phi_p'(\zeta_p)) = p^{p-2}$. Pela Observação (1.4.2), o p-ésimo polinômio ciclotômico é dado por $\phi_p(x) = \dfrac{x^p - 1}{x - 1}$. Derivando ambos os lados teremos $\phi_p'(x) = \dfrac{(x-1)p\,x^{p-1} - (x^p - 1)}{(x-1)^2}$. Substituindo x por ζ_p temos que $\phi_p'(\zeta_p) = \dfrac{(\zeta_p - 1)p\,\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2}$.

Como $\zeta_p^p = 1$, pois ζ_p é uma raiz p-ésima da unidade, temos que $\phi'_p(\zeta_p) = \dfrac{p\,\zeta_p^{-1}(\zeta_p - 1)}{(\zeta_p - 1)^2}$, ou seja, $\phi'_p(\zeta_p) = \dfrac{p}{(\zeta_p - 1)\zeta_p}$, e daí $\phi'_p(\zeta_p) = \dfrac{-p}{(1 - \zeta_p)\zeta_p}$. Aplicando a norma e usando a sua linearidade obtemos que

$$\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\phi'_p(\zeta_p)) = \frac{\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-p)}{\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p)\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p)} = \frac{(-p)^{p-1}}{p \cdot 1} = \frac{p^{p-1}}{p} = p^{p-2},$$

como queríamos. Portanto

$$D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1,\, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2},$$

como queríamos provar. ∎

Proposição 1.4.7 *([22]) Seja $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raiz p-ésima da unidade e p um número primo. Se $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, então o discriminante de $\mathbb{L}$ sobre $\mathbb{Q}$ é dado por*

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

Proposição 1.4.8 *Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, p um número primo e r um inteiro maior que 1, então o discriminante de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por*

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

Demonstração: Sejam p um número primo, r um inteiro maior que 1 e ζ_p uma raiz p^r-ésima da unidade. Vimos, pelo Teorema (1.4.3), que $\{1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\varphi(p^r)-1}\}$ é uma base integral de $\mathbb{Z}[\zeta_{p^r}]$. Pela Proposição (1.3.14) temos que

$$\mathcal{D}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\varphi(p^r)-1}) = \pm\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})).$$

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

$$\phi'_{p^r}(x) = \frac{p^r x^{p^r-1}(x^{p^{r-1}} - 1) - (x^{p^r} - 1)p^{r-1}x^{p^{r-1}-1}}{(x^{p^{r-1}} - 1)^2},$$

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

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

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

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

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

$$\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})) = \frac{\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(-p^r)}{\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_p)\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r})}.$$

Como o p^r-ésimo polinômio ciclotômico tem grau $(p-1)pr-1$ e seu termo independente é igual a 1 segue que $\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = \pm 1$. Além disso,

$$\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$$

e

$$\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_p) = \mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\mathcal{N}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_p)}(1-\zeta_p)) = (\mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p))^{p^{r-1}} = p^{p^{r-1}}.$$

Portanto

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

o que prova a proposição. ∎

Proposição 1.4.9 *([16]) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, onde r é um número inteiro positivo. Se $\mathbb{L} = \mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1})$ é o subcorpo maximal real de $\mathbb{K}$, então o discriminante de $\mathbb{L}$ é dado por $|\mathcal{D}_{\mathbb{L}}| = 2^{\beta}$, onde $\beta = (r-1)n-1$.* ∎

Teorema 1.4.4 *([29]) Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raíz n-ésima primitiva da unidade. O discriminante do corpo $\mathbb{K} = \mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por*

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

onde p é um número primo e φ é função de Euler. ∎

1.5 Codiferente

Nesta seção, apresentamos o conceito de codiferente e suas principais propriedades. Para isto, sejam A um anel de Dedekind, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}$ uma extensão separável de $\mathbb{L}$ de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre A.

Definição 1.5.1 *Seja M um subconjunto de $\mathbb{K}$. O conjunto $M^* = \{x \in \mathbb{K} : Tr_{\mathbb{K}/\mathbb{L}}(xy) \in A, \forall\ y \in M\}$ é definido como o* **codiferente de M sobre** $\mathbb{L}$. *Em particular, quando $M = \mathcal{O}_{\mathbb{K}}$*

chamamos de **codiferente de $\mathbb{K}$ sobre $\mathbb{L}$** *ao conjunto* $\mathcal{O}_{\mathbb{K}}{}^{*} = \{x \in \mathbb{K} : Tr_{\mathbb{K}/\mathbb{L}}(xy) \in A, \forall\ y \in \mathcal{O}_{\mathbb{K}}\}$. *Neste caso, denotamos* $\mathcal{O}_{\mathbb{K}}{}^{*}$ *por* $\Delta(\mathbb{K}/\mathbb{L})^{-1}$.

Exemplo 1.5.1 *Sejam* $A = \mathbb{Z}$, $\mathbb{L} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *onde* d *é um inteiro livre de quadrados e* $d \equiv 2$ *ou* $3 \pmod 4$. *Vimos no Teorema (1.4.1) que* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d};\ x, y \in \mathbb{Z}\}$ *é o anel de inteiros de* $\mathbb{K}$ *sobre* $\mathbb{Z}$. *Temos que*

$$\Delta(\mathbb{K}/\mathbb{L})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}].$$

De fato, se $x \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$, *então* $x = \frac{1}{2\sqrt{d}}(a + b\sqrt{d})$; $a, b \in \mathbb{Z}$. *Dado* $y = c + e\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$, *temos que* $Tr(xy) = Tr\left(\left(\frac{1}{2\sqrt{d}}(a + b\sqrt{d})\right)(c + e\sqrt{d})\right) = Tr\left(\frac{1}{2\sqrt{d}}ac + \frac{ae}{2} + \frac{bc}{2} + \frac{be\sqrt{d}}{2}\right) = ae + bc \in \mathbb{Z}$. *Assim,* $x \in \Delta(\mathbb{K}/\mathbb{L})^{-1}$. *Logo,* $\frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}] \subset \Delta(\mathbb{K}/\mathbb{L})^{-1}$. *Reciprocamente, se* $x = a + b\sqrt{d} \in \Delta(\mathbb{K}/\mathbb{L})^{-1}$, *então* $a, b \in \mathbb{Q}$, $x \in \mathbb{K}$ *e* $Tr(xy) \in \mathbb{Z}$, $\forall y \in \mathbb{Z}[\sqrt{d}]$. *Tomando* $y = 1$, *temos que* $Tr(xy) = Tr(a + b\sqrt{d}) = 2a \in \mathbb{Z}$. *Assim,* $a = \frac{m}{2}; m \in \mathbb{Z}$. *Tomando* $y = \sqrt{d}$, *temos que* $Tr(xy) = Tr(a\sqrt{d} + bd) = 2db \in \mathbb{Z}$. *Assim,* $b = \frac{n}{2d}; n \in \mathbb{Z}$. *Logo* $x = \frac{m}{2} + \frac{n}{2d}\sqrt{d} = \frac{1}{2\sqrt{d}}(n + m\sqrt{d}) \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. *Desta forma,* $\Delta(\mathbb{K}/\mathbb{L})^{-1} \subset \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. *Portanto,* $\Delta(\mathbb{K}/\mathbb{L})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$.

Exemplo 1.5.2 *Sejam* $A = \mathbb{Z}$, $\mathbb{L} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *onde* d *é um inteiro livre de quadrados e* $d \equiv 2$ *ou* 3 $(mod\ 4)$. *Se* $M = \mathbb{Z}[\sqrt{d}]$, *então, pelo Exemplo (1.5.1), temos que* $M^{*} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. *Mostremos que* $M^{**} = M = \mathbb{Z}[\sqrt{d}]$. *De fato, se* $x = a + b\sqrt{d} \in M^{**}$, *então* $a, b \in \mathbb{Q}$, $x \in \mathbb{K}$ *e* $Tr(xy) \in \mathbb{Z}, \forall y \in M^{*} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. *Tomando* $y = \frac{\sqrt{d}}{2\sqrt{d}} \in M^{*}$, *temos que* $Tr(xy) = Tr\left(\frac{a}{2} + \frac{bd}{2\sqrt{d}}\right) = Tr\left(\frac{a}{2} + \frac{b\sqrt{d}}{2}\right) = a \in \mathbb{Z}$. *Tomando* $y = \frac{1}{2\sqrt{d}} \in M^{*}$, *temos que* $Tr(xy) = Tr\left(\frac{a}{2\sqrt{d}} + \frac{b}{2}\right) = b \in \mathbb{Z}$. *Logo,* $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. *Desta forma,* $M^{**} \subset \mathbb{Z}[\sqrt{d}]$. *Agora, se* $x \in \mathbb{Z}[\sqrt{d}]$, *então* $x = a + b\sqrt{d}$; $a, b \in \mathbb{Z}$. *Dado* $y = \frac{1}{2\sqrt{d}}(c + d\sqrt{d}) \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$, *temos que* $Tr(xy) \in \mathbb{Z}$, *pois* $y \in M^{*} = \Delta(\mathbb{K}/\mathbb{L})^{-1}$. *Logo,* $\mathbb{Z}[\sqrt{d}] \subset M^{**}$. *Portanto,* $M^{**} = \mathbb{Z}[\sqrt{d}] = M$.

Proposição 1.5.1 *([13]) Sejam* M *um subconjunto de* $\mathbb{K}$ *e* M^{*} *o codiferente de* M *sobre* $\mathbb{L}$. *Temos que:*

1. *Se* $\mathcal{O}_{\mathbb{K}}M \subseteq M$, *então* M^{*} *é um* $\mathcal{O}_{\mathbb{K}}$*-módulo.*

2. *Se* $M_1 \subseteq M_2 \subseteq \mathbb{K}$, *então* $M_2^{*} \subseteq M_1^{*} \subseteq \mathbb{K}$.

3. $\mathcal{O}_{\mathbb{K}} \subseteq \Delta(\mathbb{K}/\mathbb{L})^{-1}$.

Demonstração: 1) Suponhamos que $\mathcal{O}_{\mathbb{K}}M \subseteq M$. Vamos mostrar que se $b \in \mathcal{O}_{\mathbb{K}}$ e $x \in M^*$ então $bx \in M^*$. Se $b \in \mathcal{O}_{\mathbb{K}}$, $x \in M^*$e $y \in M$, temos que $Tr((bx)y) = Tr(x(by)) \in \mathcal{A}$, pois $by \in \mathcal{O}_{\mathbb{K}}M \subset M$. Assim, $bx \in M^*$. As demais propriedades seguem de forma análoga. Logo, M^* é um $\mathcal{O}_{\mathbb{K}}$- módulo.
2) Seja $M_1 \subseteq M_2$. Dado $x_2 \in M_2^*$, então $x_2 \in \mathbb{K}$ e $Tr(x_2y) \in A$, para todo $y \in M_2$. Como $M_1 \subset M_2$, segue que $Tr(x_2y) \in A$, para todo $y \in M_1$. Logo, $x_2 \in M_1^*$. Portanto, $M_2^* \subseteq M_1^* \subseteq \mathbb{K}$.
3) Como $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre A e A é integralmente fechado segue que $Tr(\mathcal{O}_{\mathbb{K}}) \subset A$. Assim, se $x, y \in \mathcal{O}_{\mathbb{K}}$, então $Tr(xy) \in A$ e, deste modo, $x \in \Delta(\mathbb{K}/\mathbb{L})^{-1}$. Portanto, $\mathcal{O}_{\mathbb{K}} \subseteq \Delta(\mathbb{K}/\mathbb{L})^{-1}$. ∎

Seja $\mathbb{K}_1$ o espaço dual de $\mathbb{K}$. Pelo Lema (1.3.2), temos que existe um isomorfismo

$$\varphi : \mathbb{K} \longrightarrow \mathbb{K}_1, \text{ tal que } \varphi(x) = S_x, \text{ onde } x \in \mathbb{K} \text{ e } S_x(y) = Tr(xy), \text{ para } y \in \mathbb{K}.$$

Sejam $\{x_1, \cdots, x_n\}$ uma $\mathbb{L}$-base de $\mathbb{K}$ e $\{x_1^*, \ldots, x_n^*\}$ um conjunto de elementos de $\mathbb{K}$ tal que $\{\varphi_{x_1^*}, \ldots, \varphi_{x_n^*}\}$ seja uma base dual de $\{x_1^*, \cdots, x_n^*\}$, isto é, $\varphi_{x_i^*}(x_j) = Tr(x_i^*x_j) = \delta_{ij}$, onde $\delta_{ii} = 1$ e $\delta_{ij} = 0$ se $i \neq j$. Temos que, $\{x_1^*, \cdots, x_n^*\}$ é também uma base de $\mathbb{K}$, chamada de **base complementar** de $\{x_1, \cdots, x_n\}$.

Proposição 1.5.2 *([13]) Com as notações acima, se* $\{x_1, \cdots, x_n\}$ *é uma* $\mathbb{L}$*-base de* $\mathbb{K}$ *e* $\{x_1^*, \cdots, x_n^*\}$ *uma base complementar de* $\{x_1, \cdots, x_n\}$*, então* $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1, \cdots, x_n)\mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1^*, \cdots, x_n^*) = 1$.

Demonstração: Sejam $\sigma_1, \cdots, \sigma_n$ os $\mathbb{L}$-homomorfismos de $\mathbb{K}$. Tomando

$$X = (\sigma_i(x_j))_{i,j=1}^n \text{ e } X^* = (\sigma_i(x_j^*))_{i,j=1}^n$$

e denotando por X^t a matriz transposta de X, temos que

$$(X^*)^t X = \begin{pmatrix} \sigma_1(x_1^*) & \cdots & \sigma_n(x_1^*) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_n^*) & \cdots & \sigma_n(x_n^*) \end{pmatrix} \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & & \sigma_n(x_n) \end{pmatrix} = (Tr(x_i^*x_j))_{i,j=1}^n = I_n.$$

Assim, $\det(X^*)^t \det(X) = 1$. Pela Proposição (1.3.13), temos que

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1, \ldots, x_n) = \det(X)^2 \text{ e } \mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1^*, \ldots, x_n^*) = \det(X^*)^2.$$

Portanto, $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1, \ldots, x_n)\mathcal{D}_{\mathbb{K}/\mathbb{L}}(x_1^*, \ldots, x_n^*) = 1$. ∎

Proposição 1.5.3 *([13]) Se M é um subconjunto de $\mathbb{K}$ e M^* o codiferente de M sobre $\mathbb{L}$, então:*

1. *M^* é um A-módulo.*
2. *Se M é um A-módulo livre com base $\{x_1, \cdots, x_n\}$ então M^* é um A-módulo livre com base $\{x_1^*, \cdots, x_n^*\}$, onde $\{x_1^*, \cdots, x_n^*\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$ tal que $Tr(x_i^* x_j) = \delta_{ij}$; $\delta_{ij} = 0$, se $i \neq j$ e $\delta_{ij} = 1$, se $i = j$.*
3. *$M^{**} = M$.*

Demonstração: 1) Sejam x_1 e $x_2 \in M^*$. Se $y \in M$, temos que

$$Tr((x_1 + x_2)y) = Tr(x_1 y) + Tr(x_2 y) \in A.$$

Assim, $x_1 + x_2 \in M^*$. Agora se $a \in A$, $x \in M^*$, dado $y \in M$, temos que

$$Tr((ax)y) = aTr(xy) \in A.$$

Assim $ax \in M^*$. As demais propriedades seguem de forma análoga. Portanto, M^* é um A-módulo.
2) Sejam $\{x_1, \ldots, x_n\}$ uma A-base de M e $\{x_1^*, \cdots, x_n^*\}$ uma $\mathbb{L}$-base de $\mathbb{K}$ tal que $Tr(x_i^* x_j) = 0$ se $i \neq j$, e $Tr(x_i^* x_i) = 1$. Se $x = \sum_{i=0}^{n} a_i x_i^* \in \sum_{i=1}^{n} A x_i^*$, então

$$Tr(xx_j) = Tr\left(\left(\sum_{i=0}^{n} a_i x_i^*\right) x_j\right) = \sum_{i=0}^{n} a_i Tr(x_i^* x_j) = a_j \in A, \text{ para } j = 1, \ldots, n.$$

Desta forma, pela linearidade da função traço, segue que $Tr(xy) \in A, \forall y \in M$. Portanto, $\sum_{i=1}^{n} A x_i^* \subseteq M^*$. Reciprocamente, se $\sum_{i=1}^{n} a_i x_i^* \in M^*$, com $a_i \in \mathbb{L}$, para $i = 1, \cdots, n$, então,

$$a_j = Tr\left(\left(\sum_{i=1}^{n} a_i x_i^*\right) x_j\right) \in A, \text{ para } j = 1, \ldots, n,$$

e, deste modo, $M^* \subseteq \sum_{i=1}^{n} A x_i^*$. Assim, $M^* = \sum_{i=1}^{n} A x_i^*$. Portanto, M^* é um A-módulo livre com base $\{x_1^*, \cdots, x_n^*\}$.
3) Visto que $\{x_1^*, \cdots, x_n^*\}$ é uma base de M^* e $\{x_1, \cdots, x_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$ que satisfaz $Tr(x_i^* x_j) = \delta_{ij}$, de forma análoga ao que foi feito anteriormente, mostramos que $M^{**} =$

$\sum_{i=1}^{n} Ax_i = M.$ ∎

Proposição 1.5.4 *([13]) Se $\mathbb{K} = \mathbb{L}(\alpha)$, onde α é inteiro sobre $\mathbb{L}$ e $[\mathbb{L}(\alpha) : \mathbb{L}] = n$, então $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo finitamente gerado.*

Demonstração: Temos que $A[\alpha] \subset \mathcal{O}_{\mathbb{K}}$. Assim, pelo item *(2)* da Proposição (1.5.1), temos que $\Delta(\mathbb{K}/\mathbb{L})^{-1} = \mathcal{O}_{\mathbb{K}}^* \subset A[\alpha]^*$. Agora, como α é inteiro sobre A, temos que $A[\alpha]$ é um A-módulo finitamente gerado por $\{1, \alpha, \cdots, \alpha^{n-1}\}$. Como $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$, segue que $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é linearmente independente sobre A. Logo, $A[\alpha]$ é um A-módulo livre. Pelo item *(2)* da Proposição (1.5.3), temos que $A[\alpha]^*$ é um A-módulo livre finitamente gerado. Logo, como A é noetheriano segue, pelo Corolário (1.1.2), que $A[\alpha]^*$ é um A-módulo noetheriano. Como $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo, pelo item *1.* da Proposição (1.5.1), segue que $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um A-módulo. Desta forma, temos que $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um A-submódulo de um A-módulo noetheriano $A[\alpha]^*$. Portanto, $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um A-módulo finitamente gerado. Desta forma, existem $x_1, \cdots, x_m \in \Delta(\mathbb{K}/\mathbb{L})^{-1}$ tal que $\Delta(\mathbb{K}/\mathbb{L})^{-1} = \sum_{i=1}^{m} Ax_i$. Em particular, como $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo, segue que $\Delta(\mathbb{K}/\mathbb{L})^{-1} \subset \sum_{i=1}^{m} \mathcal{O}_{\mathbb{K}} x_i \subset \Delta(\mathbb{K}/\mathbb{L})^{-1}$. Logo, $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo finitamente gerado. ∎

Corolário 1.5.1 *([13]) Se $\mathbb{K} = \mathbb{L}[\alpha]$, onde α é inteiro sobre $\mathbb{L}$ e $[\mathbb{L}[\alpha] : \mathbb{L}] = n$, então $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Pela Proposição (1.5.4), temos que $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo finitamente gerado. Assim, se tomarmos d um fator comum entre os denominadores dos geradores de $\Delta(\mathbb{K}/\mathbb{L})^{-1}$, temos que $d\Delta(\mathbb{K}/\mathbb{L})^{-1} \subseteq \mathcal{O}_{\mathbb{K}}$. Portanto, $\Delta(\mathbb{K}/\mathbb{L})^{-1}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$. ∎

1.6 Conclusão do capítulo

Neste capítulo vimos muitos dos resultados que irão nos fornecer uma base teórica para o desenvolvimento dos demais capítulos. Dentre outras, destacamos a importância da definição de corpos de números vista em (1.2.4) pois todo o trabalho será desenvolvido através de corpos de números, em particular os corpos quadráticos e os corpos ciclotômicos, definidos em (1.4.1) e (1.4.2), respectivamente. As definições de anéis dos inteiros, de traço, norma e discriminante, vistas na Seção (1.3) também serão de grande utilidade neste trabalho. Dentre os resultados, destacamos a importância dos Teoremas (1.1.3), (1.2.2), (1.3.3), (1.3.4), (1.4.1), (1.4.3) e (1.4.4). A definição de codiferente será utilizada na definição de reticulado ideal no Capítulo (6).

Capítulo 2

Aplicação das formas quadráticas aos corpos ciclotômicos

Nesta seção, apresentamos algumas aplicações das formas quadráticas aos corpos ciclotômicos. Nosso objetivo é encontrar expressões para calcular o traço de um elemento da forma $x\overline{x}$, onde x é um inteiro algébrico do anel dos inteiros de um corpo ciclotômico. Veremos inicialmente as aplicações aos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um número primo, e depois, resultados mais gerais serão vistos para corpos ciclotômicos da forma $\mathbb{Q}(\zeta_n)$, onde n é um inteiro positivo. O estudo deste capítulo se deve a necessidade de encontrar o raio máximo de empacotamento de um reticulado que, no Capítulo (5), veremos que será equivalente a minimizar a forma traço.

2.1 Aplicações aos corpos $\mathbb{Q}(\zeta_p)$

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p)$ um corpo ciclotômico, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ seu anel dos inteiros e $x = \sum_{i=0}^{p-2} a_i\zeta_p^i \in \mathbb{Z}[\zeta_p]$, um inteiro algébrico. Sendo $\overline{\zeta_p} = \zeta_p^{-1}$ segue que $\overline{x} = \sum_{i=0}^{p-2} a_i\zeta_p^{-i}$ e então,

$$\begin{aligned} x\overline{x} &= \left(\sum_{i=0}^{p-2} a_i\zeta_p^i\right)\left(\sum_{i=0}^{p-2} a_i\zeta_p^{-i}\right) = (a_0^2 + \cdots + a_{p-2}^2) + (a_0a_1 + \cdots + a_{p-3}a_{p-2})(\zeta_p + \zeta_p^{-1}) + \cdots + \\ &+(a_0a_{p-3} + a_1a_{p-2})(\zeta_p^{p-3} + \zeta_p^{-(p-3)}) + a_0a_{p-2}(\zeta_p^{p-2} + \zeta_p^{-(p-2)}). \end{aligned}$$

Por outro lado, fazendo $x_i = \zeta_p^i + \zeta_p^{-i}$ e $A_i = a_0a_i + a_1a_{i+1} + \cdots + a_{p-2-i}a_{p-2}$, temos que

$$x\overline{x} = A_0 + A_1x_1 + \cdots + A_{p-2}x_{p-2}. \tag{2.1.1}$$

Teorema 2.1.1 *([23]) Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$ é um corpo ciclotômico, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ seu anel dos inteiros*

e $x = \sum_{i=0}^{p-2} a_i \zeta_p^i \in \mathbb{Z}[\zeta_p]$, *onde* p *é um número primo, então,*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0 \leq i < j \leq p-2} (a_i - a_j)^2.$$

Demonstração: Seja $x = \sum_{i=0}^{p-2} a_i \zeta_p^i \in \mathbb{Z}[\zeta_p]$, com $a_i \in \mathbb{Z}$, $i = 1, \ldots, p-2$. Pela Equação (2.1.1) temos que $x\overline{x} = A_0 + A_1 x_1 + \cdots + A_{p-2} x_{p-2}$, onde $A_i = a_0 a_i + a_1 a_{i+1} + \cdots + a_{p-2-i} a_{p-2}$. Observe que

$$Tr_{\mathbb{K}/\mathbb{Q}}(x_i) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i + \zeta_p^{-i}) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i) + Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^{-i}) = -1 - 1 = -2$$

e como o coeficiente x_0 de A_0 é igual a 1 temos

$$Tr_{\mathbb{K}/\mathbb{Q}}(1) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}].1 = p - 1.$$

Assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = (p-1)A_0 - 2(A_1 + A_2 + \cdots + A_{p-2}) = (p-1)A_0 -$$

$$-2(a_0a_1 + \cdots + a_{p-3}a_{p-2} + a_0a_2 + \cdots + a_{p-4}a_{p-2} + \cdots + a_0a_{p-3} + a_1a_{p-2} + a_0a_{p-2}).$$

Logo,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i^2 + 2\sum_{0 \leq i < j \leq p-2} a_i a_j\right]$$

e, portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i\right]^2. \tag{2.1.2}$$

Fazendo algumas operações no segundo membro da Equação 2.1.2, temos que

$$\begin{aligned} p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i\right]^2 &= p(a_0^2 + \cdots + a_{p-2}^2) - [(a_0^2 + \cdots + a_{p-2}^2) + a_0a_1 + \cdots + a_{p-3}a_{p-2}] \\ &= (p-1)\sum_{i=0}^{p-2} a_i^2 - \sum_{o \leq i < j \leq p-2} a_i a_j = \sum_{i=0}^{p-2} a_i^2 + (p-2)\sum_{i=0}^{p-2} a_i^2 - \sum_{o \leq i < j \leq p-2} a_i a_j \\ &= \sum_{i=0}^{p-2} a_i^2 + \sum_{o \leq i < j \leq p-2} (a_i - a_j)^2. \end{aligned}$$

Portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0\leq i<j\leq p-2} (a_i - a_j)^2,$$

como queríamos provar. ∎

Observação 2.1.1 *Quando $\mathbb{K} = \mathbb{Q}(\zeta_p)$, temos que*

$$min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x});\ x \in \mathcal{O}_{\mathbb{K}},\ x \neq 0\} = p - 1.$$

Esta minimização da forma quadrática será utilizada quando estudarmos os reticulados algébricos, no cálculo da densidade de centro desses reticulados.

2.2 Aplicações aos corpos $\mathbb{Q}(\zeta_n)$

Sejam n um número inteiro positivo, $\mathbb{Q}(\zeta_n)$ um corpo ciclotômico, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ seu anel de inteiros e $x = \sum_{i=1}^{\varphi(n)-1} a_i\zeta_n^i \in \mathcal{O}_{\mathbb{K}}$ um inteiro algébrico, onde φ é a função de Euler.

Como $x = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{\varphi(n)-1}\zeta^{\varphi(n)-1}$ segue que $\overline{x} = a_1\zeta^{-1} + a_2\zeta^{-2} + \ldots + a_{\varphi(n)}^{-\varphi(n)}$. Assim, $x\overline{x} = (a_0^2+a_1^2+\ldots+a_{\varphi(n)-1}^2)+(a_0a_1+a_1a_2+\ldots+a_{\varphi(n)-2}a_{\varphi(n)-1})(\zeta+\zeta^{-1})+(a_0a_2+a_1a_3+\ldots+a_{\varphi(n)-3}a_{\varphi(n)-1})(\zeta^2+\zeta^{-2})+\ldots+a_0a_{\varphi(n)-1}(\zeta^{\varphi(n)-1}+\zeta^{-(\varphi(n)-1)})$. Tomando $x_i = \zeta^i + \zeta^{-i}$, com $i = 1, \ldots, \varphi(n) - 1$ e $A_j = \sum_{k=1}^{\varphi(n)-(j+1)} a_ka_{j+1}$, para $j = 1, \ldots, \varphi(n) - 1$, temos:

$$x\overline{x} = A_0 + \sum_{i=1}^{\varphi(n)-1} A_ix_i.$$

Deste modo,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) &= Tr_{\mathbb{K}/\mathbb{Q}}(A_0 + \sum_{i=1}^{\varphi(n)-1} A_ix_i) = \varphi(n)A_0 + \sum_{i=1}^{\varphi(n)-1} A_iTr_{\mathbb{K}/\mathbb{Q}}(x_i) \\ &= \varphi(n)A_0 + 2\sum_{i=1}^{\varphi(n)-1} A_iTr_{\mathbb{K}/\mathbb{Q}}(\zeta_i), \end{aligned}$$

uma vez que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta + \zeta^{-1}) = 2Tr_{\mathbb{K}/\mathbb{Q}}(\zeta)$. Além disso, se $mdc(k, n) = 1$ então $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta^k)$.

A seguir apresentamos alguns resultados que irão auxiliar na prova do resultado principal desta seção que será o Teorema (2.2.1).

Lema 2.2.1 *([23]) Sejam j, n números inteiros positivos e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico. Se $mdc(j, n) = d$ então*

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

Demonstração: Como j é um número inteiro então $\zeta_n^j \in \mathbb{Q}(\zeta_n)$. Mas, $\zeta_n^j = \zeta_{n/d}^{j/d}$, logo $\mathbb{Q}(\zeta_{n/d}^{j/d}) \subset \mathbb{Q}(\zeta_n)$. Agora, consideremos as seguintes extensões $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n/d}^{j/d}) \subset \mathbb{Q}(\zeta_n)$. Como $mdc(j, n) = d$, segue que $mdc(j/d, n/d) = 1$, o que implica que $\zeta_{n/d}^{j/d}$ é um gerador do conjunto das raízes n/d-ésimas da unidade. Deste modo temos que $\mathbb{Q}(\zeta_{n/d}^{j/d}) = \mathbb{Q}(\zeta_{n/d})$ e por propriedades da função traço vistas na Seção (1.3.2) temos que

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

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

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

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

Lema 2.2.2 *([23]) Sejam p_i um número primo, $\mathbb{Q}(\zeta_{p_i})$ um corpo ciclotômico e j, a_i inteiros positivos, onde $a_i \geq 1$. Se $mdc(j, {p_i}^{a_i}) = 1$, então*

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

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

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

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

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

o que prova o lema. ∎

Definição 2.2.1 *Seja $n = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$, onde $a_k \geq 1$, para $k = 1, 2, \dots, s$. Considere a função*

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

A função μ definida acima é chamada função de Möbius.

Lema 2.2.3 *([23]) Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico. Se $n = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$, onde $a_k \geq 1$, para todo $k = 1, 2, \dots, s$, e j é um número inteiro com $mdc(j, n) = d$, então*

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

onde μ é a função de Möbius.

Demonstração: Pelo Lema 2.2.1, temos que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_n^j) = \dfrac{\phi(n)}{\phi(n/d)}\ Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d})$. Logo basta mostrarmos que

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

Temos por hipótese que $mdc(j, n) = d$, e assim $mdc(j/d, n/d) = 1$. Para simplificar, tomamos $n/d = m$ e $j/d = i$, e assim $mdc(i, m) = 1$. Como $n = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$ e $d|n$, segue que $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$, onde $0 \leq \alpha_i \leq a_i$, para $i = 1, 2, \dots, s$. Mas, sem perda de generalidade, podemos supor $\alpha_i > 0$. Se $m = 1$, então $Tr_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(\zeta_1^i) = Tr_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(1) = 1 = \mu(1)$, o que prova que o resultado vale. Se $m \neq 1$, então temos os seguintes casos:
1) m é livre de quadrados. Neste caso a demonstração será feita por indução sobre a quantidade de números primos na decomposição de m. Se m é livre de quadrados, então $m = p_1p_2\dots p_s$. Se $s = 1$, e como $mdc(i, p_1) = 1$, pelo Lema 2.2.2 segue que $Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^i) = -1 = \mu(p_1)$. Agora, suponhamos que a igualdade seja verdadeira para $s = k$, ou seja,

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

Dado $m = p_1p_2\dots p_{k+1}$, sejam $a = p_1p_2\dots p_k$ e $b = p_{k+1}$. Logo $mdc(a, b) = 1$, e assim existem $u, v \in \mathbb{Z}$ tais que $au + bv = 1$. Além disso

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

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

$$(\zeta_m^i)^{ab/t} = (\zeta_b^{iu}\zeta_a^{iv})^{ab/t} = ((\zeta_b^{iu}\zeta_a^{iv})^{ab})^{1/t} = 1^{1/t} = 1.$$

Assim, como $mdc(i,m) = 1$, segue que ζ_m^i é um gerador do conjunto das raízes m-ésimas da unidade. Logo $\circ(\zeta_m^i) = m$, e assim $m|\frac{ab}{t}$, ou seja, $ab|\frac{ab}{t}$ o que é um absurdo. Portanto, $mdc(iu,b) = 1$ e analogamente $mdc(iv,a) = 1$. Por propriedades da funcão traço temos que

$$\begin{array}{lll} Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m^i) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_m^i)) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_b^{iu}\zeta_a^{iv})) \\ & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_b^{iu}) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^{iu}) \\ & = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^{iu})Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}) & = (-1)(-1)^k \\ & = (-1)^{k+1}. & \end{array}$$

Portanto, dado $n/d = p_1p_2\dots p_s$, temos que $Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}) = \mu(n/d)$.

2) m não é livre de quadrados. Analogamente ao caso (1), a demonstração será feita por indução sobre a quantidade de números primos na decomposição de m. Como m não é livre de quadrados, segue que $m = p_1^{a_1}p_2^{a_2}\dots p_s^{a_s}$, onde pelo menos um a_l é maior que 1, para $l = 1,2,\dots,s$. Se $s = 1$, então $m = p_1^{a_1}$, com $a_1 > 1$, e como $mdc(i,m) = 1$, pelo Lema 2.2.2, segue que

$$Tr_{\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}}(\zeta_{p_1^{a_1}}^i) = 0 = \mu(p_1^{a_1}).$$

Agora, suponhamos que a igualdade é verdadeira para $s = k$. Deste modo, temos que

$$Tr_{\mathbb{Q}(\zeta_{p_1^{a_1}\dots p_k^{a_k}})/\mathbb{Q}}(\zeta_{p_1^{a_1}\dots p_k^{a_k}}^i) = \mu(p_1^{a_1}\dots p_k^{a_k}) = 0,$$

pois existe pelo menos um a_l maior que 1, para $l = 1,2,\dots,k$. Agora, dado $m = p_1^{a_1}\dots p_{k+1}^{a_{k+1}}$, sejam $a = p_1^{a_1}$ e $b = p_2^{a_2}\dots p_{k+1}^{a_{k+1}}$. Supondo $a_1 > 1$ e como $mdc(a,b) = 1$, existem $u,v \in \mathbb{Z}$ tais que $au + bv = 1$. Assim

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

Com raciocínio análogo ao ítem (a) conclui-se que $mdc(iu,b) = mdc(iv,a) = 1$. Assim, temos que

$$\begin{array}{lll} Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m^i) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_m^i)) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_b^{iu}\zeta_a^{iv})) \\ & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_b^{iu}) & = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^{iu}) \\ & = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^{iu})Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^{iv}) & = 0. \end{array}$$

Portanto, dado $n/d = p_1^{a_1}\dots p_s^{a_s}$, temos que $Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{j/d}) = 0 = \mu(n/d)$, pois pelo menos um a_l é maior que 1, para $l = 1,2,\dots,s$. ∎

Lema 2.2.4 *([23]) Sejam n um inteiro positivo e $\mathbb{K} = \mathbb{Q}(\zeta_n)$ um corpo ciclotômico. Se $n = p_1^{a_1}\dots p_s^{a_s}$, onde $a_k \geq 1$, para $k = 1,2,\dots s$, e i é um inteiro, onde $i < \phi(n)$, e $d = mdc(i,n)$,*

então

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_n^i) \neq 0 \Leftrightarrow d = (n/P)t_j \text{ e } i = (n/P)j,$$

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

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

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

(A prova de que $\phi(n) = \phi(p_1 \dots p_s) = \phi(p_1) \dots \phi(p_s)$ é feita por indução). Logo, se $j \geq \phi(P)$, então $i = (n/P)j = ((\phi(n))/(\phi(P))j \geq ((\phi(n))/(\phi(P))(\phi(P) = \phi(n)$, o que é um absurdo, e portanto $j = 1, 2, \dots, \phi(P) - 1$. Agora, se $d = (n/P)t_j$, onde $t_j = mdc(j, P)$, para $j = 1, 2, \dots, \phi(P) - 1$, então os valores que t_j pode assumir são 1 e $p_{\alpha_1} \dots p_{\alpha_t}$, onde $1 \leq \alpha_k \leq s$ (para $k = 1, 2, \dots, t$ e $t = 1, 2, \cdots, s$) e $\alpha_k \neq \alpha_l$ se $k \neq l$. Logo, $d = p_1^{a_1-1} \dots p_s^{a_s-1}$ ou $d = p_1^{a_1-1} \dots p_{\alpha_1}^{a_{\alpha_1}} \dots p_{\alpha_t}^{a_{\alpha_t}} \dots p_s^{a_s-1}$, e assim $n/d = p_1 \dots p_s$ ou $n/d = p_1 \dots p_{\alpha_1-1} p_{\alpha_1+1} \dots p_{\alpha_t-1} p_{\alpha_t+1} \dots p_s$. Portanto, $\mu(n/d) = \pm 1 \neq 0$. Portanto, pelo Lema 2.2.3, temos que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_n^i) = \frac{\phi(n)}{\phi(n/d)}\mu(n/d) \neq 0,$$

como queríamos provar. ∎

Munidos dos resultados vistos acima, temos condições de provar o principal resultado deste capítulo que nos fornece uma expressão para calcular o traço $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$, onde $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é um corpo ciclotômico e x é um inteiro algébrico deste corpo.

Teorema 2.2.1 *([23]) Sejam* n *um inteiro positivo,* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *um corpo ciclotômico,* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ *seu anel dos inteiros e* $x = \sum_{i=1}^{n} a_i \zeta^{\varphi(n)-1} \in \mathcal{O}_{\mathbb{K}}$ *um inteiro algébrico. Se* $n = p_1^{a_1} \dots p_s^{a_s}$,

com $a_k \geq 1$, *para* $k = 1, 2, \ldots s$, $n \neq 2^r$, $r \geq 2$, *então*

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

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

Demonstração: Temos que

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

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

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

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

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

Pelo Lema 2.2.3, temos que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_n^i) = \dfrac{\phi(n)}{\phi(n/d)}\ \mu(n/d)$, onde $d = mdc(i, n)$, e deste modo podemos escrever

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = m\sum_{i=0}^{m-1} a_i^2 + 2\sum_{i=0}^{m-1} A_i \frac{\mu(n/d)}{\phi(n/d)}\ m. \tag{2.2.3}$$

Pelo Lema 2.2.4, temos que o somatório $\displaystyle\sum_{i=0}^{m-1} A_i \frac{\mu(n/d)}{\phi(n/d)}\ m$ é não nulo quando $d = (n/P)t_j$, onde $t_j = mdc(j, P)$ e $i = (n/P)j$, para $j = 1, 2, \ldots, \phi(P) - 1$, e temos ainda que $\phi(n) = (n/P)\phi(P)$. Temos que $mdc((P/t_j), t_j) = 1$, pois caso contrário, se $mdc((P/t_j), t_j) = t > 1$, então, $t \mid (P/t_j)$ e $t \mid t_j$. Logo existem $k_1, k_2 \in \mathbb{Z}$ tais que $P/t_j = tk_1$ e $t_j = tk_2$, e assim $P = t^2 k_1 k_2$, ou seja, $t^2 | P$. Agora, como $t > 1$ segue que $t^2 > 1$, e portanto, $t^2 = p_{\alpha_1} \ldots p_{\alpha_r}$, onde $p_{\alpha_k} \in \{p_1, \ldots p_s\}$, para $k = 1, 2, \ldots, r$, o que é um absurdo, pois os p_k's são distintos. Assim, $\phi(P) = \phi((P/t_j).t_j) =$

$\phi(P/t_j)\phi(t_j)$, ou seja, $\phi(P/t_j) = \phi(P)/\phi(t_j)$. Retomando a Equação (2.2.3) temos que

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

o que prova o teorema. ■

2.3 Conclusão do capítulo

Nosso objetivo ao estudar as formas quadráticas e suas aplicações aos corpos ciclotômicos neste capítulo, foi obter uma expressão para a função traço de um elemento da forma $x\overline{x}$, onde x é um inteiro algébrico do anel dos inteiros de um corpo ciclotômico, e minimiza-la a fim de obtermos um raio máximo de empacotamento e, consequentemente, podermos calcular a densidade de centro de um reticulado. O resultado que forneceu esta condição foi o Teorema (2.2.1), onde obtemos uma expressão para o cálculo da forma traço que desejamos minimizar.

Capítulo 3

Reticulados

Neste capítulo faremos um estudo sobre os reticulados, definindo-os e apresentando suas principais propriedades. As definições serão feitas na Seção (3.1). Na Seção (3.2), apresentamos a matriz de Gram de um reticulado e seu determinante. O estudo dos reticulados surgiu a partir do problema de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem o maior espaço possível. Este é o problema de empacotamento que veremos na Seção (3.3). Assim, estudar empacotamentos equivale estudar os reticulados. Na Seção (3.4) apresentamos dois conceitos muito importantes nesta teoria, a diversidade e a distância produto mínima de um reticulado. Após isto, na Seção (3.5), apresentamos alguns exemplos de reticulados conhecidos na literatura, entre eles, reticulados com densidade de centro ótima.

3.1 Definição

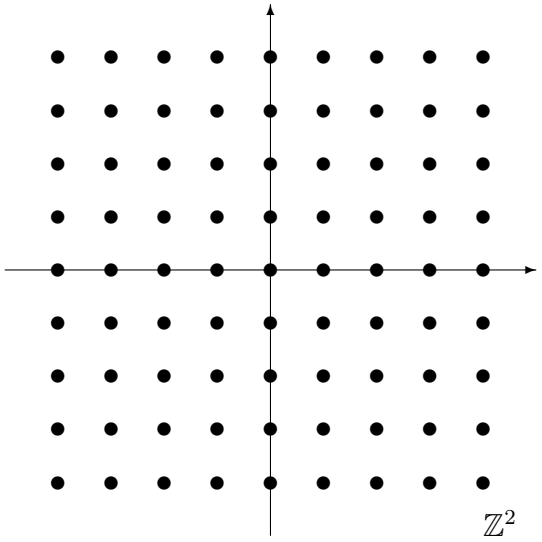
Veremos nesta seção a definição e alguns exemplos de reticulados no $\mathbb{R}^n$ e de algumas de suas propriedades como a sua matriz geradora e o seu volume.

Definição 3.1.1 *Sejam $\beta = \{v_1, \cdots, v_m\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. Chamamos de* **reticulado** *de dimensão m e base β ao subconjunto do $\mathbb{R}^n$ da forma*

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

Observação 3.1.1 *Se $m = n$, dizemos que Λ é um reticulado completo e que $\beta = \{v_1, \cdots, v_n\}$ é uma base completa do reticulado.*

Exemplo 3.1.1 *Seja $\beta = \{(1,0),(0,1)\}$ a base canônica de $\mathbb{Z}^2$. Temos que $\Lambda = \mathbb{Z}^2$ é um reticulado gerado por β.*



Observação 3.1.2 *A base de um reticulado não é única, no Exemplo* 3.1.1, $\beta' = \{(2,1),(-1,3)\}$ *também é uma base do reticulado* $\mathbb{Z}^2$*, pois o reticulado gerado por* β' *está contido em* $\mathbb{Z}^2$*.*

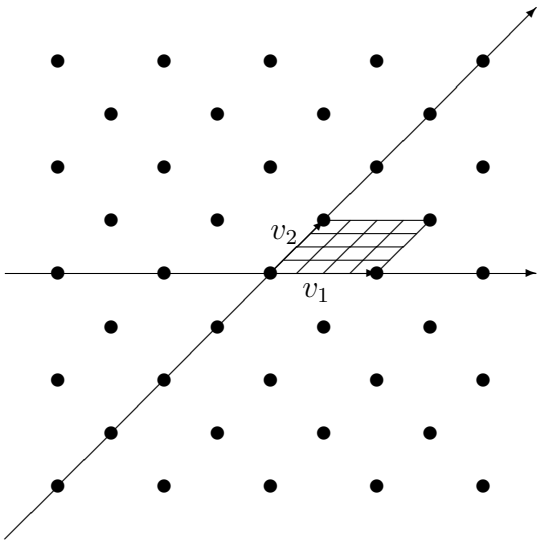
Observação 3.1.3 *Dado um reticulado* Λ *no* $\mathbb{R}^n$ *gerado por uma base* β *temos que uma condição necessária e suficiente para que um outro conjunto de vetores linearmente independentes* β' *de* $\mathbb{R}^n$ *também seja uma base deste reticulado é* β' *estar contida em* Λ *e a matriz mudança de base de* β *para* β' *ter entradas inteiras e determinante* ± 1*.*

Definição 3.1.2 *Seja* $\Lambda \subset \mathbb{R}^n$ *um reticulado, com base* $\beta = \{v_1, \cdots, v_n\}$*. O conjunto*

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

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

Exemplo 3.1.2 *Temos que* $\Lambda = \{(a,b) \in \mathbb{Z}^2; a+b \equiv 0 (mod\ 2)\}$ *é um reticulado gerado pelos vetores* $v_1 = (2,0)$ *e* $v_2 = (1,1)$ *com região fundamental dada por*



A proposição abaixo nos diz que dado um reticulado Λ, além da região fundamental $\mathcal{P}_\beta$, também existem outras regiões que podem ser obtidas por translações de $\mathcal{P}_\beta$, tais como $\mathcal{P}_\beta + l$, com $l \in \Lambda$ associadas a uma base β do reticulado Λ.

Proposição 3.1.1 *([27]) Cada elemento do $\mathbb{R}^n$ pertence a exatamente um dos conjuntos $\mathcal{P}_\beta + l$, para todo $l \in \Lambda$.*

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

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

Mas, podemos separar a parte inteira de cada coeficiente a_i, ou seja, podemos escrever $a_i = \alpha_i + \theta_i$, onde $\alpha_i \in \mathbb{Z}$, $0 \leq \theta_i < 1$ e $\theta_i \in \mathbb{R}^n$, para $i = 1, 2, \ldots, n$. Assim, podemos reescrever x da seguinte maneira:

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

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

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

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

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

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

Assim,

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

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

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

Como $0 \leq \theta_i, \gamma_i < 1$, segue que $-1 < \theta_i - \gamma_i < 1$. Mas, pela igualdade acima, e pelo fato de que $\delta_i - \alpha_i \in \mathbb{Z}$, concluímos que $\delta_i = \alpha_i$, para $i = 1, 2, \ldots, n$. Assim, $l_1 = l_2$, e portanto x pertence

a exatamente um dos conjuntos $\mathcal{P}_\beta + l$, com $l \in \Lambda$. ■

Observação 3.1.4 *Uma propriedade importante dos reticulados é que podemos ladrilhar $\mathbb{R}^n$ com estas regiões. Isto significa que cada ponto de $\mathbb{R}^n$ está em um das translações de $\mathcal{P}_\beta$ e que duas destas regiões só se tocam nos bordos ou não têm interseção.*

Observação 3.1.5 *Note que um reticulado Λ do $\mathbb{R}^n$ é um conjunto discreto do $\mathbb{R}^n$ pois para qualquer subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, temos que $\Lambda \cap \mathbb{K}$ é finito.*

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

Teorema 3.1.1 *([24]) Se Λ é um subgrupo discreto do $\mathbb{R}^n$, então Λ é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

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

$$x_j = jx - \sum_{i=1}^{r} \lceil j\lambda_i \rceil e_i \ \in \ \Lambda, \tag{3.1.1}$$

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

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

Dessa forma, se tomarmos $j = 1$ na Equação (3.1.1) temos que $x_1 = x - \sum_{i=1}^{r} \lceil \lambda_i \rceil e_i$, ou seja, $x = x_1 + \sum_{i=1}^{r} \lceil \lambda_i \rceil e_i$. Assim, como $x_1 \in \mathcal{P}_\beta \cap \Lambda$ e este é finito, segue que Λ é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, do fato de $\mathcal{P}_\beta \cap \Lambda$ ser finito e $\mathbb{N}$ ser infinito, existem inteiros j e k, tais que $x_j = x_k$. Da Equação (3.1.1), segue que

$$x_j = x_k \implies jx - \sum_{i=1}^{r} \lceil j\lambda_i \rceil e_i = kx - \sum_{i=1}^{r} \lceil k\lambda_i \rceil e_i$$

$$
\begin{aligned}
&\Longrightarrow \quad (j-k)x = \sum_{i=1}^{r}(\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil)e_i \\
&\Longrightarrow \quad (j-k)\sum_{i=1}^{r}\lambda_i e_i = \sum_{i=1}^{r}(\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil)e_i \\
&\Longrightarrow \quad (j-k)\lambda_i = \lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil \\
&\Longrightarrow \quad \lambda_i = \frac{\lceil j\lambda_i\rceil - \lceil k\lambda_i\rceil}{(j-k)},
\end{aligned}
$$

ou seja, $\lambda_i \in \mathbb{Q}$. Assim, Λ é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, que são combinações lineares com coeficientes racionais dos $e_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto $d\Lambda$. Temos que $d\Lambda \subset \sum_{i=1}^{r}\mathbb{Z}e_i$. Como $\mathbb{Z}$ é principal, segue que existe uma base $\{f_1, \cdots, f_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r}\mathbb{Z}e_i$ e inteiros α_i, tal que $\{\alpha_1 f_1, \cdots, \alpha_r f_r\}$ gera $d\Lambda$ sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo $d\Lambda$ tem o mesmo posto de Λ e como $\sum_{i=1}^{r}\mathbb{Z}e_i \subset \Lambda$, segue que o posto de $d\Lambda \geq r$. Pela maximalidade de r decorre que o posto de $d\Lambda$ é r e os $\alpha_i's$ são não nulos, pois caso contrário $d\Lambda$ não teria posto r. Assim os $f_i's$ são linearmente independentes sobre $\mathbb{R}$, uma vez que $\{e_1, \cdots, e_r\}$ é linearmente independente sobre $\mathbb{R}$. Portanto, $d\Lambda$ é gerado por r vetores linearmente independentes sobre $\mathbb{R}$ e consequentemente Λ também é gerado por r vetores linearmente independentes sobre $\mathbb{R}$. ■

Observação 3.1.6 *Segue do Teorema* 3.1.1 *que qualquer subgrupo discreto do* $\mathbb{R}^n$ *é um reticulado.*

Definição 3.1.3 *Seja* $\Lambda \subset \mathbb{R}^n$ *um reticulado, com* $\mathbb{Z}$*-base* $\beta = \{v_1, \cdots, v_n\}$. *A* **matriz geradora** *do reticulado* Λ *é definida como sendo a matriz*

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

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

Definição 3.1.4 *Sejam* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado,* $\beta = \{v_1, \cdots, v_n\}$ *uma* $\mathbb{Z}$*-base de* Λ *e* $\mathcal{P}_\beta$ *sua região fundamental. Definimos o* **volume da região fundamental** $\mathcal{P}_\beta$, *como o módulo do determinante da matriz geradora de* Λ *na base* β *e denotamos por* $\mathcal{V}ol(\mathcal{P}_\beta)$.

Definição 3.1.5 *Seja* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado com* $\mathbb{Z}$*-base* $\beta = \{v_1, v_2, \cdots, v_n\}$. *Definimos o* **volume do reticulado** Λ *como* $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P}_\beta)$.

Observação 3.1.7 *Observe que se β' for uma outra base para Λ, segue que $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\Lambda')$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido definir o volume de Λ como sendo o volume de uma região fundamental.*

3.2 Matriz de Gram e o determinante de um reticulado

Nesta seção definiremos a matriz de Gram e o determinante de um reticulado.

Definição 3.2.1 *Sejam Λ um reticulado e M sua matriz geradora. Definimos a* **matriz de Gram** *associada a matriz geradora por*

$$G = M^t M.$$

Observação 3.2.1 *A matriz de Gram G é uma matriz simétrica.*

A matriz de Gram guarda informações métricas importantes sobre a base escolhida. Vimos que um reticulado tem várias bases diferentes. No exemplo a seguir veremos que as suas matrizes de Gram podem mudar dependendo da base escolhida.

Exemplo 3.2.1 *Consideremos o reticulado $\Lambda = \mathbb{Z}^2$ gerado por $\beta = \{(n, n+1), (-n-1, n)\}$, $n \in \mathbb{Z}$. Temos que $\beta' = \{(n, n+1), (-1, 2n+1)\}$, $n \in \mathbb{Z}$ também é uma base de Λ. Assim, as matrizes geradoras das bases β e β' são, respectivamente,*

$$M = \begin{pmatrix} n & -n-1 \\ n+1 & n \end{pmatrix}$$

e

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

E, as matrizes de Gram correspondentes serão dadas respectivamente por,

$$G = \begin{pmatrix} 2n^2+2n+1 & 0 \\ 0 & 2n^2+2n+1 \end{pmatrix}$$

e

$$G' = \begin{pmatrix} 2n^2+2n+1 & 2n^2+2n+1 \\ 2n^2+2n+1 & 4n^2+4n+2 \end{pmatrix}.$$

No resultado a seguir veremos que o determinante das matrizes de Gram de um reticulado é o mesmo e esse só depende do reticulado.

Proposição 3.2.1 *([15]) Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado com base β e matriz de Gram G. Se β' for uma outra base de Λ, então* $\det(G) = \det(G')$*, onde G' é a matriz de Gram de Λ com relação a base β'.*

Demostração: Consideremos as bases $\beta = \{v_1, v_2, \ldots, v_n\}$ e $\beta' = \{u_1, u_2, \ldots, u_n\}$ de Λ. Como β é base de Λ, podemos escrever $u_i = \sum_{j=1}^{n} a_{ij} v_j$, para $i = 1, 2, \ldots, n$ e $a_{ij} \in \mathbb{Z}$. Sejam M e M' as matrizes geradoras associadas a bases β e β', respectivamente. A transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$, que leva v_i em u_i, faz a mudança de base e tem matriz A com determinante ± 1. Daí,

$$M' = AM$$

e então

$$\begin{aligned} \det(G') &= \det(M'^T M') = \det(M^T A^T A M) \\ &= \det(M^T)\det(A^T)\det(A)\det(M) \\ &= \det(M^T M) = \det(G), \end{aligned}$$

como queríamos. ∎

Exemplo 3.2.2 *No Exemplo* 3.2.1*, ambas as matrizes de Gram têm determinante igual a* $(2n^2 + 2n + 1)^2$.

Definição 3.2.2 *Definimos o* **determinante** *de Λ como o determinante de uma matriz de Gram de Λ e denotamos por $det(\Lambda)$, e, este número é o quadrado do volume de uma região fundamental de Λ.*

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

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas identicas no espaço n-dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Definição 3.3.1 *1. Um* **empacotamento esférico***, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto e que este arranjo de esferas ocupe o "maior espaço possível".*

2. *Um* **empacotamento reticulado** *é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* Λ *no* $\mathbb{R}^n$.

Observação 3.3.1 *Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Definição 3.3.2 *Dado um empacotamento no* $\mathbb{R}^n$, *associado a um reticulado* Λ, *com* $\beta = \{v_1, \cdots, v_n\}$ *uma* $\mathbb{Z}$*-base, definimos a sua* **densidade de empacotamento**, $\Delta(\Lambda)$, *como sendo a proporção do espaço* $\mathbb{R}^n$ *coberta pela união das esferas.*

Como queremos que este arranjo de esferas ocupe o "maior espaço possível"no $\mathbb{R}^n$, o interessante é estudar empacotamentos associados a um reticulado Λ em que as esferas tenham raio máximo.

Para determinarmos este raio, observe que como Λ é um conjunto discreto do $\mathbb{R}^n$ então fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n;\ |x| \leq k\}$ com o reticulado Λ é um conjunto finito. Assim, faz sentido definirmos o número $\Lambda_{min} = min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\}$.

Definição 3.3.3 *Sejam* $\Lambda \subset \mathbb{R}^n$ *um reticulado e* $\Lambda_{min} = min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\}$. *O número* $(\Lambda_{min})^2$ *é chamado de* **norma mínima** *de* Λ.

Observação 3.3.2 *O maior raio para o qual é possível distribuir esferas centradas nos pontos de* Λ *e obter um empacotamento é* $\rho = \Lambda_{min}/2$.

Sendo $\Lambda \subset \mathbb{R}^n$ um reticulado e denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, podemos obter uma expressão para calcular a densidade de empacotamento de Λ. Temos que

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

Como o valor de $\mathcal{V}ol(\mathcal{B}(1))$ é conhecido, podemos reduzir nosso estudo ao cálculo de $\dfrac{\rho^n}{\mathcal{V}ol(\Lambda)}$ que definiremos a seguir.

Definição 3.3.4 *Seja* $\Lambda \subset \mathbb{R}^n$ *um reticulado. Definimos a* **densidade de centro** *de* Λ *por*

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

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

Exemplo 3.3.1 *Se* $\Lambda \subset \mathbb{Z}^2$ *com base* $\beta = \{(1,0),(0,2)\}$, *então* $\rho = 1/2$, $\mathcal{V}ol(\mathcal{B}(1)) = \pi.1 = \pi$, *o volume do reticulado é dado por*

$$\mathcal{V}ol(\Lambda) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = 1.2 = 2,$$

a densidade de empacotamento é dada por

$$\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(1)).\frac{\rho^2}{\mathcal{V}ol(\Lambda)} = \pi\frac{1}{4}.\frac{1}{2} = \frac{\pi}{8}$$

e a densidade de centro é dada por

$$\delta(\Lambda) = \frac{\rho^2}{\mathcal{V}ol(\Lambda)} = \frac{1}{4}.\frac{1}{2} = \frac{1}{8}.$$

Observação 3.3.3 *Uma vez que* $\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(1)).\dfrac{\rho^n}{\mathcal{V}ol(\Lambda)}$ *e* $\delta(\Lambda) = \dfrac{\rho^n}{\mathcal{V}ol(\Lambda)}$*, segue que*

$$\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(1)).\delta(\Lambda)\ .$$

Exemplo 3.3.2 *Se* $\Lambda = \mathbb{Z}^3$ *com base* $\beta = \{(4,0,0),(0,3,0),(0,2,1)\}$ *então* $\rho = \sqrt{5}/2$*,* $\mathcal{V}ol(\mathcal{B}(1)) = 4\pi/3.1 = 4\pi/3$ *e o volume do reticulado é dado por*

$$\mathcal{V}ol(\Lambda) = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 2 & 1 \end{pmatrix} = 4.3 = 12,$$

a densidade de centro é dada por

$$\delta(\Lambda) = \frac{\rho^2}{\mathcal{V}ol(\Lambda)} = \left(\frac{\sqrt{5}}{2}\right)^2.\frac{1}{12} = \frac{5\sqrt{5}}{96}.$$

e então, a densidade de empacotamento é dada por

$$\Delta(\Lambda) = \mathcal{V}ol(\mathcal{B}(1)).\delta(\Lambda) = \frac{4\pi}{3}.\frac{5\sqrt{5}}{96} = \frac{5\sqrt{5}\pi}{72}.$$

Exemplo 3.3.3 *Seja* $\Lambda = \mathbb{Z}^n$ *um reticulado do* $\mathbb{R}^n$*, gerado pelos vetores* $v_1 = (1,0,\ldots,0)$*,* $v_2 = (0,1,\ldots,0),\ldots,v_n = (0,0,\ldots,1)$*. A forma quadrática* $|v|^2 = x_1^2 + \cdots + x_n^2$ *assume o valor mínimo quando um dos* $x_i = 1$*, para* $i = 1,\cdots,n$ *e os demais nulos. Assim* $|v|^2 = 1$ *e* $\rho = \dfrac{1}{2}$*. Visto que* $v(\Lambda) = |\det B|$*, e* B *neste caso é a matriz identidade, temos que o* $\mathcal{V}ol(\Lambda) = 1$*, e portanto,* $\delta(\Lambda) = \dfrac{1}{2^n}$*.*

3.4 Diversidade e distância produto mínima

Nesta seção veremos dois outros parâmetros que são a diversidade e a distância produto mínima de um reticulado. Estes parâmetros são muito importantes na teoria de reticulados pois podemos classificar um reticulado, quanto a sua eficácia, a partir destes parâmetros.

Definição 3.4.1 *Sejam $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ dois vetors no $\mathbb{R}^n$. Definimos a* **diversidade**, *ou a* **distância de Hamming**, *de x e y como*

$$div(x, y) = \#\{i,\ x_i \neq y_i,\ i = 1, \ldots, n\}.$$

Definição 3.4.2 *Dado um subconjunto $S \subseteq \mathbb{R}^n$, a* **diversidade**, *ou a distância mínima de Hamming, de S é definida por*

$$div(S) = min\{div(x, y) \mid x \neq y, x,\ y \in S\}.$$

Como todo reticulado é um subconjunto do $\mathbb{R}^n$, podemos estender as Definições (3.4.1) e (3.4.2) para reticulados. E, como reticulados têm estrutura de grupo, segue que a soma de quaisquer dois pontos de Λ está em Λ, assim, podemos reformular a definição de distância de Hamming entre dois vetores para apenas um vetor.

Definição 3.4.3 *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $x = (x_1, \ldots, x_n) \in \Lambda$.*

1. *A* **diversidade** *de x é definida como o número de $x_i's$ não nulos.*
2. *A* **diversidade** *de Λ é definida como*

$$div(\Lambda) = min\{div(x);\ x \in \Lambda,\ x \neq 0\}.$$

Exemplo 3.4.1 *Consideremos o reticulado $\Lambda = \{(x_1, x_2, x_3) \in \mathbb{Z}^3 \mid x_1 + x_2 + x_3 é\ um\ número\ par\}$. Temos que uma matriz geradora para este reticulado é dada por*

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

Assim, qualquer elemento de Λ pode ser escrito da forma

$$a_1(-1, 1, 0) + a_2(-1, -1, 1) + a_3(0, 0, -1),$$

com $a_i \in \mathbb{Z}$. Dessa forma, teremos que

$$div(\Lambda) = \min\{div(x);\ x \in \Lambda,\ x \neq 0\} = 1.$$

Mais adiante veremos que este reticulado é conhecido como D_3.

Definição 3.4.4 *Sejam Λ um reticulado em $\mathbb{R}^n$ com diversidade $l \leq n$ e $x = (x_1, \cdots, x_n) \in \Lambda$. Definimos:*

1. *A* **distância l-produto** *de x por $d_p^l(x) = \prod_{x_i \neq 0} |x_i|$.*
2. *A* **distância l-produto mínima** *de Λ por*

$$d_{p,min}^l(\Lambda) = min\{d_p^l(x) \mid x \neq 0, x \in \Lambda\}.$$

Definição 3.4.5 *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $x = (x_1, \cdots, x_n) \in \Lambda$.*

1. *A* **distância produto** *de x é definida como $d_p(x) = \prod_{i=1}^{n} |x_i|$.*
2. *A* **distância produto mínima** *de Λ é definida como*

$$d_{p,min}(\Lambda) = min\{d_p(x) \mid x \in \Lambda, x \neq 0\}.$$

Exemplo 3.4.2 *Temos no Exemplo (3.4.1) que o ponto $(-3, 1, 3)$ é um ponto de Λ. Assim,*

$$d_p{}^1(-3, 1, 3) = 3.1.3 = 9.$$

3.5 Exemplos de reticulados conhecidos

Nesta seção veremos exemplos de reticulados conhecidos na literatura. É conhecido e provado que as densidades de centro dos reticulados que veremos nesta seção, a saber: A_1, A_2, D_3, D_4, D_5, E_6, E_7 e E_8, de dimensões 1 a 8, respectivamente, são as melhores e possuem densidade de centro ótima. Para dimensões maiores como 12 e 24 sabe-se que a densidade de centro dos reticulados K_{12} e Λ_{24} são ótimas. Já para outras dimensões são conhecidas as densidades de centro, mas não se sabe se são ótimas.

3.5.1 Reticulado n-dimensional A_n

O reticulado n-dimensional A_n, onde $n \geq 1$, é definido por

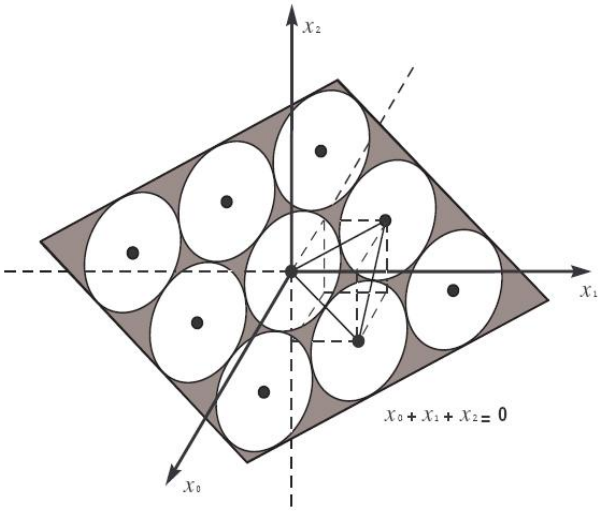
$$A_n = \{(x_0, x_1, \cdots, x_n) \in \mathbb{Z}^{n+1} : \ x_0 + x_1 + \cdots + x_n = 0\}.$$

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

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

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

Exemplo 3.5.1 Reticulado 2-dimensional A_2. *O reticulado A_2 é formado por todos os pontos (x_0, x_1, x_2) de $\mathbb{Z}^3$ que pertencem ao plano $x_0 + x_1 + x_2 = 0$, contido em $\mathbb{R}^3$. A figura a seguir mostra a disposição dos pontos do reticulado no espaço tridimensional, assim como o empacotamento associado.*



Temos que:

- *Uma matriz geradora para este reticulado é*

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

- *O raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$;*

- *A densidade de centro é*

$$\delta(A_2) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)} = 2^{-2/2}(2+1)^{-1/2} = \frac{1}{2\sqrt{3}} = 0,28868.$$

O reticulado A_2 possui densidade de centro ótima para a dimensão 2.

3.5.2 Reticulado n-dimensional D_n

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

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

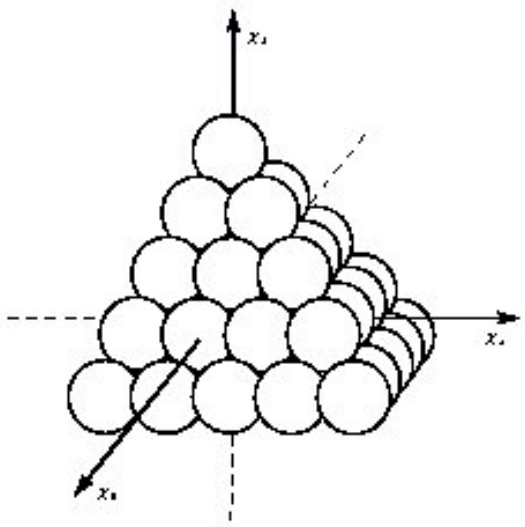
Este reticulado pode ser obtido "colorindo" os pontos de $\mathbb{Z}^n$ alternadamente com preto e branco e tomando os pontos pretos.

Uma matriz geradora M de D_n, é dada por:

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

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

Exemplo 3.5.2 Reticulado 3-dimensional D_3. *O reticulado D_3 é formado por todos os pontos $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_1 + x_2 + x_3$ é um número par. A figura abaixo mostra o arranjo das esferas do empacotamento associado a D_3.*



Este é o empacotamento normalmente encontrado em bancas de frutas (pirâmide de laranjas) ou empilhamento de balas de canhão, encontrado nos memoriais de guerra.

Temos que:

- *Uma matriz geradora para D_3 é dada por*

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

- *O raio de empacotamento é $\rho = \sqrt{2}/2$;*

- *A densidade de centro é*

$$\delta(D_3) = \frac{1}{4\sqrt{2}} \cong 0,17678.$$

O reticulado D_3 possui densidade de centro ótima para a dimensão 3.

Exemplo 3.5.3 Reticulado 4-dimensional D_4. *O reticulado D_4 é formado por todos os pontos $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ tal que $x_1 + x_2 + x_3 + x_4$ é um número par.*

Temos que:

- *Uma matriz geradora para D_4 é dada por*

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

- *o raio de empacotamento é $\rho = \sqrt{2}/2$;*

- *A densidade de centro é*

$$\delta(D_4) = \frac{1}{8} = 0,125;$$

- *Cada esfera do empacotamente é tangenciada por exatamente 24 esferas.*

O reticulado D_4 possui densidade de centro ótima para a dimensão 4.

Exemplo 3.5.4 Reticulado 5-dimensional D_5. *O reticulado D_5 é formado por todos os pontos $(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$ tal que $x_1 + x_2 + x_3 + x_4 + x_5$ é um número par.*

Temos que:

- *Uma matriz geradora para D_5 é dada por*

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

- *O raio de empacotamento é $\rho = \sqrt{2}/2$;*

- *A densidade de centro é*

$$\delta(D_5) = \frac{1}{8\sqrt{2}} = 0,08839.$$

O reticulado D_5 possui densidade de centro ótima para a dimensão 5.

3.5.3 Reticulado 8-dimensional E_8:

O reticulado E_8 é definido por

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

Temos que:

- Uma matriz geradora é dada por

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

- O raio de empacotamento é $\rho = \sqrt{2}/2$;

- A densidade de centro é $\delta(E_8) = \frac{1}{16} = 0,06250$;

- Cada esfera do empacotamento é tangenciada por exatamente 240 esferas.

O reticulado E_8 possui densidade de centro ótima para a dimensão 8.

A partir do reticulado E_8 podemos definir outros reticulados de dimensões 6 e 7 que veremos nos exemplos a seguir.

Exemplo 3.5.5 Reticulado 6-dimensional E_6: *O reticulado E_6 é definido por*

$$E_6 = \{x \in E_8 : xv = 0,\ \forall v \in V\},$$

onde V é um A_2-subreticulado em E_8. Temos que:

- *Uma matriz geradora é dada por*

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

- *O raio de empacotamento é $\rho = \sqrt{2}/2$;*
- *A densidade de centro é $\delta(E_6) = \frac{1}{8\sqrt{3}} = 0,07217$*
- *Cada esfera do empacotamento é tangenciada por exatamente 72 esferas.*

O reticulado E_6 possui densidade de centro ótima para a dimensão 6.

Exemplo 3.5.6 Reticulado 7-dimensional E_7: *O reticulado E_7 é definido por*

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

Temos que:

- *Uma matriz geradora é dada por*

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

- *O raio de empacotamento é* $\rho = \sqrt{2}/2$*;*
- *A densidade de centro é* $\delta(E_7) = \frac{1}{16} = 0,06250$*.*

O reticulado E_7 *possui densidade de centro ótima para a dimensão* 7*.*

3.5.4 Reticulado laminado Λ_n

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

Para dimensões até 8, podemos estabelecer a seguinte equivalência entre os reticulados laminados e os reticulados vistos nos exemplos acima:

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

Para dimensões 12 e 24 os reticulados laminados $\Lambda_{12} = K_{12}$ e Λ_{24} também são reticulados ótimos para estas dimensões.

3.6 Conclusão do Capítulo

Neste capítulo apresentamos o conceito central de nosso trabalho, os reticulados e suas principais propriedades. Vimos na Seção (3.3) que estudar reticulados é equivalente ao estudo de empacotamentos esféricos. Ainda nesta seção, obtemos uma expressão para o cálculo da densidade de centro de um reticulado em (3.3.4), expressão que procuraremos melhorar nos próximos capítulos. Na Seção (3.4), vimos outros dois parâmetros que foram a diversidade e a distância produto mínima de um reticulado. Esses conceitos são muito importantes pois em [6], vemos que quanto maior for a diversidade e a distância produto mínima de um reticulado, menor a probabilidade de ocorrer erro em um dado código associado a este reticulado. Estes conceitos serão mais explorados no Capítulo (6). Como vimos na Seção (3.5) os reticulados A_1, A_2, D_3, D_4, D_5, E_6, E_7, E_8, K_{12} e Λ_{24} possuem densidades de centro ótimas para suas dimensões. No entanto, no Capítulo (4) apresentamos outros exemplos de reticulados de dimensões 2 e 3 que possuem a mesma densidade de centro dos reticulados A_2 e D_3 e, no Capítulo (5) apresentamos também outros exemplos de reticulados de dimensões 2, 4, 6, 8 e 12 que possuem a mesma densidade de centro dos reticulados A_2, D_4, E_6, E_8 e K_{12}. Além disso, estes reticulados algébricos possuem propriedades algébricas de melhor visualização dos mesmos.

Capítulo 4

Reticulados de dimensões 2 e 3 via polinômios

Neste capítulo apresentamos construções de reticulados de dimesões 2 e 3 a partir de polinômios irredutíveis no corpo dos números racionais. Deste modo, iremos obter versões rotacionadas dos reticulados A_2 e D_3, definidos anteriormente, utilizando polinômios de grau 2 e 3 irredutíveis em $\mathbb{Q}$, respectivamente. Na Seção (4.1) apresentamos uma construção de reticulados de dimensão 2 via polinômios de grau 2 com raízes reais e, na Seção (4.2), via polinômios de grau 2 com raízes complexas conjugadas. Na Seção (4.3) apresentamos uma construção de reticulados de dimensão 3 via polinômios de grau 3 com raízes reais. Em ambos os casos para dimensão 2 e, para a dimensão 3 obtemos exemplos de reticulados com densidade de centro ótima para dimensões 2 e 3, respectivamente.

4.1 Reticulados de dimensão 2 via polinômios de grau 2 com raízes reais

Nosso objetivo nesta seção é obter reticulados rotacionados do reticulado Λ_2 via polinômios de grau 2 com raízes reais. Para isso, sejam $f(x) = x^2 + ax + b$, onde $a, b \in \mathbb{Z}$ e $\alpha, \beta \in \mathbb{R}$ as raízes de f. Como queremos que α e β sejam reais devemos ter

$$\Delta = a^2 - 4b > 0.$$

Seja $\Lambda_f \subset \mathbb{R}^2$ um reticulado gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta) \;\; e \;\; v_2 = (\beta, \alpha)$. Temos que uma matriz geradora de Λ_f será dada por

$$M = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}. \tag{4.1.1}$$

Sendo ρ o raio de empacotamento do reticulado Λ_f segue pela Definição (3.3.4) que a

densidade de centro de Λ_f é dada por

$$\delta(\Lambda_f) = \frac{\rho^2}{\mathcal{V}ol(\Lambda_f)} = \frac{\rho^2}{|det(M)|}.$$

Assim, para calcularmos a densidade de centro de Λ_f precisamos encontrar expressões para o cálculo de ρ e de $det(M)$. O resultado que veremos a seguir nos dá uma expressão para o módulo do determinante da matriz M.

Proposição 4.1.1 *([26]) Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, $\alpha, \beta \in \mathbb{R}$ as raízes de f e M a matriz dada em (4.1.1). O módulo do determinante da matriz M é dado por*

$$|\det(M)| = |a|\sqrt{\Delta}, \quad onde \;\; \Delta = a^2 - 4b.$$

Demonstração: Sejam α e β as raízes de f. Como vimos, para que α e β sejam reais devemos ter $\Delta = a^2 - 4b > 0,\ a, b \in \mathbb{Z}$. Assim,

$$\alpha = \frac{-a + \sqrt{\Delta}}{2} \;\text{ e }\; \beta = \frac{-a - \sqrt{\Delta}}{2}.$$

Logo,

$$\begin{aligned} |\det(M)| &= \left|\det\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}\right| = \left|\left(\frac{-a+\sqrt{\Delta}}{2}\right)^2 - \left(\frac{-a-\sqrt{\Delta}}{2}\right)^2\right| \\ &= \left|\frac{a^2 - 2a\sqrt{\Delta} + \Delta}{4} - \frac{a^2 + 2a\sqrt{\Delta} + \Delta}{4}\right| \\ &= \left|\frac{-4a\sqrt{\Delta}}{4}\right| = |-a\sqrt{\Delta}| = |a|\sqrt{\Delta}, \end{aligned}$$

onde $\Delta = a^2 - 4b > 0,\ a, b \in \mathbb{Z}$. O que prova a proposição. ∎

Exemplo 4.1.1 *Sejam $f(x) = x^2 + 3x + 1$ um polinômio de grau 2 com raízes reais α e β. Temos que: $\Delta = 3^2 - 4.1 = 5 > 0$. Assim, se Λ_f é o reticulado com base $\{(\alpha, \beta), (\beta, \alpha)\}$ e matriz geradora M, segue pela Proposição (4.1.1) que*

$$|\det(M)| = |a|\sqrt{\Delta} = 3\sqrt{5}.$$

Pela Observação (3.3.2), vimos que o maior raio de empacotamento de um reticulado Λ é $\rho = \frac{\Lambda_{min}}{2}$, onde $(\Lambda_{min})^2$ é a norma mínima de Λ. Assim, para que tenhamos um raio de empacotamento máximo devemos encontrar um vetor de Λ_f cuja norma seja mínima. A seguir,

veremos uma expressão para o cálculo da norma de um vetor de Λ_f. Iniciamos com um resultado mais geral.

Proposição 4.1.2 *([26]) Se Λ_f é um reticulado de dimensão n gerado pela base $\{v_1, \ldots, v_n\}$, $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, com $a_i \in \mathbb{Z}$ e $v \in \Lambda_f$, tal que $v = z_1v_1 + \ldots + z_nv_n$, $z_i \in \mathbb{Q}$, então,*

$$|v|^2 = (a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^{n} z_i^2 + 2 \sum_{1 \leq i < j \leq n} Tr(\alpha_i\alpha_j) z_i z_j,$$

onde α_i, $i = 1, \ldots, n$ são as raízes de f.

Demonstração: Temos que

$$|v|^2 = v.v = \left(\sum_{i=1}^{n} z_i v_i \right) \left(\sum_{j=1}^{n} z_j v_j \right) = \sum_{i=1}^{n} v_i v_i z_i^2 + 2 \sum_{1 \leq i < j \leq n} v_i v_j z_i z_j. \tag{4.1.2}$$

Seja $G = Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$, daí $v_i = (\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n))$. Assim,

$$\begin{aligned} v_i v_i &= (\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n)).(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n)) \\ &= \sigma_i(\alpha_1)^2 + \cdots \sigma_i(\alpha_n)^2 \\ &= \alpha_1^2 + \cdots + \alpha_n^2 \\ &= (\alpha_1 + \cdots \alpha_n)^2 - 2 \sum_{1 \leq i < j \leq n} \alpha_i\alpha_j \\ &= a_{n-1}^2 - 2a_{n-2}. \end{aligned}$$

Logo, a primeira parcela da Equação (4.1.2) pode ser reescrita da seguinte forma:

$$\sum_{i=1}^{n} v_i v_i z_i^2 = (a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^{n} z_i^2.$$

Para a segunda parcela teremos:

$$\begin{aligned} v_i v_j &= (\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n)).(\sigma_j(\alpha_1), \ldots, \sigma_j(\alpha_n)) \\ &= \sigma_i(\alpha_1)\sigma_j(\alpha_1) + \cdots + \sigma_i(\alpha_n)\sigma_j(\alpha_n). \end{aligned}$$

Assim,

$$\sigma_i^{-1}(v_i v_j) = \alpha_1\sigma_k(\alpha_1) + \cdots + \alpha_n\sigma_k(\alpha_n),$$

onde $\sigma_k = \sigma_i^{-1}\sigma_j$. Como, $\sum_{i=1}^{n} \alpha_i\sigma_k(\alpha_i) = Tr(\alpha_1\sigma_k(\alpha_1))$, segue que

$$v_i v_j = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_1\sigma_k(\alpha_1)) \in \mathbb{Z}.$$

Daí,

$$\begin{aligned} Tr(\alpha_i\alpha_j) &= \sum_{l=1}^{n}\sigma_l(\alpha_i\alpha_j) = \sum_{l=1}^{n}\sigma_l(\sigma_i(\alpha_1)\sigma_j(\alpha_1)) \\ &= \sum_{l=1}^{n}\sigma_l(\sigma_i(\alpha_1))\sigma_l(\sigma_j(\alpha_1)) = \sum_{l=1}^{n}\sigma_i(\sigma_l(\alpha_1))\sigma_j(\sigma_l(\alpha_1)) \\ &= \sum_{l=1}^{n}\sigma_i(\alpha_l)\sigma_j(\alpha_l) = \sum_{l=1}^{n}\sigma_i^{-1}\sigma_i(\alpha_l)\sigma_i^{-1}\sigma_j(\alpha_l) \\ &= \sum_{l=1}^{n}\alpha_l\sigma_k(\alpha_l) = Tr(\alpha_1\sigma_k(\alpha_1)). \end{aligned}$$

Portanto,

$$|v|^2 = (a_{n-1}^2 - 2a_{n-2})\sum_{i=1}^{n} z_i^2 + 2\sum_{1\leq i<j\leq n} Tr(\alpha_i\alpha_j)z_iz_j,$$

como queríamos mostrar. ■

Corolário 4.1.1 *([26]) Se $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes reais α e β, Λ_f é o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Q}$, então,*

$$|v|^2 = a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2.$$

Demonstração: Pela Proposição (4.1.2) temos que:

$$|v|^2 = (a^2 - 2b)(z_1^2 + z_2^2) + 2Tr(\alpha\beta)z_1z_2.$$

Assim,

$$\begin{aligned} |v|^2 &= (a^2 - 2b)(z_1^2 + z_2^2) + 2(2b)z_1z_2 \\ &= a^2(z_1^2 + z_2^2) - 2b(z_1^2 + z_2^2 - z_1z_2) \\ &= a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2 \end{aligned}$$

como queríamos. ■

Agora que temos uma expressão para calcular a norma de um vetor de Λ_f resta saber onde este vetor atinge norma mínima e daí teremos o raio de empacotamento do reticulado e portanto podemos calcular efetivamente a densidade de centro de reticulado Λ_f.

Exemplo 4.1.2 *Nas condições do Exemplo (4.1.1), seja $v = z_1v_1 + z_2v_2 \in \Lambda_f$. Pelo Corolário (4.1.1) segue que*

$$|v|^2 = 9(z_1^2 + z_2^2) - 2(z_1 - z_2)^2$$

e, este vetor assume valor mínimo 7 quando tomamos $z_1 = 1$ *e* $z_2 = 0$*. Logo,* $\rho = \frac{\sqrt{7}}{2}$ *e portanto,*

$$\delta(\Lambda_f) = \frac{\rho^2}{|det(M)|} = \frac{(\frac{\sqrt{7}}{2})^2}{3\sqrt{5}} = \frac{7}{12\sqrt{5}} \cong 0,143.$$

O resultado que veremos a seguir nos dá uma condição sobre o polinômio f para que o reticulado Λ_f tenha densidade de centro ótima para dimensão 2.

Teorema 4.1.1 *([26]) Sejam* $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ *com raízes reais* α *e* β*,* Λ_f *o reticulado de dimensão* 2 *gerado pela base* $\{v_1, v_2\}$*, onde* $v_1 = (\alpha, \beta)$ *e* $v_2 = (\beta, \alpha)$*. Se* f *satisfaz a condição* $\frac{a^2}{6} = b$*, então o reticulado* Λ_f *possui densidade de centro ótima.*

Demonstração: Seja $f(x) = x^2 + ax + b,\ a, b \in \mathbb{Z}$ tal que $\frac{a^2}{6} = b$ e seja $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Q}$ um vetor de Λ_f. Pelo Corolário (4.1.1) temos que

$$\begin{aligned} |v|^2 &= a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2 \\ &= 6b({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2. \end{aligned}$$

Observe que esta forma quadrática assume valor mínimo $4b$ quando $z_1 = 1$ e $z_2 = 0$. Logo,

$$\rho = \frac{\Lambda_{min}}{2} = \frac{\sqrt{4b}}{2}. \tag{4.1.3}$$

Agora, pela Proposição (4.1.1), temos

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = \sqrt{6b}\sqrt{2b} = 2\sqrt{3}b. \tag{4.1.4}$$

Por, (4.1.3) e (4.1.4) segue que a densidade de centro de Λ_f será dada por

$$\delta(\Lambda_f) = \frac{(\frac{\sqrt{4b}}{2})^2}{2\sqrt{3}b} = \frac{b}{2\sqrt{3}b} = \frac{1}{2\sqrt{3}} \cong 0,28868,$$

que é a mesma densidade de centro do reticulado Λ_2. Portanto, Λ_f possui densidade de centro ótima para dimensão 2. ∎

Exemplo 4.1.3 *Sejam* $f(x) = x^2 + 6x + 6,\ \alpha, \beta \in \mathbb{R}$ *as raízes de* f *e* $v = z_1v_1 + z_2v_2 \in \Lambda_f$*, onde* $v_1 = (\alpha, \beta)$ *e* $v_2 = (\beta, \alpha)$*. Temos que:* $|v|^2 = 36({z_1}^2 + {z_2}^2) - 12(z_1 - z_2)^2$*, que assume o valor mínimo* 24*, logo*

$$\rho = \frac{\sqrt{24}}{2}.$$

Temos ainda que

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = 6\sqrt{12} = 12\sqrt{3}.$$

Portanto,

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det(M)|} = \frac{(\frac{\sqrt{24}}{2})}{12\sqrt{3}} = \frac{24}{48\sqrt{3}} = \frac{1}{2\sqrt{3}},$$

que é a densidade ótima para dimensão 2.

Exemplo 4.1.4 *Sejam* $f(x) = x^2 + 12x + 24$, $\alpha, \beta \in \mathbb{R}$ *as raízes de* f *e* $v = z_1v_1 + z_2v_2 \in \Lambda_f$, $v_1 = (\alpha, \beta)$ *e* $v_2 = (\beta, \alpha)$. *Temos que:* $|v|^2 = 144({z_1}^2 + {z_2}^2) - 48(z_1 - z_2)^2$ *assume valor mínimo* 48, *logo*

$$\rho = \frac{\sqrt{48}}{2}.$$

Temos ainda que,

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = 12\sqrt{12} = 24\sqrt{3}.$$

Com isso

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det(M)|} = \frac{(\frac{\sqrt{48}}{2})}{12\sqrt{3}} = \frac{12}{2\sqrt{3}} = \frac{1}{2\sqrt{3}},$$

que é a densidade ótima para dimensão 2.

Observação 4.1.1 *Observe que através do Teorema (4.1.1) temos uma "família"de reticulados de dimensão 2 com densidade de centro ótima.*

4.2 Reticulados de dimensão 2 via polinômios de grau 2 com raízes complexas conjugadas

Nosso objetivo nesta seção é obter reticulados rotacionados do reticulado Λ_2 via polinômios de grau 2 com raízes complexas conjugadas. Para isso, sejam $f(x) = x^2 + ax + b$, onde $a, b \in \mathbb{Z}$ e $\gamma_1, \gamma_2 \in \mathbb{C}$ as raízes de f. Como queremos que f não tenha reais devemos ter

$$\Delta = a^2 - 4b < 0.$$

Assim, tomemos $\gamma_1 = \alpha + i\beta$ e $\gamma_2 = \alpha - i\beta$, com $\alpha, \beta \in \mathbb{R}$ e $\beta \neq 0$ as raízes de f.

Seja $\Lambda_f \subset \mathbb{R}^2$ um reticulado gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$. Temos que uma matriz geradora de Λ_f será dada por

$$M = \begin{pmatrix} \alpha & \beta \\ \alpha & -\beta \end{pmatrix} \tag{4.2.5}$$

e a densidade de centro de Λ_f é dada por

$$\delta(\Lambda_f) = \frac{\rho^2}{\mathcal{V}ol(\Lambda_f)} = \frac{\rho^2}{|det(M)|},$$

onde ρ é o raio de empacotamento de Λ_f.

Da mesma forma como no caso anterior, queremos encontrar expressões para o calcular ρ e $\det(M)$. No resultado a seguir veremos uma expressão para o cálculo de $\det(M)$.

Proposição 4.2.1 *([26]) Se $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes complexas $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$ e M é a matriz dada em (4.2.5), então o determinante de M é dado por*

$$\det(M) = \frac{a\sqrt{-\Delta}}{2}, \quad \textit{onde} \quad \Delta = a^2 - 4b < 0.$$

Demonstração: Sejam $\gamma_1 = \alpha + i\beta$ e $\gamma_2 = \alpha - i\beta$, com $\alpha, \beta \in \mathbb{R}$ e $\beta \neq 0$ as raízes de f. Temos que:

$$\gamma_1 = \frac{-a + \sqrt{-\Delta}}{2} \quad \text{e} \quad \gamma_2 = \frac{-a - \sqrt{-\Delta}}{2}.$$

Assim, $\alpha = \frac{-a}{2}$ e $\beta = \frac{\sqrt{-\Delta}}{2}$. Logo,

$$M = \begin{pmatrix} \alpha & \beta \\ \alpha & -\beta \end{pmatrix} = \begin{pmatrix} \frac{-a}{2} & \frac{\sqrt{-\Delta}}{2} \\ \frac{-a}{2} & -\frac{\sqrt{-\Delta}}{2} \end{pmatrix}.$$

Então,

$$\det(M) = \frac{a\sqrt{-\Delta}}{4} + \frac{a\sqrt{-\Delta}}{4} = \frac{a\sqrt{-\Delta}}{2},$$

como queríamos mostrar. ■

Exemplo 4.2.1 *Sejam $f(x) = x^2 + x + 3$ um polinômio de grau 2 com raízes complexas conjugadas $\alpha + i\beta, \alpha - i\beta \in \mathbb{C}$. Temos que: $\Delta = 1^2 - 4.3 = -11 < 0$. Assim, se Λ_f é o reticulado com base $\{(\alpha, \beta), (\alpha, -\beta)\}$ e matriz geradora M, segue pela Proposição (4.2.1) que*

$$\det(M) = \frac{a\sqrt{-\Delta}}{2} = \frac{\sqrt{11}}{2}.$$

Vejamos agora um resultado que nos dá uma expressão para o cálculo da norma de um vetor de Λ_f.

Proposição 4.2.2 *([26]) Se $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes complexas conjugadas $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$, Λ_f é o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Q}$, então,*

$$|v|^2 = \frac{a^2}{4}({z_1}^2 + {z_2}^2) + \frac{4b - a^2}{4}(z_1 - z_2)^2.$$

Demonstração: Sejam $\gamma_1 = \alpha + i\beta$ e $\gamma_2 = \alpha - i\beta$, com $\alpha, \beta \in \mathbb{R}$ e $\beta \neq 0$ as raízes de f e $v = z_1v_1 + z_2v_2$, com $v_1 = (\alpha, \beta)$, $v_2 = (\alpha, -\beta)$ e $z_1, z_2 \in \mathbb{Q}$. Temos que:

$$v = z_1(\alpha, \beta) + z_2(\alpha, -\beta) = (\alpha(z_1 + z_2), \beta(z_1 - z_2)).$$

Logo,

$$\begin{aligned} |v|^2 &= \alpha^2(z_1 + z_2)^2 + \beta^2(z_1 - z_2)^2 \\ &= \left(\frac{-a}{2}\right)^2 (z_1 + z_2)^2 + \left(\frac{\sqrt{-\Delta}}{2}\right)^2 (z_1 - z_2)^2 \\ &= \frac{a^2}{4}(z_1 + z_2)^2 + \frac{4b - a^2}{4}(z_1 - z_2)^2, \end{aligned}$$

como queríamos mostrar. ■

Exemplo 4.2.2 *Nas condições do Exemplo (4.2.1), seja $v = z_1v_1 + z_2v_2 \in \Lambda_f$. Pela Proposição (4.2.2) segue que*

$$|v|^2 = \frac{({z_1}^2 + {z_2}^2) + 11(z_1 - z_2)^2}{4}$$

e, este vetor assume o valor mínimo 1 quando tomamos $z_1 = 1$ e $z_2 = 0$. Logo, $\rho = \frac{1}{2}$ e portanto,

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det(M)|} = \frac{\left(\frac{1}{2}\right)^2}{\left|\frac{\sqrt{11}}{2}\right|} = \frac{1}{2\sqrt{11}}.$$

Com o seguinte teorema, temos novamante um família de reticulados de posto 2 com densidade de centro otima.

Teorema 4.2.1 *([26]) Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes complexas conjugadas $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$, Λ_f o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$. Se f satisfaz a condição $a^2 = b$, então o reticulado Λ_f possui densidade de centro ótima.*

Demonstração: Seja $f(x) = x^2 + ax + b$, $a, b \in \mathbb{Z}$ tal que $a^2 = b$ e seja $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Q}$ um vetor de Λ_f. Pela Proposição (4.2.2) temos que

$$\begin{aligned} |v|^2 &= \frac{a^2}{4}({z_1}^2 + {z_2}^2) + \frac{4b - a^2}{4}(z_1 - z_2)^2 \\ &= \frac{b}{4}({z_1}^2 + {z_2}^2) + \frac{3b}{4}(z_1 - z_2)^2. \end{aligned}$$

Observe que esta forma quadrática assume valor mínimo b quando $z_1 = 1$ e $z_2 = 0$. Logo,

$$\rho = \frac{\Lambda_{min}}{2} = \frac{\sqrt{b}}{2}. \tag{4.2.6}$$

Agora, pela Proposição (4.2.1), temos

$$|\det(M)| = \left|\frac{a\sqrt{-(a^2-4b)}}{2}\right| = \sqrt{b}\sqrt{3b} = b\sqrt{3}. \tag{4.2.7}$$

Por, (4.2.6) e (4.2.7) segue que a densidade de centro de Λ_f será dada por

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det(M)|} = \frac{(\frac{\sqrt{b}}{2})^2}{b\sqrt{3}} = \frac{b}{2b\sqrt{3}} = \frac{1}{2\sqrt{3}} \cong 0,28868,$$

que é a mesma densidade de centro do reticulado Λ_2. Portanto, Λ_f possui densidade de centro ótima para dimensão 2. ■

Exemplo 4.2.3 *Sejam $f(x) = x^2 + x + 1$, $\alpha \pm i\beta \in \mathbb{C}$ as raízes de f e $v = z_1v_1 + z_2v_2 \in \Lambda_f$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$. Temos que: $|v|^2 = \frac{1}{4}({z_1}^2 + {z_2}^2) + \frac{3}{4}(z_1 - z_2)^2$, que assume o valor mínimo 1, quando $z_1 = 1$ e $z_2 = 0$. Logo*

$$\rho = \frac{1}{2}.$$

Temos ainda que

$$|\det(M)| = \left|\frac{a\sqrt{-(a^2-4b)}}{2}\right| = \frac{\sqrt{3}}{2}.$$

Portanto,

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det(M)|} = \frac{\left(\frac{\sqrt{1}}{2}\right)}{\frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}} \cong 0,28868,$$

que é a densidade ótima para dimensão 2.

4.3 Reticulados de dimensão 3 via polinômios de grau 3 com raízes reais

Nosso objetivo nesta seção é obter reticulados rotacionados do reticulado Λ_3 via polinômios de grau 3 com raízes reais. Sejam $f(x) = x^3 + ax^2 + bx + c$ com $a, b, c \in \mathbb{Z}$ e $\alpha, \beta, \gamma \in \mathbb{C}$ as raízes de f. Queremos que f possua somente raízes reais. Iniciamos mostrando um resultado que nos garante esta condição.

Proposição 4.3.1 *([26]) Seja $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Para que as raízes de f sejam reais é necessário e suficiente que*

$$a^2 - 3b > 0 \quad e \quad (\sqrt{a^2-3b})^3 > \left|\frac{2a^2 - 9ab + 27c}{2}\right|.$$

Demonstração: Uma condição necessária e suficiente para que as raízes de f sejam todas reais é que sua derivada se anule em dois pontos distintos e que a função f aplicada nestes pontos tenham sinais distintos. Assim, se $f(x) = x^3 + ax^2 + bx + c$, com $a, b, c \in \mathbb{Z}$ temos que sua derivada é dada por $f'(x) = 3x^2 + 2ax + b$ cujas raízes são

$$x_1 = \frac{-a - \sqrt{a^2 - 3b}}{3} \quad \text{e} x_2 = \frac{-a + \sqrt{a^2 - 3b}}{3}.$$

Daí, segue que $a^2 - 3b > 0$ deve ser um número positivo. Agora,

$$\begin{aligned} f(x_1) &= x_1^2 + ax_1^2 + bx_1 + c \\ &= \left(\frac{-a - \sqrt{a^2 - 3b}}{3}\right)^3 + a\left(\frac{-a - \sqrt{a^2 - 3b}}{3}\right)^2 + b\left(\frac{-a - \sqrt{a^2 - 3b}}{3}\right) + c \\ &= \frac{1}{27}(2a^3 + 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c) \end{aligned}$$

e, portanto, $f(x_1) > 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > \frac{2a^2 - 9ab + 27c}{2}.$$

Analogamente,

$$f(x_2) = \frac{1}{27}(2a^3 + 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c)$$

e, portanto, $f(x_2) < 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > \frac{2a^2 - 9ab + 27c}{2}.$$

Logo, para que as raízes de f sejam reais devemos ter

$$a^2 - 3b > 0 \ \text{ e } \ (\sqrt{a^2 - 3b})^3 > \left|\frac{2a^2 - 9ab + 27c}{2}\right|,$$

como queríamos. ■

Sejam $\alpha, \beta, \gamma \in \mathbb{R}$ as raízes de $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ que satisfazem as condições da Proposição (4.3.1) e

$$\begin{cases} v_1 = (\alpha, \beta, \gamma) \\ v_2 = (\gamma, \alpha, \beta) \\ v_3 = (\beta, \gamma, \alpha) \end{cases},$$

vetores do $\mathbb{R}^3$. Consideremos $\Lambda_f \subset \mathbb{R}^3$ o reticulado gerado pela base $\{v_1, v_2, v_3\}$, onde v_1, v_2 e v_3 são como definidos acima. Temos que uma matriz geradora de Λ_f será

$$M = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{pmatrix} \tag{4.3.8}$$

e sua densidade de centro será dada por:

$$\delta(\Lambda_f) = \frac{\rho^3}{|det(M)|},$$

onde ρ é o raio de empacotamento de Λ_f.

Da mesma forma como para dimensão 2, queremos encontrar expressões para o calcular ρ e $\det(M)$. No resultado a seguir veremos uma expressão para o cálculo de $\det(M)$.

Proposição 4.3.2 *([26]) Se $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ com raízes reais α, β, γ e M é a matriz dada em (4.3.8), então o determinante de M é dado por*

$$\det(M) = -a(a^2 - 3b).$$

Demonstração: Temos que o determinante de M será dado por

$$\det(M) = \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma.$$

Das relações de Girard segue que:

$$\begin{cases} \alpha + \beta + \gamma = -a \\ \alpha\beta + \alpha\gamma + \beta\gamma = b \\ \beta\gamma\alpha = -c \end{cases},$$

assim,

$$(\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) = a^2,$$

logo,

$$\alpha^2 + \beta^2 + \gamma^2 = a^2 - 2b. \tag{4.3.9}$$

Como $\alpha + \beta + \gamma = -a$, multiplicando o lado esquerdo da Equação (4.3.9) por $\alpha + \beta + \gamma$ e o lado direito por $-a$ teremos

$$\alpha^3 + \beta^3 + \gamma^3 + \alpha\beta^2 + \beta\alpha^2 + \beta\gamma^2 + \gamma\alpha^2 + \gamma\beta^2$$

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

Logo,

$$\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma = -a(a^2-2b)+ab = -a^3+3ab.$$

Portanto, $\det(M) = -a(a^2-3b)$ o que prova a proposição. ∎

Exemplo 4.3.1 *Sejam $f(x) = x^3-9x^2+23x-15$ um polinômio de grau 3 com raízes reais α,β,γ. Se Λ_f é o reticulado com base $\{v_1,v_2,v_3\}$ e matriz geradora M, segue pela Proposição (4.3.2) que*

$$\det(M) = -a(a^2-3b) = 108.$$

Agora, veremos um resultado que nos dará uma expressão para o cálculo da norma de um vetor de Λ_f.

Proposição 4.3.3 *([26]) Se $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$ com raízes reais α,β,γ, Λ_f é o reticulado de dimensão 3 gerado pela base $\{v_1,v_2,v_3\}$, onde $v_1 = (\alpha,\beta,\gamma)$, $v_2 = (\gamma,\alpha,\beta)$, $v_3 = (\beta,\gamma,\alpha)$, e $v \in \Lambda_f$, tal que $v = z_1v_1+z_2v_2+z_3v_3$, com $z_1,z_2,z_3 \in \mathbb{Q}$. Então,*

$$|v|^2 = (a^2-2b)(z_1^2+z_2^2+z_3^2)+2b(z_1z_2+z_1z_3+z_2z_3).$$

Demonstração: Temos que:

$$
\begin{aligned}
v &= z_1v_1+z_2v_2+z_3v_3\\
&= z_1(\alpha,\beta,\gamma)+z_2(\gamma,\alpha,\beta)+z_3(\beta,\gamma,\alpha)\\
&= (\alpha z_1+\gamma z_2+\beta z_3, \beta z_1+\alpha z_2+\gamma z_3, \gamma z_1+\beta z_2+\alpha z_3).
\end{aligned}
$$

Então,

$$
\begin{aligned}
|v|^2 &= (\alpha z_1+\gamma z_2+\beta z_3)^2+(\beta z_1+\alpha z_2+\gamma z_3)^2+(\gamma z_1+\beta z_2+\alpha z_3)^2\\
&= (\alpha^2+\beta^2+\gamma^2)(z_1^2+z_2^2+z_3^2)+2(\alpha\beta+\alpha\gamma+\beta\gamma)(z_1z_2+z_1z_3+z_2z_3)\\
&= (a^2-2b)(z_1^2+z_2^2+z_3^2)+2b(z_1z_2+z_1z_3+z_2z_3),
\end{aligned}
$$

como queríamos mostrar. ∎

Exemplo 4.3.2 *Nas condições do Exemplo (4.3.1), seja $v = z_1v_1+z_2v_2+z_3v_3 \in \Lambda_f$. Pela*

Proposição (4.3.3) segue que

$$|v|^2 = 35(z_1^2 + z_2^2 + z_3^2) + 46(z_1z_2 + z_1z_3 + z_2z_3)$$

e, este vetor assume o valor mínimo 24 *quando tomamos* $z_1 = 1$, $z_2 = -1$ *e* $z_3 = 0$. *Logo,* $\rho = \frac{\sqrt{24}}{2}$ *e portanto,*

$$\delta(\Lambda_f) = \frac{\rho^3}{|\det(M)|} = \frac{(\sqrt{6})^3}{108} = \frac{\sqrt{6}}{18}.$$

Teorema 4.3.1 *([26]) Sejam* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ *com raízes reais* α, β, γ, Λ_f *o reticulado de dimensão* 3 *gerado pela base* $\{v_1, v_2, v_3\}$, *onde* $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$, $v_3 = (\beta, \gamma, \alpha)$. *Se* f *satisfaz*

$$\left(\frac{a}{2}\right)^2 = b \quad e \quad c(27c + 4a^3 - 18ab) < 0,$$

então o reticulado Λ_f *possui densidade de centro ótima.*

Demonstração: Pela Proposição (4.3.3) temos que

$$\begin{aligned} |v|^2 &= (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_1z_3 + z_2z_3) \\ &= 2b(z_1^2 + z_2^2 + z_3^2 + z_1z_2 + z_1z_3 + z_2z_3). \end{aligned}$$

Observe que esta forma quadrática assume valor mínimo $2b$ quando $z_1 = 1$ e $z_2 = z_3 = 0$. Logo,

$$\rho = \frac{\Lambda_{min}}{2} = \frac{\sqrt{2b}}{2}. \tag{4.3.10}$$

Agora, pela Proposição (4.3.2), temos

$$|\det(M)| = |-a(a^2 - 3b)| = |ab|. \tag{4.3.11}$$

Por, (4.3.10) e (4.3.11) segue que a densidade de centro de Λ_f será dada por

$$\delta(\Lambda_f) = \frac{\rho^3}{|\det(M)|} = \frac{(\frac{\sqrt{2b}}{2})^3}{|ab|} = \frac{1}{4\sqrt{2}} \cong 0,17678,$$

que é a mesma densidade de centro do reticulado Λ_3. Portanto, Λ_f possui densidade de centro ótima para dimensão 3. ∎

Exemplo 4.3.3 *Sejam* $f(x) = x^3 - 6x^2 + 9x - 1$ *com raízes reais* α, β, γ, Λ_f *um reticulado de dimensão* 3 *gerado pela base* $\{v_1, v_2, v_3\}$, *onde* $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$, $v_3 = (\beta, \gamma, \alpha)$, *e*

$v \in \Lambda_f$, *tal que* $v = z_1v_1 + z_2v_2 + z_3v_3$, *com* $z_1, z_2, z_3 \in \mathbb{Q}$. *Temos que:* $|v|^2 = 18(z_1^2 + z_2^2 + z_3^2) + 18(z_1z_2 + z_1z_3 + z_2z_3)$, *que assume o valor mínimo* 18, *quando* $z_1 = 1$ *e* $z_2 = z_3 = 0$. *Logo,*

$$\rho = \frac{\sqrt{18}}{2} = \frac{3\sqrt{2}}{2}.$$

Temos ainda que

$$|det(M)| = |-a(a^2 - 3b)| = 54.$$

Portanto,

$$\delta(\Lambda_f) = \frac{\rho^3}{|\det(M)|} = \frac{\frac{3\sqrt{2}}{2}}{54} = \frac{\sqrt{2}}{8} = \frac{1}{4\sqrt{2}} \cong 0,17678,$$

que é a densidade de centro ótima para essa dimensão.

4.4 Conclusão do capítulo

Neste capítulo apresentamos uma forma de encontrar reticulados de dimensões 2 e 3 utilizando polinômios irredutíveis em $\mathbb{Q}$ de graus 2 e 3, respectivamente. Nos resultados (4.1.1), (4.2.1) e (4.3.1) mostramos que através deste método é possível obter reticulados com densidade de centro ótima para dimensões 2 e 3 via polinômios. Acreditamos que, da mesma forma como foi feito para dimensões 2 e 3, pode-se obter reticulados com densidade de centro ótima para dimensões maiores. O grande desafio desse método é determinar a matriz geradora do reticulado através das raízes do polinômio em questão e também minimizar a forma quadrática, que repesenta o quadrado da norma de um vetor nesse reticulado.

Capítulo 5

Reticulados algébricos

No Capítulo (3) apresentamos o conceito de reticulados e vimos que podemos classificar os reticulados quanto a sua densidade de centro. Neste capítulo, apresentamos a geração de reticulados no $\mathbb{R}^n$ a partir do método de Minkowski fazendo uso de ideais do anel dos inteiros algébricos de um corpo de números. A partir do homomorfismo canônico (ou de Minkowski), Bayer em [6], definiu outros homomorfismos que neste trabalho chamamos de pertubarções do homomorfismo canônico. Na Seção (5.1) definiremos estes homomorfismos e veremos que pode-se obter reticulados tanto a partir do homomorfismo canônico quanto a partir de suas perturbações. Na Seção (5.2) apresentamos uma construção de reticulados rotacionados de dimensões 2, 4, 6, 8 e 12 dos reticulados já conhecidos A_2, D_4, E_6, E_8 e K_{12}, vistos no Capítulo (3), a partir das perturbações do homomorfismo canônico. Este método é um aperfeiçoamento do método utilizado por Ferrari em [11], quando obteve reticulados rotacionados de dimensões 2, 4, 6 e 8 apartir do homomorfismo canônico.

5.1 Reticulados via o homomorfismo canônico e suas perturbações

Nesta seção iremos definir o homomorfismo canônico e suas perturbações e, mostrar como obtemos reticulados a partir destes homomorfismos que, neste trabalho, chamaremos de reticulados algébricos.

5.1.1 Homomorfismo canônico

Iniciamos esta seção mostrando como podemos construir o homomorfismo canônico e depois colocamos sua definição propriamente dita. Após isto, mostramos que a partir deste homomorfismo podemos obter reticulados no $\mathbb{R}^n$.

Sejam $\mathbb{K}$ um corpo de números de grau n. Temos pelo Teorema (1.2.2) que existem exatamente n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$. Consideremos $\phi : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Assim, para todo $i = 1, \cdots, n$, temos que $\phi \circ \sigma_i = \sigma_k$, para algum $1 \leq k \leq n$

e, $\sigma_i = \sigma_k$ se, somente se, $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$. Desta forma, podemos ordenar os monomorfismos $\sigma_1, \cdots, \sigma_n$ de tal forma que até um determinado índice r_1 tenhamos $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ $(1 \leq i \leq r_1)$, ou seja, de modo que os monomorfismos $\sigma_1, \cdots, \sigma_{r_1}$ sejam reais e, os demais monomorfismos serão todos imaginários. Como os monomorfismos imaginários aparecem sempre aos pares, temos que o número $n - r_1$ é par e, assim, podemos escrever $n - r_1 = 2r_2$, ou seja, $n = r_1 + 2r_2$.

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

Definição 5.1.1 *Seja $x \in \mathbb{K}$. O homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por*

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

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

Exemplo 5.1.1 *Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, onde $i^2 = -1$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a + bi) = a - bi$, com $a, b \in \mathbb{Q}$. Neste caso, temos que $r_1 = 0$ e $r_2 = 1$, ou seja, $\mathbb{K}$ é um corpo totalmente imaginário. Para $x = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos*

$$\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b).$$

Exemplo 5.1.2 *Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$, com $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 2$ e $r_2 = 0$, ou seja, $\mathbb{K}$ é um corpo totalmente real. Para $x = a + b\sqrt{3} \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos*

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

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser formalmente obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$.

Nos resultados a seguir veremos como obter reticulados utilizando o homomorfismo canônico e também uma fórmula para calcularmos a densidade de centro destes reticulados.

Teorema 5.1.1 *([24]) Seja $\mathbb{K}$ um corpo de números de grau n. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $(x_j)_{1 \leq j \leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, com volume dado por:*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} |\det_{1 \leq j,k \leq n}(\sigma_j(x_k))|,$$

onde r_2 é o número de pares de monomorfismos imaginários.

Demonstração: Para melhor entendimento, faremos inicialmente a prova para $n = 3$. Seja $\{x_1, x_2, x_3\}$ uma $\mathbb{Z}$-base de M. Pelo homomorfismo canônico $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$, para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$, para $j = 1, 2, 3$, com respeito a base canônica do $\mathbb{R}^n$, são dadas por:

$$\sigma_{\mathbb{K}}(x_j) = (\sigma_1(x_j), \Re\sigma_2(x_j), \Im\sigma_2(x_j)). \tag{5.1.1}$$

Consideremos D como sendo o determinante da matriz cujas colunas são as coordenadas de (5.1.1).

$$D = \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ \Re(\sigma_2(x_1)) & \Re(\sigma_2(x_2)) & \Re(\sigma_2(x_3)) \\ \Im(\sigma_2(x_1)) & \Im(\sigma_2(x_2)) & \Im(\sigma_2(x_3)) \end{vmatrix}$$

Para o cálculo do determinante D, considere as seguintes fórmulas:

$$\Re(z) = \frac{1}{2}(z + \overline{z}) \text{ e } \Im(z) = \frac{1}{2}(z - \overline{z}), \tag{5.1.2}$$

para todo $z \in \mathbb{C}$. Assim,

$$D = \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ \frac{1}{2}[\sigma_2(x_1) + \overline{\sigma_2(x_1)}] & \frac{1}{2}[\sigma_2(x_2) + \overline{\sigma_2(x_2)}] & \frac{1}{2}[\sigma_2(x_3) + \overline{\sigma_2(x_3)}] \\ \frac{1}{2i}[\sigma_2(x_1) - \overline{\sigma_2(x_1)}] & \frac{1}{2i}[\sigma_2(x_2) - \overline{\sigma_2(x_2)}] & \frac{1}{2i}[\sigma_2(x_3) - \overline{\sigma_2(x_3)}] \end{vmatrix}$$

Por propriedades elementares de determinantes, podemos colocar em evidência $\frac{1}{2}$ que multiplica a 2º linha e $\frac{1}{2i}$ que multiplica a 3º linha. Deste modo,

$$D = \left(\frac{1}{2}\right)\left(\frac{1}{2i}\right) \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ \sigma_2(x_1) + \overline{\sigma_2(x_1)} & \sigma_2(x_2) + \overline{\sigma_2(x_2)} & \sigma_2(x_3) + \overline{\sigma_2(x_3)} \\ \sigma_2(x_1) - \overline{\sigma_2(x_1)} & \sigma_2(x_2) - \overline{\sigma_2(x_2)} & \sigma_2(x_3) - \overline{\sigma_2(x_3)} \end{vmatrix}.$$

Agora, somando a terceira linha na segunda linha teremos:

$$D = \left(\frac{1}{2}\right)\left(\frac{1}{2i}\right) \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ 2\sigma_2(x_1) & 2\sigma_2(x_2) & 2\sigma_2(x_3) \\ \sigma_2(x_1) - \overline{\sigma_2(x_1)} & \sigma_2(x_2) - \overline{\sigma_2(x_2)} & \sigma_2(x_3) - \overline{\sigma_2(x_3)} \end{vmatrix}$$

Colocando 2 que multiplica a segunda linha em evidência e em seguida subtraindo da segunda linha à terceira linha, segue que:

$$D = \left(\frac{1}{2}\right)\left(\frac{1}{2i}\right) 2 \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ \sigma_2(x_1) & \sigma_2(x_2) & \sigma_2(x_3) \\ \overline{\sigma_2(x_1)} & \overline{\sigma_2(x_2)} & \overline{\sigma_2(x_3)} \end{vmatrix}.$$

Como $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ para $i = 1, \cdots, r_2$ temos que $\overline{\sigma_2(x_j)} = \sigma_3(x_j)$, para $j = 1, 2, 3$. Daí,

$$D = \left(\frac{1}{2i}\right) \begin{vmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \sigma_1(x_3) \\ \sigma_2(x_1) & \sigma_2(x_2) & \sigma_2(x_3) \\ \sigma_3(x_1) & \sigma_3(x_2) & \sigma_3(x_3) \end{vmatrix} = \left(\frac{1}{2i}\right) \det_{1\leq j,k\leq 3}(\sigma_j(x_k)).$$

Como $\{x_1, x_2, x_3\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então pela Proposição (1.3.13) segue que $\det_{1\leq j,\, k\leq 3}(\sigma_j(x_k)) \neq 0$, e portanto $D \neq 0$. Assim, os vetores $\{\sigma_{\mathbb{K}}(x_1), \sigma_{\mathbb{K}}(x_2), \sigma_{\mathbb{K}}(x_3)\}$ do $\mathbb{R}^3$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$. Como por hipótese, $\{x_1, x_2, x_3\}$ formam uma $\mathbb{Z}$-base de M então dado $m \in M$, temos que $m = \sum_{j=1}^{3} a_j x_j,\ a_j \in \mathbb{Z}$. E, daí

$$\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{3} a_j \sigma_{\mathbb{K}}(x_j),\ a_j \in \mathbb{Z}.$$

Logo, $\sigma_{\mathbb{K}}(M) = \{\sum_{j=1}^{3} a_j \sigma_{\mathbb{K}}(x_j)\ :\ a_j \in \mathbb{Z}\}$ é um reticulado do $\mathbb{R}^3$, com volume dado por:

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = |D| = |2i^{-1}\det(\sigma_j(x_k))| = 2^{-1}|\det(\sigma_j(x_k))| = \frac{|det(\sigma_j(x_k))|}{2},$$

o que prova o resultado para $n = 3$. Veremos agora que o resultado é válido para todo n. Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$\sigma_{\mathbb{K}}(x_j) = (\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \quad (5.1.3)$$

Agora calculemos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (5.1.3) fazendo uso das fórmulas dadas em (5.1.2) e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)$-ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)$-ésima linha da sua posterior, para $l = 1, \ldots, r_2$. E, como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}},\ j = 1, \cdots, r_2$, temos que

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

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

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

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

$$= (2i)^{-r_2} \det(\sigma_j(x_k)).$$

Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue pela Proposição (1.3.13) que $\det(\sigma_j(x_k)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$, ou seja, $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$. Do fato de $\{x_1, \dots, x_n\}$ ser uma $\mathbb{Z}$-base de M, segue que $m = \sum_{j=1}^{n} a_j x_j$, com $a_j \in \mathbb{Z}$, e portanto, $m \in M$. Assim, $\sigma_{\mathbb{K}}(m) = \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j)$, com $a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}$. Portanto, $\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = |D| = 2^{-r_2} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|$. ∎

Corolário 5.1.1 *([24]) Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathfrak{a})$ são reticulados, com volumes dados respectivamente por:*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2} |\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} \quad e \quad \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{a})) = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})).\mathcal{N}(\mathfrak{a}),$$

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

Demonstração: Pelo Teorema (1.3.3) temos que $\mathfrak{a}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n. Daí, pelo Teorema (5.1.1), segue que $\sigma_{\mathbb{K}}(\mathfrak{a})$ e $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}_{\mathbb{K}}$, o seu volume será

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

pois pela Proposição (1.3.13) temos que $\mathcal{D}_{\mathbb{K}} = \det(\sigma_i(x_k))^2$. Para calcularmos o volume de $\sigma_{\mathbb{K}}(\mathfrak{a})$, observe que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ cujo índice é dado por $\mathcal{N}(\mathfrak{a})$ uma vez que $\mathcal{O}_{\mathbb{K}}/\mathfrak{a} \simeq \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})/\sigma_{\mathbb{K}}(\mathfrak{a})$. Além disso, como a região fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de

$\mathcal{N}(\mathfrak{a})$ cópias de uma região fundamental de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, segue que

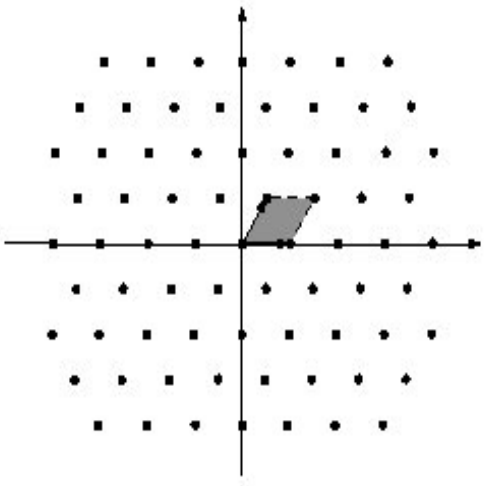
$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a}) = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))\mathcal{N}(\mathfrak{a}),$$

o que conclui a demonstração. ■

Exemplo 5.1.3 *Seja o corpo quadrático* $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. *Pelo Teorema (1.4.1) temos que seu anel dos inteiros é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ *com* $\mathbb{Z}$*-base* $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$. *Como* $\mathbb{K}$ *é totalmente imaginário, segue que* $r_1 = 0$ *e* $r_2 = 1$. *Assim, dado* $x = a + b(\frac{1+\sqrt{-3}}{2})$ *temos que a imagem do homomorfismo canônico* $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{R}^2$ *é dado por*

$$\begin{aligned}
\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) &= (\Re[\sigma_1(a + b(\frac{1+\sqrt{-3}}{2}))], \Im[\sigma_1(a + b(\frac{1+\sqrt{-3}}{2}))]) \\
&= (\Re[a + \frac{b}{2} + \frac{\sqrt{3}b}{2}i], \Im[a + \frac{b}{2} + \frac{\sqrt{3}b}{2}i]) \\
&= (a + \frac{b}{2}, \frac{\sqrt{3}b}{2}).
\end{aligned}$$

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



e cujo volume é dador por

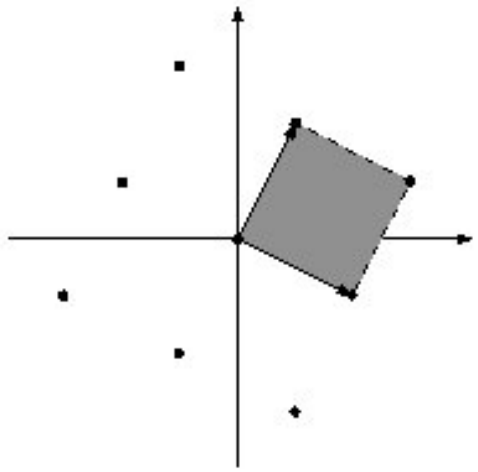
$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2}\left|\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\frac{1+\sqrt{-3}}{2}) \\ \sigma_2(1) & \sigma_2(\frac{1+\sqrt{-3}}{2}) \end{pmatrix}\right| = \frac{1}{2}\left|\det\begin{pmatrix} 1 & \frac{1+\sqrt{-3}}{2} \\ 1 & \frac{1-\sqrt{-3}}{2}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

Exemplo 5.1.4 *Seja o corpo quadrático* $\mathbb{K} = \mathbb{Q}(i)$, *onde* $i^2 = -1$. *Pelo Teorema (1.4.1) temos que seu anel dos inteiros é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ *(anel dos inteiros de Gauss) com* $\mathbb{Z}$*-base* $\{1, i\}$. *Como* $\mathbb{K}$

é totalmente imaginário, segue que $r_1 = 0$ *e* $r_2 = 1$. *Seja* $\mathfrak{a} = \langle 2 - i \rangle$ *um ideal principal de* $\mathbb{Z}[i]$. *Assim, dado* $x \in \mathfrak{a}$, *temos que* $x = (2 - i)(a + bi) = (2a + b) + (2b - a)i$, *onde* $a, b \in \mathbb{Z}$. *Logo, a imagem do homomorfismo canônico* $\sigma_{\mathbb{K}}(\mathfrak{a}) \subseteq \mathbb{R}^2$ *é dado por*

$$\begin{aligned} \sigma_{\mathbb{K}}(\mathfrak{a}) &= (\Re[\sigma_1((2a + b) + (2b - a)i)], \Im[\sigma_1((2a + b) + (2b - a)i)]) \\ &= (2a + b, 2b - a). \end{aligned}$$

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



O volume $\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$ *é dado por*

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

e pelo Teorema (1.3.4) temos que $\mathcal{N}(\mathfrak{a}) = |\mathcal{N}(2 - i)| = 5$. *Portanto,*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{a})) = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})).\mathcal{N}(\mathfrak{a}) = 1.5 = 5.$$

Observação 5.1.1 *Como consequência dos resultados anteriores, podemos obter uma expressão para o cálculo da densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *a partir da expressão dada em (3.3.4). Temos que:*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{a})))^n}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})}, \tag{5.1.4}$$

onde $\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \dfrac{1}{2} \min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$.

Nosso objetivo nos resultados que veremos a seguir é melhorar a expressão (5.1.4).

Proposição 5.1.1 *([8]) Se $\mathbb{K}$ é um corpo de números de grau n e $x \in \mathbb{K}$, então*

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

onde

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

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

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

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

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

Observe que

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

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

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

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

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

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

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

e, como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, segue que $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}Tr(x\overline{x})$. Agora, se $r_2 = 0$, ou seja, $\mathbb{K}$ for um corpo totalmente real, teremos

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

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

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

Logo,

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

o que conclui a demonstração. ∎

Observação 5.1.2 *Pela Proposição (5.1.1) temos que*

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

pode ser escrito da seguinte forma:

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

onde

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

Na Proposição (5.1.2) veremos que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ será a mesma tanto se $\mathbb{K}$ for totalmente real ou totalmente imaginário.

Proposição 5.1.2 *([11]) Seja $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário. Se $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$ e $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ é dada por:*

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

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

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

Observação (5.1.2) temos que

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

E, como $t = min\{Tr(x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$ segue que $\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2}\sqrt{t}$. Assim, pela Equação (5.1.4) tem-se que

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

Agora, suponhamos que $\mathbb{K}$ seja um corpo totalmente imaginário. Pela Observação (5.1.2) temos que

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

Além disso, como $r_1 = 0$ e $= r_1 + 2r_2$ segue que $r_2 = \frac{n}{2}$. Assim, pela Equação (5.1.4) temos que

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

Portanto, se $\mathbb{K}$ for um corpo totalmente real ou totalmente imaginário temos que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ será dada por

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

como queríamos provar. ■

Exemplo 5.1.5 *Seja o corpo quadrático* $\mathbb{K} = \mathbb{Q}(\sqrt{-17})$. *Pelo Teorema (1.4.1) temos que* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-17}]$ *e pelo Teorema (1.4.3)* $\mathcal{D}_{\mathbb{K}} = -68$. *Assim, se* $x \in \mathcal{O}_{\mathbb{K}}$, *então*

$$x = a + b\sqrt{-17} = a + b\sqrt{17}i$$

e

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

Logo, $Tr(x\overline{x}) = 2(a^2 + 17b^2)$ *e então* $t = 2$, *quando* $a = 1\,e\,b = 0$. *Assim*

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

5.1.2 Perturbação σ_α

Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \cdots, \sigma_n$ os homomorfismos de $\mathbb{K}$ em $\mathbb{C}$, ordenados de modo que σ_i é real para $i = 1, \cdots, r_1$ e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ para $j = 1, \cdots, r_2$, onde r_2 representa a metade dos homomorfismos imaginários e $r_1 + 2r_2 = n$. Nesta seção apresentamos a perturbação σ_α do homomorfismo canônico. Temos que esta perturbação também irá gerar reticulados no $\mathbb{R}^n$ e, partir dela, iremos obter reticulados rotacionados de dimensões 2, 4, 6, 8 e 12.

Definição 5.1.2 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \cdots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Um elemento $\alpha \in \mathbb{K}$ tal que $\sigma_i(\alpha) \in \mathbb{R}^+$, para todo $i = 1, \cdots, n$, é chamado de* **totalmente positivo**.

Definição 5.1.3 *Seja $\alpha \in \mathbb{K}$ totalmente positivo. A* **perturbação $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ do homomorfismo canônico** *(ou de Minkowski) é definida como*

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

onde as notações $\Re(y)$ e $\Im(y)$ representam as partes real e imaginária de um número complexo y, respectivamente.

Teorema 5.1.2 *([11]) Seja $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, \cdots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, com volume dado por:*

$$\mathcal{V}ol(\sigma_\alpha(M)) = b_\alpha |\det_{1 \leq j,\, k \leq n}(\sigma_j(x_k))|,$$

onde

$$b_\alpha = \begin{cases} (\mathcal{N}(\alpha))^{\frac{1}{2}}, \text{ se } \mathbb{K} \text{ for totalmente real} \\ 2^{\frac{-n}{2}}(\mathcal{N}(\alpha))^{\frac{1}{2}}, \text{ se } \mathbb{K} \text{ for totalmente imaginário,} \end{cases}$$

e, $\mathcal{N}(\alpha)$ é a norma do elemento α.

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

$$\sigma_\alpha(x) = (\sqrt{\alpha_i}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \ldots, \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))), \quad (5.1.5)$$

onde $\alpha_i = \sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2, \ldots, r_1 + r_2$ e $\alpha \in \mathbb{K}$. O determinante D da matriz cuja j-ésima coluna dada pela Equação (5.1.5) é dado por:

$$D = \begin{vmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \dots & \sqrt{\alpha_1}\sigma_1(x_j) & \dots & \sqrt{\alpha_1}\sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_j) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) \\ \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_1)) & \dots & \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_j)) & \dots & \Re(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_n)) \\ \Im(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_1)) & \dots & \Im(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_j)) & \dots & \Im(\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_1)) & \dots & \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_j)) & \dots & \Re(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_n)) \\ \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_1)) & \dots & \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_j)) & \dots & \Im(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_n)) \end{vmatrix}.$$

Utilizando as fórmulas dadas em (5.1.2) e depois, como $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$, colocando em evidência cada $\sqrt{\alpha_i}$ que multiplica a i-ésima linha além de $\frac{1}{2}$ e $\frac{1}{2i}$, temos

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

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

onde

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

Por propriedades elementares de determinantes, a saber, adição da (r_1+2l)-ésima linha à sua anterior e em seguida colocando 2 evidência que multiplica a (r_1+2l-1)-ésima linha e, pela subtração da (r_1+2l-1)-ésima linha à sua posterior, onde $l=1,\cdots,r_2$, temos

$$D=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}\alpha_{r_1+1}\cdots\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n)\\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n)\\ \dfrac{\sigma_{r_1+1}(x_1)}{\sigma_{r_1+1}(x_1)} & \dots & \dfrac{\sigma_{r_1+1}(x_j)}{\sigma_{r_1+1}(x_j)} & \dots & \dfrac{\sigma_{r_1+1}(x_n)}{\sigma_{r_1+1}(x_n)}\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \dfrac{\sigma_{r_1+r_2}(x_1)}{\sigma_{r_1+r_2}(x_1)} & \dots & \dfrac{\sigma_{r_1+r_2}(x_j)}{\sigma_{r_1+r_2}(x_j)} & \dots & \dfrac{\sigma_{r_1+r_2}(x_n)}{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

Como $\sigma_{r_1+r_2+j}=\overline{\sigma_{r_1+j}},\ j=1,\cdots,r_2$, temos que

$$D=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}\alpha_{r_1+1}\cdots\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n)\\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n)\\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n)\\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}$$

$$=(2i)^{-r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}\alpha_{r_1+1}\cdots\alpha_{r_1+r_2}\det_{1\leq j,\,k\leq n}(\sigma_j(x_k)).$$

Como $\{x_1,\cdots,x_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue pela Proposição (1.3.13) que $\det(\sigma_j(x_k))\neq 0$, e portanto, $D\neq 0$. Assim, os vetores $\sigma_\alpha(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_\alpha(M)$ e, para cada $m\in M$ temos que $m=\sum_{j=1}^{n}a_jx_j$, com $a_j\in\mathbb{Z}$. Assim, $\sigma_\alpha(m)=\sum_{j=1}^{n}a_j\sigma_\alpha(x_j)$, com $a_j\in\mathbb{Z}$, ou seja, $\sigma_\alpha(M)=\left\{\sum_{j=1}^{n}a_j\sigma_\alpha(x_j);\ a_j\in\mathbb{Z}\right\}$ é um reticulado e,

$$\mathcal{V}ol(\sigma_\alpha(M))=\ |D|=2^{-r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}\alpha_{r_1+1}\cdots\alpha_{r_1+r_2}|\det_{1\leq j,\,k\leq n}(\sigma_j(x_k))|.$$

Agora, temos dois casos a considerar:

1. Se $r_2 = 0$ então

$$\begin{aligned}\mathcal{V}ol(\sigma_\alpha(M)) &= \sqrt{\alpha_1 \cdots \alpha_{r_1}} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))| \\ &= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^{\frac{1}{2}} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))| \\ &= (\mathcal{N}(\alpha))^{\frac{1}{2}} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|.\end{aligned}$$

2. Se $r_1 = 0$ então

$$\mathcal{V}ol(\sigma_\alpha(M)) = \prod_{i=1}^{r_2} \sigma_i(\alpha) |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|.$$

Como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}},\ j = 1, \cdots, r_2$, segue que $\sigma_{r_2+j}(\alpha) = \overline{\sigma_j(\alpha)} = \sigma_j(\alpha)$ pois $\sigma_j(\alpha) \in \mathbb{R}$. Assim, $\prod_{i=1}^{r_2} \sigma_i(\alpha) = (\mathcal{N}(\alpha))^{\frac{1}{2}}$ e como $n = 2r_2$ segue que

$$\mathcal{V}ol(\sigma_\alpha(M)) = 2^{\frac{-n}{2}} (\mathcal{N}(\alpha))^{\frac{1}{2}} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|,$$

o que prova o teorema. ∎

Corolário 5.1.2 *([11]) Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathcal{D}_\mathbb{K}$ é o discriminante de $\mathbb{K}$, $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ e $\sigma_\alpha(\mathfrak{a})$ são reticulados, com respectivos volumes,*

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = b_\alpha |\mathcal{D}_\mathbb{K}|^{\frac{1}{2}} \quad e \quad \mathcal{V}ol(\sigma_\alpha(\mathfrak{a})) = b_\alpha |\mathcal{D}_\mathbb{K}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a}),$$

onde b_α é como no Teorema (5.1.2), $\mathcal{N}(\alpha)$ é a norma do elemento α e $\mathcal{N}(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$.

Demonstração: Pelo Teorema (1.3.3) temos que $\mathfrak{a}$ e $\mathcal{O}_\mathbb{K}$ são $\mathbb{Z}$-módulos livres de posto n. Daí, pelo Teorema (5.1.2), segue que $\sigma_\alpha(\mathfrak{a})$ e $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ são reticulados do $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}_\mathbb{K}$, o seu volume será

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = b_\alpha |\mathcal{D}_\mathbb{K}|^{\frac{1}{2}},$$

pois pela Proposição (1.3.13) temos que $\mathcal{D}_\mathbb{K} = \det(\sigma_i(x_k))^2$. Para calcularmos o volume de $\sigma_\alpha(\mathfrak{a})$, observe que $\sigma_\alpha(\mathfrak{a})$ é um subgrupo de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ cujo índice é dado por $\mathcal{N}(\mathfrak{a})$, uma vez que $\mathcal{O}_\mathbb{K}/\mathfrak{a} \simeq \sigma_\alpha(\mathcal{O}_\mathbb{K})/\sigma_\alpha(\mathfrak{a})$. Além disso, como a região fundamental de $\sigma_\alpha(\mathfrak{a})$ é a união disjunta de

$\mathcal{N}(\mathfrak{a})$ cópias de uma região fundamental de $\sigma_\alpha(\mathcal{O}_\mathbb{K})$, segue que

$$\mathcal{V}ol(\sigma_\alpha(\mathfrak{a})) = b_\alpha|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a}) = \mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K}))\mathcal{N}(\mathfrak{a}),$$

o que conclui a demonstração. ■

Observação 5.1.3 *Como consequência dos resultados anteriores, podemos obter uma expressão para o cálculo da densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ a partir da expressão dada em (3.3.4). Assim*

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{(\rho(\sigma_\alpha(\mathfrak{a})))^n}{b_\alpha|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})}, \tag{5.1.6}$$

onde $\rho(\sigma_\alpha(\mathfrak{a})) = \dfrac{1}{2}\min\{|\sigma_\alpha(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$.

Temos como meta melhorar a expressão (5.1.6), para isto, faremos uso da Proposição (5.1.3) e da Observação (5.1.4) que veremos a seguir.

Proposição 5.1.3 *([11]) Se $\mathbb{K}$ é um corpo de números de grau n, $x \in \mathbb{K}$ e $\alpha \in \mathbb{K}$ totalmente positivo, então*

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

onde

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

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

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

Como $\sigma_\alpha(x) \in \mathbb{R}^n$, segue que

$$|\sigma_\alpha(x)|^2 = (\sqrt{\alpha_1}\sigma_1(x))^2 + \cdots + (\sqrt{\alpha_{r_1}}\sigma_{r_1}(x))^2 + (\sqrt{\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x))^2 + \cdots + (\sqrt{\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x))^2.$$

Observe que $[\Re(\sigma_j(x))]^2 + [\Im(\sigma_j(x))]^2 = \sigma_j(x)\overline{\sigma_j(x)} = \sigma_j(x\overline{x})$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Assim,

$$|\sigma_\alpha(x)|^2 = \alpha_1(\sigma_1(x))^2 + \cdots + \alpha_{r_1}(\sigma_{r_1}(x))^2 + \alpha_{r_1+1}\sigma_{r_1+1}(x\overline{x}) + \cdots + \alpha_{r_1+r_2}\sigma_{r_1+r_2}(x\overline{x}).$$

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

$$|\sigma_\alpha(x)|^2 = \alpha_1\sigma_1(x\overline{x}) + \cdots + \alpha_{r_2}\sigma_{r_2}(x\overline{x})$$

$$\begin{aligned} &= \sigma_1(\alpha)\sigma_1(x\overline{x}) + \cdots + \sigma_{r_2}(\alpha)\sigma_{r_2}(x\overline{x}) \\ &= \sigma_1(\alpha\overline{x(x)}) + \cdots + \sigma_{r_2}(\alpha\overline{x(x)}) \\ &= \sigma_{r_2+1}(\alpha x\overline{x}) + \cdots + \sigma_{r_2+r_2}(\alpha x\overline{x}) \end{aligned}$$

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

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

e, como os $\sigma_i(\alpha x\overline{x})$ são os conjugados de $\alpha x\overline{x}$, segue que $|\sigma_\alpha(x)|^2 = \dfrac{1}{2}Tr(\alpha x\overline{x})$. Agora, se $r_2 = 0$, ou seja, $\mathbb{K}$ for um corpo totalmente real, teremos

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

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

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

Logo,

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

o que conclui a demonstração. ∎

Observação 5.1.4 *Pela Proposição (5.1.3) temos que*

$$\rho(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2}\min\{|\sigma_\alpha(x)|,\ x\in\mathfrak{a},\ x\neq 0\}$$

pode ser escrito da seguinte forma:

$$\rho(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2}\min\{\sqrt{c_\alpha Tr(\alpha x\overline{x})},\ x\in\mathfrak{a},\ x\neq 0\},$$

onde

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

Na Proposição (5.1.4) veremos que a densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ será a mesma se $\mathbb{K}$ for totalmente real ou totalmente imaginário.

Proposição 5.1.4 *([11]) Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathcal{O}_\mathbb{K}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_\mathbb{K}$ o discriminante de $\mathbb{K}$ e $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então a densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ é dada por:*

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}}\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})},$$

onde $t_\alpha = \min\{Tr(\alpha x\overline{x}),\, x \in \mathfrak{a},\, x \neq 0\}$, $\mathcal{N}(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$ e $\mathcal{N}(\alpha)$ é a norma do elemento α.

Demosntração: Suponhamos que $\mathbb{K}$ seja um corpo totalmente real então temos que $r_2 = 0$, $b_\alpha = (\mathcal{N}(\alpha))^{\frac{1}{2}}$ e pela Observação (5.1.4) que

$$\rho(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2}\min\{\sqrt{Tr(\alpha x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0\}.$$

E, como $t_\alpha = min\{Tr(\alpha x\overline{x}),\, x \in \mathfrak{a},\, x \neq 0\}$ segue que $\rho(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2}\sqrt{t_\alpha}$. Assim, pela Equação (5.1.6) temos

$$\begin{aligned}\delta(\sigma_\alpha(\mathfrak{a})) &= \frac{(\frac{1}{2}\sqrt{t_\alpha})^n}{(\mathcal{N}(\alpha))^{\frac{1}{2}}|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} = \frac{2^{-n}(\sqrt{t_\alpha})^n}{(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} \\ &= \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}}\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}.\end{aligned}$$

Agora, suponhamos que $\mathbb{K}$ seja um corpo totalmente imaginário. Pela Observação (5.1.4) temos que

$$\rho(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2}\min\{\sqrt{\frac{1}{2}Tr(\alpha x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0\} = \frac{1}{2}\sqrt{\frac{1}{2}t}.$$

Além disso, $b_\alpha = 2^{\frac{-n}{2}}(\mathcal{N}(\alpha))^{\frac{1}{2}}$ e, como $r_1 = 0$ e $= r_1 + 2r_2$ segue que $r_2 = \frac{n}{2}$. Assim, pela Equação (5.1.6) temos:

$$\begin{aligned}\delta(\sigma_\alpha(\mathfrak{a})) &= \frac{\left(\frac{1}{2}\sqrt{\frac{1}{2}t_\alpha}\right)^n}{2^{\frac{-n}{2}}(\mathcal{N}(\alpha))^{\frac{1}{2}}|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} = \frac{(\frac{1}{2})^n(\frac{1}{2})^{\frac{n}{2}}t_\alpha^{\frac{n}{2}}}{2^{\frac{-n}{2}}(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} \\ &= \frac{(\frac{1}{2})^n t_\alpha^{\frac{n}{2}}}{(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}}\frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}.\end{aligned}$$

Portanto, se $\mathbb{K}$ for um corpo totalmente real ou totalmente imaginário temos que a densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ será dada por

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \frac{t_\alpha^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})},$$

como queríamos provar. ∎

5.1.3 Perturbação $\sigma_{2\alpha}$

Nesta seção apresentamos a perturbação $\sigma_{2\alpha}$ do homomorfismo canônico. Obteremos reticulados no $\mathbb{R}^n$ a partir desta perturbação e também iremos utilizá-la no Capítulo (6) para definirmos um reticulado ideal e para mostrar alguns resultados.

Definição 5.1.4 *Seja $\alpha \in \mathbb{K}$ totalmente positivo. A* **perturbação** $\sigma_{2\alpha} : \mathbb{K} \longrightarrow \mathbb{R}^n$ **do homomorfismo canônico** *(ou de Minkowski) é definida como*

$$\sigma_{2\alpha}(x) = (\sqrt{\alpha_i}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x)), \ldots, \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))),$$

onde notações $\Re(y)$ e $\Im(y)$ representam as partes real e imaginária de um número complexo y, respectivamente.

Teorema 5.1.3 *([11]) Seja $\mathbb{K}$ um corpo de números de grau n. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, \cdots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{2\alpha}(M)$ é um reticulado no $\mathbb{R}^n$, com volume dado por:*

$$\mathcal{V}ol(\sigma_{2\alpha}(M)) = (\mathcal{N}(\alpha))^{\frac{1}{2}} |\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|,$$

$\mathcal{N}(\alpha)$ é a norma do elemento α.

Demonstração: Para cada j fixado, as coordenadas de $\sigma_{2\alpha}(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$\sigma_{2\alpha}(x) = (\sqrt{\alpha_i}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \ldots, \Re(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)), \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x))), \tag{5.1.7}$$

onde $\alpha_i = \sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2, \ldots, r_1 + r_2$ e $\alpha \in \mathbb{K}$. O determinante D da matriz cuja j-ésima coluna dada pela Equação (5.1.7) é dado por:

$$D = \begin{vmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \dots & \sqrt{\alpha_1}\sigma_1(x_j) & \dots & \sqrt{\alpha_1}\sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_j) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) \\ \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x_1)) & \dots & \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x_j)) & \dots & \Re(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x_n)) \\ \Im(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x_1)) & \dots & \Im(\sqrt{2\alpha_{r_1+1}}\sigma_{r_1+1}(x_j)) & \dots & \Im(2\sqrt{\alpha_{r_1+1}}\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_1)) & \dots & \Re(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_j)) & \dots & \Re(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_n)) \\ \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_1)) & \dots & \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_j)) & \dots & \Im(\sqrt{2\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x_n)) \end{vmatrix}.$$

Utilizando as fórmulas dadas em (5.1.2) e depois, como $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$, colocando em evidência cada $\sqrt{\alpha_i}$ que multiplica a i-ésima linha além de $\frac{1}{2}$ e $\frac{1}{2i}$, temos que

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

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

onde

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

Por propriedades elementares de determinantes, a saber, adição da (r_1+2l)-ésima linha à sua anterior e em seguida colocando 2 evidência que multiplica a (r_1+2l-1)-ésima linha e, pela subtração da (r_1+2l-1)-ésima linha à sua posterior, onde $l=1,\cdots,r_2$, temos que

$$D=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}2\alpha_{r_1+1}\cdots 2\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n)\\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n)\\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n)\\ \overline{\sigma_{r_1+1}(x_1)} & \dots & \overline{\sigma_{r_1+1}(x_j)} & \dots & \overline{\sigma_{r_1+1}(x_n)}\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1+r_2}(x_1) & \dots & \sigma_{r_1+r_2}(x_j) & \dots & \sigma_{r_1+r_2}(x_n)\\ \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

Como $\sigma_{r_1+r_2+j}=\overline{\sigma_{r_1+j}},\ j=1,\cdots,r_2$, segue que

$$D=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}2\alpha_{r_1+1}\cdots 2\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n)\\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n)\\ \sigma_{r_1+1}(x_1) & \dots & \sigma_{r_1+1}(x_j) & \dots & \sigma_{r_1+1}(x_n)\\ \sigma_{r_1+2}(x_1) & \dots & \sigma_{r_1+2}(x_j) & \dots & \sigma_{r_1+2}(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1+2r_2}(x_1) & \dots & \sigma_{r_1+2r_2}(x_j) & \dots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}$$

$$=(2i)^{-r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}2\alpha_{r_1+1}\cdots 2\alpha_{r_1+r_2}\det_{1\leq j,\,k\leq n}(\sigma_j(x_k)).$$

Como $\{x_1,\cdots,x_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue pela Proposição (1.3.13), que $\det(\sigma_j(x_k))\neq 0$, e portanto, $D\neq 0$. Assim, os vetores $\sigma_{2\alpha}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{2\alpha}(M)$ e, para cada $m\in M$ temos que $m=\sum_{j=1}^{n}a_jx_j$, com $a_j\in\mathbb{Z}$. Assim, $\sigma_{2\alpha}(m)=\sum_{j=1}^{n}a_j\sigma_{2\alpha}(x_j)$, com $a_j\in\mathbb{Z}$, ou seja, $\sigma_{2\alpha}(M)=\left\{\sum_{j=1}^{n}a_j\sigma_{2\alpha}(x_j);\ a_j\in\mathbb{Z}\right\}$ é um reticulado e,

$$\mathcal{V}ol(\sigma_{2\alpha}(M))=\ |D|=2^{-r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}2\alpha_{r_1+1}\cdots 2\alpha_{r_1+r_2}|\det_{1\leq j,\,k\leq n}(\sigma_j(x_k))|.$$

Agora, temos dois casos a considerar:

1. Se $r_2 = 0$ então

$$\begin{aligned}\mathcal{V}ol(\sigma_{2\alpha}(M)) &= \sqrt{\alpha_1 \cdots \alpha_{r_1}}|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))| \\ &= \left(\prod_{i=1}^{n}\sigma_i(\alpha)\right)^{\frac{1}{2}}|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))| \\ &= (\mathcal{N}(\alpha))^{\frac{1}{2}}|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|.\end{aligned}$$

2. Se $r_1 = 0$ então

$$\mathcal{V}ol(\sigma_{2\alpha}(M)) = 2^{r_2}\prod_{i=1}^{r_2}2^{-r_2}\sigma_i(\alpha)|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|.$$

Como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}},\ j = 1, \cdots, r_2$, segue que $\sigma_{r_2+j}(\alpha) = \overline{\sigma_j(\alpha)} = \sigma_j(\alpha)$ pois $\sigma_j(\alpha) \in \mathbb{R}$. Assim, $\prod_{i=1}^{r_2}\sigma_i(\alpha) = (\mathcal{N}(\alpha))^{\frac{1}{2}}$ e portanto

$$\mathcal{V}ol(\sigma_{2\alpha}(M)) = (\mathcal{N}(\alpha))^{\frac{1}{2}}|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|,$$

como queríamos provar. ∎

Corolário 5.1.3 *([11]) Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha \in \mathbb{K}$. Se $\mathcal{D}_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{2\alpha}(\mathfrak{a})$ são reticulados, com respectivos volumes,*

$$\mathcal{V}ol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})) = (\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}} \quad e \quad \mathcal{V}ol(\sigma_{2\alpha}(\mathfrak{a})) = (\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a}),$$

onde $\mathcal{N}(\alpha)$ é a norma do elemento α e $\mathcal{N}(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$.

Demonstração: Pelo Teorema (1.3.3) temos que $\mathfrak{a}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n. Daí, pelo Teorema (5.1.3), segue que $\sigma_{2\alpha}(\mathfrak{a})$ e $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}_{\mathbb{K}}$, o seu volume será

$$\mathcal{V}ol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})) = (\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}},$$

pois pela Proposição (1.3.13) temos que $\mathcal{D}_{\mathbb{K}} = \det(\sigma_i(x_k))^2$. Para calcularmos o volume de $\sigma_{2\alpha}(\mathfrak{a})$, observe que $\sigma_{2\alpha}(\mathfrak{a})$ é um subgrupo de $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})$ cujo índice é dado por $\mathcal{N}(\mathfrak{a})$, uma vez

que $\mathcal{O}_{\mathbb{K}}/\mathfrak{a} \simeq \sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})/\sigma_{2\alpha}(\mathfrak{a})$. Além disso, como a região fundamental de $\sigma_{2\alpha}(\mathfrak{a})$ é a união disjunta de $\mathcal{N}(\mathfrak{a})$ cópias de uma região fundamental de $\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}})$, segue que

$$\mathcal{V}ol(\sigma_{2\alpha}(\mathfrak{a})) = (\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a}) = \mathcal{V}ol(\sigma_{2\alpha}(\mathcal{O}_{\mathbb{K}}))\mathcal{N}(\mathfrak{a}),$$

o que conclui a demonstração. ■

Definição 5.1.5 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ seu anel dos inteiros, $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ e, $\sigma_{\mathbb{K}}$, σ_α e $\sigma_{2\alpha}$ o homomorfismo canônico e suas perturbações. Os reticulados $\sigma_{\mathbb{K}}(\mathfrak{a})$, $\sigma_\alpha(\mathfrak{a})$ e $\sigma_{2\alpha}(\mathfrak{a})$, neste trabalho, serão chamados de* **reticulado algébrico**.

Observação 5.1.5 *Como consequência dos resultados anteriores, podemos obter uma expressão para o cálculo da densidade de centro do reticulado $\sigma_{2\alpha}(\mathfrak{a})$ a partir da expressão dada em (3.3.4). Temos que:*

$$\delta(\sigma_{2\alpha}(\mathfrak{a})) = \frac{(\rho(\sigma_{2\alpha}(\mathfrak{a})))^n}{\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})}, \tag{5.1.8}$$

onde $\rho(\sigma_{2\alpha}(\mathfrak{a})) = \dfrac{1}{2}\min\{|\sigma_{2\alpha}(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$.

Temos como meta melhorar a Expressão (5.1.8), a partir da Proposição (5.1.5) e da Observação (5.1.6) que veremos a seguir..

Proposição 5.1.5 *([11]) Se $\mathbb{K}$ é um corpo de números de grau n e $\alpha \in \mathbb{K}$ totalmente positivo, então*

$$|\sigma_{2\alpha}(x)|^2 = Tr(\alpha x\overline{x}),$$

onde $x \in \mathbb{K}$.

Demonstração: Sejam $\sigma_1, \cdots, \sigma_n$ os n monomorfismos de $\mathbb{K}$ de tal forma que $r_1 + 2r_2 = n$, onde r_1 são os monormorfismos reais e r_2 a metade dos monomorfismos imaginários. Assim, para $x \in \mathbb{K}$ temos pela perturbação $\sigma_{2\alpha}$ do homomorfismo canônico que

$$\sigma_{2\alpha}(x) = (\sqrt{\alpha_1}\sigma_1(x), \cdots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1}}\Re\sigma_{r_1+1}(x), \cdots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x)).$$

Como $\sigma_{2\alpha}(x) \in \mathbb{R}^n$, segue que

$$|\sigma_{2\alpha}(x)|^2 = (\sqrt{\alpha_1}\sigma_1(x))^2 + \cdots + (\sqrt{\alpha_{r_1}}\sigma_{r_1}(x))^2 + (\sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x))^2 + \cdots + (\sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x))^2.$$

Observe que $[\Re(\sigma_j(x))]^2 + [\Im(\sigma_j(x))]^2 = \sigma_j(x)\overline{\sigma_j(x)} = \sigma_j(x\overline{x})$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Assim,

$$|\sigma_{2\alpha}(x)|^2 = \alpha_1(\sigma_1(x))^2 + \cdots + \alpha_{r_1}(\sigma_{r_1}(x))^2 + 2\alpha_{r_1+1}\sigma_{r_1+1}(x\overline{x}) + \cdots + 2\alpha_{r_1+r_2}\sigma_{r_1+r_2}(x\overline{x}).$$

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

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

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

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

e, como os $\sigma_i(\alpha x\overline{x})$ são os conjugados de $\alpha x\overline{x}$, segue que $|\sigma_{2\alpha}(x)|^2 = \dfrac{1}{2}Tr(\alpha x\overline{x})$. Agora, se $r_2 = 0$, ou seja, $\mathbb{K}$ for um corpo totalmente real, teremos

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

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

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

Logo,

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

o que conclui a demonstração. ∎

Observação 5.1.6 *Pela Proposição (5.1.5) temos que*

$$\rho(\sigma_{2\alpha}(\mathfrak{a})) = \frac{1}{2}\min\{|\sigma_{2\alpha}(x)|,\ x \in \mathfrak{a},\ x \neq 0\}$$

pode ser escrito da seguinte forma:

$$\rho(\sigma_{2\alpha}(\mathfrak{a})) = \frac{1}{2}\min\{\sqrt{Tr(\alpha x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0\}.$$

Na Proposição (5.1.6) veremos que a densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ será a mesma se $\mathbb{K}$ for totalmente real ou totalmente imaginário.

Proposição 5.1.6 *([11]) Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário e $\alpha \in \mathbb{K}$ totalmente positivo. Se $\mathcal{O}_\mathbb{K}$ é o anel dos inteiros de $\mathbb{K}$, $\mathcal{D}_\mathbb{K}$ o discriminante de $\mathbb{K}$ e $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então a densidade de centro do reticulado $\sigma_{2\alpha}(\mathfrak{a})$ é dada por:*

$$\delta(\sigma_{2\alpha}(\mathfrak{a})) = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \frac{t_{2\alpha}^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})},$$

onde $t_{2\alpha} = \min\{Tr(\alpha x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$, $\mathcal{N}(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$ e $\mathcal{N}(\alpha)$ é a norma do elemento α.

Demosntração: Pela Observação (5.1.6) temos que

$$\rho(\sigma_{2\alpha}(\mathfrak{a})) = \frac{1}{2}\min\{\sqrt{Tr(\alpha x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0\}.$$

E, como $t_{2\alpha} = \min\{Tr(\alpha x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$ segue que $\rho(\sigma_{2\alpha}(\mathfrak{a})) = \frac{1}{2}\sqrt{t_{2\alpha}}$. Assim, pela Equação (5.1.8) temos

$$\delta(\sigma_{2\alpha}(\mathfrak{a})) = \frac{(\frac{1}{2}\sqrt{t_{2\alpha}})^n}{(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} = \frac{2^{-n}(\sqrt{t_{2\alpha}})^n}{(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}\mathcal{N}(\mathfrak{a})} = \frac{1}{2^n(\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|)^{\frac{1}{2}}} \frac{t_{2\alpha}^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})},$$

como queríamos provar. ∎

5.2 Uma construção de reticulados algébricos rotacionados de dimensões 2, 4, 6, 8 e 12 via a perturbação σ_α do homomorfismo canônico

Nesta seção apresentamos reticulados algébricos que são versões rotacionadas dos reticulados A_2, D_4, E_6, E_8 e K_{12}, por meio da perturbação σ_α do homomorfismo canônico e de ideais principais. Este método começou a ser formulado e usado por Ferrari, em [11], quando obteve versões rotacionadas dos reticulados A_2, D_4, E_6 e E_8 via o homomorfismo canônico. Neste trabalho aperfeiçoamos este método, adequando-o para a perturbação σ_α já que neste caso temos mais um parâmetro a encontrar, a saber, a norma do elemento α.

A construção proposta consiste em igualar a fórmula da densidade de centro dada em (5.1.4) aos valores já conhecidos para estas dimensões, que sabemos que são ótimas, e trabalhar para encontrar convenientes valores de seus parâmetros para que tenhamos os resultados desejados. Para isso, o auxílio do programa Mathematica foi indispensável.

Veremos a seguir como este processo foi feito para cada uma das dimensões citadas acima e exemplos de reticulados algébricos rotacionados encontrados através deste processo.

5.2.1 Reticulados algébricos rotacionados de dimensão 2

Nosso objetivo nesta seção é encontrar reticulados algébricos rotacionados de dimensão 2, fazendo uso de um corpo de números $\mathbb{K}$ de grau 2, através de ideais principais do seu anel dos inteiros $\mathcal{O}_{\mathbb{K}}$, utilizando a perturbação σ_α do homomorfismo canônico e que tenha densidade de centro ótima.

Para isso, seja o corpo $\mathbb{K} = \mathbb{Q}(\zeta_6)$. Temos através do Teorema (1.4.2) que $[\mathbb{K} : \mathbb{Q}] = 2$ e, do Teorema (1.4.3) que o anel dos inteiros deste corpo é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_6]$ e uma base integral é $\{1, \zeta_6\}$. Pelo Teorema (1.4.4) segue que o discriminante é $\mathcal{D}_{\mathbb{K}} = -3$ e, pela Proposição (1.4.5) que os monormorfismos são $\sigma_i(\zeta_6) = {\zeta_6}^i$, com $i = 1, 5$.

Queremos encontrar reticulados cuja densidade de centro é a mesma do reticulado A_2, ou seja, $\dfrac{1}{2\sqrt{3}}$ utlizando a perturbação σ_α do homomorfismo canônico que é dada por:

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_5(\alpha)}\sigma_5(x)),$$

com $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$.

Para isso, basta igualarmos a fórmula da densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ é $\dfrac{1}{2\sqrt{3}}$ que teremos novos reticulados com densidade de centro ótima. Já temos que $n = 2$ e $\mathcal{D}_{\mathbb{K}} = 3$. Assim, precisamos encontrar convenientes α, $\mathfrak{a}$ e t_α para que tenhamos $\delta(\sigma_\alpha(\mathfrak{a})) = \dfrac{1}{2\sqrt{3}}$.

Na Tabela (5.1), apreentamos algumas combinações possíveis de $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathfrak{a})$ e t_α que nos darão o resultado desejado.

$\mathcal{N}(\mathfrak{a})$	$\mathcal{N}(\alpha)$	t_α
1	4	4
3	16	24
4	25	40
7	9	42

Tabela 5.1:

Temos que um ideal principal de $\mathcal{O}_{\mathbb{K}}$ é da forma $\mathfrak{a} =< a_0 + a_1\zeta_6 >$, assim a norma deste ideal é dada pela seguinte expressão:

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}(< a_0 + a_1\zeta_6 >) = |\mathcal{N}(a_0 + a_1\zeta_6)| = \prod_{i=1,5} \sigma_i(a_0 + a_1\zeta_6) = a_0^2 + a_0a_1 + a_1^2. \quad (5.2.9)$$

Alguns ideais de $\mathcal{O}_{\mathbb{K}}$ que satisfazem a norma $\mathcal{N}(\mathfrak{a})$ são dados na Tabela (5.2)

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$
1	$\pm\mathcal{O}_{\mathbb{K}},\ \pm\zeta_6\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_6)\mathcal{O}_{\mathbb{K}}$
3	$\pm(1+\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(2-\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(1-2\zeta_6)\mathcal{O}_{\mathbb{K}}$
4	$\pm2\mathcal{O}_{\mathbb{K}},\ \pm2\zeta_6\mathcal{O}_{\mathbb{K}},\ \pm(2-2\zeta_6)\mathcal{O}_{\mathbb{K}}$
7	$\pm(3-\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(3-2\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(2+\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(1-3\zeta_6)\mathcal{O}_{\mathbb{K}}$

Tabela 5.2:

Como estamos trabalhando com a perturbação σ_α do homomorfismo canônico, o elemento α tem que satisfazer as condições $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$. Mas, no corpo $\mathbb{K} = \mathbb{Q}(\zeta_6)$, temos que estas condições irão ocorrer somente quando $\alpha \in \mathbb{N}$. Assim, $\sigma_i(\alpha) = \alpha$, com $i = 1, 5$, e portanto,

$$\mathcal{N}(\alpha) = \prod_{i=1,5} \sigma_i(\alpha) = \alpha^2.$$

Na Tabela (5.3), temos alguns possíveis resultados

α	$\mathcal{N}(\alpha)$
2	4
3	9
4	16
5	25

Tabela 5.3:

Observação 5.2.1 *Os valores entre* 1 *e* 7 *que não foram colocados na Tabela (5.1), não satisfazem a expressão da* $\mathcal{N}(\mathfrak{a})$ *dada em (5.2.9) e, os valores de* $\mathcal{N}(\alpha)$ *vistos na mesma tabela foram tomados de forma arbritária, pois como vimos qualquer número natural poderia ter sido tomado neste caso.*

Utilizando os dados vistos nas Tabelas (5.1), (5.2) e (5.3), veremos na tabela a seguir, algumas combinações de α e $\mathfrak{a}$ para que tenhamos t_α desejado e então reticulados com densidade de centro ótima para densidade 2.

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$	$\mathcal{N}(\alpha)$	α	t_α
1	$\pm\mathcal{O}_{\mathbb{K}},\ \pm\zeta_6\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_6)\mathcal{O}_{\mathbb{K}}$	2	4	4
3	$\pm(1+\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(2-\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(1-2\zeta_6)\mathcal{O}_{\mathbb{K}}$	16	4	24
4	$\pm2\mathcal{O}_{\mathbb{K}},\ \pm2\zeta_6\mathcal{O}_{\mathbb{K}},\ \pm(2-2\zeta_6)\mathcal{O}_{\mathbb{K}}$	25	5	40
7	$\pm(3-\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(3-2\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(2+\zeta_6)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_6)\mathcal{O}_{\mathbb{K}}$	9	3	42

Tabela 5.4:

Agora, iremos ilustrar alguns exemplos utilizando os dados da Tabela (5.4).

Exemplo 5.2.1 *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_6)$, $\mathfrak{a} = (1 - 2\zeta_6)\mathcal{O}_\mathbb{K}$ *um ideal de* $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_6]$ *e* $\alpha = 4 \in \mathcal{O}_\mathbb{K}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_\mathbb{K} = -3$, $\mathcal{N}(\mathfrak{a}) = 3$ *e* $\mathcal{N}(\alpha) = 16$. *Dado* $x \in \mathfrak{a}$, *podemos escrever* $x = (1 - 2\zeta_6)(a_0 + a_1\zeta_6)$, *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x}) = 24a_0^2 + 24a_0a_1 + 24a_1^2$ *e, emtão* $t_\alpha = min\{Tr(\alpha x\bar{x}) \ : \ x \in \mathfrak{a}, \ x \neq 0\} = 24$, *com* $a_0 = 1$ *e* $a_1 = 0$. *Portanto, a densidade de centro do reticulado* $\sigma_\mathbb{K}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})} = \frac{1}{2\sqrt{3}} \cong 0,28868$$

que é a mesma densidade de centro do reticulado A_2.

Exemplo 5.2.2 *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_6)$, $\mathfrak{a} = (3 - \zeta_6)\mathcal{O}_\mathbb{K}$ *um ideal de* $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_6]$ *e* $\alpha = 3 \in \mathcal{O}_\mathbb{K}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 2$, $\mathcal{D}_\mathbb{K} = -3$, $\mathcal{N}(\mathfrak{a}) = 7$ *e* $\mathcal{N}(\alpha) = 9$. *Dado* $x \in \mathfrak{a}$, *podemos escrever* $x = (3 - \zeta_6)(a_0 + a_1\zeta_6)$, *onde* $a_0, a_1 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x}) = 24a_0^2 + 24a_0a_1 + 24a_1^2$ *e, então* $t_\alpha = min\{Tr(\alpha x\bar{x}) \ : \ x \in \mathfrak{a}, \ x \neq 0\} = 24$, *com* $a_0 = 1$ *e* $a_1 = 0$. *Portanto, a densidade de centro do reticulado* $\sigma_\mathbb{K}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^n(|\mathcal{D}_\mathbb{K}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})} = \frac{1}{2\sqrt{3}} \cong 0,28868$$

que é a mesma densidade de centro do reticulado A_2.

5.2.2 Reticulados algébricos rotacionados de dimensão 4

Nesta seção, o objetivo é obter reticulados algébricos que são versões rotacionadas do reticulado D_4. Para isso, faremos uso do corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_8)$. Temos que $[\mathbb{K} : \mathbb{Q}] = 4$, o anel dos inteiros deste corpo é dado por $\mathcal{O}_\mathbb{K} = \mathbb{Z}(\zeta_8)$, uma base integral é $\{1, \zeta_8, {\zeta_8}^2, {\zeta_8}^3\}$, o discriminante é $\mathcal{D}_\mathbb{K} = 256$ e, os monormorfismos são $\sigma_i(\zeta_8) = {\zeta_8}^i$, com $i = 1, 3, 5, 7$.

A perturbação $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^4$ é dado por:

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_3(\alpha)}\sigma_3(x), \sqrt{\sigma_5(\alpha)}\sigma_5(x), \sqrt{\sigma_7(\alpha)}\sigma_7(x)),$$

onde $\sigma_i(\alpha) > 0, \ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 5, 7$.

Sabemos que para dimensão 4, o reticulado com densidade de centro recorde nesta dimensão é o D_4, cuja densidade de centro é $\frac{1}{8}$. Assim, basta igualarmos a fórmula da densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ é $\frac{1}{8}$ que teremos novos reticulados com densidade de centro ótima. Já temos que $n = 4$ e $\mathcal{D}_\mathbb{K} = 256$. Assim, precisamos encontrar convenientes α, $\mathfrak{a}$ e t_α para que tenhamos $\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{8}$. Na Tabela (5.5), apresentamos algumas combinações possíveis de $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathfrak{a})$ e t_α que darão o resultado desejado.

$\mathcal{N}(\mathfrak{a})$	$\mathcal{N}(\alpha)$	t_α	$\mathcal{N}(\mathfrak{a})$	$\mathcal{N}(\alpha)$	t_α
1	4	8	8	16	32
1	64	16	9	4	24
2	16	16	9	64	48
4	4	16	16	4	32
4	64	32	16	64	64

Tabela 5.5:

Temos que um ideal principal de $\mathcal{O}_{\mathbb{K}}$ é da forma $\mathfrak{a} =< a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3 >$, onde $a_0, a_1, a_2 \in \mathbb{Z}$ e assim, a norma deste ideal é dada pela seguinte expressão:

$$\begin{aligned}
\mathcal{N}(\mathfrak{a}) &= \mathcal{N}(< a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3 >) \\
&= |\mathcal{N}(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)| \\
&= \left| \prod_{i=1,3,5,7} \sigma_i(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3) \right| \\
&= a_0^4 + a_1^4 - 4a_0a_1^2a_2 + 2a_0^2a_2^2 + a_2^4 + 4a_0^2a_1a_3 - 4a_1a_2^2a_3 + 2a_1^2a_3^2 + 4a_0a_2a_3^2 + a_3^4.
\end{aligned}$$

Alguns ideais $\mathfrak{a}$ que satisfazem a norma $\mathcal{N}(\mathfrak{a})$ são dados na Tabela (5.6).

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$
1	$\pm\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(-1+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1-\zeta_8+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(-1+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$
2	$\pm(2+2\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(2+\zeta_8-{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8)\mathcal{O}_{\mathbb{K}}, \pm(-1+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm({\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}, \pm(\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(-1-\zeta_8+2{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}, \pm(1-2\zeta_8+2{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$ $\pm(-1+\zeta_8)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(-{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$
4	$\pm(2+\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-2{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$
8	$\pm(3+3\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+3\zeta_8+3{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(-1+\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-3+\zeta_8+{\zeta_8}^2-3{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_8-3{\zeta_8}^2-3{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$
9	$\pm(2+2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_8+2{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8-{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(2-2\zeta_8+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$
16	$\pm(2+\zeta_8+2{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(2+2\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm2\mathcal{O}_{\mathbb{K}},\ \pm(2-2{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(2\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(2-2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(-2+2\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(-2+\zeta_8-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-2+2{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$

Tabela 5.6:

Observação 5.2.2 *Observamos que os ideais da Tabela (5.6) são apenas alguns ideais, tomados de forma aleatória, com estas normas e com os escalares variando entre* -3 *e* 3.

Para o elemento α, como precisamos ter $\sigma_i(\alpha) \in \mathbb{R}^+$, tomamos α no subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_8)$, o corpo $\mathbb{L} = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$. O anel dos inteiros deste corpo é $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_8 + \zeta_8^{-1}]$ e, $\{1, \zeta_8 + \zeta_8^{-1}\}$ é uma base integral de $\mathbb{L}$. Assim, podemos escrever $\alpha = b_0 + b_1(\zeta_8 + \zeta_8^{-1})$ e então a norma desse elemento é dada por

$$\mathcal{N}(\alpha) = \prod_{i=1,3,5,7} \sigma_i(b_0 + b_1(\zeta_8 + \zeta_8^{-1})) = b_0^4 - 4b_0^2b_1^2 + 4b_1^4. \tag{5.2.10}$$

Observação 5.2.3 *Os valores para $\mathcal{N}(\mathfrak{a})$ entre 1 e 16 que não estão na Tabela (5.5) nos fornecem valores para $\mathcal{N}(\alpha)$ que não são convenientes para o nosso estudo, pois estes não satisfazem a expressão para $\mathcal{N}(\alpha)$ dada em (5.2.10).*

Abaixo veremos alguns elementos α's que irão satisfazer a Equação (5.2.10) e também $\alpha_i = \sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 5, 7$:

$\mathcal{N}(\alpha)$	α
4	$2 \pm (\zeta_8 + \zeta_8^{-1})$, $10 \pm 7(\zeta_8 + \zeta_8^{-1})$
16	$6 \pm 4(\zeta_8 + \zeta_8^{-1})$
64	$4 \pm 2(\zeta_8 + \zeta_8^{-1})$

Tabela 5.7:

Observação 5.2.4 *Os valores da Tabela (5.7) foram encontrados variando $\mathcal{N}(\alpha)$ de 1 a 100 e os escalares $b_1's$, com $i = 0, 1$, percorrendo o intervalo de -15 a 15.*

Utilizando os dados das Tabelas (5.5), (5.6) e (5.7), apresentamos algumas combinações de α e $\mathfrak{a}$ para que tenhamos t_α desejado. Dessa forma, obtemos reticulados com densidade de centro ótima para densidade 4. Para isso, seja $\gamma = \zeta_8 + \zeta_8^{-1}$.

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$	$\mathcal{N}(\alpha)$	α	t_α
1	$\pm\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(-1+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	4	$2-\gamma,$ $10-7\gamma$	8
1	$\pm\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(1-{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	64	$4-2\gamma$	16
2	$\pm(2+2\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(2+\zeta_8-{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_8)\mathcal{O}_{\mathbb{K}}, \pm(1-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm({\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}, \pm(\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}}$	16	$6-4\gamma$	16
2	$\pm(1+\zeta_8-2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}, \pm(1-2\zeta_8+2{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$ $\pm(1-\zeta_8)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm({\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	16	$6+4\gamma$	16
4	$\pm(1-2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-2{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	4	$2+\gamma,$ $10+7\gamma$	16
4	$\pm(1-2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_8+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8-2{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	64	$4+2\gamma$	32

8	$\pm(3+3\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+3\zeta_8+3{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-1+\zeta_8+{\zeta_8}^2+{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	16	$6-4\gamma$	32
8	$\pm(1+\zeta_8-{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-3+\zeta_8+{\zeta_8}^2-3{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_8-3{\zeta_8}^2-3{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_8+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	16	$6+4\gamma$	32
9	$\pm(2+2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_8+2{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1-\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	4	$2-\gamma,$ $10-7\gamma$	24
9	$\pm(2+2\zeta_8+{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+2\zeta_8+2{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(1-\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(1+{\zeta_8}^2-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	64	$4-2\gamma$	48
16	$\pm(-2+\zeta_8-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-2+2{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm2\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},$ $\pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(2-2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm(-2+2\zeta_8-{\zeta_8}^2)\mathcal{O}_{\mathbb{K}}$	4	$2+\gamma,$ $10+7\gamma$	32
16	$\pm(2+\zeta_8+2{\zeta_8}^2)\mathcal{O}_{\mathbb{K}},\ \pm(2+2\zeta_8-{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm2\mathcal{O}_{\mathbb{K}},\ \pm\zeta_8\mathcal{O}_{\mathbb{K}},$ $\pm(2-2{\zeta_8}^2-2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^2\mathcal{O}_{\mathbb{K}},\ \pm{\zeta_8}^3\mathcal{O}_{\mathbb{K}},\ \pm(2\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$	64	$4-2\gamma,$	64

Tabela 5.8:

Agora, apresentaremos alguns exemplos utilizando os dados fornecidos pela Tabela (5.8).

Exemplo 5.2.3 *Sejam o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_8)$, $\mathfrak{a}=(3-\zeta_8-{\zeta_8}^2+3{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$ *um ideal de* $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\zeta_8]$ *e* $\alpha=6+4\zeta_8+4{\zeta_8}^{-1}\in\mathcal{O}_{\mathbb{K}}$. *Temos que* $n=[\mathbb{K}:\mathbb{Q}]=4$, $\mathcal{D}_{\mathbb{K}}=256$, $\mathcal{N}(\mathfrak{a})=8$ *e* $\mathcal{N}(\alpha)=16$. *Dado* $x\in\mathfrak{a}$, *podemos escrever* $x=(3-\zeta_8-{\zeta_8}^2+3{\zeta_8}^3)(a_0+a_1\zeta_8+a_2{\zeta_8}^2+a_3{\zeta_8}^3)$, *onde* $a_0,a_1,a_2,a_3\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x})=32a_0^2-32a_0a_1+32a_1^2-32a_1a_2+32a_2^2+32a_0a_3-32a_2a_3+32a_3^2$ *e, então* $t_\alpha=min\{Tr(\alpha x\bar{x})\ :\ x\in\mathfrak{a},\ x\neq 0\}=32$, *com* $a_0=1$ *e* $a_1=a_2=a_3=0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a}))=\frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}=\frac{1}{8}=0,125,$$

que é a mesma densidade de centro do reticulado D_4.

Exemplo 5.2.4 *Sejam o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_8)$, $\mathfrak{a}=(2\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)\mathcal{O}_{\mathbb{K}}$ *um ideal de* $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\zeta_8]$ *e* $\alpha=4-2\zeta_8-2{\zeta_8}^{-1}\in\mathcal{O}_{\mathbb{K}}$. *Temos que* $n=[\mathbb{K}:\mathbb{Q}]=4$, $\mathcal{D}_{\mathbb{K}}=256$, $\mathcal{N}(\mathfrak{a})=16$ *e* $\mathcal{N}(\alpha)=64$. *Dado* $x\in\mathfrak{a}$, *podemos escrever* $x=(2\zeta_8+2{\zeta_8}^2+2{\zeta_8}^3)(a_0+a_1\zeta_8+a_2{\zeta_8}^2+a_3{\zeta_8}^3)$, *onde* $a_0,a_1,a_2,a_3\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x})=32a_0^2+32a_0a_1+32a_1^2+32a_1a_2+32a_2^2-32a_0a_3+32a_2a_3+32a_3^2$ *e, então* $t_\alpha=min\{Tr(\alpha x\bar{x})\ :\ x\in\mathfrak{a},\ x\neq 0\}=32$, *com* $a_0=1$ *e* $a_1=a_2=a_3=0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a}))=\frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}=\frac{1}{8}=0,125,$$

que é a mesma densidade de centro do reticulado D_4.

5.2.3 Reticulados algébricos rotacionados de dimensão 6

Nesta seção, o objetivo é obter reticulados algébricos que são versões rotacionadas do reticulado E_6. Para isso, faremos uso do corpo $\mathbb{K} = \mathbb{Q}(\zeta_9)$. Temos que $[\mathbb{K} : \mathbb{Q}] = 6$, o anel dos inteiros deste corpo é dado por $\mathcal{O}_\mathbb{K} = \mathbb{Z}(\zeta_9)$, uma base integral é $\{1, \zeta_9, {\zeta_9}^2, {\zeta_9}^3, {\zeta_9}^4, {\zeta_9}^5\}$, discriminante $\mathcal{D}_\mathbb{K} = 3^9$ e, os monormorfismos são $\sigma_i(\zeta_9) = {\zeta_9}^i$, com $i = 1, 2, 4, 5, 7, 8$.

Neste caso, a perturbação $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^6$ do homomorfismo canônico é dada por:

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_2(\alpha)}\sigma_2(x), \sqrt{\sigma_4(\alpha)}\sigma_4(x), \sqrt{\sigma_5(\alpha)}\sigma_5(x), \sqrt{\sigma_7(\alpha)}\sigma_7(x), \sqrt{\sigma_8(\alpha)}\sigma_8(x))$$

onde $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2, 4, 5, 7, 8$.

Sabemos que para dimensão 6, o reticulado com densidade de centro recorde nesta dimensão é o E_6, cuja densidade de centro é $\frac{1}{2^3\sqrt{3}}$. Assim, basta igualarmos a fórmula da densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ é $\frac{1}{2^3\sqrt{3}}$ que teremos novos reticulados com densidade de centro ótima. Já temos que $n = 6$ e $|\mathcal{D}_\mathbb{K}| = 3^9$. Assim, precisamos encontrar convenientes α, $\mathfrak{a}$ e t_α para que tenhamos $\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^3\sqrt{3}}$.

Na Tabela (5.9), apresentamos algumas combinações possíveis de $\mathcal{N}(\alpha)$, $\mathcal{N}(\mathfrak{a})$ e t_α que darão o resultado desejado.

$\mathcal{N}(\mathfrak{a})$	$\mathcal{N}(\alpha)$	t_α
1	81	18
3	9	18
9	1	18
9	64	36
27	81	54
81	9	54

Tabela 5.9:

Um ideal principal de $\mathcal{O}_\mathbb{K}$ é da forma

$$\mathfrak{a} =< a_0 + a_1\zeta_9 + a_2{\zeta_9}^2 + a_3{\zeta_9}^3 + a_4{\zeta_9}^4 + a_5{\zeta_9}^5 >,$$

com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$. A norma deste ideal é calculada da seguinte forma:

$$\begin{aligned} \mathcal{N}(\mathfrak{a}) &= \mathcal{N}(< a_0 + a_1\zeta_9 + a_2{\zeta_9}^2 + a_3{\zeta_9}^3 + a_4{\zeta_9}^4 + a_5{\zeta_9}^5 >) \\ &= |\mathcal{N}(a_0 + a_1\zeta_9 + a_2{\zeta_9}^2 + a_3{\zeta_9}^3 + a_4{\zeta_9}^4 + a_5{\zeta_9}^5)|, \end{aligned}$$

e pela definição de norma de um elemento temos

$$\mathcal{N}(\mathfrak{a}) = \left| \prod_{i=1,2,4,5,7,8} \sigma_i(a_0 + a_1\zeta_9 + a_2{\zeta_9}^2 + a_3{\zeta_9}^3 + a_4{\zeta_9}^4 + a_5{\zeta_9}^5) \right|.$$

Resolvendo, chegamos a seguinte espressão:

$$\begin{aligned}
\mathcal{N}(\mathfrak{a}) \;=\; & a_0^6 - a_0^3a_1^3 + a_1^6 + 3a_0^4a_1a_2 - 6a_0a_1^4a2 + 9a_0^2a_1^2a_2^2 - a_0^3a_2^3 - a_1^3a_2^3 + 3a_0a_1a_2^4 + a_2^6 - 3a_0^5a_3 \\
& +6a_0^2a_1^3a_3 - 15a_0^3a_1a_2a_3 + 3a_1^4a_2a_3 - 9a_0a_1^2a_2^2a_3 - 3a_0^2a_2^3a_3 - 6a_1a_2^4a_3 + 6a_0^4a_3^2 - 3a_0a_1^3a_3^2 + \\
& 18a_0^2a_1a_2a_3^2 + 9a_1^2a_2^2a_3^2 + 6a_0a_2^3a_3^2 - 7a_0^3a_3^3 - a_1^3a_3^3 - 15a_0a_1a_2a_3^3 - a2^3a_3^3 + 6a_0^2a_3^4 + 3a_1a_2a_3^4 \\
& -3a_0a_3^5 + a_3^6 - 3a_0^3a_1^2a_4 - 3a_1^5a_4 + 3a_0^4a_2a_4 + 12a_0a_1^3a_2a_4 - 9a_0^2a_1a_2^2a_4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 \\
& -9a_0^2a_1^2a_3a_4 + 3a_0^3a_2a_3a_4 - 15a_1^3a_2a_3a_4 + 9a_0a_1a_2^2a_3a_4 + 3a_2^4a_3a_4 + 18a_0a_1^2a_3^2a_4 - 9a_0^2a_2a_3^2a_4 \\
& -9a_1a_2^2a_3^2a_4 - 3a_1^2a_3^3a_4 + 12a_0a_2a_3^3a_4 - 6a_2a_3^4a_4 + 6a_0^3a_1a_4^2 + 6a_1^4a_4^2 - 9a_0a_1^2a_2a_4^2 + 9a_0^2a_2^2a_4^2 \\
& -3a_1a_2^3a_4^2 - 9a_0^2a_1a_3a_4^2 + 18a_1^2a_2a_3a_4^2 - 9a_0a_2^2a_3a_4^2 - 9a_0a_1a_3^2a_4^2 + 9a_2^2a_3^2a_4^2 + 6a_1a_3^3a_4^2 - a_0^3a_4^3 \\
& -7a_1^3a_4^3 + 3a_0a_1a_2a_4^3 - a_2^3a_4^3 + 6a_0^2a_3a_4^3 - 15a_1a_2a_3a_4^3 - 3a_0a_3^2a_4^3 - a_3^3a_4^3 + 6a_1^2a_4^4 + 3a_0a_2a_4^4 \\
& +3a_2a_3a_4^4 - 3a_1a_4^5 + a_4^6 + 3a_0^4a_1a_5 + 3a_0a_1^4a_5 - 9a_0^2a_1^2a_2a_5 + 6a_0^3a_2^2a_5 - 3a_1^3a_2^2a_5 + 3a_0a_1a_2^3a_5 \\
& -3a_2^5a_5 + 3a_0^3a_1a3a_5 + 3a_1^4a_3a_5 + 9a_0a_1^2a_2a_3a_5 - 9a_0^2a_2^2a_3a_5 + 12a_1a_2^3a_3a_5 - 9a_0^2a_1a_3^2a_5 \\
& -9a_1^2a_2a_3^2a_5 - 9a_0a_2^2a_3^2a_5 + 12a_0a_1a_3^3a_5 + 6a_2^2a_3^3a_5 - 6a_1a_3^4a_5 - 6a_0^4a_4a_5 - 15a_0a_1^3a_4a_5 \\
& +9a_0^2a_1a_2a_4a_5 - 9a_1^2a_2^2a_4a_5 + 12a_0a_2^3a_4a_5 + 12a_0^3a_3a_4a_5 + 3a_1^3a_3a_4a_5 - 9a_0a_1a_2a_3a_4a_5 \\
& -15a_2^3a_3a_4a_5 - 9a_0^2a_3^2a_4a_5 + 9a_1a_2a_3^2a_4a_5 + 3a_0a_3^3a_4a_5 + 3a_3^4a_4a_5 + 18a_0a_1^2a_4^2a_5 - 9a_0^2a_2a_4^2a_5 \\
& +18a_1a_2^2a_4^2a_5 - 9a_1^2a_3a_4^2a_5 + 9a_0a_2a_3a_4^2a_5 - 9a_2a_3^2a_4^2a_5 - 15a_0a_1a_4^3a_5 - 3a_2^2a_4^3a_5 + 12a_1a_3a_4^3a_5 \\
& +3a_0a_4^4a_5 - 6a_3a_4^4a_5 + 9a_0^2a_1^2a_5^2 - 3a_0^3a_2a_5^2 + 6a_1^3a_2a_5^2 - 9a_0a_1a_2^2a_5^2 + 6a_2^4a_5^2 - 9a_0a_1^2a_3a_5^2 \\
& +18a_0^2a_2a_3a_5^2 - 9a_1a_2^2a_3a_5^2 + 9a_1^2a_3^2a_5^2 - 9a_0a_2a_3^2a_5^2 - 3a_2a_3^3a_5^2 - 9a_0^2a_1a_4a_5^2 - 9a_1^2a_2a_4a_5^2 \\
& -9a_0a_2^2a_4a_5^2 + 9a_0a_1a_3a_4a_5^2 + 18a_2^2a_3a_4a_5^2 - 9a_1a_3^2a_4a_5^2 + 9a_0^2a_4^2a_5^2 - 9a_1a_2a_4^2a_5^2 - 9a_0a_3a_4^2a_5^2 \\
& +9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - a_0^3a_5^3 - a_1^3a_5^3 + 12a_0a_1a_2a_5^3 - 7a_2^3a_5^3 - 3a_0^2a_3a_5^3 + 3a_1a_2a_3a_5^3 \\
& +6a_0a_3^2a_5^3 - a_3^3a_5^3 + 6a_1^2a_4a_5^3 + 3a_0a_2a_4a_5^3 - 15a_2a_3a_4a_5^3 - 3a_1a_4^2a_5^3 - a_4^3a_5^3 - 6a_0a_1a_5^4 \\
& +6a_2^2a_5^4 + 3a_1a_3a_5^4 + 3a_0a_4a_5^4 + 3a_3a_4a_5^4 - 3a_2a_5^5 + a_5^6
\end{aligned}$$

Observação 5.2.5 *Os valores de $\mathcal{N}(\mathfrak{a})$ que estão na Tabela (5.9) são os únicos no intervalo de 1 a 100 que satisfazem a fórmula para $\mathcal{N}(\mathfrak{a})$, variando os escalares a_i's entre -1 e 1, $i = 0, 1, 2, 3, 4, 5$ e também, que nos darão reticulados com densidades de centro ótima.*

Alguns ideais $\mathfrak{a}$ que satisfazem a norma $\mathcal{N}(\mathfrak{a})$ são dados na Tabela (5.10)

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$
1	$\pm(1+\zeta_9+\zeta_9{}^2+\zeta_9{}^3+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}}, \pm(\zeta_9-\zeta_9{}^2+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_9-\zeta_9{}^2-\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}}, \pm(1-\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_9-\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_9+\zeta_9{}^2+\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}}$
3	$\pm(1+\zeta_9+\zeta_9{}^2+\zeta_9{}^3-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9-\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_9+\zeta_9{}^3+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_9{}^2+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_9-\zeta_9{}^2+\zeta_9{}^3+\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_9{}^2-\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9-\zeta_9{}^2-\zeta_9{}^3)\mathcal{O}_{\mathbb{K}}$
9	$\pm(1+\zeta_9+\zeta_9{}^2+\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9{}^2+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_9+\zeta_9{}^2+\zeta_9{}^3)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_9{}^3+\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_9-\zeta_9{}^2-\zeta_9{}^3+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_9-\zeta_9{}^2-\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$ $\pm(1+\zeta_9{}^2+\zeta_9{}^3-\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9-\zeta_9{}^2+\zeta_9{}^3+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}}$
27	$\pm(1+\zeta_9-\zeta_9{}^3-\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_9+\zeta_9{}^2-\zeta_9{}^3+\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_9+\zeta_9{}^2-\zeta_9{}^4-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1+\zeta_9{}^2-\zeta_9{}^3-\zeta_9{}^5)\mathcal{O}_{\mathbb{K}}$
81	$\pm(1-\zeta_9{}^2-\zeta_9{}^3+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_9-\zeta_9{}^3+\zeta_9{}^4)\mathcal{O}_{\mathbb{K}},\ \pm(\zeta_9-\zeta_9{}^2-\zeta_9{}^4+\zeta_9{}^5)\mathcal{O}_{\mathbb{K}},$

Tabela 5.10:

Observação 5.2.6 *Observamos que os ideais da Tabela (5.10) são apenas alguns ideais, tomados de forma aleatória, com estas normas e com os escalares variando entre* -1 *e* 1.

Como estamos trabalhando com a perturbação σ_α do homomorfismo canônico, precisamos ter $\sigma_i(\alpha) \in \mathbb{R}^+$. Para isso tomamos α no subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_9)$, que é o corpo $\mathbb{L} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, pois este é um corpo totalmente real. Temos que o anel dos inteiros deste corpo é $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}(\zeta_9 + \zeta_9^{-1})$ e, $\{1, \zeta_9 + \zeta_9{}^{-1}, \zeta_9{}^2 + \zeta_9{}^{-2}\}$ é uma base integral de $\mathbb{L}$. Assim, o elemento α pode ser escrio da seguinte forma

$$\alpha = b_0 + b_1(\zeta_9 + \zeta_9^{-1}) + b_2(\zeta_9{}^2 + \zeta_9{}^{-2})$$

e, a norma desse elemento é dada por

$$\mathcal{N}(\alpha) = \prod_{i=1,2,4,5,7,8} \sigma_i(b_0 + b_1(\zeta_9 + \zeta_9^{-1}) + b_2(\zeta_9{}^2 + \zeta_9{}^{-2})),$$

que resolvendo temos

$$\begin{aligned}\mathcal{N}(\alpha) \;=\; & b_0^6 - 6b_0^4b_1^2 - 2b_0^3b_1^3 + 9b_0^2b_1^4 + 6b_0b_1^5 + b_1^6 + 6b_0^4b_1b_2 + 12b_0^3b_1^2b_2 - 18b_0^2b_1^3b_2 - 42b_0b_1^4b_2 \\ & -12b_1^5b_2 - 6b_0^4b_2^2 - 6b_0^3b_1b_2^2 + 27b_0^2b_1^2b_2^2 + 60b_0b_1^3b_2^2 + 42b_1^4b_2^2 - 2b_0^3b_2^3 - 18b_0^2b_1b_2^3 \\ & -48b_0b_1^2b_2^3 - 34b_1^3b_2^3 + 9b_0^2b_2^4 + 12b_0b_1b_2^4 - 3b_1^2b_2^4 + 6b_0b_2^5 + 6b_1b_2^5 + b_2^6.\end{aligned}$$

Além de satisfazer a expressão da norma $\mathcal{N}(\alpha)$, ainda precisamos ter $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2, 4, 5, 7, 8$, pois estamos trabalhando com σ_α. Na Tabela (5.11), apresentamos alguns elementos α's que satisfazem a fórmula da norma $\mathcal{N}(\alpha)$ e também $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 2, 4, 5, 7, 8$.

$\mathcal{N}(\alpha)$	α
1	$2+(\zeta_9+\zeta_9^{-1})$, $2+(\zeta_9^2+\zeta_9^{-2})$, $2-(\zeta_9+\zeta_9^{-1})-(\zeta_9^2+\zeta_9^{-2})$, $3-2(\zeta_9+\zeta_9^{-1})+(\zeta_9^2+\zeta_9^{-2})$, $3+3(\zeta_9+\zeta_9^{-1})+2(\zeta_9^2+\zeta_9^{-2})$
9	$2-(\zeta_9+\zeta_9^{-1})$, $2-(\zeta_9^2+\zeta_9^{-2})$, $2+(\zeta_9+\zeta_9^{-1})+(\zeta_9^2+\zeta_9^{-2})$, $5-3(\zeta_9+\zeta_9^{-1})+2(\zeta_9^2+\zeta_9^{-2})$, $5-2(\zeta_9+\zeta_9^{-1})-5(\zeta_9^2+\zeta_9^{-2})$, $5+(\zeta_9+\zeta_9^{-1})-2(\zeta_9^2+\zeta_9^{-2})$, $5+5(\zeta_9+\zeta_9^{-1})+3(\zeta_9^2+\zeta_9^{-2})$
64	$4+2(\zeta_9+\zeta_9^{-1})$, $4+2(\zeta_9^2+\zeta_9^{-2})$, $4-2(\zeta_9+\zeta_9^{-1})-2(\zeta_9^2+\zeta_9^{-2})$
81	$3+2(\zeta_9+\zeta_9^{-1})+(\zeta_9^2+\zeta_9^{-2})$, $3-(\zeta_9+\zeta_9^{-1})-2(\zeta_9^2+\zeta_9^{-2})$, $3-(\zeta_9+\zeta_9^{-1})+(\zeta_9^2+\zeta_9^{-2})$

Tabela 5.11:

Observação 5.2.7 *Os valores da Tabela (5.11) foram encontrados variando* $\mathcal{N}(\alpha)$ *de* 1 *a* 100 *e os escalares* $b_1's$*, com* $i=0,1,2$*, percorrendo o intervalo de* -5 *a* 5.

A partir dos resultados vistos nas Tabelas (5.9), (5.10) e (5.11), apresentaremos a Tabela (5.12) com as combinações encontradas de α e $\mathfrak{a}$ que nos fornecerão t_α e, com isso densidades de centro recordes para dimensão 6. Para isso, sejam $\gamma_1=\zeta_9+\zeta_9{}^{-1}$ e $\gamma_2=\zeta_9{}^2+\zeta_9{}^{-2}$.

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$	$\mathcal{N}(\alpha)$	α	t_α
1	$\pm(1+\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9-\zeta_9^2+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1-\zeta_9^4-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9-\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9-\zeta_9^2-\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$	81	$3-\gamma_1-2\gamma_2$, $3-\gamma_1+\gamma_2$, $3+2\gamma_1+\gamma_2$	18
3	$\pm(1+\zeta_9+\zeta_9^2+\zeta_9^3-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9-\zeta_9^4-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9+\zeta_9^3+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9^2+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1-\zeta_9-\zeta_9^2+\zeta_9^3+\zeta_9^4-\zeta_9^5)\mathcal{O}_\mathbb{K}$,	9	$2-\gamma_1$, $2-\gamma_2$, $2+\gamma_1+\gamma_2$, $5-3\gamma_1+2\gamma_2$, $5-2\gamma_1-5\gamma_2$, $5+\gamma_1-2\gamma_2$, $5+5\gamma_1+3\gamma_2$	18
9	$\pm(1+\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9^2+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9+\zeta_9^2+\zeta_9^3)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9-\zeta_9^2-\zeta_9^3+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(1-\zeta_9-\zeta_9^2-\zeta_9^4-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9^2+\zeta_9^3-\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$,	1	$2+\gamma_1$, $2+\gamma_2$, $2-\gamma_1-\gamma_2$, $3+3\gamma_1+2\gamma_2$ $3-2\gamma_1+\gamma_2$,	18
9	$\pm(1+\zeta_9+\zeta_9^2+\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9^2+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9+\zeta_9^2+\zeta_9^3)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9^3+\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(\zeta_9-\zeta_9^2-\zeta_9^3+\zeta_9^4)\mathcal{O}_\mathbb{K}$, $\pm(1-\zeta_9-\zeta_9^2-\zeta_9^4-\zeta_9^5)\mathcal{O}_\mathbb{K}$, $\pm(1+\zeta_9^2+\zeta_9^3-\zeta_9^4+\zeta_9^5)\mathcal{O}_\mathbb{K}$,	64	$4+2\gamma_1$, $4+2\gamma_2$, $4-2\gamma_1-2\gamma_2$	36

27	$\pm(1-\zeta_9+{\zeta_9}^2-{\zeta_9}^3+{\zeta_9}^4-{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$, $\pm(1+\zeta_9-{\zeta_9}^3-{\zeta_9}^4)\mathcal{O}_{\mathbb{K}}$, $\pm(\zeta_9+{\zeta_9}^2-{\zeta_9}^4-{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$ $\pm(1+{\zeta_9}^2-{\zeta_9}^3-{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$	81	$3+2\gamma_1+\gamma_2$, $3-\gamma_1-2\gamma_2$, $3-\gamma_1+\gamma_2$	54
81	$\pm(1-\zeta_9-{\zeta_9}^3+{\zeta_9}^4)\mathcal{O}_{\mathbb{K}}$, $\pm(\zeta_9-{\zeta_9}^2-{\zeta_9}^4+{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$	9	$5-3\gamma_1+2\gamma_2$,	54

Tabela 5.12:

Agora, veremos alguns exemplos de reticulados via ideais principais e utilizando a perturbação σ_α, a partir dos dados fornecidos na Tabela (5.12).

Exemplo 5.2.5 *Sejam o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_9)$, $\mathfrak{a}=(1+\zeta_9+{\zeta_9}^2+{\zeta_9}^3-{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$, *um ideal de* $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\zeta_9]$ *e* $\alpha=2+\zeta_9+\zeta_9^{-1}+{\zeta_9}^2+\zeta_9^{-2}\in\mathcal{O}_{\mathbb{K}}$. *Temos que* $n=[\mathbb{K}:\mathbb{Q}]=6$, $\mathcal{D}_{\mathbb{K}}=3^9$, $\mathcal{N}(\mathfrak{a})=3$ *e* $\mathcal{N}(\alpha)=9$. *Dado* $x\in\mathfrak{a}$, *podemos escrever* $x=(1+\zeta_9+{\zeta_9}^2+{\zeta_9}^3-{\zeta_9}^5)(a_0+a_1\zeta_9+a_2{\zeta_9}^2+a_3{\zeta_9}^3+a_4{\zeta_9}^4+a_5{\zeta_9}^5)$, *onde* $a_0,a_1,a_2,a_3,a_4,a_5\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x})=108c_0^2+162c_0c_1+108c_1^2+36c_0c_2+162c_1c_2+108c_2^2-108c_0c_3+36c_1c_3+162c_2c_3+108c_3^2-198c_0c_4-108c_1c_4+36c_2c_4+162c_3c_4+108c_4^2-198c_0c_5-198c_1c_5-108c_2c_5+36c_3c_5+162c_4c_5+108c_5^2$ *e, então* $t_\alpha=min\{Tr(\alpha x\bar{x})\ :\ x\in\mathfrak{a},\ x\neq 0\}=18$, *com* $c_0=0,c_1=-1,c_2=1,c_3=0,c_4=-1,c_5=0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a}))=\frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}=\frac{1}{2^6(3^9.9)^{\frac{1}{2}}}\frac{18^{\frac{6}{2}}}{3}=\frac{1}{2^3\sqrt{3}}\cong 0,07217,$$

que é a mesma densidade de centro do reticulado E_6.

Exemplo 5.2.6 *Sejam o corpo* $\mathbb{K}=\mathbb{Q}(\zeta_9)$, $\mathfrak{a}=(\zeta_9+{\zeta_9}^2-{\zeta_9}^4-{\zeta_9}^5)\mathcal{O}_{\mathbb{K}}$, *um ideal de* $\mathcal{O}_{\mathbb{K}}=\mathbb{Z}[\zeta_9]$ *e* $\alpha=3-\zeta_9-\zeta_9^{-1}+{\zeta_9}^2+\zeta_9^{-2}\in\mathcal{O}_{\mathbb{K}}$. *Temos que* $n=[\mathbb{K}:\mathbb{Q}]=6$, $\mathcal{D}_{\mathbb{K}}=3^9$, $\mathcal{N}(\mathfrak{a})=27$ *e* $\mathcal{N}(\alpha)=81$. *Dado* $x\in\mathfrak{a}$, *podemos escrever* $x=(\zeta_9+{\zeta_9}^2-{\zeta_9}^4-{\zeta_9}^5)(a_0+a_1\zeta_9+a_2{\zeta_9}^2+a_3{\zeta_9}^3+a_4{\zeta_9}^4+a_5{\zeta_9}^5)$, *onde* $a_0,a_1,a_2,a_3,a_4,a_5\in\mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x})=54c_0^2+54c_0c1+54c_1^2+54c_1c_2+54c_2^2-54c_0c_3+54c_2c_3+54c_3^2-54c_0c_4-54c_1c_4+54c_3c_4+54c_4^2-54c_0c_5-54c_1c_5-54c_2c_5+54c_4c_5+54c_5^2$ *e, então* $t_\alpha=min\{Tr(\alpha x\bar{x})\ :\ x\in\mathfrak{a},\ x\neq 0\}=54$, *com* $c_0=1,c_1=c_2=c_3=c_4=c_5=0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a}))=\frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})}=\frac{1}{2^6(3^9.81)^{\frac{1}{2}}}\frac{54^{\frac{6}{2}}}{27}=\frac{1}{2^3\sqrt{3}}\cong 0,07217,$$

que é a mesma densidade de centro do reticulado E_6.

5.2.4 Reticulados algébricos rotacionados de dimensão 8

Nesta seção, o objetivo é obter versões rotacionadas do reticulado E_8. Para isso, faremos uso do corpo ciclotômico $\mathbb{K}=\mathbb{Q}(\zeta_{20})$. Temos que $[\mathbb{K}:\mathbb{Q}]=8$, o anel dos inteiros deste corpo é dado

por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}(\zeta_{20})$, uma base integral é $\{1, \zeta_{20}, \zeta_{20}^2, \zeta_{20}^3, \zeta_{20}^4, \zeta_{20}^5, \zeta_{20}^6, \zeta_{20}^7\}$, discriminante $\mathcal{D}_{\mathbb{K}} = 2^8 5^6$ e, os monormorfismos são: $\sigma_i(\zeta_{20}) = \zeta_{20}^i$, com $i = 1, 3, 7, 9, 11, 13, 17, 19$. Assim, a perturbação $\sigma_\alpha : \mathbb{K} \to \mathbb{R}^8$ do homomorfismo canônico é dada por:

$$\sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{\sigma_3(\alpha)}\sigma_3(x), \sqrt{\sigma_7(\alpha)}\sigma_7(x), \sqrt{\sigma_9(\alpha)}\sigma_9(x), \sqrt{\sigma_{11}(\alpha)}\sigma_{11}(x),$$

$$\sqrt{\sigma_{13}(\alpha)}\sigma_{13}(x), \sqrt{\sigma_{17}(\alpha)}\sigma_{17}(x), \sqrt{\sigma_{19}(\alpha)}\sigma_{19}(x))$$

onde $\sigma_i(\alpha) > 0,\ \sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 7, 9, 11, 13, 17, 19$.

Como vimos, para dimensão 8, o reticulado com densidade de centro recorde é o E_8, cuja densidade de centro é $\frac{1}{16}$. Assim, basta igualarmos a fórmula da densidade de centro do reticulado $\sigma_\alpha(\mathfrak{a})$ é $\frac{1}{16}$ que teremos novos reticulados com densidade de centro ótima. Já temos que $n = 8$ e $|\mathcal{D}_{\mathbb{K}}| = 2^8 5^6$. Assim, precisamos encontrar convenientes $\mathfrak{a}$ e t_α para que tenhamos $\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{16}$.

Na Tabela (5.13), apresentamos algumas combinações possíveis de $\mathcal{N}(\mathfrak{a})$, $\mathcal{N}(\alpha)$ e t_α que darão o resultado desejado.

$\mathcal{N}(\mathfrak{a})$	$\mathcal{N}(\alpha)$	t_α
16	25	40
80	1	40
256	25	40

Tabela 5.13:

Um ideal principal de $\mathcal{O}_{\mathbb{K}}$ é da forma

$$\mathfrak{a} =< a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7 >,$$

com $a_i \in \mathbb{Z}$, para todo $i = 0, \cdots, 7$. A norma deste ideal é calculada da seguinte forma:

$$\begin{aligned} \mathcal{N}(\mathfrak{a}) &= \mathcal{N}(< a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7 >) \\ &= |\mathcal{N}(a_0 + a_1\zeta_{20} + a_2\zeta_{20}^2 + a_3\zeta_{20}^3 + a_4\zeta_{20}^4 + a_5\zeta_{20}^5 + a_6\zeta_{20}^6 + a_7\zeta_{20}^7)|, \end{aligned}$$

e pela definição de norma de um elemento temos que

$$\mathcal{N}(\mathfrak{a}) = \left| \prod_{i=1,3,7,9,11,13,17,19} \sigma_i \left(\sum_{j=1}^{7} a_j \zeta_{20}^j \right) \right|$$

e, fazendo os cáculos obtemos uma expressão para $\mathcal{N}(\mathfrak{a})$. Alguns ideais que satisfazem esta expressão são dados na Tabela (5.14)

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$
16	$\pm(1-2\zeta_{20}-\zeta_{20}^5+2\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$, $\pm(1-\zeta_{20}^3+\zeta_{20}^4-\zeta_{20}^6-\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$
80	$\pm(2-\zeta_{20}^2+2\zeta_{20}^4-2\zeta_{20}^6+\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$, $\pm(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6)\mathcal{O}_{\mathbb{K}}$
256	$\pm(2+\zeta_{20}+2\zeta_{20}^4-\zeta_{20}^6)\mathcal{O}_{\mathbb{K}}$, $\pm(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4)\mathcal{O}_{\mathbb{K}}$

Tabela 5.14:

Para que $\sigma_i(\alpha) \in \mathbb{R}$ tomemos α no subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, que é o corpo $\mathbb{L} = \mathbb{Q}(\zeta_{20}+\zeta_{20}^{-1})$, pois este é um corpo totalmente real. Temos que o anel dos inteiros deste corpo é $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{20}+\zeta_{20}^{-1})$ e, $\{1, \zeta_{20}+{\zeta_{20}}^{-1}, {\zeta_{20}}^2+{\zeta_{20}}^{-2}, {\zeta_{20}}^3+{\zeta_{20}}^{-3}\}$ é uma base integral de $\mathbb{L}$. Assim, o elemento α pode ser escrio da seguinte forma

$$\alpha = b_0 + b_1(\zeta_9+\zeta_9^{-1}) + b_2({\zeta_9}^2+{\zeta_9}^{-2}) + b_3({\zeta_{20}}^3+{\zeta_{20}}^{-3})$$

e, a norma desse elemento é dada por:

$$\mathcal{N}(\alpha) = \prod_{i=1,3,7,9,11,13,17,19} \sigma_i(b_0 + b_1(\zeta_9+\zeta_9^{-1}) + b_2({\zeta_9}^2+{\zeta_9}^{-2}) + b_3({\zeta_{20}}^3+{\zeta_{20}}^{-3})).$$

Além de satisfazer a expressão da norma $\mathcal{N}(\alpha)$, precisamos ter $\sigma_i(\alpha) > 0$, $\sigma_i(\alpha) \in \mathbb{R}$, para todo $i = 1, 3, 7, 9, 11, 13, 17, 19$, pois estamos trabalhando com σ_α. Temos, por exemplo, que os elementos

$$2-(\zeta_9+\zeta_9^{-1})+({\zeta_9}^2+{\zeta_9}^{-2}) \quad \text{e} \quad 2-({\zeta_9}^2+{\zeta_9}^{-2}) \tag{5.2.11}$$

satisfazem essas condições.

A partir dos dados das Tabelas (5.13) e (5.14) e dos elementos dados em (5.2.11), apresentamos na Tabela (5.15) as combinações encontradas de α e $\mathfrak{a}$ que darão t_α e, com isso reticulados com densidades de centro recordes para a dimensão 8. Sejam $\gamma_1 = \zeta_{20}+\zeta_{20}^{-1}$ e $\gamma_2 = \zeta_{20}^2+\zeta_{20}^{-2}$.

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$	$\mathcal{N}(\alpha)$	α	t_α
16	$\pm(1-2\zeta_{20}-\zeta_{20}^5+2\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$, $\pm(1-\zeta_{20}^3+\zeta_{20}^4-\zeta_{20}^6-\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$	25	$2-\gamma_1+\gamma_2$	40
80	$\pm(2-\zeta_{20}^2+2\zeta_{20}^4-2\zeta_{20}^6+\zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$, $\pm(1-\zeta_{20}^2-\zeta_{20}^3-\zeta_{20}^4-\zeta_{20}^6)\mathcal{O}_{\mathbb{K}}$	1	$3-\gamma_2$	40
256	$\pm(2+\zeta_{20}+2\zeta_{20}^4-\zeta_{20}^6)\mathcal{O}_{\mathbb{K}}$, $\pm(1+\zeta_{20}+\zeta_{20}^2+\zeta_{20}^3+\zeta_{20}^4)\mathcal{O}_{\mathbb{K}}$	25	$2-\gamma_1+\gamma_2$	40

Tabela 5.15:

Observação 5.2.8 *Observe que para dimensão 8, encontramos menos exemplos, isso se deve*

ao custo computacional que ocorre para dimensões grandes devido a quantidade de elementos na base que aumenta junto com a dimensão do corpo.

Agora, vamos ilustrar no exemplo a seguir, um reticulado com densidade de centro ótima para dimensão 8, a partir dos dados da Tabela (5.15).

Exemplo 5.2.7 *Sejam o corpo* $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, $\mathfrak{a} = (2 + 2\zeta_{20} - \zeta_{20}^3 + \zeta_{20}^4 + \zeta_{20}^5 - \zeta_{20}^6 - \zeta_{20}^7)\mathcal{O}_{\mathbb{K}}$, *um ideal de* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$ *e* $\alpha = 3 - (\zeta_{20} + \zeta_{20}^{-1}) - (\zeta_{20}^2 + \zeta_{20}^{-2}) + (\zeta_{20}^3 + \zeta_{20}^{-3}) \in \mathcal{O}_{\mathbb{K}}$. *Temos que* $n = [\mathbb{K} : \mathbb{Q}] = 8$, $\mathcal{D}_{\mathbb{K}} = 2^8 5^6$, $\mathcal{N}(\mathfrak{a}) = 16$ *e* $\mathcal{N}(\alpha) = 25$. *Dado* $x \in \mathfrak{a}$, *podemos escrever* $x = (2+2\zeta_{20}-\zeta_{20}^3+\zeta_{20}^4+\zeta_{20}^5-\zeta_{20}^6-\zeta_{20}^7)(a_0+a_1\zeta_{20}+a_2\zeta_{20}^2+a_3\zeta_{20}^3+a_4\zeta_9 20^4+a_5\zeta_{20}^5+a_6\zeta_{20}^6+a_7\zeta_{20}^7)$, *onde* $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Z}$. *Assim,* $Tr(\alpha x\bar{x}) = 40a_0^2+40a_0a_1+40a_1^2+40a_0a_2+40a_1a_2+40a_2^2+40a_0a_3+40a_1a_3+40a_2a_3+40a_3^2+40a_1a_4+40a_2a_4+40a_3a_4+40a_4^2+40a_2a_5+40a_3a_5+40a_4a_5+40a_5^2+40a_3a_6+40a_4a_6+40a_5a_6+40a_6^2-20a_2a_7+20a_3a_7+40a_4a_7+80a_6a_7+80a_7^2$ *e, então* $t_\alpha = min\{Tr(\alpha x\bar{x}) \ : \ x \in \mathfrak{a}, \ x \neq 0\} = 40$, *com* $a_0 = 0, a_1 = 0, a_2 = -1, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_\alpha(\mathfrak{a})) = \frac{1}{2^n(|\mathcal{D}_{\mathbb{K}}|\mathcal{N}(\alpha))^{\frac{1}{2}}}\frac{(t_\alpha)^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})} = \frac{1}{2^8(2^8 5^6.25)^{\frac{1}{2}}}\frac{40^{\frac{8}{2}}}{16} = \frac{1}{16} \cong 0,06250,$$

que é a mesma densidade de centro do reticulado E_8.

5.2.5 Reticulados algébricos rotacionados de dimensão 12

Apresentamos nesta seção, reticulados algébricos que são versões rotacionadas do reticulado K_{12}, que é o reticulado com densidade de centro recorde para dimensão 12, através da perturbação σ_α do homomorfismo canônico e utilizando ideais principais. Neste caso, tomamos em todo processo $\alpha = 1$, para facilitar as contas. Daí, trabalhar com a perturbação σ_α é equivalente a trabalharmos com o homomorfismo canônico.

Para isso, consideremos o corpo $\mathbb{K} = \mathbb{Q}(\zeta_{21})$. Temos que $[\mathbb{K} : \mathbb{Q}] = 12$, o anel dos inteiros deste corpo é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}(\zeta_{21})$, uma base integral é $\{1, \zeta_{21}, \zeta_{21}^2, \zeta_{21}^3, \zeta_{21}^4, \zeta_{21}^5, \zeta_{21}^6, \zeta_{21}^7, \zeta_{21}^8, \zeta_{21}^9, \zeta_{21}^{10}, \zeta_{21}^{11}\}$, discriminante $\mathcal{D}_{\mathbb{K}} = 3^6 7^{10}$ e, os monormorfismos são:

$$\sigma_i(\zeta_{21}) = \zeta_{21}^i, \text{ com } i = 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, , 20.$$

Como dissemos, para dimensão 12, o reticulado com densidade de centro recorde é o K_{12}, cuja densidade de centro é $\frac{1}{27}$. Assim, basta igualarmos a fórmula da densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ é $\frac{1}{27}$ que teremos novos reticulados com densidade de centro ótima. Já temos que $n = 12$ e $|\mathcal{D}_{\mathbb{K}}| = 3^6 7^{10}$. Assim, precisamos encontrar convenientes $\mathfrak{a}$ e t para que tenhamos $\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{27}$. Utilizando programa Mathematica, temos que uma combinação satisfatória é

tomar $\mathcal{N}(\mathfrak{a}) = 7$ e $t = 28$. Um ideal principal de $\mathcal{O}_{\mathbb{K}}$ é da forma

$$\mathfrak{a} =< a_0 + a_1\zeta_{21} + a_2\zeta_{21}^2 + a_3\zeta_{21}^3 + a_4\zeta_{21}^4 + a_5\zeta_{21}^5 + a_6\zeta_{21}^6 + a_7\zeta_{21}^7 + a_8\zeta_{21}^8 + a_9\zeta_{21}^9 + a_{10}\zeta_{21}^{10} + a_{11}\zeta_{21}^{11} >,$$

com $a_i \in \mathbb{Z}$, para todo $i = 0, \cdots, 11$. A norma deste ideal é calculada da seguinte forma

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}\left(< \sum_{j=1}^{11} a_j\zeta_{21}^j >\right) = \left|\mathcal{N}\left(\sum_{j=1}^{11} a_j\zeta_{21}^j\right)\right|,$$

e pela definição de norma de um elemento temos que

$$\mathcal{N}(\mathfrak{a}) = \left|\prod_{i=1,2,4,5,8,10,11,13,16,17,19,20} \sigma_i\left(\sum_{j=1}^{11} a_j\zeta_{21}^j\right)\right|$$

e, fazendo os cálculos obtemos uma expressão para $\mathcal{N}(\mathfrak{a})$. Na Tabela (5.16) apresentamos alguns ideais $\mathfrak{a}$ que possuem $\mathcal{N}(\mathfrak{a}) = 7$.

$\mathcal{N}(\mathfrak{a})$	$\mathfrak{a}$
7	$\pm(1+\zeta_{21}^6-\zeta_{21}^8)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_{21}^4+\zeta_{21}^6)\mathcal{O}_{\mathbb{K}},$ $\pm(1-\zeta_{21}^2+\zeta_{21}^6)\mathcal{O}_{\mathbb{K}},\ \pm(1-\zeta_{21}^2+\zeta_{21}^8)\mathcal{O}_{\mathbb{K}},$ $\pm(\zeta_{21}^2-\zeta_{21}^4+\zeta_{21}^8)\mathcal{O}_{\mathbb{K}}$

Tabela 5.16:

Observação 5.2.9 *1. Os ideais da Tabela (5.16) foram obtidos tomando $a_1 = a_3 = a_5 = a_7 = a_9 = a_{10} = a_{11} = 0$ e os demais escalares variando entre -1 e 1.*

2. Tomando qualquer um dos ideais da Tabela (5.16) temos $t = 28$ e portanto reticulados com densidade de centro recorde.

Através do Exemplo (5.2.8), vamos ilustrar um reticulado com densidade de centro ótima para dimensão 12, a partir dos dados da Tabela (5.16).

Exemplo 5.2.8 *Sejam o corpo $\mathbb{K} = \mathbb{Q}(\zeta_{21})$, $\mathfrak{a} = (\zeta_{21}^2 - \zeta_{21}^4 + \zeta_{21}^8)\mathcal{O}_{\mathbb{K}}$, um ideal de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{21}]$. Temos que $n = [\mathbb{K} : \mathbb{Q}] = 12$, $\mathcal{D}_{\mathbb{K}} = 3^6 7^{10}$, $\mathcal{N}(\mathfrak{a}) = 7$. Dado $x \in \mathfrak{a}$, podemos escrever $x = (\zeta_{21}^2-\zeta_{21}^4+\zeta_{21}^8)(a_0+a_1\zeta_{21}+a_2\zeta_{21}^2+a_3\zeta_{21}^3+a_4\zeta_{21}^4+a_5\zeta_{21}^5+a_6\zeta_{21}^6+a_7\zeta_{21}^7+a_8\zeta_{21}^8+a_9\zeta_{21}^9+a_{10}\zeta_{21}^{10}+a_{11}\zeta_{21}^{11})$, onde $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11} \in \mathbb{Z}$. Assim,*

$Tr(\alpha x\bar{x}) = 28a_0^2 + 28a_1^2 + 28a_0a_{10} - 14a_1a_{10} + 28a_{10}^2 + 28a_0a_{11} + 28a_1a_{11} + 28a_{11}^2 - 14a_0a_2 - 14a_{11}a_2 + 28a_2^2 - 14a_0a_3 - 14a_1a_3 - 28a_{10}a_3 + 28a_3^2 - 14a_0a_4 - 14a_1a_4 - 28a_{11}a_4 - 14a_2a_4 + 28a_4^2 + 28a_0a_5 - 14a_1a_5 + 28a_{10}a_5 - 14a_2a_5 - 14a_3a_5 + 28a_5^2 + 28a_1a_6 - 14a_{10}a_6 + 28a_{11}a_6 - 14a_2a_6 - 14a_3a_6 - 14a_4a_6 + 28a_6^2 - 28a_0a_7 - 14a_{10}a_7 - 14a_{11}a_7 + 28a_2a_7 - 14a_3a_7 - 14a_4a_7 - 14a_5a_7 + 28a_7^2 -$

$28a_1a_8 - 14a_{10}a_8 - 14a_{11}a_8 + 28a_3a_8 - 14a_4a_8 - 14a_5a_8 - 14a_6a_8 + 28a_8^2 - 14a_0a_9 - 14a_{11}a_9 - 28a_2a_9 + 28a_4a_9 - 14a_5a_9 - 14a_6a_9 - 14a_7a_9 + 28a_9^2$
e, então $t = min\{Tr(\alpha x\bar{x}) \ : \ x \in \mathfrak{a}, \ x \neq 0\} = 28$, *com* $a_0 = 0, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = -1, a_8 = 0, a_9 = 0, a_{10} = 0, a_{11} = 0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2^n|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}}\frac{t^{\frac{n}{2}}}{\mathcal{N}(\mathfrak{a})} = \frac{1}{2^{12}|3^67^{10}|^{\frac{1}{2}}}\frac{28^{\frac{12}{2}}}{7} = \frac{1}{3^3} \cong 0,037037,$$

que é a mesma densidade de centro do reticulado K_{12}.

5.3 Conclusão do capítulo

Consideramos este, o capítulo mais importante deste trabalho, pois aqui demos nossa contribuição para a teoria de reticulados, apresentando novos exemplos de reticulados rotacionados de dimensões 2, 4, 6, 8 e 12 por meio da construção proposta na Seção (5.2). Iniciamos este capítulo definindo os homomorfismos que iriamos trabalhar e mostrando que, através destes, podemos obter reticulados no $\mathbb{R}^n$ utilizando o anel dos interiros algébricos de um corpo de números. Para a perturbação σ_α, por exemplo, isto é provado no Corolário (5.1.2). Note que em todos os exemplos apresentados neste capítulo, trabalhamos com os corpos ciclotômicos e seu subcorpo maximal real pois, como havíamos dito no Capítulo (1), estes corpos são muito interessantes de se trabalhar quando tratamos de reticulados, já que neles sabemos qual é o seu anel dos inteiros, temos uma $\mathbb{Z}$-base e uma expressão para calcularmos seu discriminante, fatores estes, importantes quando calculamos a densidade de centro de um reticulado. Também utilizamos muito os conceitos de forma quadrática, vistos no capítulo (2), pois como vimos, uma das maiores dificuldades ao calcular a densidade de centro é encontrar uma expressão para a função traço e minimizá-la. Ressaltamos ainda que, a obtenção de reticulados rotacionados neste trabalho foi feita através da perturbação σ_α do homomorfismo canônico, mas poderiamos ter feito o mesmo processo utilizando a perturbação $\sigma_{2\alpha}$ que o grau de difilculdade seria o mesmo já que a fórmula da densidade de centro é a mesma para ambas as perturbações, como pode ser visto nas Proposições (5.1.4) e (5.1.6). Mas, isso não significa que os reticulados encontrados seriam os mesmos. Decidimos, neste capítulo, trabalhar com a perturbação σ_α para mostrar os resultados e, como veremos no Capítulo (6), iremos utilizar a perturbação $\sigma_{2\alpha}$ para mostrarmos os resultados do capítulo. E, como foi dito, para o homomorfismo canônico, o estudo já foi feito por Ferrari, em [11].

Capítulo 6

Reticulados Ideais

No Capítulo (5) apresentamos reticulados a partir das perturbações do homomorfismo canônico e denominamos estes por reticulados algébricos. Neste capítulo apresentamos os reticulados ideais, que são definidos a partir de um ideal fracionário e uma forma bilinear simétrica, como veremos na Seção (6.1), onde veremos também algumas propriedades destes reticulados. Na Seção (6.2), veremos também que os reticulados ideais são obtidos a partir do homomorfismo $\sigma_{2\alpha}$. Na Seção (6.3) veremos os conceitos de diversidade e distância produto mínima de um reticulado ideal. Vimos que o interessante é ter reticulados com diversidade e distância produto mínima alta. Assim, na Seção (6.4) iremos procurar reticulados rotacionados do reticulado $\mathbb{Z}^n$ com esta propriedade. Para estas construções de $\mathbb{Z}^n$-reticulados rotacionados, utilizaremos o subcorpo maximal dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_{2^r})$, onde p é um número primo e r é um inteiro positivo.

6.1 Definição

Nesta seção veremos a definição de reticulado ideal e de alguns de seus parâmetros.

Definição 6.1.1 *Um* **reticulado inteiro** *é um par (L, b), onde L é um $\mathbb{Z}$-módulo livre de posto n, e $b : L \times L \to \mathbb{Z}$ é uma forma $\mathbb{Z}$-bilinear simétrica. Se $\{v_1, v_2, \ldots, v_n\}$ é uma base de L então a matriz que representa a forma bilinear b é dada por $(b(v_i, v_j))_{i,j=1}^n$ e, o* **determinante** *de b é o determinante da matriz de b em alguma base de L.*

Observação 6.1.1 *Temos que b pode ser diagonalizada sobre os números reais e, b é isomorfa a soma ortogonal de r cópias de $\langle 1 \rangle$ e s cópias de $\langle -1 \rangle$, para inteiros não negativos r e s.*

Definição 6.1.2 *Definimos a* **assinatura** *de b pelo par (r,s) e denotamos esta assinatura por $sign(b) = (r, s)$.*

Definição 6.1.3 *Dizemos que o reticulado (L, b) é* **par** *se $b(x, x)$ é um número par para todo $x \in L$. Caso contrário, dizemos que o reticulado (L, b) é* **ímpar**.

Definição 6.1.4 *O reticulado (L, b) é* **positivo** *se $b(x, x) > 0$ para todo $x \in L$, $x \neq 0$. Nesse caso, o* **mínimo** *de (L, b) é definido por $min(L, b) = min\{b(x, x)$ tal que $x \in L$, $x \neq 0\}$. O valor $b(x, x)$ é chamado de* **comprimento quadrático** *de x.*

Sejam $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, $\phi : \mathbb{K} \to \mathbb{K}$ a conjugação complexa com corpo fixo dado por $\mathbb{F} = \{x \in \mathbb{K} | \phi(x) = x\} = \mathbb{Q}$ e $[\mathbb{K} : \mathbb{F}] = 2$, $\mathfrak{I}$ um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\alpha \in \mathbb{F}$ tal que $\alpha\mathfrak{I}\phi(\mathfrak{I}) \subset \Delta(\mathbb{K}/\mathbb{Q})^{-1}$, onde $\Delta(\mathbb{K}/\mathbb{Q})^{-1} = \{x \in \mathbb{K} | Tr \subseteq \mathbb{Z}\}$ é o codiferente de $\mathbb{K}/\mathbb{Q}$ como definido em (1.5.1).

Proposição 6.1.1 *([22]) Nas condições anteriores, se $b_\alpha : \mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}$ é tal que $b_\alpha(x, y) = Tr(\alpha x\phi(y))$, então b_α está bem definida e é uma forma bilinear simétrica.*

Demonstração: Como $\alpha\mathfrak{I}\phi(\mathfrak{I}) \subset \Delta(\mathbb{K}/\mathbb{Q})^{-1} = \{x \in \mathbb{K} | Tr \subseteq \mathbb{Z}\}$ segue que $Tr(\alpha x\phi(y)) \in \mathbb{Z}$, para todo $(x, y) \in \mathfrak{I} \times \mathfrak{I}$. Logo, b_α está bem definida. Para mostrar que b_α é uma forma bilinear simétrica observe que como $\mathbb{K}$ é totalmente real ou um CM-corpo segue que a conjugação complexa comuta com todos os homomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Assim,

$$\begin{aligned} b_\alpha(x, y) &= Tr(\alpha x\phi(y)) = Tr(\phi(\phi(\alpha)\phi(x)y)) \\ &= \phi(Tr(\phi(\alpha)\phi(x)y)) = Tr(\alpha\phi(x)y) \\ &= b_\alpha(y, x), \end{aligned}$$

como queríamos demonstrar. ∎

Através das condições dadas acima podemos definir um reticulado ideal.

Definição 6.1.5 *Sejam $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, $\mathfrak{I}$ um ideal fracionário de $\mathbb{K}$, $\alpha \in \mathbb{F} = \{x \in \mathbb{K} | \phi(x) = x\}$ tal que $\alpha\mathfrak{I}\phi(\mathfrak{I}) \subset \Delta(\mathbb{K}/\mathbb{Q})^{-1}$, onde ϕ é a conjugação complexa. Um* **reticulado ideal** *é um reticulado inteiro $(\mathfrak{I}, b_\alpha)$, onde $b_\alpha : \mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}$ é tal que $b_\alpha(x, y) = Tr(\alpha x\phi(y))$. Dizemos que o par $(\mathfrak{I}, b_\alpha)$ é um* **$\mathcal{O}_{\mathbb{K}}$-reticulado**, *ou que é obtido por uma construção traço escalonada.*

Definição 6.1.6 *Quando $\alpha = 1$, dizemos que $(\mathfrak{I}, b)$ é obtido por uma construção traço ou que é do tipo traço.*

Proposição 6.1.2 *([5]) Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ seu anel dos inteiros e ϕ a conjugação complexa. Se existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \phi(\gamma) = 1$, então o $\mathcal{O}_{\mathbb{K}}$-reticulado é par.*

Demonstração: Mostremos que o $\mathcal{O}_{\mathbb{K}}$-reticulado $(\mathfrak{I}, b_\alpha)$ é par, onde $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ e $b_\alpha : \mathfrak{I} \times \mathfrak{I} \to \mathbb{Z}$ é tal que $b_\alpha(x,y) = Tr(\alpha x\phi(y))$, com $\alpha \in \mathbb{F}$ e $\alpha\mathfrak{I}\phi(\mathfrak{I}) \subset \Delta(\mathbb{K}/\mathbb{Q})^{-1}$. Seja $x \in \mathfrak{I}$ e $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \phi(\gamma) = 1$. Temos que:

$$\begin{aligned} b_\alpha(x,x) &= Tr(\alpha x\phi(x)) = Tr((\gamma+\phi(\gamma))(\alpha x\phi(x))) \\ &= Tr(\gamma\alpha x\phi(x) + \phi(\gamma)\alpha x\phi(x)) = Tr(\gamma\alpha x\phi(x)) + Tr(\phi(\gamma)\alpha x\phi(x)) \\ &= Tr(\gamma\alpha x\phi(x)) + Tr(\phi(\gamma\phi(\alpha)\phi(x)x)) = Tr(\gamma\alpha x\phi(x)) + \phi(Tr(\gamma\alpha\phi(x)x)) \\ &= 2\Re(Tr(\gamma\alpha x\phi(x))) \in 2\mathbb{Z}. \end{aligned}$$

Portanto, $b_\alpha(x,x)$ é um número par. ∎

Proposição 6.1.3 *([5]) Sejam $\mathbb{K}$ um corpo de números, ϕ uma involução sobre $\mathbb{K}$ e $\mathbb{F}$ o corpo fixo da involução. Suponhamos que $\mathbb{F}$ seja totalmente real e $\mathbb{K}$ totalmente imaginário. Se $\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal fracionário e $(\mathfrak{I}, b)$ é um $\mathcal{O}_{\mathbb{K}}$-reticulado do tipo traço, então $min(\mathfrak{I}, b) \geq [\mathbb{K} : \mathbb{Q}]$.*

Demonstração: Por hipótese $(\mathfrak{I}, b)$ é um $\mathcal{O}_{\mathbb{K}}$-reticulado do tipo traço. Assim, se $x \in \mathfrak{I}$ então $b(x,x) = Tr(x\phi(x))$. Sejam $n = [\mathbb{K} : \mathbb{Q}]$ e $\sigma_1, \cdots, \sigma_n$ os n homomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$. Pela desigualdade entre as médias aritmética e geométrica dos homomorfirmos aplicados no elemento $x\phi(x) \in \mathfrak{I}\phi(\mathfrak{I})$, temos que

$$\frac{\sum_{i=1}^{n} \sigma(x\phi(x))}{n} \geq \left[\prod_{i=1}^{n} \sigma(x\phi(x))\right]^{1/n},$$

e então

$$\sum_{i=1}^{n} \sigma(x\phi(x)) \geq n\left[\prod_{i=1}^{n} \sigma(x\phi(x))\right]^{1/n}.$$

Logo, $Tr(x\phi(x)) \geq nN(x\phi(x))^{1/n}$. Como $x \in \mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$, segue que $N(x\phi(x)) \geq 1$. Portanto $min(\mathfrak{I}, b) \geq [\mathbb{K} : \mathbb{Q}]$. ∎

6.2 Reticulados ideais obtidos a partir da perturbação $\sigma_{2\alpha}$ do homomorfismo canônico

Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, \cdots, \sigma_n$ os n homomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$, $\alpha \in \mathbb{K}$ tal que $\alpha_i \in \mathbb{R}$ e $\sigma_i(\alpha) > 0$, para todo $i = 1, \cdots, n$ e $\sigma_{2\alpha} : \mathbb{K} \to \mathbb{R}^n$ a perturbação $\sigma_{2\alpha}$ do homomorfismo canônico, como definida em (5.1.4).

O principal fator para definirmos tanto o homomorfismo canônico quanto suas perturbações é termos uma $\mathbb{Z}$-base de n elementos. Como todo ideal $\mathfrak{I}$ de $\mathcal{O}_{\mathbb{K}}$ possui uma $\mathbb{Z}$-base de n elementos, então podemos construir reticulados a partir de $\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$.

Assim, se $\{w_1, \cdots, w_n\}$ for uma $\mathbb{Z}$-base de $\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$, então temos pelo resultado (5.1.3) que a imagem de $\sigma_{2\alpha}(\mathfrak{I})$ em $\mathbb{R}^n$ é um reticulado com base $\{\sigma_\alpha(w_1), \cdots, \sigma_\alpha(w_n)\}$ e matriz geradora dada por:

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_n}\sigma_n(w_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_1) & \cdots & \sqrt{2\alpha_{r_2}}\Im\sigma_{r_2}(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_n}\sigma_n(w_2) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_2) & \cdots & \sqrt{2\alpha_{r_2}}\Im\sigma_{r_2}(w_2) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_n}\sigma_n(w_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_n) & \cdots & \sqrt{2\alpha_{r_2}}\Im\sigma_{r_2}(w_n) \end{pmatrix}, \quad (6.2.1)$$

onde $\alpha_i = \sigma_i(\alpha)$, para todo $i = 1, \cdots, n$.

Observação 6.2.1 *A matriz de Gram associada ao reticulado $\sigma_{2\alpha}(\mathfrak{I})$ é dada por $G = MM^t = (g_{ij})_{i,j=1}^n$, onde*

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{r_1} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) + \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_i))\sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_j)) + \\ &\quad \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}}\Im(\sigma_{r_1+k}(w_i))\sqrt{2\alpha_{r_1+k}}\Im(\sigma_{r_1+k}(w_j)) \\ &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \\ &\quad \sum_{k=1}^{r_2} 2\alpha_{r_1+k}[\Re(\sigma_{r_1+k}(w_i))\Re(\sigma_{r_1+k}(w_j)) + \Im(\sigma_{r_1+k}(w_i))\Im(\sigma_{r_1+k}(w_j))]. \end{aligned} \quad (6.2.2)$$

Proposição 6.2.1 *([22]) Se $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, então o reticuado $\sigma_{2\alpha}(\mathfrak{I})$ é um reticulado ideal.*

Demonstração: Para provarmos que o reticulado $\sigma_{2\alpha}(\mathfrak{I})$ é um reticulado ideal precisamos mostrar que a forma bilinear associada é do tipo traço. Vimos que a matriz de Gram associada a este reticulado tem entradas dadas por (6.2.2). Como por hipótese $\mathbb{K}$ é totalmente real ou um CM-corpo temos que a conjugação complexa comuta com todos os σ_i, para $i = 1, \cdots, n$. Assim,

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(w_i)\sigma_{r_1+k}(\overline{w_j})) \\ &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(w_i\overline{w_j})) \\ &= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\sigma_{r_1+k}(w_i\overline{w_j}) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\overline{\sigma_{r_1+k}(w_i\overline{w_j})} \end{aligned}$$

$$= \quad Tr_{\mathbb{K}/\mathbb{Q}}(\alpha w_i \overline{w_j}).$$

Logo, a matriz de Gram é do tipo traço e portanto, sua matriz geradora M define um reticulado ideal. ■

Observação 6.2.2 *Para que o reticulado ideal $\sigma_{2\alpha}(\mathfrak{I})$ seja definido positivo, basta que $\alpha \in \mathbb{K}$ seja positivo.*

A seguir apresentamos uma expressão para calcularmos o determinante do reticulado ideal $(\mathfrak{I}, b_\alpha)$ que é denotado por $det(b_\alpha)$.

Proposição 6.2.2 *([22]) Sejam $\mathbb{K}$ um corpo de números totalmente real ou um CM-corpo, $\mathfrak{I}$ um ideal fracionário não nulo de $\mathcal{O}_\mathbb{K}$, $\mathcal{D}_\mathbb{K}$ o discriminante de $\mathbb{K}$ e b_α a forma bilinear simétrica associada. Se $(\mathfrak{I}, b_\alpha)$ é um reticulado ideal, então*

$$|det(b_\alpha)| = \mathcal{N}(\alpha)\mathcal{N}(\mathfrak{I})^2|\mathcal{D}_\mathbb{K}|.$$

Demonstração: Se $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_\mathbb{K}$ então pelo Lema (1.3.6) existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathfrak{I} \subset \mathcal{O}_\mathbb{K}$. Denotemos por $\mathfrak{a} = d\mathfrak{I}$. Como $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\mathfrak{a}$ é um $\mathbb{Z}$-submódulo de $\mathcal{O}_\mathbb{K}$, pelo Teorema (1.1.3) segue que existe uma $\mathbb{Z}$-base $\{w_1, \cdots, w_n\}$ de $\mathcal{O}_\mathbb{K}$ e inteiros $a_1, \cdots, a_n$ tais que $\{a_1 w_1, \cdots, a_n w_n\}$ é uma $\mathbb{Z}$-base de $\mathfrak{a}$. Como $\mathfrak{a} = d\mathfrak{I}$ segue que $\mathfrak{I} - d^{-1}\mathfrak{a}$ e então $\{a_1 d^{-1} w_1, \cdots, a_n d^{-1} w_N\}$ é uma $\mathbb{Z}$-base de $\mathfrak{I}$. Assim, a matriz de b_α é dada por:

$$\begin{pmatrix} Tr(\alpha a_1 d^{-1} w_1 \overline{a_1 d^{-1} w_1}) & \cdots & Tr(\alpha a_1 d^{-1} w_1 \overline{a_n d^{-1} w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha a_n d^{-1} w_n \overline{a_1 d^{-1} w_1}) & \cdots & Tr(\alpha a_n d^{-1} w_n \overline{a_n d^{-1} w_n}) \end{pmatrix}$$

$$= \begin{pmatrix} a_1^2 Tr(\alpha (d^{-1})^2 w_1 \overline{w_1}) & \cdots & a_1 a_n Tr(\alpha (d^{-1})^2 w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ a_1 a_n Tr(\alpha (d^{-1})^2 w_n \overline{w_1}) & \cdots & a_n^2 Tr(\alpha (d^{-1})^2 w_n \overline{w_n}) \end{pmatrix}.$$

Calculando o determinante desta matriz temos que

$$det(b_\alpha) = (a_1 \cdots a_n)^2 det \begin{pmatrix} Tr(\alpha (d^{-1})^2 w_1 \overline{w_1}) & \cdots & Tr(\alpha (d^{-1})^2 w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha (d^{-1})^2 w_n \overline{w_1}) & \cdots & Tr(\alpha (d^{-1})^2 w_n \overline{w_n}) \end{pmatrix}$$

$$= (a_1 \cdots a_n)^2 ((d^{-1})^2)^n det \begin{pmatrix} Tr(\alpha w_1 \overline{w_1}) & \cdots & Tr(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha w_n \overline{w_1}) & \cdots & Tr(\alpha w_n \overline{w_n}) \end{pmatrix}.$$

Pela Proposição (1.3.10) temos que $\mathcal{N}(\mathfrak{a}) = |a_1 \cdots a_n|$. Assim,

$$det(b_\alpha) = \mathcal{N}(\mathfrak{a})^2((d^{-1})^2)^n det(H), \tag{6.2.3}$$

onde

$$H = \begin{pmatrix} Tr(\alpha w_1 \overline{w_1}) & \cdots & Tr(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha w_n \overline{w_1}) & \cdots & Tr(\alpha w_n \overline{w_n}) \end{pmatrix}.$$

Mas, note que H pode ser escrita da forma $H = MM^{\perp}$, onde

$$M = ST = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix} \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}$$

e $\perp$ denota a transposta conjugada. Assim,

$$\begin{aligned} det(H) &= det(MM^{\perp}) = det(M)det(M^{\perp}) \\ &= det(ST)det((ST)^{\perp}) = det(S)det(T)det(T^{\perp})det(S^{\perp}) \\ &= (det(T))^2 det(S)det(S^{\perp}) = (det(T))^2 |det(S)|^2. \end{aligned}$$

Mas, temos que

$$(det(T))^2 = \sigma_1(\alpha) \cdots \sigma_n(\alpha) = \mathcal{N}(\alpha). \tag{6.2.4}$$

Por outro lado,

$$det(S) = det(\sigma_i(w_j))_{i,j=1}^n = \sqrt{\mathcal{D}_{\mathbb{K}}}. \tag{6.2.5}$$

Logo, substituindo as Equações (6.2.4) e (6.2.5) na Equação (6.2.3) temos que

$$det(b_\alpha) = \mathcal{N}(\mathfrak{a})^2((d^{-1})^2)^n \mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|.$$

Agora, como $d \in \mathbb{Z}$, segue que $\mathcal{N}(\mathfrak{I}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(d^{-1}) = \mathcal{N}(\mathfrak{a})(d^{-1})^n$ e assim, $\mathcal{N}(\mathfrak{I})^2 = \mathcal{N}(\mathfrak{a})^2((d^{-1})^n)^2$. Portanto,

$$det(b_\alpha) = \mathcal{N}(\mathfrak{I})^2 \mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|,$$

como queríamos. ∎

6.3 Diversidade e distância produto mínima de um reticulado ideal

Nesta seção apresentamos alguns resultados sobre a diversidade e a distância produto mínima de um reticulado ideal a partir dos conceitos de diversidade e de distância produto mínima de

um reticulado vistos no Capítulo (3).

Vimos que os reticulados ideais podem ser dados por uma matriz geradora, esta é uma vantagem de se trabalhar com os reticulados ideais. Uma outra vantagem é que os pontos do reticulado são imagens de inteiros algébricos através do homomorfismo canônico ou suas perturbações aplicado em $\mathcal{O}_{\mathbb{K}}$. Assim, podemos estabelecer uma correspondência entre os pontos $x \in \Lambda \subseteq \mathbb{R}^n$ e os inteiros algébricos, como veremos na observação a seguir.

Observação 6.3.1 *A partir da matriz geradora M dada em (6.2.1), podemos expressar um ponto do reticulado como*

$$\begin{aligned} x &= (x_1, \cdots, x_{r_1}, x_{r_1+1}, \cdots, x_{r_1+r_2}) \\ &= (\sum_{i=1}^{n} \beta_i \sqrt{\alpha_1}\sigma_1(w_i), \cdots, \sum_{i=1}^{n} \beta_i \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_i)), \cdots, \sum_{i=1}^{n} \beta_i \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_i))) \\ &= (\sqrt{\alpha_1}\sigma_1(\sum_{i=1}^{n} \beta_i w_i), \cdots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(\sum_{i=1}^{n} \beta_i w_i)), \cdots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(\sum_{i=1}^{n} \beta_i w_i))) \end{aligned}$$

com $\beta_i \in \mathbb{Z}$, para todo $i = 1, \cdots, n$. Portanto,

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

para algum inteiro algébrico $y = \sum_{i=1}^{n} \beta_i w_i \in \mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$. Esta correspondência entre um vetor $x \in \mathbb{R}^n$ e um inteiro algébrico $y \in \mathcal{O}_{\mathbb{K}}$ facilita o cálculo de algumas propriedades de reticulados, como a diversidade e a distância produto mínima, que em geral são difíceis de calcular.

O resultado que veremos a seguir fornece uma expressão para calcularmos a diversidade de reticulados ideais.

Proposição 6.3.1 *([22]) Se $\mathbb{K}$ é um corpo de números de grau n e $\mathfrak{I}$ um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então o reticulado ideal $\Lambda = (\mathfrak{I}, b_\alpha)$ tem diversidade $div(\Lambda) = r_1 + r_2$.*

Demonstração: Seja $x \in \Lambda$ não nulo. Pela Observação (6.3.1), x pode ser escrito da seguinte forma:

$$x = \sigma_\alpha(y) = (\sqrt{\alpha_1}\sigma_1(y), \cdots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(y)), \cdots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(y))),$$

onde $y \in \mathfrak{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Como tomamos $x \neq 0$ segue que $y \neq 0$ e, sendo assim, temos que $\sigma_i(y) \neq 0$, para todo $i = 1, \cdots, n$. Logo, podemos afirmar que os primeiros r_1 coeficientes de x são não nulos. Asim, o número mínimo de coeficientes não nulos dos $2r_2$ que restaram é r_2, pois as

partes real e imaginária de um homomorfismo complexo não podem se anular simultaneamente. Logo, $div(\Lambda) = min\{div(x) : x \in \Lambda,\ x \neq 0\} \geq r_1 + r_2$, onde $div(x)$ é definida como o número de x_i' não nulos. Seja agora, $\beta \in \mathfrak{I}$ tal que $\beta \neq 0$. Como $\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{K}}$, segue que β é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$. Assim, existem $a_0, a_1, \cdots, a_n \in \mathbb{Z}$ tal que $\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_1\beta + a_0 = 0$ e $a_0 \neq 0$. Então,

$$-a_0 = \beta^m + a_{m-1}\beta^{m-1} + \cdots + a_1\beta \in \mathfrak{I}.$$

Como $-a_0 \in \mathbb{Z}$, segue que $\sigma_i(-a_0) = -a_0$, para todo $i = 1, \cdots, n$. Logo, $div(\sigma_{2\alpha}(-a_0)) = r_1 + r_2$. Portanto, $div(\Lambda) = r_1 + r_2$. ■

Corolário 6.3.1 *([22]) Seja $\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$ um ideal. Um reticulado ideal $\Lambda = (\mathfrak{I}, b_\alpha)$ pode ser imerso no $\mathbb{R}^n$, com*

1. *diversidade n se $\mathbb{K}$ é totalmente real.*
2. *diversidade $\dfrac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.*

Demonstração: Segue diretamente da Proposição (6.3.1). ■

Segue $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $x \in \Lambda$. Como vimos, a distância produto mínima de Λ é definida como a menor das distâncias $d_p(x) = \prod_{i=1}^{n}$, onde $x \in \Lambda,\ x \neq 0$. O resultado que veremos a seguir fornece uma expressão para calcularmos a distância produto mínima de um reticulado ideal $\Lambda = (\mathfrak{I}, b_\alpha)$.

Teorema 6.3.1 *([22]) Se $\mathbb{K}$ é um corpo de números totalmente real de grau n com discriminante $\mathcal{D}_{\mathbb{K}}$ e $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulado ideal é dada por:*

$$d_{p,min}(\Lambda) = \min(\mathfrak{I})\frac{|det(b_\alpha)|}{\mathbb{D}_{\mathbb{K}}},$$

onde $\min(\mathfrak{I}) = \min_{0 \neq y \in \mathfrak{I}} \dfrac{|\mathcal{N}(y)|}{\mathcal{N}(\mathfrak{I})}$.

Demonstração: Como $\mathbb{K}$ é totalmente real de grau n segue que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, para todo $i = 1, \cdots, n$ e, pela Proposição (6.3.1), temos que a diversidade de Λ é n. Se $x \in \Lambda \subset \mathbb{R}^n$, temos pela Observação (6.3.1), que x pode ser escrito como $x = \sigma_\alpha(y) = (\sqrt{\sigma_1(\alpha)}\sigma_1(y), \cdots, \sqrt{\sigma_n(\alpha)}\sigma_n(y))$. Assim,

$$d_{p,min}(\Lambda) \quad = \quad \min\{d_p(x) : x \in \Lambda,\ x \neq 0\} = \min_{0 \neq x \in \Lambda} \prod_{i=1}^{n} |x_i|$$

$$
\begin{aligned}
&= \min_{0\neq y\in\mathfrak{I}} \prod_{i=1}^{n} \left|\sqrt{\sigma_i(\alpha)}\sigma_i(y)\right| = \prod_{i=1}^{n}\sqrt{\sigma_i(\alpha)}\min_{0\neq y\in\mathfrak{I}}\prod_{i=1}^{n}|\sigma_i(y)| \\
&= \sqrt{\mathcal{N}(\alpha)}\min_{0\neq y\in\mathfrak{I}}|\mathcal{N}(y)|\,.
\end{aligned}
$$

Pela Proposição (6.2.2), temos que $|det(b_\alpha)| = \mathcal{N}(\alpha)\mathcal{N}(\mathfrak{I})^2|\mathcal{D}_\mathbb{K}|$, e deste modo $\sqrt{\mathcal{N}(\alpha)} = \frac{\sqrt{|det(b_\alpha)|}}{\mathcal{N}(\mathfrak{I})\sqrt{|\mathcal{D}_\mathbb{K}|}}$. Assim,

$$
\begin{aligned}
d_{p,min}(\Lambda) &= \frac{\sqrt{|det(b_\alpha)|}}{\mathcal{N}(\mathfrak{I})\sqrt{|\mathcal{D}_\mathbb{K}|}}\min_{0\neq y\in\mathfrak{I}}|\mathcal{N}(y)| \\
&= \frac{\sqrt{|det(b_\alpha)|}}{\sqrt{|\mathcal{D}_\mathbb{K}|}}\frac{\min_{0\neq y\in\mathfrak{I}}|\mathcal{N}(y)|}{\mathcal{N}(\mathfrak{I})} \\
&= \min(\mathfrak{I})\frac{\sqrt{|det(b_\alpha)|}}{\sqrt{|\mathcal{D}_\mathbb{K}|}},
\end{aligned}
$$

como queríamos provar. ∎

Lema 6.3.1 *([13]) Nas condições do Teorema (6.3.1), se $\mathfrak{I}$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então*

$$\min_{0\neq x\in\mathfrak{I}}|\mathcal{N}(x)| = \mathcal{N}(\mathfrak{I}).$$

Demonstração: Se $\mathfrak{I}\subseteq\mathcal{O}_\mathbb{K}$ é um ideal principal então existe $a\in\mathfrak{I}$ tal que $\mathfrak{I} =< a >$ e assim, $\mathcal{N}(\mathfrak{I}) = |\mathcal{N}(a)|$. Se $x\in\mathfrak{I}$, com $x\neq 0$, temos que $x = ay$, para algum $y\in\mathcal{O}_\mathbb{K}$. Assim,

$$|\mathcal{N}(x)| = |\mathcal{N}(a)||\mathcal{N}(y)| \geq \mathcal{N}(\mathfrak{I})$$

e, esta igualdade é verdadeira se, e somente se, $\mathcal{N}(y) = \pm 1$ e, isto ocorrerá se, e somente se, y é uma unidade de $\mathcal{O}_\mathbb{K}$. Logo, $|\mathcal{N}(x)| = \mathcal{N}(\mathfrak{I})$ quando $x = ay$, com y sendo uma unidade de $\mathcal{O}_\mathbb{K}$. Portanto, $\min_{0\neq x\in\mathfrak{I}}|\mathcal{N}(x)| = \mathcal{N}(\mathfrak{I})$. ∎

Corolário 6.3.2 *([22]) Nas condições do Teorema (6.3.1), se $\mathfrak{I}$ é um ideal principal de $\mathcal{O}_\mathbb{K}$ então a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, b_\alpha)$ é dado por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{|\det(b_\alpha)|}{|D_\mathbb{K}|}}.$$

Demonstração: Segue imediatamente do Teorema (6.3.1) e do Lema (6.3.1). ∎

6.4 Construções de $\mathbb{Z}^n$-reticulados rotacionados utilizando reticulados ideais

Oggier, em [22], mostrou que quanto maior for a diversidade $div(\Lambda)$ e a distância produto mínima $d_{p,min}(\Lambda)$ de um reticulado, menor é a probabilidade de ocorrerem erros em um dado código reticulado. Assim, faz sentido procuramos e estudarmos reticulados Λ com $div(\Lambda)$ alta e $d^l_{p,min}(\Lambda)$ máxima. Para isso, iremos estudar os $\mathbb{Z}^n$-reticulados e versões rotacionadas dele. A importância de estudar estes reticulados está no fato destes reticulados apresentarem implementações práticas. Deste modo, apresentamos duas construções de $\mathbb{Z}^n$-reticulados rotacionados. Na Seção (6.4.2), apresentamos a construção via o subcorpo maximal real dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um número primo e, na Seção (6.4.3), apresentamos outra construção via o subcorpo maximal real dos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$, onde r é um número inteiro positivo.

6.4.1 O reticulado $\mathbb{Z}^n$

Definição 6.4.1 *O reticulado $\mathbb{Z}^n$ é um reticulado n-dimensional definido por*

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

Temos que a base canônica $\beta = \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ é uma base para o reticulado $\mathbb{Z}^n$. Assim, a matriz identidade Id_n é uma matriz geradora M deste reticulado. Uma matriz de Gram para $\mathbb{Z}^n$ é dada por $G = M^tM = Id_n$. E, portanto, pela Definição (3.2.2) segue que $det(\mathbb{Z}^n) = 1$.

Como vimos no Corolário (6.3.1) os corpos de números totalmente reais tem diversidade máxima. Assim, para obtermos um reticulado ideal semelhante ao reticulado $\mathbb{Z}^n$, $n \geq 2$, com alta diversidade e distância produto mínima máxima, iremos trabalhar com corpos de números totalmente reais.

Sejam $\mathbb{L}$ um corpo de números totalmente real de grau n e $\mathcal{O}_\mathbb{L}$ seu anel de inteiros. Queremos encontrar um reticulado ideal $\Lambda = (\mathcal{O}_\mathbb{L}, b_\alpha)$ que seja um $\mathbb{Z}^n$-reticulado rotacionado, ou seja, um reticulado com as mesmas propriedades de $\mathbb{Z}^n$.

Observe que se multiplicarmos todos os pontos do reticulado $\mathbb{Z}^n$ pelo escalar $\sqrt{c}$, onde $c \in \mathbb{Z}$ teremos um outro reticulado $(\sqrt{c}\mathbb{Z})^n$ que será uma versão escalar de $\mathbb{Z}^n$, e que $\beta = \{(\sqrt{c}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \sqrt{c})\}$ é uma base para o reticulado $(\sqrt{c}\mathbb{Z})^n$ e, como $det(\mathbb{Z}^n) = 1$ segue que $det(\sqrt{c}\mathbb{Z}) = c^n$.

Daí, nas duas construções que apresentamos nas seções posteriores em vez de trabalharmos com o reticulado $\mathbb{Z}^n$, iremos trabalhar com sua versão escalar $(\sqrt{c}\mathbb{Z})^n$. Para isso, primeiramente

iremos encontrar $\alpha \in \mathbb{L}$ totalmente positivo tal que o reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ seja isomorfo ao reticulado $(\sqrt{c}\mathbb{Z})^n$. Após encontrarmos tal reticulado multiplicamos sua matriz geradora por $1/\sqrt{c}$ e assim, obtemos uma versão rotacionada de $\mathbb{Z}^n$.

6.4.2 Construção de $\mathbb{Z}^n$-reticulados rotacionados via o corpo ciclotômico $\mathbb{Q}(\zeta_p)$

Nesta seção, veremos a construção de $\mathbb{Z}^n$-reticulados rotacionados, $n \geq 2$, via o subcorpo maximal real $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ do corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo e $p \geq 5$, utilizando reticulados ideais. Desta forma, serão obtidos $\mathbb{Z}^n$-reticulados rotacionados para $n = \dfrac{p-1}{2}$, com p primo, $p \geq 5$.

Consideremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde $p \geq 5$ é um número primo e, $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ o subcorpo maximal real de $\mathbb{K}$. Pelo Teorema (1.4.2) temos que $[\mathbb{K} : \mathbb{Q}] = p - 1$ e pelo Teorema (1.4.3) que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ é o anel dos inteiros de $\mathbb{L}$ e, pelo Corolário (1.4.1), segue que $[\mathbb{K} : \mathbb{L}] = 2$. Assim, pela Observação (1.2.1), temos que $[\mathbb{L} : \mathbb{Q}] = \frac{p-1}{2} = n$.

Seja $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ um reticulado ideal, com $\alpha \in \mathbb{L}$ totalmente positivo e b_α a forma bilinear simétrica associada a Λ. Pela Proposição (6.2.2), para que $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ seja isomorfo ao reticulado $(\sqrt{c}\mathbb{Z})^n$, temos que o elemento $\alpha \in \mathbb{L}$ deve satisfazer a seguinte relação

$$\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)\mathcal{N}(\mathfrak{I})^2|\mathcal{D}_{\mathbb{L}}| = c^n,$$

onde $c^n = det((\sqrt{c}\mathbb{Z})^n)$, o que equivale a dizer que $\det(\Lambda) = c^n$. Como $\mathfrak{I} = \mathcal{O}_{\mathbb{L}}$, segue pela Proposição (1.3.9) que devemos ter

$$\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)|\mathcal{D}_{\mathbb{L}}| = c^n. \tag{6.4.6}$$

Queremos encontrar $\alpha \in \mathbb{L}$ totalmente positivo que satisfaça a Equação (6.4.6). Pela Proposição (1.4.7), temos que $\mathcal{D}_{\mathbb{L}} = p^{\frac{p-3}{2}}$. Assim,

$$\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)|\mathcal{D}_{\mathbb{L}}| = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)p^{\frac{p-3}{2}} = c^{\frac{p-1}{2}},$$

para algum $c \in \mathbb{Z}$. Tomando $c = p$ temos $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = p$. Assim, encontremos $\alpha \in \mathbb{L}$ totalmente positivo tal que $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = p$. Observe que $p\mathbb{Z}[\zeta_p] = (1-\zeta_p)^{p-1}\mathbb{Z}[\zeta_p]$, e assim $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) = p$. Usando a transitividade da norma (vista na Observação (1.3.3)), temos que

$$\begin{aligned} p &= \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(1-\zeta_p) = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\mathcal{N}_{\mathbb{K}/\mathbb{L}}(1-\zeta_p)) \\ &= \mathcal{N}_{\mathbb{L}/\mathbb{Q}}((1-\zeta_p)(1-\zeta_p^{-1})). \end{aligned} \tag{6.4.7}$$

Logo, tomando $\alpha = (1-\zeta_p)(1-\zeta_p{}^{-1}) = 2 - (\zeta_p + \zeta_p^{-1})$, temos que $\alpha \in \mathbb{L}$ é totalmente positivo

pois,

$$|\zeta_p + \zeta_p^{-1}| = |2\cos\frac{2\pi}{p}| < 2, \quad p \geq 5$$

e, pela Equação (6.4.7) segue que $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = p$.

Observação 6.4.1 *Note que, encontrar um elemento $\alpha \in \mathbb{L}$ totalmente positivo tal que $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)|\mathcal{D}_{\mathbb{L}}| = c^n$ não garante que $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$, ou seja, esta é apenas uma condição necessária.*

Agora, através de uma construção explícita, iremos mostrar que $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ é isomorfo a $\mathbb{Z}^n$. Pelo Teorema (1.4.3), temos que $\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^{\frac{p-1}{2}}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. No resultado a seguir encontramos uma outra $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{L}}$.

Lema 6.4.1 *([13]) Se $e_n^{'} = e_n$, $e_j^{'} = \sum_{i=j}^{n} e_i$, $j = 1, \cdots, n-1$, então $\{e_1^{'}, \cdots, e_n^{'}\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta + \zeta^{-1}]$.*

Demonstração: Mostremos que $\{e_1^{'}, \cdots, e_n^{'}\}$ é linearmente independente sobre $\mathbb{Z}$. De fato, seja $\sum_{i=1}^{n} a_i\overline{e_i} = 0$; $a_i \in \mathbb{Z}$. Temos que $\sum_{i=1}^{n} a_i e_i^{'} = a_1e_1 + (a_1+a_2)e_2 + \cdots + (a_1 + \cdots + a_{n-1})e_{n-1} + (a_1 + \cdots + a_n)e_n = 0$. Como $\{e_1, \cdots, e_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}}$, segue que $a_1 = \cdots = a_n = 0$. Mostremos agora que $\{e_1^{'}, \cdots, e_n^{'}\}$ gera $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Seja $x \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Temos que $x = \sum_{i=1}^{n} a_i e_i$; $a_i \in \mathbb{Z}$. Seja $b_1 = a_1$. Temos que $x = \sum_{i=2}^{n}(a_i - a_1)e_i + a_1(e_1 + \cdots + e_n) = \sum_{i=2}^{n}(a_i - a_1)e_i + b_1e_1^{'}$. Se $b_2 = (a_2 - a_1)$, então $x = \sum_{i=3}^{n}(a_i - a_1 - (a_2 - a_1))e_i + b_2e_2^{'} + b_1e_1^{'}$. Continuando desta forma, tomando $b_j = a_j - a_{j-1}$, $j = 2, \cdots, n$, temos que $x = \sum_{i=1}^{n} b_i e_i^{'}$. Portanto, $\{e_1^{'}, \cdots, e_n^{'}\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}}$. ∎

Proposição 6.4.1 *([13]) Se $\alpha = 2 - (\zeta_p + \zeta_p^{-1}) \in \mathbb{L}$ e $b_\alpha(x, y) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha xy)$, para todo $x, y \in \mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, então:*

1. $b_\alpha(e_i, e_i) = \begin{cases} p, & \text{se } i = n; \\ 2p, & \text{caso contrário.} \end{cases}$

2. $b_\alpha(e_i, e_j) = \begin{cases} -p, & \text{se } |i-j| = 1; \\ 0, & \text{caso contrário} \end{cases}$

Demonstração: Para simplificar a notação vamos denotar por $\sigma_k(\zeta_p)$ e por $\alpha_j = \sigma_j(\alpha)$, os conjugados de ζ_p e α, respectivamente. Temos que

$$Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^k + \zeta_p^{-k}) = -1, \text{ para } k = 1, \ldots, n.$$

De fato, como o polinômio ciclotômico de ζ_p é $f(x) = x^{p-1} + \cdots + x + 1$ e ζ_p^k, $k = 1, \cdots, n$ são conjugados de ζ_p, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^k) = -1$, $k = 1, \cdots, n$. Assim, como $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^k) = Tr_{\mathbb{L}/\mathbb{Q}}(Tr_{\mathbb{K}|\mathbb{L}}(\zeta_p^k))$, segue que $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^k + \zeta_p^{-k}) = -1$, para todo $k = 1, \cdots, n$. Desta forma, temos que

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha(\zeta_p^k + \zeta_p^{-k})) &= \sum_{j=1}^{n} \sigma_j(\alpha)\sigma_j(\zeta_p^k + \zeta_p^{-k}) \\ &= \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta_p^k + \zeta_p^{-k}) \\ &= \sum_{j=1}^{n} (2 - \sigma_j(\zeta_p - \zeta_p^{-1}))\sigma_j(\zeta_p^k + \zeta_p^{-k}) \\ &= -2 - \sum_{j=1}^{n} \sigma_j(\zeta_p^{k+1} + \zeta_p^{-k-1} + \zeta_p^{-k+1} + \zeta_p^{k-1}) \\ &= \begin{cases} -2 + 1 - 2n = -p, & \text{se } k = \pm 1 (\text{mod } p) \\ -2 + 1 + 1 = 0, & \text{caso contrário.} \end{cases} \end{aligned}$$

Agora, vamos calcular $b_\alpha(e_i, e_j)$. Temos que

$$\begin{aligned} b_\alpha(e_i, e_i) &= Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i^2) = \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta_p^{2i} + \zeta_p^{-2i} + 2) \\ &= \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta_p^{2i} + \zeta_p^{-2i}) + 2\sum_{j=1}^{n}(2 - \sigma_j(\zeta + \zeta_p^{-1})) \\ &= \begin{cases} p, & \text{se } i = n; \\ 2p, & \text{caso contrário.} \end{cases} \end{aligned}$$

e assim,

$$\begin{aligned} b_\alpha(e_i, e_j) &= Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i e_j) = \sum_{j=1}^{n}(\alpha_j \sigma_j(\zeta_p^{i+j} + \zeta_p^{-(i+j)})) + \sum_{j=1}^{n}(\alpha_j \sigma_j(\zeta_p^{i-j} + \zeta_p^{-(i-j)})) \\ &= \begin{cases} -p, & \text{se } |i - j| = 1; \\ 0, & \text{caso contrário,} \end{cases} \end{aligned}$$

o que prova o teorema. ■

Corolário 6.4.1 *([13]) Se $B_\alpha(x, y) = \frac{1}{p} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha xy)$, então a matriz de B_α na base $\{e_1, \ldots, e_n\}$ é dada por*

$$\begin{pmatrix} 2 & -1 & 0 & \cdots & \cdots & 0 \\ -1 & 2 & -1 & \cdots & \vdots & \vdots \\ 0 & -1 & 2 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & -1 & 0 \\ \vdots & \vdots & \vdots & -1 & 2 & -1 \\ 0 & \cdots & \cdots & 0 & -1 & 1 \end{pmatrix}. \tag{6.4.8}$$

Demonstração: Segue diretamente da Proposição (6.4.1). ∎

Proposição 6.4.2 *([22]) Se* $e_n^{'} = e_n$ *e* $e_j^{'} = \sum_{i=j}^{n} e_i$, *para* $j = 1, \cdots, n-1$, *então* $\frac{1}{p} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i^{'} e_j^{'}) = \delta_{ij}$, *onde* δ_{ij} *é o delta de Kronecker.*

Demonstração: Sejam G a matriz do Corolário (6.4.1) e

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

Temos que $TGT^t = I_n$. Agora, $G = MM^t$, onde $M = \frac{1}{\sqrt{p}} NA$, com

$$N = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix} \text{ e } A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Assim, $I_n = T(MM^t)T^t = (TM)(TM)^t$. Seja agora $e_n^{'} = e_n$, $e_j^{'} = \sum_{i=j}^{n} e_i$; $j = 1, \cdots, n-1$ uma outra base de $\mathcal{O}_{\mathbb{L}}$. Temos que

$$\begin{pmatrix} \sigma_1(e_1^{'}) & \cdots & \sigma_n(e_1^{'}) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n^{'}) & \cdots & \sigma_n(e_n^{'}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}.$$

Desta forma, $\overline{M} = \frac{1}{\sqrt{p}} TNA$ é uma matriz geradora do reticulado $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$. Como $\overline{M}\,\overline{M}^t =$

$\frac{1}{p} T\,N\,A\,A^t\,N^t\,T^t \;=\; T\,M\,M^t\,T^t \;=\; I_n$, segue que $\frac{1}{p} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i^{'} e_j^{'}) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker. ∎

Da Proposição (6.4.2), segue que o reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{L}}, \frac{1}{p} b_\alpha)$, com $\alpha = 2 - (\zeta_p + \zeta_p^{-1})$, homomorfismos de $\mathbb{L}$ dados por $\sigma_k(e_j) = \zeta_p^{kj} + \zeta_p^{-kj} = 2\cos\left(\frac{2\pi kj}{p}\right)$, $k, j = 1, \ldots, n$ e matriz geradora $M = \frac{1}{\sqrt{p}} TNA$, com T, N e A são como na demonstração da proposição, é isomorfo ao reticulado $\mathbb{Z}^n$. Logo, seguindo os passos da demonstração da Proposição (6.4.2), pode-se construir $\mathbb{Z}^n$-reticulados rotacionados para $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$.

O resultado que veremos a seguir fornece uma expressão para calcularmos a distância produto mínima desses reticulados.

Proposição 6.4.3 *([22]) Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ o subcorpo maximal real de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde $p \geq 5$, e $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ o anel dos inteiros de $\mathbb{L}$. Se $\Lambda = (\mathcal{O}_{\mathbb{L}}, \frac{1}{p} b_\alpha)$, com $\alpha = 2 - (\zeta_p + \zeta_p^{-1})$, é um reticulado ideal de dimensão $n = \frac{p-1}{2}$, então $d_{p,min}(\Lambda) = p^{\frac{3-p}{4}}$.*

Demonstração: Pelo Corolário (6.3.2), temos que a distância produto mínima de Λ é dada por

$$d_{p,min}(\Lambda) = \sqrt{\frac{|\det(\Lambda)|}{|D_{\mathbb{L}}|}} = \frac{1}{\sqrt{|\mathcal{D}_{\mathbb{L}}|}},$$

uma vez que $det(\Lambda) = 1$. Como o disriminante de $\mathbb{L}$ satisfaz $|\mathcal{D}_{\mathbb{L}}| = p^{\frac{p-3}{2}}$, segue que $d_{p,min}(\Lambda) = p^{\frac{3-p}{4}}$. ∎

A tabela a seguir fornece a distância produto mínima desta construção ciclotômica em algumas dimensões.

p	n	$d_{p,min}(\Lambda)$	$\sqrt[n]{d_{p,min}}$
5	2	$\frac{1}{\sqrt{5}}$	$0,66870$
7	3	$\frac{1}{7}$	$0,522757$
11	5	$\frac{1}{11^2}$	$0,383215$
13	6	$\frac{1}{\sqrt{13^5}}$	$0,343444$
17	8	$\frac{1}{\sqrt{17^7}}$	$0,289520$
19	9	$\frac{1}{19^4}$	$0,27187$
23	11	$\frac{1}{23^5}$	$0,240454$

Tabela 6.1: Distância produto mínima para a construção ciclotômica em $\mathbb{Q}(\zeta_p)$.

Exemplo 6.4.1 *Sejam $p = 5$, $\mathbb{L} = \mathbb{Q}(\zeta_5)$ e $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. Consideremos a $\mathbb{Z}$-base $\{e_1, e_2\}$ de $\mathbb{Z}[\zeta_5 + \zeta_5^{-1}]$, onde $e_1 = \zeta_5 + \zeta_5^{-1}$, $e_2 = \zeta_5^2 + \zeta_5^{-2}$ e $\alpha = 2 - (\zeta_5 + \zeta_5^{-1})$. Temos que o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ é dado por $\{\sigma_1, \sigma_2\}$, onde $\sigma_1(\zeta_5^k + \zeta_5^k) = \zeta_5^k + \zeta_5^{-k}; k = 1, 2$ e $\sigma_2(\zeta_5^k + \zeta_5^k) =$*

$\zeta_5^{2k} + \zeta_5^{-2k}; k = 1, 2$. *Consideremos o reticulado ideal* $(\mathcal{O}_{\mathbb{K}}, \frac{1}{5}b_\alpha)$, *onde* $b_\alpha(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(xy)$. *Vimos que* $(\mathcal{O}_{\mathbb{K}}, \frac{1}{5}b_\alpha)$ *é um* $\mathbb{Z}^2$*-reticulado rotacionado com matriz geradora* $M = \frac{1}{\sqrt{5}}TNA$, *onde*

$$N = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad e \quad A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{pmatrix}.$$

Logo,

$$M = \frac{1}{\sqrt{5}} \begin{pmatrix} -1,175570506 & -1,902113035 \\ -1,902113034 & 1,175570503 \end{pmatrix}.$$

Tal reticulado possui $d_{p,min} = \frac{1}{\sqrt{5}}$, *visto que* $|\mathcal{D}_{\mathbb{K}/\mathbb{Q}}| = 5$.

6.4.3 Construção de $\mathbb{Z}^n$-reticulados rotacionados via o corpo ciclotômico $\mathbb{Q}(\zeta_{2^r})$

Nesta seção, veremos a construção de $\mathbb{Z}^n$-reticulados rotacionados, $n \geq 2$, via o subcorpo maximal real $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ do corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, onde r é um inteiro positivo e $r \geq 3$, utlilizando reticulados ideais. Desta forma, serão obtidos $\mathbb{Z}^n$-reticulados rotacionados para $n = 2^{r-2}$, $r \geq 3$.

Consideremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, $r \geq 3$ e, $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ o subcorpo maximal real de $\mathbb{K}$. Pelo Teorema (1.4.2) temos que $[\mathbb{K} : \mathbb{Q}] = 2^{r-1}$ e pelo Teorema (1.4.3) que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{2^r} + \zeta_{2^r}^{-1}]$ é o anel dos inteiros de $\mathbb{L}$ e $\{1, \zeta_{2^r} + \zeta_{2^r}^{-1}, \cdots, \zeta_{2^r}^{n-1} + \zeta_{2^r}^{-(n-1)}\}$ é uma $\mathbb{Z}$-base de $\mathbb{L}$. Pelo Corolário (1.4.1), segue que $[\mathbb{K} : \mathbb{L}] = 2$. Assim, pela Observação (1.2.1), tem-se que $[\mathbb{L} : \mathbb{Q}] = 2^{r-2} = n$.

Seja $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ um reticulado ideal, com $\alpha \in \mathbb{L}$ totalmente positivo e b_α a forma bilinear simétrica associada a Λ. Como na Seção (6.4.2), para que $\Lambda = (\mathcal{O}_{\mathbb{L}}, b_\alpha)$ seja isomorfo ao reticulado $(\sqrt{c}\mathbb{Z})^n$, queremos encontrar $\alpha \in \mathbb{L}$ totalmente positivo que satisfaça a Equação (6.4.6).

Na Proposição (1.4.9), vimos que $|\mathcal{D}_{\mathbb{L}}| = 2^\beta$, onde $\beta = (r-1)n - 1$. Assim,

$$\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)|\mathcal{D}_{\mathbb{L}}| = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha)2^\beta = c^n,$$

onde $\beta = (r-1)n - 1$, $n = 2^{r-2}$, $r \geq 3, c \in \mathbb{Z}$. Tomando $c = 2^{r-1}$ temos $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = 2$. Assim, encontremos $\alpha \in \mathbb{L}$ totalmente positivo tal que $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = 2$. Observe que $2\mathbb{Z}[\zeta_{2^r}] = (1 - \zeta_{2^r})^{\varphi(2^r)}\mathbb{Z}[\zeta_{2^r}]$, e assim $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{2^r}) = 2$. Usando a transitividade da norma, temos que

$$\begin{aligned} 2 &= \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{2^r}) = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\mathcal{N}_{\mathbb{K}/\mathbb{L}}(1 - \zeta_{2^r})) \\ &= \mathcal{N}_{\mathbb{L}/\mathbb{Q}}((1 - \zeta_{2^r})(1 - \zeta_{2^r}^{-1})). \end{aligned} \tag{6.4.9}$$

Logo, tomando $\alpha = (1-\zeta_{2^r})(1-\zeta_{2^r}{}^{-1}) = 2-(\zeta_{2^r}+\zeta_{2^r}^{-1})$, temos que $\alpha \in \mathbb{L}$ é totalmente positivo

pois,

$$|\zeta_{2^r} + \zeta_{2^r}^{-1}| = |2\cos\frac{\pi}{2^{r-1}}| < 2, \quad r \geq 3$$

e, pela Equação (6.4.9) segue que $\mathcal{N}_{\mathbb{L}/\mathbb{Q}}(\alpha) = 2$.

Como vimos na Observação (6.4.1) esta é apenas uma condição necessária para que Λ seja isomorfo a $\mathbb{Z}^n$. Agora, faremos uma construção explícita para mostrarmos este isomorfismo.

Lema 6.4.2 *([13]) Se $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) = \begin{cases} 0, & se \quad mdc(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & se \quad mdc(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & se \quad mdc(k, 2^r) > 2^{r-1}. \end{cases}$$

Demonstração: Temos que o polinômio minimal de ζ_{2^r} sobre $\mathbb{Q}$ é dado por $\phi_{2^r}(x) = x^{2^{r-1}} + 1$. Desta forma, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) = 0$, para todo k tal que $mdc(k, 2^r) = 1$, pois se $mdc(k, 2^r) = 1$, então $\zeta_{2^r}^k$ é conjugado de ζ_{2^r}. Agora, seja k tal que $mdc(k, 2^r) > 1$. Temos três casos para analisar:

1º caso: $mdc(k, 2^r) < 2^{r-1}$.

Seja $mdc(k, 2^r) = 2^s$, onde $s < r - 1$. Assim, $k = 2^s j$; $j \in \mathbb{Z}$ e $\zeta_{2^r}^k = \zeta_{2^r}^{2^s j} = \zeta_{2^{r-s}}^j$. Segue então que

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) &= Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^{r-s}}^j) = Tr_{\mathbb{Q}(\zeta_{2^{r-s}})/\mathbb{Q}}(Tr_{\mathbb{K}/\mathbb{Q}(\zeta_{2^{r-s}})}(\zeta_{2^{r-s}}^j)) \\ &= Tr_{\mathbb{Q}(\zeta_{2^{r-s}})/\mathbb{Q}}(p^s\zeta_{2^{r-s}}^j) = p^s Tr_{\mathbb{Q}(\zeta_{2^{r-s}})/\mathbb{Q}}(\zeta_{2^{r-s}}^j) = 0, \end{aligned}$$

pois $mdc(j, 2^{r-1}) = 1$.

2º caso: $mdc(k, 2^r) = 2^{r-1}$.

Temos que o polinômio minimal de ζ_2 sobre $\mathbb{Q}$ é $\phi_2(x) = x+1$. Desta forma, $Tr_{\mathbb{Q}(\zeta_2)/\mathbb{Q}}(\zeta_2^k) = -1$, para todo k tal que $mdc(k, 2) = 1$ e $\zeta_{2^r}^k = \zeta_{2^r}^{2^{r-1}j} = \zeta_2^j$, onde $k = 2^{r-1}j$ e $mdc(j, 2) = 1$. Segue, então, que

$$Tr_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}}(\zeta_2^j) = Tr_{\mathbb{Q}(\zeta_2)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}(\zeta_2)}(\zeta_2^j)) = 2^{r-1}Tr_{\mathbb{Q}(\zeta_2)/\mathbb{Q}}(\zeta_2) = -2^{r-1}.$$

Assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_2^j) = -2^{r-1}.$$

3º caso: $mdc(k, 2^r) > 2^{r-1}$.

Neste caso, temos que $mdc(k, 2^r) = 2^r$ e, desta forma,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) = Tr_{\mathbb{K}/\mathbb{Q}}(1) = 2^{r-1},$$

o que prova o lema. ∎

Lema 6.4.3 *([13]) Se $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ é o subcorpo maximal real de $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, então*

$$Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = \begin{cases} 0, & se \;\; mdc(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & se \;\; mdc(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & se \;\; mdc(k, 2^r) > 2^{r-1}. \end{cases}$$

Demonstração: Pela transitividade da forma traço, temos que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_{2^r}^k) + Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^{-k}) = Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = Tr_{\mathbb{L}/\mathbb{Q}}(Tr_{\mathbb{K}|\mathbb{L}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k})) = 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}).$$

Desta forma, pelo Lema (6.4.2), tem-se que:
1º caso: Se $mdc(k, 2^r) < 2^{r-1}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) + Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^{-k}) = 0$, isto é, $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = 0$.
2º caso: Se$mdc(k, 2^r) = 2^{r-1}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) + Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^{-k}) = -2^{r-1} - 2^{r-1} = 2(-2^{r-1})$, isto é, $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = -2^{r-1}$.
3º caso: Se $mdc(k, 2^r) > 2^{r-1}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^k) + Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{2^r}^{-k}) = 2^{r-1} + 2^{r-1} = 2(2^{r-1})$, isto é, $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^k + \zeta_{2^r}^{-k}) = 2^{r-1}$, como queríamos provar. ∎

Proposição 6.4.4 *([13]) Sejam $e_0 = 1$ e $e_i = \zeta_{2^r}^i + \zeta_{2^r}^{-i}$, para $i = 1, \cdots, n-1$ e $b_\alpha : \mathcal{O}_\mathbb{L} \times \mathcal{O}_\mathbb{L} \longrightarrow \mathbb{Z}$ tal que $b_\alpha(x, y) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha xy)$. Tem-se que:*

1. *Se $i = 0, 1, \cdots, n-1$, então $b_\alpha(e_i, e_i) = \begin{cases} 2n, & se \; i = 0; \\ 4n, & se \; i \neq 0. \end{cases}$*

2. *Se $i \neq 0$, então $b_\alpha(e_i, e_0) = \begin{cases} -2n, & se \; i = 1; \\ 0, & se \; i \neq 1. \end{cases}$*

3. *Se $i \neq 0, j \neq 0$ e $i \neq j$, então $b_\alpha(e_i, e_j) = \begin{cases} -2n, & se \; |i - j| = 1; \\ 0, & caso \; contrário. \end{cases}$*

Demonstração: Vamos calcular $b_\alpha(e_i, e_0)$, para $i = 0, 1, \cdots, n-1$. Para $i = 0$, temos que

$$b_\alpha(e_0, e_0) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_0^2) = Tr_{\mathbb{L}/\mathbb{Q}}(\alpha) = Tr_{\mathbb{L}/\mathbb{Q}}(2) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r} + \zeta_{2^r}^{-1}) = 2(2^{r-2}) = 2^{r-1},$$

pois, pelo Lema (6.4.3), temos que $mdc(1, 2^r) < 2^{r-1}$. Agora, para todo $i = 1, \cdots, n-1$, temos que

$$\begin{aligned} b_\alpha(e_i, e_0) &= Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i) = Tr_{\mathbb{L}/\mathbb{Q}}((2 - (\zeta_{2^r} + \zeta_{2^r}^{-1}))(\zeta_{2^r}^i + \zeta_{2^r}^{-i})) \\ &= Tr_{\mathbb{L}/\mathbb{Q}}(2\zeta_{2^r}^i + 2\zeta_{2^r}^{-i} - \zeta_{2^r}^{i+1} - \zeta_{2^r}^{1-i} - \zeta_{2^r}^{i-1} - \zeta_{2^r}^{-1-i}) \\ &= 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^i + \zeta_{2^r}^{-i}) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i+1} + \zeta_{2^r}^{-(i+1)}) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i-1} + \zeta_{2^r}^{-(i-1)}) \\ &= \begin{cases} -2n, \text{ se } i = 1 \\ 0, \text{ caso contrário.} \end{cases} \end{aligned}$$

Vamos calcular $b_\alpha(e_i, e_i)$, para $i = 1, \cdots, n-1$. Como $mdc(2i, 2^r), mdc(2i+1, 2^r), mdc(2i-1, 2^r) < 2^{r-1}$, para todo $i = 1, \cdots, n-1$, segue que

$$\begin{aligned} b_\alpha(e_i, e_i) &= Tr_{\mathbb{L}/\mathbb{Q}}(\alpha {e_i}^2) = Tr_{\mathbb{L}/\mathbb{Q}}((2 - \zeta_{2^r} + \zeta_{2^r}^{-1})(\zeta_{2^r}^{2i} + \zeta_{2^r}^{-2i} + 2)) \\ &= 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{2i} + \zeta_{2^r}^{-2i}) + Tr_{\mathbb{L}/\mathbb{Q}}(4) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{2i+1} + \zeta_{2^r}^{-(2i+1)}) \\ &- Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{2i-1} + \zeta_{2^r}^{-(2i-1)}) \\ &= 4n. \end{aligned}$$

Finalmente, para todo $i \neq 0$, $j \neq 0$ e $i \neq j$, como $mdc(i+j, 2^r), mdc(i-j, 2^r), mdc(i+j+1, 2^r), mdc(i+j-1, 2^r) < 2^{r-1}$, segue que

$$\begin{aligned} b_\alpha(e_i, e_j) &= Tr_{\mathbb{L}/\mathbb{Q}}(\alpha e_i e_j) = Tr_{\mathbb{L}/\mathbb{Q}}((2 - (\zeta_{2^r} + \zeta_{2^r}^{-1}))(\zeta_{2^r}^i + \zeta_{2^r}^{-i})(\zeta_{2^r}^j + \zeta_{2^r}^{-j})) \\ &= 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i+j} + \zeta_{2^r}^{-(i+j)}) + 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i-j} + \zeta_{2^r}^{-(i-j)} - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i+j+1} + \zeta_{2^r}^{-(i+j+1)}) \\ &- Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i-j+1} + \zeta_{2^r}^{-(i-j+1)}) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{-i+j+1} + \zeta_{2^r}^{-(-i+j+1)}) - Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_{2^r}^{i+j-1} + \zeta_{2^r}^{-(i+j-1)}) \\ &= \begin{cases} -2n, \text{ se } |i-j| = 1 \\ 0, \text{ caso contrário,} \end{cases} \end{aligned}$$

o que prova a proposição. ∎

Corolário 6.4.2 *([13]) Se $Q_\alpha(x, y) = \frac{1}{2^{r-1}} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha xy)$, então a matriz de Q_α na base $\{e_0, e_1, \cdots, e_{n-1}\}$ é*

$$G = \begin{pmatrix} 1 & -1 & 0 & \cdots & & & \\ -1 & 2 & -1 & 0 & \cdots & & \\ 0 & -1 & 2 & \cdots & & & \\ & & & & \vdots & & \\ & & & & 2 & -1 & 0 \\ & & & \vdots & -1 & 2 & -1 \\ & & & \vdots & 0 & -1 & 2 \end{pmatrix}.$$

Demonstração: Segue diretamente da Proposição (6.4.4). ∎

Proposição 6.4.5 *([2]) Se* $\{f_0, f_1, \cdots, f_{n-1}\}$, *onde* $f_i = -\sum_{j=0}^{n-1-i} e_j$, *para todo* $i = 0, 1, \cdots, n-1$, *é uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{L}}$, *então* $\frac{1}{2^{r-1}} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, *onde* δ_{ij} *é o delta de Kronecker.*

Demonstração: Sejam G a matriz do Corolário (6.4.2) e

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

Temos que $TGT^t = I_n$. Agora, como G é a matriz de Gram do reticulado $\Lambda = (\mathcal{O}_{\mathbb{L}}, \frac{1}{2^{r-1}} b_\alpha)$, temos que $G = MM^t$, onde $M = \dfrac{1}{\sqrt{2^{r-1}}} NA$, com

$$N = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix} \text{ e } A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Assim, $I_n = TMM^tT^t = (TM)(TM)^t$. Seja agora $f_i = -\sum_{j=0}^{n-1-i} e_j$; $j = 0, 1, \cdots, n-1$, uma outra base de $\mathcal{O}_{\mathbb{L}}$. Temos que

$$\begin{pmatrix} \sigma_1(f_0) & \cdots & \sigma_n(f_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(f_{n-1}) & \cdots & \sigma_n(f_{n-1}) \end{pmatrix} = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}.$$

Logo, $\overline{M} = \dfrac{1}{\sqrt{2^{r-1}}} TNA$ é uma matriz geradora do reticulado $\Lambda = (\mathcal{O}_{\mathbb{L}}, \frac{1}{2^{r-1}} b_\alpha)$. Como $\overline{MM}^t = \dfrac{1}{p} TNAA^tN^tT^t = TMM^tT^t = I_n$, segue que $\dfrac{1}{p} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha \overline{e_i e_j}) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker. ∎

Da Proposição (6.4.5), segue que o reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{L}}, \dfrac{1}{2^{r-1}} b_\alpha)$, com $\alpha = 2 - (\zeta_{2^r} + \zeta 2^{r-1})$, homomorfismos de $\mathbb{L}$ dados por $\sigma_k(e_j) = \zeta_p^{kj} + \zeta_p^{-kj} = 2\cos\left(\frac{\pi kj}{2^{r-1}}\right)$, $k, j = 0, \ldots, n-1$ e matriz geradora $M = \dfrac{1}{\sqrt{2^{r-1}}} TNA$, com T, N e A são como na demonstração da proposição, é isomorfo ao reticulado $\mathbb{Z}^n$.

Logo, seguindo os passos da demonstração da Proposição (6.4.5), pode-se construir $\mathbb{Z}^n$-reticulados rotacionados para $n = 2, 4, 8, 16, 32, 64, 128, 256, 512, \cdots$.

Proposição 6.4.6 *([2]) Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ *o subcorpo maximal real de* $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, *onde* $r \geq 3$, *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{2^r} + \zeta_{2^r}^{-1}]$ *o anel dos inteiros de* $\mathbb{L}$. *Se* $\Lambda = (\mathcal{O}_{\mathbb{L}}, \dfrac{1}{2^{r-1}} b_\alpha)$, *com* $\alpha = 2 - (\zeta_{2^r} + \zeta_{2^r}^{-1})$,

é um reticulado ideal de dimensão $n = 2^{r-2}$*, então* $d_{p,min}(\Lambda) = \dfrac{1}{\sqrt{2^{\beta}}}$*, onde* $\beta = (r-1)2^{r-2} - 1$.

Demonstração: Pelo Corolário (6.3.2), temos que a distância produto mínima de Λ é dada por

$$d_{p,min}(\Lambda) = \sqrt{\frac{|\det(\Lambda)|}{|D_{\mathbb{L}}|}} = \frac{1}{\sqrt{|\mathcal{D}_{\mathbb{L}}|}},$$

uma vez que $det(\Lambda) = 1$. Como o disriminante de $\mathbb{L}$ satisfaz $|\mathcal{D}_{\mathbb{L}}| = 2^{\beta}$, onde $\beta = (r-1)2^{r-2} - 1$, segue que $d_{p,min}(\Lambda) = \dfrac{1}{\sqrt{2^{\beta}}}$. ∎

A tabela a seguir fornece a distância produto mínima desta construção ciclotômica em algumas dimensões.

r	n	$\sqrt[n]{d_{p,min}}$
3	2	0,594604
4	4	0,385553
5	8	0,261068
6	16	0,180648
7	32	0,126361
8	64	0,0888683
9	128	0,0626695
10	256	0,044254
11	512	0,0312712
12	1024	0,0221046

Tabela 6.2: Distância produto mínima para a construção ciclotômica em (ζ_{2^r}).

Exemplo 6.4.2 *Sejam* $n = 2^4$*,* $\zeta_{2^r} = \zeta_{2^4}$*,* $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$ *e* $\mathbb{L} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$*. Temos que uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{L}}$ *é* $\{e_0 = 1, e_1 = \zeta_{2^r} + \zeta_{2^r}^{-1}, e_2 = \zeta_{2^r}^2 + \zeta_{2^r}^{-2}, e_3 = \zeta_{2^r}^3 + \zeta_{2^r}^{-3}\}$*, o grupo de Galois de* $\mathbb{L}$ *sobre* $\mathbb{Q}$ *é dado por* $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{15}\}$*, onde* $\sigma_i(\zeta_{2^r}) = \zeta_{2^r}^i$*, para* $i = 1, 3, 5, 7$ *e o grupo de Galois de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $Gal(\mathbb{L}/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$*. Seja* $\alpha = 2 - (\zeta_{2^r} + \zeta_{2^r}^{-1})$ *e* $b_{\alpha}(x, y) = \dfrac{1}{8} Tr_{\mathbb{L}/\mathbb{Q}}(\alpha x y)$*. A matriz geradora do* $\mathbb{Z}^n$*- reticulado rotacionado é dada por* $R = \dfrac{1}{\sqrt{2^{4-1}}} TMA$*, onde*

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

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_3(1) & \sigma_5(1) & \sigma_7(1) \\ \sigma_1(\zeta + \zeta_p^{-1}) & \sigma_3(\zeta + \zeta_p^{-1}) & \sigma_5(\zeta + \zeta_p^{-1}) & \sigma_7(\zeta + \zeta_p^{-1}) \\ \sigma_1(\zeta_p^2 + \zeta_p^{-2}) & \sigma_3(\zeta_p^2 + \zeta_p^{-2}) & \sigma_5(\zeta_p^2 + \zeta_p^{-2}) & \sigma_7(\zeta_p^2 + \zeta_p^{-2}) \\ \sigma_1(\zeta_p^3 + \zeta_p^{-3}) & \sigma_3(\zeta_p^3 + \zeta_p^{-3}) & \sigma_5(\zeta_p^3 + \zeta_p^{-3}) & \sigma_7(\zeta_p^3 + \zeta_p^{-3}) \end{pmatrix} \quad e$$

$$A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 & 0 & 0 \\ 0 & \sqrt{\sigma_3(\alpha)} & 0 & 0 \\ 0 & 0 & \sqrt{\sigma_7(\alpha)} & 0 \\ 0 & 0 & 0 & \sqrt{\sigma_7(\alpha)} \end{pmatrix}.$$

6.5 Conclusão do capítulo

Iniciamos este capítulo, na Seção (6.1), definindo alguns conceitos que são necessários para definirmos um reticulado ideal. Após isto, apresentamos alguns resultados. Na Seção (6.2), vimos que podemos obter reticulados ideais a partir da perturbação $\sigma_{2\alpha}$ do homomorfismo canônico. A partir disto, vimos através da Proposição (6.2.2) uma fórmula para o determinante de um reticulado ideal que foi muito utilizado em outros resultados. Ressaltamos, como no Capítulo (5), que todos os resultados apresentados neste capítulo utilizando a perturbação $\sigma_{2\alpha}$, poderiam ter sido mostrados utilizando a perturbação σ_α. Foi somente uma questão de escolha trabalhar com a perturbação σ_α nas construções do Capítulo (5) e utilizar a perturbação $\sigma_{2\alpha}$ neste capítulo. Na Seção (6.3) definimos a diversidade e a distância produto mínima de um reticulado ideal e, obtemos na Proposição (6.3.1) uma expressão para calcular a diversidade de um reticulado ideal e no Teoreama (6.3.1) mostramos que a distância produto mínima de um reticulado ideal pode ser obtido a partir do determinante do reticulado e do discriminante do corpo de números. Finalizando o capítulo, apresentamos duas construções de $\mathbb{Z}^n$-reticulados rotacionados a partir dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_{2^r})$, juntamente com exemplos de reticulados obtidos a partir desta construção e o valor de suas distância produto mínima.

Conclusão

Este trabalho foi dedicado ao estudo de métodos para obter famílias de reticulados com boas densidades de centro e, com diversidade e distância produto mínima alta. Para isso, inicialmente fizemos um estudo sobre a teoria algébrica dos números que nos forneceu uma base teórica para este trabalho, as formas quadráticas, que nos possibilitaram obter uma expressão para o cálculo da forma traço e, a definição de reticulado e de seus principais parâmetros.

O primeiro método apresentado foi o de obter reticulados via polinômios irredutíveis no corpo dos números racionais. Neste trabalho abordamos os casos para dimensão 2, utilizando polinômios irredutíveis de grau 2 com raízes reais e raízes complexas conjugadas e, para dimensão 3, utilizando polinômios irredutíveis de grau 3 com raízes reais. Através deste método encontramos reticulados com as mesmas densidades de centro dos reticulados A_2 e D_3, ou seja, reticulados com densidade de centro ótima para dimensões 2 e 3, respectivamente. Acreditamos que, a partir deste método, pode ser encontrado reticulados com densidade de centro ótima para dimensões maiores. O grande desafio é determinar a matriz geradora do reticulado através das raízes do polinômio e também minimizar a forma quadrática.

Para apresentar o segundo método, inicialmente fizemos um estudo sobre o homomorfismo canônico e suas perturbações e, vimos que, podemos obter reticulados via estes homomorfismos. Daí, apresentamos uma construção de reticulados rotacionados de dimensões 2, 4, 6, 8 e 12 dos reticulados conhecidos $A_2,\ D_4,\ E_6,\ E_8$ e K_{12}. Já que sabemos que a densidade de centro destes reticulados são ótimas, este método consiste em igualar a fórmula da densidade de centro a estes valores sabidos e trabalhar para encontrar convenientes valores de seus parâmetros para que tenhamos os resultados desejados. Para dimensões ímpares, por falta de tempo, fizemos apenas alguns testes, e não encontramos resultados satisfatórios. Mas acreditamos que seja possível encontrar reticulados rotacionados de dimensões ímpares utilizando esta mesma teoria.

Os dois casos vistos acima visam obter bons reticulados com relação à sua densidade de centro pois, como vimos, encontrar empacotamentos reticulados densos é equivalente a encontrar códigos corretores de erros eficientes. Mas, no último caso apresentado, nosso objetivo foi classificar os reticulados quanto a sua diversidade e distância produto mínima. Pois, como pode ser visto em [22], para termos uma transmissão com pequena probabilidade de erros, devemos utilizar reticulados com diversidade e distância produto mínima alta. E, como foi visto

neste trabalho, quando consideramos corpos de números totalmente reais temos diversidade máxima e quanto menor for o discriminante do corpo em questão, maior é a sua distância produto mínima. Assim, apresentamos construções de reticulados rotacionados do reticulado $\mathbb{Z}^n$ via o anel dos inteiros algébricos dos subcorpos maximais reais dos corpos $\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\zeta_{2^r})$, onde p é um número primo e r um inteiro positivo, pois estes reticulados encontrados gozam destas propriedades sobre a diversidade e distância produto mínima.

Como podemos observar pelo exposto acima, ainda há muitos resultados que podem ser obtidos utilizando esta teoria e partindo dos resultados apresentados neste trabalho.

Referências Bibliográficas

[1] ALVES, C. **Reticulados via corpos ciclotômicos**. 2005, 125f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[2] ANDRADE, A. A.; ALVES, C.; CARLOS, T. B. **Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$.** International Journal of Applied Mathematics, Sofia, v. 19, n. 3, p. 321-331, 2006.

[3] ANDRADE, A.A.; FERRARI, A,J.; BENEDITO, C.W.O.; COSTA, S.I.R. **Constructions of algebraic lattices.** Submetido à revista CAM - Computational and Applied Mathematics, 2010.

[4] BAYER-FLUCKIGER, E. **Ideal lattices**. In: Conference in honor of Alan Baker, 2002, Cambridge. Proceedings ... Cambridge: Cambridge University Press, 2002, p.

[5] BAYER-FLUCKIGER, E. **Lattices and number fields**. Contemporary Mathematics, Providence, v. 241, p. 69-84, 1999.

[6] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. **New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel.** IEEE Transactions on Information Theory, New-York, v. 50, n. 4, p. 702-714, Apr. 2004. 2003.

[7] BOUTROS, J.; VITERBO, E.; RATELLO, C.; BELFIORE, J. C. **Good lattice constellations for both Rayleigh fading and Gaussian channels**. IEEE Transactions Information Theory, New-York, v. 42, No. 2, p. 502-517, 1996.

[8] CONWAY, J. H.; SLOANE, N. J. A. **Sphere packing, lattices and groups**. New-York: Springer-Verlag, 1999.

[9] DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. São Paulo: Atual, 1982.

[10] ENDLER, O. **Teoria dos númros algébricos**. Projeto Euclides, 1986.

[11] FERRARI, A.J. **Reticulados algébricos via corpos abelianos**. 2008, 105f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[12] FLORES, A. L. **Reticulados em corpos abelianos**. 2000, 115f. Tese (Doutorado em Engenharia Elétrica), Faculdade de Engenharia Elétrica e da Computação, Universidade Estadual de Campinas, Campinas, 2000.

[13] JORGE, G.C. **Reticulados ideais via corpos abelianos**. 2008, 176f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[14] LANG, S. **Algebra**. New York: Addison-Wesley, 1972.

[15] LAVOR, C.C., ALVES, M.M.S, SIQUEIRA, R,M., COSTA, S.I.R. **Uma Introdução à Teoria de Códigos.** Notas em Matemática Aplicada, São Carlos, SP - SBMAC, , 2006.

[16] LOPES, J. O. D. **Discriminants of subfields of $\mathbb{Q}(\zeta_{2^r})$.** Journal of Algebra and Its Applications, New Jersey, v. 2, p. 463-469, 2003.168-184.

[17] MARCUS, D. A. **Number fields**. New-York: Springer-Verlag, 1977.

[18] MELO, F. D. **Uma forma quadrática no corpo de condutor primo**. 2005, 59f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[19] MILIES, F. C. P. **Anéis e módulos**. São Paulo: L.P.M, 1972.

[20] MONTEIRO, L. H. J. **Teoria de Galois**. In: Colóquio Brasileiro de Matemática, 7, 1969. Poços de Caldas. Atas ... Rio de Janeiro: Impa, 1969.

[21] NOBREGA, T. P. **Cúbicas reais, algumas aplicações**, In: Encontro de Álgebra, 6, 1997. Campinas. Anais ... Campinas: Unicamp, 1997.

[22] OGGIER, F. **Algebraic methods for channel coding.** 2005, 125f. Tese (Doutorado em Matemática e Informática), École Polytechnique Fédeérale de Lausanne, Lausane, 2005.

[23] RODRIGUES, T. M. **Cúbicas galoisianas**. 2003, 68f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2003.

[24] SAMUEL, P. **Algebraic theory of numbers**, Paris: Hermann, 1970.

[25] SHANNON, C.E. **A Mathematical Theory of Communication**. Bell System Technical Journal, v. 27, p. 379-423, 623-656, 1948.

[26] SOUZA, T. M. **Reticulados algébricos em corpos de números abelianos**. 2004, 85f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2004.

[27] STEWART, I. N.; TALL, D. O. **Algebraic number theory**. London: Chapman and Hall, 1987.

[28] VICENTE, J. P. G. **Reticulados de posto 3 em corpos de números**. 2000, 91f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2000.

[29] WASHINGTON, L. **Introduction to cyclotomic fields**. New York: Springer-Verlag, 1982.

Índice Remissivo

anel, 18
anel de Dedekind, 42
anel dos inteiros, 30
anel integralmente fechado, 30
anel quociente, 19
assinatura, 138

base, 21
base complementar, 54
base integral, 31

classe de equivalência, 19
CM-corpo, 26
codiferente, 52
congruência, 19
corpo, 18
corpo ciclotômico, 48
corpo de números, 25
corpo de raízes, 26
corpo fixo, 26
corpo quadrático, 46
corpo totalmente imaginário, 26
corpo totalmente real, 26

densidade de centro, 73
densidade de empacotamento, 73
determinante de um reticulado, 72
discriminante, 39
distância produto mínima de um reticulado, 76
diversidade, 75
diversidade de um reticulado, 75
divisor de zero, 18

elemento inteiro, 27
elemento totalmente positivo, 108
empacotamento esférico, 72
empacotamento reticulado, 72
extensão, 25
extensão galoisiana, 26
extensão separável, 26

função de Möbius, 60

grau da extensão, 25
grupo, 17
grupo de Galois, 26

homomorfismo canônico, 98
homomorfismo de anéis, 20
homomorfismo de módulos, 21
homomorfismo imaginário, 26
homomorfismo real, 26

ideal, 19
ideal fracionário, 43
ideal maximal, 19
ideal primo, 19
ideal principal, 19
inteiro algébrico, 30
involução, 26
isomorfismo, 20

módulo, 20
módulo finitamente gerado, 21

módulo livre, 21
módulo noetheriano, 22
matriz de Gram, 71
matriz geradora, 70
monomorfismo, 20

número algébrico, 25
número transcendente, 25
norma de um elemento, 31
norma de um ideal, 36
norma mínima de um reticulado, 73

perturbação $\sigma_{2\alpha}$ do homomorfismo canônico, 115
perturbação σ_α do homomorfismo canônico, 108
polinômio ciclotômico, 48

raíz n-ésima primitiva da unidade, 48
raio de empacotamento, 73
região fundamental, 67
reticulado, 66
reticulado ímpar, 139
reticulado algébrico, 119
reticulado ideal, 139
reticulado inteiro, 138
reticulado par, 139
reticulado positivo, 139

sequência estacionária, 22
subanel, 18
subcorpo, 18
submódulo, 20

traço, 31

volume de um reticulado, 70

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo