Elen Cristina Mazucchi

Reticulados Numéricos

cm 1 2 3 4 5 6 7 8 unesp 12 13 14 15 16 17 18 19

1910001501

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

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Biociências, Letras e Ciências Exatas

Reticulados Numéricos

Elen Cristina Mazucchi

Orientador: Prof. Dr. Antonio Aparecido de Andrade

T. 1501/06

BIBLIOTECA
Inst. de Biociências, Letras e Ciências Exatas - UNESP - S. J. Rio Preto

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

Fevereiro - 2006

São José do Rio Preto - SP

T 512 9
M 478R
15/05/2006
Doação
Autor(a)
10101039

Mazucchi, Elen Cristina.
Reticulados numéricos / Elen Cristina Mazucchi. - São José do Rio Preto : [s.n.], 2006
146 f. ; 30 cm.

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

1. Teoria dos números. 2. Teoria dos reticulados. 3. Ideais reticulados. I. Andrade, Antonio Aparecido. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título..

CDU – 512.565

BIBLIOTECA

BANCA EXAMINADORA

- Antonio Aparecido de Andrade
  Professor Doutor - IBILCE - UNESP
  Orientador

- Roseli Arbach Fernandes de Oliveira
  Professora Doutora - FEIS - UNESP
  1º Examinador

- Edson Agustini
  Professor Doutor - UFU - MG
  2º Examinador

- Edson Donizete de Carvalho
  Professor Doutor - FEIS - UNESP
  1º Suplente

- João Roberto Gerônimo
  Professor Doutor - UEM - PR
  2º Suplente

Aos meus pais, João e Ivanilda,
aos meus irmãos, João Ricardo e Laiara,
ao meu namorado Fernando,
e ao meu avô Annibal Mazucchi (*in memorian*)
dedico.

Agradecimentos

Ao concluir este trabalho, agradeço:

Primeiramente a Deus.

Ao Prof. Dr. Antonio Aparecido de Andrade, pela amizade de tantos anos, pela paciência, dedicação e incentivo.

Aos professores do Departamento de Matemática da UNESP - S.J.R.Preto, em especial ao Prof. Hermes Antônio Pedroso, pela amizade e carinho.

Aos professores da banca examinadora: Profª. Drª. Roseli Arbach Fernandes de Oliveira (FEIS - UNESP - Ilha Solteira), Prof. Dr. Edson Agustini (UFU - MG), Prof. Dr. Edson Donizete de Carvalho (FEIS - UNESP - Ilha Solteira) e Prof. Dr. João Roberto Gerônimo (UEM - PR).

À minha família pelo apoio e compreênsão nos momentos de ausência.
Aos meus pais João Mazucchi e Ivanilda Vieira Mazucchi que sempre me apoiaram, incentivaram e me mostraram que quando sonhamos e acreditamos, tudo é possível.

Ao meu namorado Fernando, por estar sempre ao meu lado nos momentos difíceis e por compartilhar os momentos de alegria.

À Cátia por compartilhar as alegrias, tristezas, dificuldades e vitórias desde o início da nossa caminhada.

Aos amigos do curso de Pós-graduação, em especial à Giovana, Fernanda, Francielle, Tatiane e Marcus, pela convivência e amizade de tantos anos.

À FAPESP pelo auxílio financeiro.

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

"Nós geralmente descobrimos o que fazer percebendo aquilo que não devemos fazer. E provavelmente aquele que nunca cometeu um erro nunca fez uma descoberta."

Samuel Smiles

unesp

Resumo

Este trabalho é dedicado a descrição de alguns métodos algébricos para obtenção de bons reticulados. Através da teoria de ideais reticulados vimos algumas construções de reticulados rotacionados, obtendo reticulados tão bons quanto os já conhecidos. Nessas construções o desempenho do reticulado está totalmente relacionado com a estrutura do corpo de números $\mathbb{K}$ com o qual estamos trabalhando.

Palavras-chave: reticulados, ideais reticulados, diversidade, distância produto mínima.

Abstract

This work is dedicated to description of some algebraic methods for attainment of good lattices. Through the theory of ideal lattices we make some lattices constructions obtained lattices so good how much already known. In these constructions, the performance of the lattices one total is related with the structure of number field $\mathbb{K}$ with which we are working.

Keywords: lattices, ideal lattices, diversity, minimum product distance.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Índice de Símbolos

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

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

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

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

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

∂f: grau do polinômio f

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

$\prod$: produtório

$\sum$: somatório

$det(A)$: determinante da matriz A

(a_{ij}): matriz

$\chi_\alpha(x)$: polinômio característico de α

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

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

$\#X$: cardinalidade do conjunto X

$min(X)$: mínimo do conjunto X

$\mathfrak{a}, \mathfrak{b}, \ldots$: ideais

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

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

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

ξ_n: $e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, raiz n-ésima primitiva da unidade

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

$D_\mathbb{K}$: discriminante absoluto do corpo $\mathbb{K}$

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

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

$\Delta(\mathcal{O}_\mathbb{L}|\mathbb{K})$: diferente de $\mathbb{L}$ sobre $\mathbb{K}$.

$(\Delta(\mathcal{O}_\mathbb{L}|\mathbb{K}))^{-1}$: codiferente de $\mathbb{L}$ sobre $\mathbb{K}$.

$\mathcal{O}_\mathbb{L}{}^*$: codiferente de $\mathbb{L}$ sobre $\mathbb{K}$.

$Ker(f)$: núcleo do homomorfismo f

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

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

$a|b$: a divide b

$\delta(\Lambda)$: densidade de centro do reticulado Λ

div : diversidade

$d_{p,min}$: distância produto mínima

E : energia da constelação

E_b : energia por bit

N_0 : potência do ruído

$erfc$: função erro

Sumário

Introdução 3

1 Teoria algébrica dos números **5**

1.1 Módulos Noetherianos 5

1.2 Anel de inteiros 11

1.3 Norma e traço 17

1.4 Discriminante 23

1.5 Anéis de Dedekind 28

1.6 Norma de um ideal 32

1.7 Anel de frações 35

2 Corpos quadráticos e ciclotômicos **40**

2.1 Corpos quadráticos 40

2.2 Corpos ciclotômicos 43

2.3 Ramificação de ideais 48

3 Codiferente e diferente **57**

3.1 Codiferente 57

3.2 Diferente 62

4 Reticulados e ideais reticulados **68**

4.1 Reticulados 68

4.2 Homomorfismo canônico 72

4.3 Ideais reticulados 80

4.4 Perturbação do homomorfismo canônico 82

4.5 Diversidade e distância produto mínima 84

4.6 O canal Rayleigh com desvanecimento 88

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

5 Construções de ideais reticulados **92**

5.1 Ideais reticulados via corpos totalmente reais 93

5.2 Construção quadrática 94

5.3 Construção ciclotômica em dimensão $n = \frac{p-1}{2}$ 96

5.4 Construção cíclica 102

5.4.1 Caso I: Somente $p > n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$ 103

5.4.2 Caso II: Somente $p = n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$ 111

5.4.3 Caso III: Pelo menos dois primos se ramificam em $\mathcal{O}_{\mathbb{K}}$ 115

5.4.4 Distância produto mínima via a construção cíclica 119

5.5 Construção mista 121

5.6 Método de Krüskemper 127

Bibliografia 134

Introdução

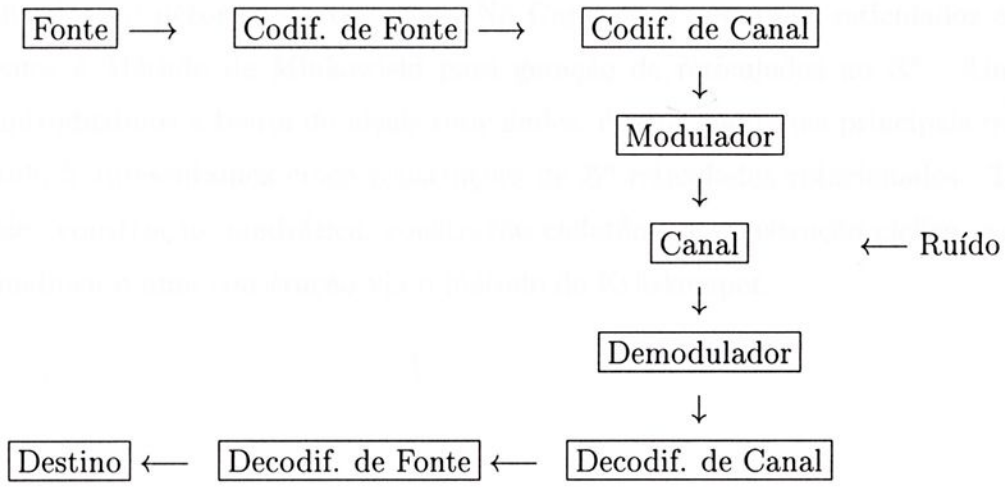
Em um sistema de comunicação digital, o objetivo é transmitir dados de uma fonte até um destino. O meio usado para esta transmissão é chamado de canal e pode ser um cabo coaxial, fibra óptica, a atmosfera (no caso de ondas de rádio), CD's, disquetes, DVD's (no caso de canais de armazenagem),etc.

Em um sistema tradicional, os dados gerados pela fonte são símbolos de um alfabeto $\mathcal{A}$. Como cada símbolo tem sua probabilidade de ocorrência, estes dados são processados pelo codificador de fonte, com o objetivo de eliminar redundâncias e desta forma compactar a informação.

As sequências geradas pelo codificador de fonte são então processadas pelo codificador de canal, que introduz redundâncias gerando sequências de símbolos de $\mathcal{A}$ que são chamadas de palavras código. Para a transmissão, o modulador associa a cada palavra código x um conjunto de símbolos analógico, que é então enviado pelo canal.

A imperfeição do canal gera distorções e o sinal recebido nem sempre coincide com o enviado. O demodulador faz então a melhor estimativa, fornecendo uma sequência r de símbolos de $\mathcal{A}$. Devido ao ruído, é possível que r não seja uma palavra código. Então, o decodificador de canal associará uma palavra código, que é a melhor estimativa.

Finalmente, o decodificador de fonte associará a esta palavra código a suposta sequência original de símbolos enviada. O diagrama abaixo ilustra o processo.



Cada uma destas etapas gerou grandes áreas de pesquisa, que se desenvolveram, de certa forma, independentemente.

A teoria dos códigos corretores de erros nasceu em 1948, com o famoso trabalho de Shannon [1], onde foi demonstrado o Teorema da Capacidade de Canal. Em linhas gerais, este

resultado diz que para transmissão de dados abaixo de uma taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter probabilidade de erro tão pequena quanto se deseja através de códigos corretores de erros eficientes.

A Teoria Algébrica dos Números tem sido bastante útil no desenvolvimento de códigos corretores de erros e reticulados. Corpos finitos foram a ferramenta chave para o desenvolvimento dos códigos binários, estruturas que despertaram gradativamente o interesse dos pesquisadores em teoria das comunicações. Recentemente, a preocupação de perder informações nas comunicações sem fio forçou os pesquisadores da teoria da codificação a trabalhar com canais com desvanecimento. Deste modo, novos critérios para a obtenção de códigos vem sendo consi-

derados com a finalidade de aperfeiçoar o desempenho dos sistemas de transmissão sem fio. É neste contexto que constelações de sinais de reticulados rotacionados têm sido propostas para transmissão sobre o canal Rayleigh com desvanecimento. Reticulados algébricos, isto é, reticulados construídos via o homomorfismo canônico de um corpo de números algébricos, são providos de uma ferramenta eficiente para construção de tais códigos reticulados. A razão é que os dois principais parâmetros para a construção desses códigos, a diversidade e a distância produto mínima do reticulado, estão diretamente relacionadas com as propriedades do corpo de números em questão.

O presente trabalho está dividido em cinco capítulos. Os Capítulos 1, 2 e 3 são dedicados a Teoria Algébrica dos Números, onde apresentamos alguns conceitos e resultados que serão utilizados no decorrer do trabalho. No Capítulo 4 definimos reticulados algébricos e fornecemos o Método de Minkowiski para geração de reticulados no $\mathbb{R}^n$. Ainda neste capítulo introduzimos a teoria de ideais reticulados, descrevendo seus principais resultados. No Capítulo 5 apresentamos cinco construções de $\mathbb{Z}^n$-reticulados rotacionados. Tais construções são: construção quadrática, construção ciclotômica, construção cíclica, construção mista e finalmente uma construção via o método de Krüskemper.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Capítulo 1

Teoria algébrica dos números

Neste capítulo introduzimos conceitos importantes da Teoria Algébricos dos Números tais como elementos inteiros sobre anéis, norma e traço de elementos. Enfocamos também as principais propriedades dos anéis Noetherianos, dos anéis de Dedekind e anéis de frações.

O objetivo deste capítulo é introduzir conceitos que serão usados nos capítulos posteriores, e os resultados podem ser encontrados nas referências [2], [3], [4], [5] e [6].

1.1 Módulos Noetherianos

Nesta seção apresentamos os conceitos de módulos e módulos Noetherianos juntamente com suas principais propriedades.

Definição 1.1.1 *Seja A um anel. Um A-**módulo** M é um grupo abeliano (aditivo) munido de uma aplicação $A \times M \longrightarrow M$, denotado por $(a, m) \longrightarrow am$, tal que, para quaisquer $a, b \in A$ e $x, y \in M$, tem-se:*

i) $a(x + y) = ax + ay$;

ii) $(a + b)x = ax + bx$;

iii) $(ab)x = a(bx)$;

iv) $1x = x$.

Definição 1.1.2 *Sejam A um anel e M um A-módulo. Um subconjunto $N \subset M$ não vazio é um A-**submódulo** de M se, com as operações herdadas de M, também é um A-módulo.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Definição 1.1.3

1. *Um A-módulo M é dito* **finitamente gerado** *se existem $x_1, \ldots, x_r \in M$ tais que $M = Ax_1 + \cdots + Ax_r$, e neste caso, dizemos que $x_1, \cdots, x_r$ formam um sistema de geradores de M.*
2. *Um conjunto de elementos $x_1, \ldots, x_r \in M$ são* **linearmente independentes** *(sobre A) se a igualdade $\sum_{i=1}^{r} a_i x_i = 0$, com $a_i \in A$, implicar que $a_1 = \cdots = a_r = 0$.*
3. *Se além disso, $x_1, \ldots, x_s$ formarem um sistema de geradores de M, então eles formam uma* **base** *de M.*

Observação 1.1.1 *É importante lembrar que nem todo módulo finitamente gerado possui uma base. Um A-módulo que possui uma base é chamado de A-módulo livre, e o número de elementos da base é chamado de* **posto de** *A.*

Definição 1.1.4 *Sejam M um A-módulo e $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ uma sequência crescente de A-submódulos de M. Esta é uma* **sequência estacionária** *se existir $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$ para todo $n \geq n_0$. A definição é análoga para sequência decrescente estacionária.*

Definição 1.1.5 *Sejam A um anel e M um A-módulo. Dizemos que M é um* **A-módulo Noetheriano** *se satisfaz uma das seguintes condições:*

1) Toda família não vazia de A-submódulos de M tem 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 considerado como um A-módulo for noetheriano.*

Proposição 1.1.1 *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 principal, 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. Temos que $I = \bigcup_{n \in N} I_n$ é um ideal de A. 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 $\forall n \geq n_0$ temos que $I_n = I_{n_0}$. ■

unesp

Teorema 1.1.1 *Sejam A um anel principal, M um A-módulo livre de posto n, e M' um A-submódulo de M. Então:*

i) M' é livre de posto q, $0 \leq q \leq n$.

ii) Se $M' \neq \langle 0 \rangle$, então existe uma base $\{e_1, \ldots, e_n\}$ de M e elementos não nulos $a_1, \ldots, a_q \in A$ tal que $\{a_1 e_1, \ldots, a_q e_q\}$ é uma base de M' e que a_i divide a_{i+1}, para $i = 1, 2, \ldots, q-1$.

Demonstração: Para $M = \langle 0 \rangle$ o resultado é trivial. Consideremos portanto $M \neq \langle 0 \rangle$. Seja $L(M, A)$ o conjunto das formas bilineares sobre M. Para $u \in L(M, A)$, $u(M')$ é um submódulo de A, um ideal de A. Como todo ideal de A é principal, podemos escrever $u(M') = Aa_u$, com $a_u \in A$. Pela Proposição (1.1.1), segue que A é um anel Noetheriano, então existe $u \in L(M, A)$ tal que Aa_u é maximal entre todos os Aa_v, $v \in L(M, A)$. Seja $\{x_1, x_2, \ldots, x_n\}$ uma base de M, a qual o identifica com A^n. Seja $P_{r_i} : M \to A$ a projeção na i-ésima coordenada, isto é, $P_{r_i}(x_j) = \delta_{ij}$. Como $M' \neq \langle 0 \rangle$, para pelo menos um $i, 1 \leq i \leq n$, $P_{r_i}(M') \neq \langle 0 \rangle$. Consequentemente, $a_u \neq 0$. Pela nossa construção, existe $e' \in M'$ tal que $u(e') = a_u$. Mostremos que para todo $v \in L(M, A), a_u \mid v(e')$. Se $d = mdc(a_u, v(e'))$, existem $b, c \in A$ tais que $d = ba_u + cv(e')$, ou seja, $d = (bu + cv)e'$. Como $w = bu + cv$ é uma forma linear sobre M, $Aa_u \subset Ad \subset w(M')$. Pela maximalidade de Aa_u segue que $Ad = Aa_u$, o que implica que $a_u \mid v(e')$. Em particular, $a_u \mid P_{r_i}(e')$, então, $P_{r_i}(e') = a_u b_i$, com $b_i \in A$. Faça $e = \sum_{i=1}^{n} b_i x_i$, então $e' = a_u e$. Como $u(e') = a_u = a_u u(e)$, segue que u(e)=1. Mostremos que :

1. $M = Ker(u) \oplus Ae$.

2. $M' = (M' \cap Ker(u)) \oplus Ae'$, onde $e' = a_u e$

1. Para todo $x \in M, x = u(x)e + (x - u(x)e)$. Observe que $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, pois $u(e) = 1$, então $x - u(x)e \in Ker(u)$. Isto mostra que $Ae + Ker(u) = M$. Além disso, $Ae \cap Ker(u) = \emptyset$. Portanto, $M = Ker(u) \oplus Ae$.

2. Para $y \in M, u(y) = ba_u$, com $b \in A$, tal que $y = ba_u e + (y - u(y)e) + be' + (y - u(y)e)$. Além disso, temos que $y - u(y)e \in Ker(u)$ e $y - u(y)e = y - be' \in M'$, ou seja, $y - u(y)e \in (M' \cap Ker(u))$ e $be' \in Ae' \subset Ae$, e isto conclui (2).

Finalmente vamos a demonstração do teorema. i) Faremos por indução sobre o posto q de M'. Se $q = 0$, $M' = \langle 0 \rangle$ e não há o que provar. Se $q > 0$, $M' \cap Ker(u)$ tem rank $q - 1$ (de acordo com (2)) e portanto, $M' \cap Ker(u)$ é livre, de acordo com a hipótese de indução. Como a soma em (2) é direta, obtemos uma base para M', adicionando e' a base

de $M' \cap Ker(u)$. Consequentemente, M' é livre de posto q. ii) Faremos indução sobre n, o posto de M. Novamente, se $n = 0$ não há o que provar. Suponhamos então $n > 0$. Pelo item i), $Ker(u)$ é livre de posto $n-1$, já que a soma em (1) é direta. Aplicaremos a hipótese de indução para o módulo livre $Ker(u)$ e para o submódulo $M' \cap Ker(u)$: se $M' \cap Ker(u) \neq \langle 0 \rangle$, existem $q \leq n$, uma base $\{e_2, \ldots, e_n\}$ de $Ker(u)$ e elementos $a_2, \ldots, a_q$ de A não nulos, tal que $\{a_2e_2, \ldots, a_qe_q\}$ é uma base para $M' \cap Ker(u)$, e tal que $a_i \mid a_{i+1}$, para $2 \leq i \leq q-1$. Com as mesmas notações acima, seja $a_1 = a_u$ e $e_1 = e$. Então, de acordo com (1), $\{e_1, e_2, \ldots, e_n\}$ é uma base para M e de acordo com (2), e do fato de $e' = a_1e_1$, segue que $\{a_1e_1, a_2e_2, \ldots, a_qe_q\}$ é uma base para M'. Falta mostrar que $a_1 \mid a_2$. Seja v uma forma linear sobre M definida pela relação $v(e_1) = v(e_2) = 1$ e $v(e_i) = 0$, para $i \geq 3$. Então $a_1 = a_u = v(a_ue_1) = v(e') \in v(M')$, então $Aa_u \subset v(M')$. Pela maximalidade de Aa_u, concluímos que $v(M') = Aa_u = Aa_1$. Como $a_2 = v(a_2e_2) \in v(M')$, temos que $a_1 \in Aa_2$, e isto implica que $a_1 \mid a_2$, e isto conclui a demonstração. ∎

Proposição 1.1.2 *Sejam A um anel, M um A-módulo e N um submódulo de M. Então M é noetheriano se, e somente se, $\frac{M}{N}$ e N são noetherianos.*

Demonstração: Suponha que M é noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de A-submódulos de N. Então $(M_n)_{n\geq 0}$ 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 $\frac{M}{N}$ é noetheriano, sejam

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

A aplicação $\varphi : S \longrightarrow T$ definida por $\varphi(L) = \frac{L}{N}$, 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 $\frac{M}{N}$, 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, $\frac{M}{N}$ é noetheriano. Reciprocamente, suponhamos que $\frac{M}{N}$ 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 N. Como N é noetheriano, segue que $(N \cap M_n)_{n\geq 0}$ é estacionária, ou seja, existe $k \in \mathbb{N}$ tal que

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Sabemos, que $M_n \subseteq M_{n+1}, \forall n \geq k$. 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, $M_n = M_{n+1}$, $\forall n \geq k$ e assim, M é noetheriano. ∎

Corolário 1.1.1 *Se $M_1, \ldots, M_n$ 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. ∎

Corolário 1.1.2 *Se A é um anel noetheriano e M é um A-módulo finitamente gerado, então M é um A-módulo noetheriano.*

Demonstração: Seja $\{e_1, \ldots, e_n\}$ um conjunto de geradores do A-módulo M. Temos que a aplicação $\varphi : A^n \longrightarrow M$ definida por $\varphi(a_1, \ldots, a_n) = a_1e_1 + \cdots + a_ne_n$, é um homomorfismo sobrejetor. Assim, pelo Teorema do Homomorfismo, temos que $\dfrac{A^n}{\ker \varphi} \simeq M$. 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. ∎

Proposição 1.1.3 *Em um anel noetheriano A todo ideal contém um produto de ideais primos.*

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 M. Temos que M não é um ideal maximal, pois caso contrário, M seria primo e assim, $M \notin F$. Assim, existem $x, y \in A - M$ tal que $xy \in M$. Notemos que $M \subsetneq \langle x \rangle + M$ e $M \subsetneq \langle y \rangle + M$. Logo, $\langle x \rangle + M$ e $\langle y \rangle + M$ não pertencem a F. Assim,

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

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

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

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

Corolário 1.1.3 *Em um domínio noetheriano, todo ideal não nulo contém um produto de ideais primos não nulos.*

Demonstração: Análoga a Proposição (1.1.3). ∎

Definição 1.1.6 *Seja A um anel. Dizemos que $a \in A$ é* **nilpotente** *se $a^n = 0$, para algum $n \geq 0$. Dizemos que A é um* **anel reduzido** *se o único elemento nilpotente de A é o zero.*

Corolário 1.1.4 *Se A é um anel noetheriano reduzido, então o ideal nulo de A é uma intersecção finita de ideais primos não nulos de A.*

Demonstração: Pela Proposição (1.1.3), temos que o ideal nulo de um anel noetheriano contém um produto de ideais primos. Portanto, $\langle 0 \rangle = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$. Vamos mostrar que $\langle 0 \rangle = \bigcap_{i=1}^{g} \mathfrak{p}_i^{e_i}$. Temos que $\langle 0 \rangle \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_g$. Por outro lado, se $x \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_g$, então $x^{e_1+e_2+\cdots+e_g} \in \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g} = \langle 0 \rangle$. Como A é reduzido, segue que $x = 0$. Portanto, $\langle 0 \rangle = \bigcap_{i=1}^{g} \mathfrak{p}_i^{e_i}$. ∎

Lema 1.1.1 *Se $\mathcal{A}_1, \mathcal{A}_2$ são ideais de um anel A e $\mathcal{A}_1 + \mathcal{A}_2 = A$ então $\mathcal{A}_1\mathcal{A}_2 = \mathcal{A}_1 \cap \mathcal{A}_2$.*

Demonstração: Temos que $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1$ e $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_2$ e assim $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1 \cap \mathcal{A}_2$. Agora, suponhamos que $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Por hipótese, $\mathcal{A}_1 + \mathcal{A}_2 = A$, assim, existem elementos $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$ tal que $1 = a_1 + a_2$. Logo, $x = a_1x + a_2x$ é a soma de dois elementos de $\mathcal{A}_1\mathcal{A}_2$. Assim, $\mathcal{A}_1 \cap \mathcal{A}_2 \subset \mathcal{A}_1\mathcal{A}_2$. Portanto, $\mathcal{A}_1\mathcal{A}_2 = \mathcal{A}_1 \cap \mathcal{A}_2$. ∎

Lema 1.1.2 *Se A é um anel e $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ é um conjunto finito de ideais de A, tais que $\mathcal{A}_i + \mathcal{A}_j = A$, para $i \neq j$, então $A/\prod_{i=1}^{n} \mathcal{A}_i \simeq \prod_{i=1}^{n} A/\mathcal{A}_i$.*

Demonstração: Faremos a prova por indução sobre n. Para o caso $n = 2$, seja a aplicação

$$\varphi : A \longrightarrow A/\mathcal{A}_1 \times A/\mathcal{A}_2,$$

definida por $\varphi(a) = (a + \mathcal{A}_1, a + \mathcal{A}_2)$, com $a \in A$. Assim $\ker(\varphi) = \mathcal{A}_1 \cap \mathcal{A}_2$, uma vez que, $\varphi(x) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $(x+\mathcal{A}_1, x+\mathcal{A}_2) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $x+\mathcal{A}_1 = \bar{0}$ e $x+\mathcal{A}_2 = \bar{\bar{0}}$ se, e somente se $x \in \mathcal{A}_1$ e $x \in \mathcal{A}_2$, se e somente se, $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Quanto a sobretividade, dados $y, z \in A$, devemos encontrar $x \in A$ tal que $(y + \mathcal{A}_1, z + \mathcal{A}_2) = (x + \mathcal{A}_1, x + \mathcal{A}_2) = \varphi(x)$.

unesp

Como $\mathcal{A}_1 + \mathcal{A}_2 = A$, existem elementos $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$ tais que $1 = a_1 + a_2$. Seja, $x = a_1 z + a_2 y$. Como $a_2 \equiv 1 (modulo\ \mathcal{A}_1)$ e $a_1 \equiv 1 (modulo\ \mathcal{A}_2)$ segue que $x \equiv y (modulo\ \mathcal{A}_1)$ e $x \equiv z (modulo\ \mathcal{A}_2)$, isto é, $x + \mathcal{A}_1 = y + \mathcal{A}_1$ e $x + \mathcal{A}_2 = z + \mathcal{A}_2$, ou seja, φ é sobrejetora. Portanto, $A/\mathcal{A}_1 \cap \mathcal{A}_2 \simeq A/\mathcal{A}_1 \times A/\mathcal{A}_2$, e pelo Lema (1.1.1), temos que

$$A/\mathcal{A}_1\mathcal{A}_2 \simeq A/\mathcal{A}_1 \times A/\mathcal{A}_2.$$

Agora, supomos que o resultado é verdadeiro para $\forall k < n$. Fazendo $\mathfrak{b} = \mathcal{A}_2 \dots \mathcal{A}_n$, temos que $\mathcal{A}_1 + \mathfrak{b} = A$, uma vez que $\mathcal{A}_1 + \mathcal{A}_i = A$, para $i \geq 2$, e assim, existem elementos $c_i \in \mathcal{A}_1$ e $a_i \in \mathcal{A}_i$ tais que $c_i + a_i = 1$. Logo, $1 = \prod_{i=2}^{n}(c_i + a_i) = c + a_2 \dots a_n$, onde c é a soma dos termos que contém no mínimo um c_i como fator. Logo, $c \in \mathcal{A}_1$. Como $a_2 \dots a_n \in \mathfrak{b}$, segue que $\mathcal{A}_1 + \mathfrak{b} = A$. Pelo caso $n = 2$, segue que $A/\mathcal{A}_1 b \simeq A/\mathcal{A}_1 \times A/b$, e por hipótese de indução temos que $A/\prod_{i=1}^{n} \mathcal{A}_i \simeq \prod_{i=1}^{n} A/\mathcal{A}_i$. ∎

Definição 1.1.7 *Um espaço vetorial V sobre um corpo $\mathbb{K}$ é uma* **$\mathbb{K}$-álgebra** *se existe uma multiplicação em V satisfazendo,*

1. $a(b+c)=ab+ac$, $\forall a, b, c \in V$,
2. $a(\alpha b)=(\alpha a)b=\alpha(ab)$, $\forall \alpha \in \mathbb{K}$ *e* $a, b \in V$,
3. $a(bc)=(ab)c$, $\forall a, b, c \in V$,
4. $\exists 1_V \in V$; $a1_V = a = 1_V a$, $\forall a \in V$

Observação 1.1.2 *Se $ab = ba$, $\forall a, b \in V$, dizemos que V é uma* **$\mathbb{K}$-álgebra comutativa**.

1.2 Anel de inteiros

Nesta seção, apresentamos o conceito de anel de inteiros e faremos um estudo sobre as suas principais propriedades.

Definição 1.2.1 *Sejam B anel e A um subanel de B. Dizemos que um elemento $\alpha \in B$ é* **inteiro** *sobre A, se α é raiz de um polinômio mônico com coeficientes em A, ou seja, existem $a_0, \dots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Essa equação é chamada de* **equação de dependência integral** *de α.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Exemplo 1.2.1 *Se* $\alpha = \sqrt{5} + \sqrt{7} \in \mathbb{R}$, *temos que* α *é inteiro sobre* $\mathbb{Z}$, *pois* α *é raiz do polinômio* $x^4 - 24x^2 + 4 \in \mathbb{Z}[x]$.

Teorema 1.2.1 *Sejam* $A \subseteq B$ *anéis e* $\alpha \in B$. *São equivalentes as seguintes afirmações:*
i) α *é inteiro sobre* A.
ii) O *anel* $A[\alpha]$ *é um* A*-módulo finitamente gerado.*
iii) Existe um subanel R *do anel* B *tal que* R *é um* A*-módulo finitamente gerado que contém* A *e* α.

Demonstração: i) $\Rightarrow$ ii) Temos que $A[\alpha] = \{\sum_i a_i\alpha^i : a_i \in A\}$. Por hipótese, temos que α é inteiro sobre A, assim, existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tais que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Seja $M = [1, \alpha, \ldots, \alpha^{n-1}]$ um A-módulo finitamente gerado. Vamos mostrar que $A[\alpha] = M$. Temos que $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)$, ou seja, $\alpha^n \in [1, \alpha, \ldots, \alpha^{n-1}]$. Agora, vamos provar por indução que $\alpha^j \in [1, \alpha, \ldots, \alpha^{n-1}]$, para $j \in \mathbb{N}$. Temos que $\alpha^j \in [1, \alpha, \ldots, \alpha^{n-1}]$, $\forall j \leq n$. Suponhamos por hipótese de indução que $\alpha^j \in [1, \alpha, \ldots, \alpha^{n-1}]$ e mostremos que $\alpha^{j+1} \in [1, \alpha, \ldots, \alpha^{n-1}]$. Por hipótese de indução existem $b_0, \ldots, b_{n-1} \in A$ tal que $\alpha^j = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$. Assim,

$$\begin{aligned}
\alpha^{j+1} &= \alpha^j\alpha \\
&= (b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0)\alpha \\
&= b_{n-1}\alpha^n + \cdots + b_1\alpha^2 + b_0\alpha \\
&= b_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) + \cdots + b_1\alpha^2 + b_0\alpha \\
&= -b_{n-1}a_{n-1}\alpha^{n-1} - \cdots - b_{n-1}a_1\alpha - b_{n-1}a_0 + \cdots + b_1\alpha^2 + b_0\alpha \\
&= -a_0b_{n-1} + (-b_{n-1}a_1 + b_0)\alpha + \cdots + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1},
\end{aligned}$$

ou seja, $\alpha^j \in [1, \alpha, \ldots, \alpha^{n-1}]$, para $j \in \mathbb{N}$. Por outro lado, $[1, \alpha, \ldots, \alpha^{n-1}] \subset A[\alpha]$. Assim, $[1, \alpha, \ldots, \alpha^{n-1}] = A[\alpha]$. Portanto, $A[\alpha]$ é um A-módulo gerado por $1, \alpha, \ldots, \alpha^{n-1}$. Para ii)$\Rightarrow$ iii) como $\alpha \in A[\alpha]$ e $A \subset A[\alpha]$, é suficiente tomar $R = A[\alpha]$. Finalmente, para iii)$\Rightarrow$ i) seja $R = \langle y_1, \ldots, y_n \rangle$ um A-módulo finitamente gerado tal que $A \subset R \subset B$ e $\alpha \in R$, ou seja, $R = Ay_1 + \cdots + Ay_n$. Como $\alpha \in R$ temos que $\alpha y_i \in R$, *para* $i = 1, \ldots, n$. Assim, existem

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$a_{ij} \in A$, com $1 \leq i, j \leq n$, de modo que

$$\begin{cases} \alpha y_1 = a_{11}y_1 + \cdots + a_{1n}y_n \\ \alpha y_2 = a_{21}y_1 + \cdots + a_{2n}y_n \\ \quad \vdots \\ \alpha y_n = a_{n1}y_1 + \cdots + a_{nn}y_n. \end{cases}$$

Logo,

$$\begin{cases} (\alpha - a_{11})y_1 - a_{12}y_2 - \cdots - a_{1n}y_n &= 0 \\ -a_{21}y_1 + (\alpha - a_{22})y_2 - \cdots - a_{2n}y_n &= 0 \\ \quad \vdots \\ -a_{n1}y_1 - a_{n2}y_2 - \cdots + (\alpha - a_{nn})y_n &= 0. \end{cases}$$

Na forma matricial, temos

$$\begin{bmatrix} (\alpha - a_{11}) & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & (\alpha - a_{22}) & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & \cdots & (\alpha - a_{nn}) \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Seja D o determinante da matriz dos coeficientes do sistema linear. Pela regra de Cramer, temos que $Dy_j = 0$, para $j = 1, \ldots, n$. Como $1 \in R$, segue que $1 = \sum_{j=1}^{n} c_j y_j$, com $c_j \in A$, e assim, $D = D \cdot 1 = D\sum_{j=1}^{n} c_j y_j = \sum_{j=1}^{n} c_j D y_j = 0$. Observemos que D é uma equação de dependência integral de α uma vez que $D = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$, onde cada $b_i \in A$. Portanto, α é inteiro sobre A. ■

Corolário 1.2.1 *Sejam $A \subseteq B$ anéis, e sejam $\alpha_1, \ldots, \alpha_n \in B$. Se α_1 é inteiro sobre A, α_2 é inteiro sobre $A[\alpha_1]$, ... e α_n é inteiro sobre $A[\alpha_1, \ldots, \alpha_{n-1}]$, então $A[\alpha_1, \ldots, \alpha_n]$ é um A-módulo finitamente gerado.*

Demonstração: Se α_1 é inteiro sobre A, então pelo Teorema (1.2.1), temos que $A[\alpha_1]$ é um A-módulo finitamente gerado. Assim, suponhamos que $R = A[\alpha_1, \ldots, \alpha_{n-1}]$ seja um A-módulo finitamente gerado por $\{v_1, v_2, \ldots, v_n\}$ e que α_n seja inteiro sobre $R = A[\alpha_1, \ldots, \alpha_{n-1}]$. Pelo Teorema (1.2.1), temos que $R[\alpha_n]$ é um R-módulo finitamente gerado. Assim, existe $\{w_1, \ldots, w_s\} \subset R[\alpha_n]$ tal que

$$R[\alpha_n] = A[\alpha_1, \ldots, \alpha_n] = \sum_{i=1}^{s} Rw_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{n} a_j v_j \right) w_i = \sum_{j,i} a_j v_j w_i.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Logo, $\{v_j w_i\}$ para $i = 1, \ldots, s$ e $j = 1, \ldots, n$, gera $R[\alpha_n]$ como um A-módulo. Portanto, $A[\alpha_1, \ldots, \alpha_n]$ é um A-módulo finitamente gerado. ∎

Observação 1.2.1 *Quando $B = \mathbb{C}$, o corpo dos complexos, e os coeficientes do polinômio são números racionais, dizemos simplesmente que α é um* **número algébrico**. *Se os coeficientes do polinômio mônico são números inteiros, α é chamado* **inteiro algébrico**.

Exemplo 1.2.2 *O elemento $\alpha = \sqrt{13}$ é um inteiro algébrico, pois é raiz do polinômio mônico $x^2 - 13 \in \mathbb{Z}[x]$. O elemento $\alpha = \sqrt{2} + \sqrt{3}$ é um inteiro algébrico, pois é raiz do polinômio mônico $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$.*

Corolário 1.2.2 *Sejam $A \subseteq B$ anéis. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A.*

Demonstração: Temos que $\alpha \pm \beta$, $\alpha\beta$ pertencem a $A[\alpha, \beta]$. Pelo Corolário (1.2.1), temos que $A[\alpha, \beta]$ é um A-módulo finitamente gerado e pelo Teorema (1.2.1), segue que $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A. ∎

Teorema 1.2.2 *Se α é uma raiz de um polinômio mônico, onde os coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Demonstração: Seja $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$, tal que $a_i, para \;\; i = 1, \ldots, n-1$ pertença ao conjunto dos números complexos que são raízes de polinômios mônicos com coeficientes em $\mathbb{Z}$. Fazendo $B = \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$, $b_0 = a_0, \ldots, b_{n-1} = a_{n-1}$ e $b_n = \alpha$ temos, pelo Corolário (1.2.1), que $\mathbb{Z}[b_0, \ldots, b_n]$ é um $\mathbb{Z}$-módulo finitamente gerado. Pelo Teorema (1.2.1) segue que α é um inteiro algébrico. ∎

Definição 1.2.2 *Sejam $A \subseteq B$ anéis. Dizemos que B* **é inteiro sobre** *A se todo elemento de B é inteiro sobre A.*

Exemplo 1.2.3 *Dentre os anéis que satisfazem esta condição está o anel dos inteiros de Gauss, $\mathbb{Z}[i]$, pois todo elemento $a + bi$ de $\mathbb{Z}[i]$ é raiz do polinômio $x^2 - 2ax + (a^2 + b^2) \in \mathbb{Z}[x]$.*

Definição 1.2.3 *Sejam $A \subseteq B$ anéis.*
(1) $\mathcal{O}_B = \{\alpha \in B : \alpha$ é inteiro sobre $A\}$ é chamado **anel de inteiros de A em B**.
(2) Se A é um domínio e $B = \mathbb{K}$ o corpo de frações de A, dizemos que $\mathcal{O}_B$ **é o anel de inteiros de A em $\mathbb{K}$**. *Além disso, se $A = \mathcal{O}_B$ dizemos que A é um anel* **integralmente fechado**.

unesp

Proposição 1.2.1 *Sejam $A \subseteq B$ anéis. Então $A \subseteq \mathcal{O}_B \subseteq B$.*

Demonstração: Pelo Corolário (1.2.2), temos que $\mathcal{O}_B$ é um subanel de B . Agora, se $\alpha \in A$, então α é raiz do polinômio $p(x) = x - \alpha$, que tem coeficientes em A. Assim, $\alpha \in \mathcal{O}_B$. Portanto, $A \subseteq \mathcal{O}_B \subseteq B$. ∎

Proposição 1.2.2 *Sejam $A \subseteq B \subseteq R$ anéis. Assim, R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

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

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

Como $A \subset B$, segue que $a_i \in B$, para $i = 0, 1, \ldots, n-1$, ou seja, α é inteiro sobre B. Portanto, R é inteiro sobre B. Agora, seja $\alpha \in B$. Como $B \subset R$, segue que $\alpha \in R$, então, por hipótese α é inteiro sobre A. Portanto, B é inteiro sobre A. Reciprocamente, seja $\alpha \in R$. Como R é inteiro sobre B, segue que existem $b_0, \ldots, b_{n-1} \in B$, não todos nulos, tal que

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

Seja $C = A[b_0, \ldots, b_{n-1}]$. Logo, α é inteiro sobre C. Como B é inteiro sobre A, segue que os $b_i's$ são inteiros sobre A. Pelo Corolário (1.2.1), segue que $C[\alpha] = A[b_0, \ldots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado. Pelo Teorema (1.2.1), temos que α é inteiro sobre A. Portanto, R é inteiro sobre A. ∎

Proposição 1.2.3 *Sejam $A \subseteq B$ anéis com B um domínio e inteiro sobre A. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração: Suponha que A seja um corpo. Seja $\alpha \in B$, $\alpha \neq 0$. Como B é inteiro sobre A então α é inteiro sobre A e, portanto, pelo Teorema (1.2.1) segue que $A[\alpha]$ é um espaço vetorial finitamente gerado sobre A, pois A é um corpo. Seja

$$\begin{aligned} \varphi : A[\alpha] &\longrightarrow A[\alpha] \\ b &\longmapsto b\alpha, \quad \forall\, b \in A[\alpha]. \end{aligned}$$

Temos que φ é A-linear e $Ker(\varphi) = \{b \in A[\alpha] : \varphi(b) = 0\} = \{0\}$, pois $\varphi(b) = 0$ se, e somente se, $b\alpha = 0$ e como B é um domínio e $\alpha \neq 0$ segue que b=0. Deste modo, φ é injetora e como estamos considerando espaços de mesma dimensão finita, segue que φ é sobrejetora.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Portanto φ é bijetora. Assim, como $1 \in A[\alpha]$ segue que exite $b' \in A[\alpha]$ tal que $b'\alpha = 1$, ou seja, α é inversível em B. Portanto B é um corpo. Reciprocamente, seja $\alpha \in A$, $\alpha \neq 0$. Como $A \subset B$ então $\alpha \in B$ e como B é um corpo segue que $\alpha^{-1} \in B$. Como B é inteiro sobre A, e $\alpha^{-1} \in B$ segue que

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

com $a_i \in A$ não todos nulos. Multiplicando por α^{n-1}, obtemos

$$\alpha^{-1} + a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1} = 0$$

e então

$$\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1}) \in A.$$

Portanto A é um corpo. ■

Proposição 1.2.4 *Se A é um domínio, então $\mathcal{O}_B$ é um anel integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações de A. Assim, $\mathbb{K}$ também é o corpo de frações de $\mathcal{O}_B$. Seja $\alpha \in \mathbb{K}$ inteiro sobre $\mathcal{O}_B$. Como $\mathcal{O}_B$ é inteiro sobre A segue da Proposição (1.2.2) que α é inteiro sobre A e, portanto, $\alpha \in \mathcal{O}_B$. Assim, $\mathcal{O}_B$ é um anel integralmente fechado.■

Proposição 1.2.5 *Se A é um anel principal, então A é um anel integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações de A. Seja $\alpha \in \mathbb{K}$ inteiro sobre A tal que $\alpha = \frac{a}{b}$, com $a, b \in A$ e $mdc(a, b) = 1$. Assim, existem $a_i \in A$, $i = 0, 1, \ldots, n-1$, não todos nulos, tal que

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

Substituindo α por $\frac{a}{b}$, temos que

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0.$$

Multiplicando por b^n, obtemos

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0b^n = 0,$$

isto é,

$$a^n = b(-a_{n-1}a^{n-1} - \cdots - a_0b^{n-1}).$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Logo b divide a^n e como $mdc(a,b) = 1$, segue que b divide a, o que implica que $a = bc$. Usando novamente o fato de $mdc(a,b) = 1$, temos que existem $x_0, y_0 \in A$ tal que $ax_0 + by_0 = 1$. Assim, $bcx_0 + by_0 = 1$ o que implica que $b(cx_0 + y_0) = 1$. Assim, b é inversível em A e $\alpha = ab^{-1} \in A$. Portanto, A integralmente fechado. ∎

Exemplo 1.2.4 *O anel $\mathbb{Z}$ dos números inteiros é integralmente fechado, pois é principal. Todo domínio fatorial é integralmente fechado.*

1.3 Norma e traço

Nesta seção, apresentamos os conceitos de norma e traço de elementos. Também provamos que o anel de inteiros é um A-módulo livre, onde A é um anel principal.

Sejam $A \subseteq B$ anéis, onde B é um A-módulo livre de posto finito n. Seja $\{e_1, \ldots, e_n\}$ uma base de B sobre A e seja $\sigma : B \longrightarrow B$ um homomorfismo. Assim,

$$\begin{aligned}
\sigma(e_1) &= a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n, \\
\sigma(e_2) &= a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n, \\
&\vdots \\
\sigma(e_n) &= a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n,
\end{aligned}$$

com $a_{ij} \in A$, onde $1 \leq i, j \leq n$. Assim, $\begin{bmatrix} \sigma(e_1) \\ \vdots \\ \sigma(e_n) \end{bmatrix} = [a_{ij}] \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}$.

Definição 1.3.1 *Definimos o* **traço** *de σ por $Tr_{B|A}(\sigma) = \sum_{i=1}^{n} a_{ii}$, a* **norma** *de σ por $N_{B|A}(\sigma) = \det(a_{ij})$ e o* **polinômio característico** *de σ por $\chi_{B|A}(x) = \det(xI - \sigma)$.*

Assim, temos que:

$$\begin{aligned}
Tr_{B|A}(\sigma + \sigma') &= Tr_{B|A}(\sigma) + Tr_{B|A}(\sigma') \\
N_{B|A}(\sigma\sigma') &= N_{B|A}(\sigma)N_{B|A}(\sigma') \\
\chi_{B|A}(x) &= det(xI - \sigma) = x^n - (Tr_{B|A}(\sigma))x^{n-1} + \cdots + (-1)^n det(\sigma).
\end{aligned}$$

Definição 1.3.2 *Sejam A um anel e B um A-módulo livre. Considere o endomorfismo $\sigma_\alpha : B \longrightarrow B$ definido por $\sigma_\alpha(x) = \alpha x$, com $\alpha \in B$. O traço de $\alpha \in B$ é definido por $Tr_{B|A}(\alpha) = Tr_{B|A}(\sigma_\alpha)$, a norma de $\alpha \in B$ por $N_{B|A}(\alpha) = det(\sigma_\alpha)$ e o polinômio característico de α por $\chi_{B|A}(x) = det(xI - \sigma_\alpha)$.*

unesp

Vale ressaltar que quando não houver dúvidas a respeito dos anéis com os quais estamos trabalhando, denotaremos $Tr_{B|A}$, $N_{B|A}$ e $\chi_{B|A}(x)$ simplesmente por Tr, N e $\chi(x)$.

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

1. $Tr_{\mathbb{L}|\mathbb{K}}(\alpha + \alpha') = Tr_{\mathbb{L}|\mathbb{K}}(\alpha) + Tr_{\mathbb{L}|\mathbb{K}}(\alpha')$
2. $Tr_{\mathbb{L}|\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}|\mathbb{K}}(\alpha)$
3. $Tr_{\mathbb{L}|\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a$
4. $N_{\mathbb{L}|\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$
5. $N_{\mathbb{L}|\mathbb{K}}(a\alpha) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}|\mathbb{K}}(\alpha)$
6. $N_{\mathbb{L}|\mathbb{K}}(\alpha\alpha') = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\alpha')$,

e se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ temos que

7. $N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(\alpha))$
8. $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = Tr_{\mathbb{M}|\mathbb{K}}(Tr_{\mathbb{L}|\mathbb{M}}(\alpha))$.

Proposição 1.3.1 *Seja $\mathbb{K}$ um corpo de característica zero ou um corpo finito. Sejam $\mathbb{L}$ uma extensão algébrica de grau n de $\mathbb{K}$, α um elemento de $\mathbb{L}$ e $\alpha_1, \ldots, \alpha_n$ as raízes do polinômio minimal de α sobre $\mathbb{K}$. Então $Tr(\alpha) = \alpha_1 + \cdots + \alpha_n$, $N(\alpha) = \alpha_1 \ldots \alpha_n$ e $\chi(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$.*

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

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

unesp

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

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

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

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

Como α é primitivo temos que

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

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

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

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

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

unesp

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, $\chi(x) = (det(xI_n - M_1))$ e $(det(xI_q - M))$ é o polinômio minimal de α sobre $\mathbb{K}$, de acordo com a primeira parte da demonstração. ∎

Observação 1.3.1 *Segue pela Proposição (1.3.1), que* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = rTr_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}|\mathbb{K}}(\alpha) = (N_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha))^r$ *e* $\chi_{\mathbb{L}|\mathbb{K}}(\alpha) = (\chi_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha))^r$, *onde* $r = [\mathbb{L} : \mathbb{K}[\alpha]]$.

Exemplo 1.3.1 *Seja* $\mathbb{L} = \mathbb{Q}(\sqrt{-1})$. *Seja* $\alpha = 3 + \sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ *e* $\chi(x) = x^2 - 6x + 10$ *o polinômio minimal de* α *sobre* $\mathbb{Q}$. *Então* $Tr_{\mathbb{L}|\mathbb{Q}}(\alpha) = 6$ *e* $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = 10$.

Exemplo 1.3.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$, $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ *e* $\mathbb{F} = \mathbb{Q}$. *Sejam* $\alpha = 3 + \sqrt{-1}$ *e* $r = [\mathbb{L} : \mathbb{Q}(\sqrt{-1})] = 2$. *Pelo Exemplo (1.3.1), temos que* $N_{\mathbb{K}|\mathbb{F}}(\alpha) = 10$ *e* $Tr_{\mathbb{K}|\mathbb{F}}(\alpha) = 6$. *Assim, pela Observação (1.3.1), temos que* $N_{\mathbb{L}|\mathbb{F}}(\alpha) = (N_{\mathbb{K}|\mathbb{F}}(\alpha))^2 = 10^2 = 100$ *e* $Tr_{\mathbb{L}|\mathbb{F}}(\alpha) = 2(Tr_{\mathbb{K}|\mathbb{F}}(\alpha)) = 2 \cdot 6 = 12$.

Proposição 1.3.2 *Se* A *é um domínio,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão finita e* $\alpha \in \mathbb{L}$ *um elemento inteiro sobre* A, *então os coeficientes do polinômio característico de* α *são inteiros sobre* A. *Em particular,* $Tr(\alpha)$ *e* $N(\alpha)$ *são inteiros sobre* A.

Demonstração: Pela Proposição (1.3.1), temos que $\chi(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Como os coeficientes de $\chi(x)$ são somas e produtos dos α_i, é suficiente mostrar que os α_i são inteiros sobre A. Pela Teoria de Galois, existe um $\mathbb{K}$-homomorfismo $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$, definido por $\sigma_i(\alpha) = \alpha_i$, para $i = 1, \ldots, n$. Como α é inteiro sobre A, segue que

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

com $a_i \in A$, não todos nulos. Aplicando σ_i, obtemos

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

ou seja, α_i é inteiro sobre A. ∎

Corolário 1.3.1 *Se* A *é um anel integralmente fechado, então os coeficientes do polinômio característico de* α, $Tr(\alpha)$ *e* $N(\alpha)$ *são elementos de* A.

Demonstração: Seja $\chi(x)$ o polinômio característico de α. Os coeficientes do polinômio são elementos de $\mathbb{K}$ e são inteiros sobre A. Como A é integralmente fechado, segue que os coeficientes estão em A. Portanto, $Tr(\alpha)$ e $N(\alpha)$ são elementos de A. ∎

unesp

Proposição 1.3.3 *Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$, onde $\det(Tr(\alpha_i\alpha_j)) \neq 0$ e $\alpha \in \mathbb{L}$. Se $Tr(\alpha\beta) = 0$ para todo $\beta \in \mathbb{L}$, implica $\alpha = 0$.*

Demonstração: Como $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, onde $a_i \in \mathbb{K}$, para $i = 1, \ldots, n$, é suficiente mostrar que $Tr(\alpha\alpha_j) = 0$, para $j = 1, \ldots, n$, então $\alpha = 0$. Assim, para $j = 1, \ldots, n$, temos que

$$0 = Tr(\alpha\alpha_j) = a_1Tr(\alpha_1\alpha_j) + a_2Tr(\alpha_2\alpha_j) + \cdots + a_nTr(\alpha_n\alpha_j).$$

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, $\alpha = 0$. ∎

Corolário 1.3.2 *Com as mesmas hipóteses da Proposição (1.3.3), segue que a aplicação $\rho : \mathbb{L} \longrightarrow Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$ definida por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = Tr(\alpha\beta)$, é um isomorfismo.*

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

$$\begin{aligned} \rho(\alpha_1 + \alpha_2)(\beta) &= S_{\alpha_1+\alpha_2}(\beta) = Tr((\alpha_1 + \alpha_2)\beta) \\ &= Tr(\alpha_1\beta) + Tr(\alpha_2\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = \rho(\alpha_1)(\beta) + \rho(\alpha_2)(\beta) \\ \rho(a\alpha)(\beta) &= S_{a\alpha}(\beta) = Tr(a\alpha\beta) = aTr(\alpha\beta) = aS_\alpha(\beta) = a\rho(\alpha)(\beta), \end{aligned}$$

para todo $\beta \in \mathbb{L}$.

Agora, seja $\alpha \in \mathbb{L}$ tal que $\rho(\alpha) = 0$. Então, $\rho(\alpha)(\beta)=S_\alpha(\beta) = Tr(\alpha\beta) = 0$, $\forall\beta \in \mathbb{L}$. Pela Proposição (1.3.3) temos que $\alpha = 0$, provando assim que ρ é injetora. Finalmente, ρ é sobrejetora, pois $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K}))$. Portanto, ρ é um isomorfismo. ∎

Teorema 1.3.1 *Se A é um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como toda extensão finita é algébrica, segue que todos os α_i são algébricos sobre $\mathbb{K}$, ou seja, existem $a_i \in A$, para $i = 0, 1, \ldots, n$, não todos nulos, tais que

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

Supondo que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1}, temos que $a_n\alpha_i$ é inteiro sobre A, uma vez que

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

Seja, $a_n\alpha_i = z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \ldots, n$. Vamos mostrar que $\{z_1, \ldots, z_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Suponhamos que $b_1z_1 + b_2z_2 + \cdots + b_nz_n = 0$, onde $b_i \in A$, para $i = 1, \ldots, n$. Assim,

$$b_1a_n\alpha_1 + b_2a_n\alpha_2 + \cdots + b_na_n\alpha_n = 0.$$

Como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ segue que $b_ia_n = 0$ e, portanto, $b_i = 0$ para $i = 1, \ldots, n$. Portanto, $\{z_1, \ldots, z_n\}$ é linearmente independente e como possui n elementos segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário (1.3.2) existe uma base dual $\{y_1, \ldots, y_n\}$ tal que

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

Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$ então $\alpha z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \ldots, n$. Pelo Corolário (1.3.1) segue que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha z_i) \in A$, para $i = 1, \ldots, n$. Como $\alpha = c_1y_1 + \cdots + c_ny_n$, com $c_i \in \mathbb{K}$, para $i = 1, \ldots, n$, segue $Tr(\alpha z_i) = c_i \in A$, para $i = 1, \ldots, n$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A-módulo livre gerado por $\{z_1, \ldots, z_n\}$. ∎

Corolário 1.3.3 *Com as mesmas hipóteses do Teorema (1.3.1), se A é um domínio principal, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Demonstração: Pelo Teorema (1.1.1) temos que um submódulo de um A-módulo livre é livre de posto menor ou igual a n. Pelo Teorema (1.3.1), segue que $\mathcal{O}_{\mathbb{L}}$ contém uma base de n elementos de $\mathbb{L}$ sobre $\mathbb{K}$. Logo, $\mathcal{O}_{\mathbb{L}}$ tem posto n. ∎

Corolário 1.3.4 *Com as mesmas hipóteses do Teorema (1.3.1), se A é um domínio principal e se $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal, então $\mathcal{A}$ é um A-módulo livre de posto n.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Sejam $\{e_1, \ldots, e_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ e $\alpha \in \mathcal{A}$, $\alpha \neq 0$. Assim, $\alpha e_1, \ldots, \alpha e_n \in \mathcal{A}$ e são linearmente independentes sobre A, uma vez que se $\alpha_1 \alpha e_1 + \cdots + \alpha_n \alpha e_n = 0$, com $\alpha_i \in A$, para $i = 1, \ldots, n$, então $\alpha_i \alpha = 0$ para $i = 1, \ldots, n$. Como A é um domínio segue que $\alpha_i = 0$, para $i = 1, \ldots, n$. ∎

Proposição 1.3.4 *Seja A um anel noetheriano e integralmente fechado. Sejam $\mathbb{K}$ o corpo de frações de A, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o fecho inteiro de A em $\mathbb{L}$. Então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado e $\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano.*

Demonstração: Pelo Teorema (1.3.1), $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A-módulo livre de posto n. Pelo Corolário (1.1.2), temos que $\mathcal{O}_B$ é um A-módulo noetheriano e, portanto, finitamente gerado. Como os ideais de $\mathcal{O}_{\mathbb{L}}$ são A- submódulos de $\mathcal{O}_{\mathbb{L}}$, segue que satisfazem a condição de maximilidade da Definição (1.1.5). Portanto, $\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano. ∎

1.4 Discriminante

Nesta seção apresentamos o conceito de discriminante, enfocando suas principais propriedades.

Definição 1.4.1 *Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Dado $(\alpha_1, \ldots, \alpha_n) \in B^n$, definimos seu* **discriminante** *por*

$$D_{B/A}(\alpha_1, \ldots, \alpha_n) = det(Tr(\alpha_i \alpha_j)).$$

Quando não houver dúvidas denotaremos o discriminante de $(\alpha_1, \ldots, \alpha_n)$ simplesmente por $D(\alpha_1, \ldots, \alpha_n)$.

Exemplo 1.4.1 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ é um corpo de números e $\{1, \sqrt{7}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então*

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

Proposição 1.4.1 *Sejam $A \subset B$, anéis, tal que B é um A-módulo livre de posto n e $(\alpha_1, \ldots, \alpha_n) \in B^n$. Se $(\beta_1, \ldots, \beta_n) \in B^n$ é um conjunto de elementos de B tais que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in A$, então*

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

unesp

Demonstração: Sejam $\beta_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^{n} a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in A$. Assim, $\beta_p\beta_q = \sum_{i=1}^{n} a_{pi}\alpha_i \sum_{j=1}^{n} a_{qj}\alpha_j = \sum_{i,j=1}^{n} a_{pi}a_{qj}\alpha_i\alpha_j$, e $Tr(\beta_p\beta_q) = Tr(\sum_{i,j}^{n} a_{pi}a_{qj}\alpha_i\alpha_j) = \sum_{i,j}^{n} a_{pi}a_{qj}Tr(\alpha_i\alpha_j)$. Na forma matricial, temos que $(Tr(\beta_p\beta_q)) = (a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t$. Pela Definição (1.4.1) temos que $D(\beta_1, \ldots, \beta_n) = det(Tr(\beta_p\beta_q))$. Logo, $D(\beta_1, \ldots, \beta_n) = det((a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t) = det(a_{pi})det(Tr(\alpha_i\alpha_j))det(a_{qj})^t = det(a_{ij})^2 D(\alpha_1, \ldots, \alpha_n)$. ∎

Observação 1.4.1 *A Proposição (1.4.1) afirma que o discriminante de quaisquer duas bases de B sobre A são associados, isto é, a matriz (a_{ij}) que expressa uma base em termos da outra, admite matriz inversa com entradas em A. Portanto, ambos $det(a_{ij})$ e $det(a_{ij})^{-1}$ são inversíveis em A.*

Definição 1.4.2 *Sejam B um anel e A um subanel de B, tal que B é um A-módulo livre de posto finito n. O discriminante de B sobre A é um ideal em A, definido por,*

$$\mathcal{D}_{B/A} = \langle D_{B/A}(\alpha_1, \ldots, \alpha_n)\rangle,$$

onde $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de B sobre A.

Proposição 1.4.2 *Sejam B um anel e $A \subseteq B$ um subanel tal que B é um A-módulo livre de posto finito n. Se $\mathcal{D}_{B/A}$ contém um elemento que não é um divisor de zero, então, para que $(\alpha_1, \ldots, \alpha_n) \in B^n$ seja uma base de B sobre A, é necessário e suficiente que, $D(\alpha_1, \ldots, \alpha_n)$ gere $\mathcal{D}_{B/A}$.*

Demonstração: Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de B sobre A, então pela Proposição (1.4.1), segue que $D(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}_{A/B}$. Reciprocamente, suponhamos que $d = D(\alpha_1, \ldots, \alpha_n)$ gera $\mathcal{D}_{A/B}$. Sejam $\{e_1, \ldots, e_n\}$ uma base de $\mathcal{D}_{A/B}$, $d' = D(e_1, \ldots, e_n)$ e $\alpha_i = \sum_{j=1}^{n} a_{ij}e_j$ com $a_{ij} \in A$, $1 \leq i \leq n$. Pela Proposição (1.4.1), segue que $d = det(a_{ij})^2 d'$. Por hipótese, $Ad = \mathcal{D}_{B/A} = Ad'$. Logo, existe um elemento $b \in A$ tal que $d' = bd$. Assim, $d = det(a_i j)^2 bd$ e, portanto, $d(1 - det(a_{ij})^2 b) = 0$. Temos que d não é um divisor de zero, pois se fosse todo elemento de $Ad = \mathcal{D}_{A/B}$ seria um divisor de zero, contrariando a hipótese. Logo, $1 - det(a_{ij})^2 b = 0$ e, portanto, $det(a_{ij})$ é inversível. Assim, a matriz $M = [a_{ij}]$ é inversível. Portanto, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de B sobre A. ∎

Lema 1.4.1 (Lema de Dedekind) *Se G é um grupo, $\mathbb{K}$ um corpo, e $\sigma_1, \ldots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então $\{\sigma_1, \ldots, \sigma_n\}$ é linearmente independente sobre $\mathbb{K}$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Suponhamos que os $\sigma_i's$ são linearmente dependentes. Seja $\sum_{i=1}^{m} a_i\sigma_i = 0$, *com* $a_i \in \mathbb{K}$ uma combinação linear com m mínimo e $a_i \neq 0$, para todo $i = 1, 2, \ldots, m$. Logo, para qualquer $x \in G$, temos que

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_m\sigma_m(x) = 0. \tag{1.1}$$

Como os homomorfismos são distintos, segue que existe $c \in G$ tal que $\sigma_1(c) \neq \sigma_m(c)$. Agora, como $cx \in G$, segue que

$$a_1\sigma_1(cx) + a_2\sigma_2(cx) + \cdots + a_m\sigma_m(cx) = 0 \tag{1.2}$$

e então

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_2(c)\sigma_2(x) + \cdots + a_m\sigma_m(c)\sigma_m(x) = 0. \tag{1.3}$$

Multiplicando (1.1) por $\sigma_1(c)$, obtemos

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_1(c)\sigma_2(x) + \cdots + a_m\sigma_1(c)\sigma_m(x) = 0. \tag{1.4}$$

Subtraindo (1.3) de (1.4) obtemos

$$a_2\sigma_2(x)(\sigma_2(c) - \sigma_1(c)) + \cdots + a_m\sigma_m(x)(\sigma_m(c) - \sigma_1(c)) = 0. \tag{1.5}$$

Como isso vale para todo $x \in G$ e m é mínimo, segue que $a_m(\sigma_m(c) - \sigma_1(c)) = 0$. Como $\sigma_m \neq 0$, segue que $\sigma_m(c) = \sigma_1(c)$ para todo $c \in G$, o que é um absurdo. ∎

Proposição 1.4.3 *Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\sigma_1, \ldots, \sigma_n$ *os* n $\mathbb{K}$*-isomorfismos distintos de* $\mathbb{L}$ *em um corpo algebricamente fechado* F *contendo* $\mathbb{K}$. *Se* $\{\alpha_1, \ldots, \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *então*

$$D(\alpha_1, \ldots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração: Temos que $D(\alpha_1, \ldots, \alpha_n) = det(Tr(\alpha_i\alpha_j))$. Como o traço de $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que $D(\alpha_1, \ldots, \alpha_n) = det(Tr(\alpha_i\alpha_j)) = det(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = det(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)) = det(\sigma_k(\alpha_i))det(\sigma_k(\alpha_j)) = (det(\sigma_i(\alpha_j))^2$, uma vez que

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Se $det(\sigma_k(\alpha_j)) = 0$, então existem $a_1, \ldots, a_n \in F$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$ para todo j. Se $\alpha \in \mathbb{L}$, então $\alpha = \sum_{i=1}^{n} b_i\alpha_i$, com $b_i \in \mathbb{K}$, e por linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$. Mas isto contradiz o Lema de Dedekind e portanto $det(\sigma_k(\alpha_j)) \neq 0$. ■

Corolário 1.4.1 *Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $\mathbb{K}$-isomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado F contendo $\mathbb{K}$. Então a forma bilinear $\psi : \mathbb{L} \times \mathbb{L} \longrightarrow \mathbb{R}$ definida por $\psi(\alpha, \beta) = Tr(\alpha\beta)$ é não degenerada, isto é, se $Tr(\alpha\beta) = 0$ para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.*

Demonstração: Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. É suficiente mostrar que se $Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \ldots, n$, então $\alpha = 0$. Temos que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, com $a_i \in \mathbb{K}$, $i = 1, \ldots, n$. Assim, se $a_1Tr(\alpha_1\alpha_j) + a_2Tr(\alpha_2\alpha_j) + \cdots + \alpha_nTr(\alpha_n\alpha_j) = Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \ldots, n$, então obtemos o seguinte sistema linear homogêneo

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

Da Proposição (1.4.3), temos que $det(Tr(\alpha_i\alpha_j) \neq 0$ e, portanto, o sistema possui solução única dada por $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ■

Definição 1.4.3 *Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$, $A = \mathbb{Z}$ e $\mathcal{O}_\mathbb{K}$ o anel de inteiros algébricos de $\mathbb{K}$. Temos que $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de* **base integral**, *e seu discriminante é chamado de* **discriminante absoluto**.

Observação 1.4.2 *Temos que base integral de $\mathcal{O}_\mathbb{K}$ é uma $\mathbb{Q}$-base de $\mathbb{K}$ mas nem toda $\mathbb{Q}$-base de $\mathbb{K}$ consistindo de inteiros algébricos é uma base integral de $\mathcal{O}_\mathbb{K}$.*

Exemplo 1.4.2 *Temos que $\{1, \sqrt{5}\}$ é uma $\mathbb{Q}$-base de $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, mas não é uma base integral de $\mathcal{O}_\mathbb{K}$, pois o elemento $\frac{1+\sqrt{5}}{2}$ é raiz de $x^2 - x - 1$ e portanto inteiro algébrico, mas não é combinação linear, com coeficientes em $\mathbb{Z}$, de 1 e $\sqrt{5}$.*

Proposição 1.4.4 *Se $\mathbb{K}$ é um corpo, $\mathbb{L} = \mathbb{K}[\alpha]$ uma extensão finita de $\mathbb{K}$ de grau n e $f(x)$ o polinômio minimal de α sobre $\mathbb{K}$, então,*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha)),$$

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

Demonstração: Se $\alpha_1, \ldots, \alpha_n$ são as raízes de $f(x)$ em alguma extensão de $\mathbb{K}$, então são conjugados de α. Pela Proposição (1.4.3) temos que $D(1, \alpha, \ldots, \alpha^{n-1}) = (det(\sigma_i(\alpha^j)))^2 = det(\alpha_i^j)^2$, com $i = 1, \ldots, n$ e $j = 0, \ldots, n-1$. Como $det(\alpha_i^j)$ é um determinante de Vandermonde segue que

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

■

Exemplo 1.4.3 *Se* $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{3})$ *e* $f(x) = x^2 - 3$ *o polinômio minimal de* $\sqrt{3}$ *sobre* $\mathbb{Q}$, *então* $D(1, \sqrt{3}) = (-1)^{\frac{2\cdot 1}{2}} N(f'(\sqrt{3})) = -N(2\sqrt{3}) = -2^2 N(\sqrt{3}) = -4(\sqrt{3})(-\sqrt{3}) = 12$.

Lema 1.4.2 *Sejam* A *um anel e* $B_1, \ldots, B_g$ *anéis contendo* A, *tais que sejam* A*-módulos livres finitamente gerados. Seja* $B = \prod_{i=1}^{g} B_i$, *como um produto de anéis, então,*

$$D_{B/A} = \prod_{i=1}^{q} D_{B_i/A}.$$

Demonstração: Faremos a prova por indução sobre g. Para o caso $g = 2$, considere $\{x_1, \ldots, x_n\}$ uma base de B_1 sobre A e $\{y_1, \ldots, y_m\}$ uma base de B_2 sobre A. Com a identificação natural de B_1 em $B_1 \times \{0\}$ e B_2 em $\{0\} \times B_2$, podemos considerar $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$ uma base de $B = B_1 \times B_2$. Como $x_i = (x_i, 0)$ e $y_i = (0, y_i)$ segue que $x_i y_i = 0$ e assim $Tr(x_i y_i) = 0$. Logo,

$$D(x_1, \ldots, x_n, y_1, \ldots, y_m) = \det \begin{pmatrix} Tr(x_i x_j) & 0 \\ 0 & Tr(y_i y_j) \end{pmatrix}$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$= \det(Tr(x_i x_j)) \det(Tr(y_i y_j)) = D(x_1, \ldots, x_n) D(y_1, \ldots, y_m).$$

Portanto, $D_{B/A} = D_{B_1/A} D_{B_2/A} = \prod_{i=1}^{2} D_{B_i/A}$. Agora, suponhamos verdadeiro para $g-1$, ou seja, se $C = \prod_{i=1}^{g-1} B_i$, então $D_{C/A} = \prod_{i=1}^{g-1} D_{B_i/A}$. Logo, $B = C \times B_g$, identificando C com $C \times \{0\}$ e B_g com $\{0\} \times B_g$. Usando o caso $g = 2$, temos por hipótese de indução que $D_{B/A} = D_{C/A} D_{B_g/A} = \prod_{i=1}^{g-1} D_{B_i/A} D_{B_g/A} = \prod_{i=1}^{g} D_{B_i/A}$. ∎

Observação 1.4.3 *Com as mesmas hipóteses do Lema (1.4.2), prova-se analogamente que se* $\alpha \in B$ *então* $\chi_{B|A}(\alpha) = \prod_{i=1}^{g} \chi_{B_i/A}(\alpha)$, $N_{B|A}(\alpha) = \prod_{i=1}^{g} N_{B_i|A}(\alpha)$ *e* $Tr_{B|A}(\alpha) = \prod_{i=1}^{g} Tr_{B_i|A}(\alpha)$.

Lema 1.4.3 *Sejam* $\mathbb{K}$ *um corpo e* $\mathbb{L}$ *uma* $\mathbb{K}$*-álgebra comutativa de dimensão finita. Então* $\mathbb{L}$ *é reduzido se, e somente se,* $D_{\mathbb{L}/\mathbb{K}} \neq \{0\}$.

Demonstração: Se $\mathbb{L}$ é reduzido pelo Corolário (1.1.4), segue que $\langle 0 \rangle = \bigcap_{i=1}^{g} \mathfrak{q}_i$, onde os $\mathfrak{q}_i$ são ideais primos distintos de $\mathbb{L}$. Assim, $\mathbb{L}/\mathfrak{q}_i$ é um domínio e uma $\mathbb{K}$-álgebra de dimensão finita. Logo, $\mathbb{L}/\mathfrak{q}_i$ é uma extensão algébrica sobre $\mathbb{K}$, ou seja, $\mathbb{L}/\mathfrak{q}_i$ é inteiro sobre $\mathbb{K}$. Como $\mathbb{K}$ é corpo, temos pela Proposição (1.2.3), que $\mathbb{L}/\mathfrak{q}_i$ é corpo. Portanto os ideais $\mathfrak{q}_i$ são maximais e consequentemente $\mathfrak{q}_i + \mathfrak{q}_j = \mathbb{L}$, para $i \neq j$. Pelo Lema (1.1.2), segue que

$$\prod_{i=1}^{g} \mathbb{L}/\mathfrak{q}_i = \mathbb{L}/\prod_{i=1}^{g} \mathfrak{q}_i = \mathbb{L}/\langle 0 \rangle = \mathbb{L}$$

e, pelo Lema (1.4.2), temos que $D_{\mathbb{L}/\mathbb{K}} = \prod_{i=1}^{g} D_{(\mathbb{L}/\mathfrak{q}_i)/\mathbb{K}}$. Pela Proposição (1.4.3), temos que $D_{(\mathbb{L}/\mathfrak{q}_i)/\mathbb{K}} \neq \langle 0 \rangle$ o que implica que $D_{\mathbb{L}/\mathbb{K}} \neq \langle 0 \rangle$. Reciprocamente, suponhamos que $\mathbb{L}$ não é reduzido. Assim, existe $x \in \mathbb{L}$, $x \neq 0$, x nilpotente. Seja $\{x_1, \ldots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $x = x_1$. Então xx_j é nilpotente, para todo $j = 1, \ldots, n$. Logo, se definirmos $\theta_{xx_j} : \mathbb{L} \longrightarrow \mathbb{L}$, onde $\theta_{xx_j}(a) = axx_j$, para $a \in \mathbb{L}$, temos que θ_{xx_j} possui os autovalores todos nulos, e portanto $Tr_{\mathbb{L}|\mathbb{K}}(xx_j) = 0$. Logo, a matriz traço $(Tr_{\mathbb{L}|\mathbb{K}}(xx_j))$ tem uma linha nula o que implica que $D(x_1, \ldots, x_n) = 0$ e assim $D_{\mathbb{L}/\mathbb{K}} = \{0\}$, o que é um absurdo. ∎

1.5 Anéis de Dedekind

Nesta seção apresentamos os anéis de Dedekind juntamente com suas principais propriedades.

Em geral, em um anel, a fatoração de seus elementos não é única, pois se considerarmos $\mathbb{Z}[\sqrt{-5}]$, temos que $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, mas nesta seção veremos que a fatoração é única para ideais de um anel de Dedekind.

Definição 1.5.1 *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.

Proposição 1.5.1 *Se $A \subseteq B$ são anéis e $\mathfrak{p} \subset B$ é um ideal primo, então $\mathfrak{p} \cap A$ é um ideal primo de A.*

Demonstração: Considere a aplicação $\varphi : A \xrightarrow{i} B \xrightarrow{\pi} B/\mathfrak{p}$, 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 e $\ker(\varphi) = A \cap \mathfrak{p}$, pois $\varphi(x) = \pi \circ i(x) = \pi(x) = x + \mathfrak{p}$ e $\varphi(x) = \bar{0}$ se, e somente se, $x \in \mathfrak{p} \cap A$. Portanto, $A/\mathfrak{p} \cap A \simeq Im(\varphi) \subset B/\mathfrak{p}$. Como $B/\mathfrak{p}$ é um domínio, segue que $A/\mathfrak{p} \cap A$ é um domínio. Portanto, $\mathfrak{p} \cap A$ é um ideal primo de A. ∎

Teorema 1.5.1 *Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$. Então $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind.*

Demonstração: Pelas Proposições (1.2.4) e (1.3.4), temos que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado e noetheriano, respectivamente. Assim, falta mostrar que todo ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ é maximal. Seja $\mathfrak{p} \subset \mathcal{O}_B$ um ideal primo não nulo. Como $A \subset \mathcal{O}_{\mathbb{L}}$ segue pela Proposição (1.5.1) 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 $\mathfrak{p} \subset \mathcal{O}_{\mathbb{L}}$ segue que $\alpha \in \mathcal{O}_{\mathbb{L}}$. Assim, existem $a_i \in A$, para $i = 0, \ldots, n-1$, não todos nulos, tais 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,

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

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 $\varphi : A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$,

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

onde i é a inclusão e π é a projeção. Assim,

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

Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre A, segue que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ é inteiro sobre $\dfrac{A}{\mathfrak{p}\cap A}$. Pela Proposição (1.2.3), temos que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ é um corpo. Portanto, $\mathfrak{p}$ é maximal. ■

Definição 1.5.2 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Um* **ideal fracionário** *de A (ou de $\mathbb{K}$ em relação a A) é um A-módulo $\mathcal{I} \subseteq \mathbb{K}$ tal que existe $d \in A-\{0\}$ onde $d\mathcal{I} \subseteq A$. Em particular, os ideais inteiros de A são ideais fracionários, basta considerar d=1.*

Proposição 1.5.2 *Se A é um domínio noetheriano, então todo ideal fracionário $\mathcal{I}$ de A é um A-módulo finitamente gerado.*

Demonstração: Como $\mathcal{I}$ é um ideal fracionário de A, segue que existe $d \in A - \{0\}$ tal que $d\mathcal{I} \subseteq A$. Assim, $\mathcal{I} \subseteq d^{-1}A$. A aplicação $\varphi : A \longrightarrow d^{-1}A$, tal que $\varphi(x) = d^{-1}x$, $x \in A$ é um isomorfismo. Assim, A é isomorfo a $d^{-1}A$. Como A noetheriano, temos que $d^{-1}A$ é noetheriano. Logo, $\mathcal{I}$ é um A-módulo finitamente gerado. ■

Lema 1.5.1 *Sejam A um anel e $\mathfrak{p}$ um ideal primo de A. Se $\mathfrak{p}$ contém um produto de ideais $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ de A, então $\mathfrak{p}$ contém pelo menos um dos $\mathfrak{a}_i$.*

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

Lema 1.5.2 *Sejam A é um anel de Dedekind que não é corpo, $\mathbb{K}$ o seu corpo de frações e $\mathcal{M}$ um ideal maximal de A, então o conjunto $\mathcal{N} = \{x \in \mathbb{K} : x\mathcal{M} \subset A\}$ é um ideal fracionário de A.*

Demonstração: Seja $\mathcal{M}$ um ideal maximal de A. Como A não é um corpo, segue que $\mathcal{M} \neq \{0\}$. Consideremos $\mathcal{N} = \{x \in \mathbb{K} : x\mathcal{M} \subset A\}$. Temos que $\mathcal{N}$ é um ideal fracionário, pois $\mathcal{N}$ é um A-módulo tal que $\mathcal{N} \subseteq \mathbb{K}$ e se $c \in \mathcal{M}$, $c \neq 0$, temos que $c\mathcal{N} \subseteq A$. Portanto, $\mathcal{N}$ é um ideal fracionário de A. ■

Proposição 1.5.3 *Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ o seu corpo de frações. Então, todo ideal maximal $\mathcal{M}$ de A é inversível.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Considere o ideal fracionário $\mathcal{N} = \{x \in \mathbb{K} : x\mathcal{M} \subset A\}$. Vamos mostrar que $\mathcal{N}\mathcal{M} = A$. Pela definição de $\mathcal{N}$ temos $\mathcal{N}\mathcal{M} \subset A$. Por outro lado, $A \subset \mathcal{N}$, pois $\mathcal{M}$ é um ideal de A. Assim, $\mathcal{M} = \mathcal{M}A \subset \mathcal{M}\mathcal{N} \subset A$. Como $\mathcal{M}$ é maximal, segue que $\mathcal{M} = \mathcal{N}\mathcal{M}$ ou $\mathcal{N}\mathcal{M} = A$. Suponhamos que $\mathcal{M} = \mathcal{N}\mathcal{M}$ e consideremos $\alpha \in \mathcal{N}$. Então $\alpha\mathcal{M} \subset \mathcal{M}$, $\alpha^2\mathcal{M} \subset \alpha\mathcal{M} \subset \mathcal{M}$ e $\alpha^n\mathcal{M} \subset \mathcal{M}$, para todo $n \in \mathbb{N}$. Seja $d \in \mathcal{M}$, $d \neq 0$. Então, $d\alpha^n \in A$. Portanto, $A[\alpha]$ é um ideal fracionário. Como A é noetheriano, pela Proposição (1.5.2), segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema (1.2.1), segue que α é inteiro sobre A. Sendo A integralmente fechado, segue que $\alpha \in$ A. Assim, $\mathcal{N} \subset A$ e como $A \subset \mathcal{N}$ segue que $\mathcal{N} = A$. Falta mostrar que esta igualdade é impossível. Seja $a \in \mathcal{M}$. Pela Proposição (1.1.3), temos que $\langle a \rangle = aA \supset \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$, onde os $\mathfrak{p}_i s$ são ideais primos não nulos de A, com n o menor valor possível. Assim, $\mathcal{M} \supset aA \supset \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$. Pelo Lema (1.5.1), $\mathcal{M}$ contém um dos $\mathfrak{p}_i$, para algum $i = 1, \ldots, n$. Sem perda de generalidade, digamos que seja $\mathfrak{p}_1$, isto é, $\mathcal{M} \supset \mathfrak{p}_1$. Como A é Dedekind, segue que $\mathcal{M} = \mathfrak{p}_1$, pois $\mathfrak{p}_1$ é maximal. Agora, considere $\mathfrak{p} = \mathfrak{q}_2 \ldots \mathfrak{q}_n$. Então, $aA \supset \mathcal{M}\mathfrak{q}$ e $aA \not\supset \mathfrak{q}$, pela minimalidade de n. Assim, existe $b \in \mathfrak{q}$ e $b \notin \langle a \rangle$ tal que $\mathcal{M}b \subset \langle a \rangle$. Logo, $\frac{b}{a}\mathcal{M} \subseteq A$ e assim $\frac{b}{a} \in \mathcal{N}$. Como $b \notin \langle a \rangle$ segue que $\frac{b}{a} \notin A$. Assim, $\mathfrak{n} \neq A$. Portanto, $\mathcal{M}\mathcal{N} = A$. ∎

Teorema 1.5.2 *Se A é um anel de Dedekind, que não é um corpo e F é o conjunto dos ideais primos de A, então todo ideal fracionário $\mathfrak{b}$ não nulo de A é um produto de ideais primos de A, de modo único, isto é, $\mathfrak{b} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$, onde $e_1, \ldots, e_n$ são inteiros positivos.*

Demonstração: Se $\mathfrak{b}$ é um ideal fracionário de A, então existe $d \in A - \{0\}$ tal que $d\mathfrak{b} \subseteq A$. Como $\mathfrak{b} = (d\mathfrak{b})(d^{-1}A)$ segue que 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. Suponhamos que $F \neq \emptyset$. Como A é noetheriano, segue que F tem um elemento maximal M. Temos que $M \neq A$, pois A é o produto da coleção vazia de ideais primos. Assim, $M \subseteq \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal maximal de A. Pelo Lema (1.5.3), temos que $\mathfrak{q} = \{x \in \mathbb{K} : x\mathfrak{p} \subset A\}$ é tal que $\mathfrak{p}\mathfrak{q} = A$. Como $M \subseteq \mathfrak{p}$ segue que $M\mathfrak{q} \subseteq \mathfrak{p}\mathfrak{q} = A$. Além disso, como $A \subset \mathfrak{q}$, segue que $M = MA \subset M\mathfrak{q} \subset A$. Temos que $M \subsetneq M\mathfrak{q}$, pois se $M = M\mathfrak{q}$ e se $\alpha \in \mathfrak{q}$, então $\alpha M \subset M$, $\alpha^2 M \subset \alpha M \subset M$ e $\alpha^n M \subset M$, para todo $n \in \mathbb{N}$. Assim, se $d \in M - \{0\}$, então $d\alpha^n \in M \subseteq A$. Portanto, $A[\alpha]$ é um ideal fracionário de A. Como A é noetheriano, pela Proposição (1.5.2), segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema (1.2.1), 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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

é um absurdo, pois $\mathfrak{p}$ é um ideal primo. Pela maximilidade de M e como $M \subseteq M\mathfrak{q}$ temos que $M\mathfrak{q} \notin F$, ou seja, $M\mathfrak{q} = \mathfrak{p}_1 \dots \mathfrak{p}_n$, onde $\mathfrak{p}_i$, $para \;\; i = 1, \dots, n$, são ideais primos de A. Multiplicando por $\mathfrak{p}$ em ambos os lados, temos que $M = \mathfrak{p}_1 \dots \mathfrak{p}_n\mathfrak{p}$, o que é um absurdo, pois $M \in F$. Portanto, $F = \emptyset$.

■

Definição 1.5.3 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Sejam $\mathfrak{b}$ e $\mathfrak{c}$ ideais fracionários de A. Dizemos que $\mathfrak{b}$* **divide** *$\mathfrak{c}$ se existe um ideal inteiro $\mathfrak{m}$ de A tal que $\mathfrak{c} = \mathfrak{b}\mathfrak{m}$.*

Lema 1.5.3 *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e $\mathfrak{b}$ e $\mathfrak{c}$ ideais fracionários de A. Então $\mathfrak{b}$ divide $\mathfrak{c}$ se, e somente se, $\mathfrak{c} \subseteq \mathfrak{b}$*

Demonstração: Se $\mathfrak{b}$ divide $\mathfrak{c}$ então existe um ideal $\mathfrak{m} \subseteq A$ tal que $\mathfrak{c} = \mathfrak{b}\mathfrak{m} \subseteq \mathfrak{b}$. Por outro lado, se $\mathfrak{c} \subseteq \mathfrak{b}$ então $\mathfrak{c}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = A$. Mas isto implica que $\mathfrak{c}\mathfrak{b}^{-1}$ é um ideal inteiro tal que $(\mathfrak{c}\mathfrak{b}^{-1})\mathfrak{b} = \mathfrak{c}$. Portanto, $\mathfrak{b}$ divide $\mathfrak{c}$. ■

Corolário 1.5.1 *O conjunto dos ideais fracionários de A formam um grupo.*

Demonstração: Pelo Lema (1.5.3), temos que todo ideal $\mathfrak{m}$ de A é inversível. Além disso, A é o elemento neutro e a multiplicação de ideais é associativa. ■

Definição 1.5.4 *Sejam A um anel de Dedekind e $\mathbb{K}$ seu corpo de frações. O grupo quociente $C(A) = \dfrac{I(A)}{F(A)}$ é chamado* **grupo das classes de ideais de** *A, onde $I(A)$ é o grupo dos ideais fracionários não nulos de A, e $F(A)$ é o subgrupo dos ideais fracionários principais de A.*

Notação: $h = \#C(A)$.

Observação 1.5.1 *Se A é um domínio de Dedekind, então, A é principal se, e somente se, $h = 1$.*

1.6 Norma de um ideal

Nesta seção definimos a norma de um ideal do anel de inteiros de um corpo de números e veremos algumas propriedades, dentre elas que a norma é multiplicativa. Para isso, consideraremos $\mathbb{K}$ um corpo de números de grau finito n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$.

Definição 1.6.1 *Seja $\mathfrak{a}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. A* **norma** *de $\mathfrak{a}$ é definida como $N(\mathfrak{a}) = \#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Observação 1.6.1 *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha \neq 0$ então pelo Corolário (1.3.1), segue que $N(\alpha) \in \mathbb{Z}$.*

Proposição 1.6.1 *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $|N(\alpha)| = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$, onde $\mathcal{O}_{\mathbb{K}}\alpha = \langle\alpha\rangle$.*

Demonstração: Pelo Corolário (1.3.3), temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\varphi : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ definido 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 (1.1.1) que existe uma base $\{e_1, \ldots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e $c_1, \ldots, c_n \in \mathbb{Z}$ tal que $\{c_1e_1, \ldots, c_ne_n\}$ é base de $\mathcal{O}_{\mathbb{K}}\alpha$. A aplicação $\psi : \mathcal{O}_{\mathbb{K}} \longrightarrow \frac{\mathbb{Z}}{c_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{c_n\mathbb{Z}}$ 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,

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

Assim, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = c_1c_2\ldots c_n$. 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, $\mu(e_1) = c_1e_1 + 0e_2 + \cdots + 0e_n, \ldots, \mu(e_n) = 0e_1 + \cdots + c_ne_n$ 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 bases de $\mathcal{O}_{\mathbb{K}}\alpha$, e portanto existe um automorfismo $v : \mathcal{O}_{\mathbb{K}}\alpha \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ tal que $v(c_ie_i) = \alpha e_i$, para $i = 1, \ldots, n$. Como a matriz mudança de base é inversível, segue que $\det(v)$ é inversível em $\mathbb{Z}$, isto é, $\det(v) = \pm 1$. Também, $(v \circ \mu)(e_i) = v(\mu(e_i)) = v(c_ie_i) = \alpha e_i$, para $i = 1, \ldots, n$. Assim, $(v \circ \mu)(a) = \alpha a$. Finalmente, $N(\alpha) = \det(v \circ \mu) = \det(v)\det(\mu) = \pm 1c_1c_2\ldots c_n = \pm\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$. Portanto, $|N(\alpha)| = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$. ∎

Proposição 1.6.2 *Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{a})$ é finita.*

Demonstração: Se $\alpha \in \mathfrak{a}$, é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathfrak{a}$ e $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}$ pode ser visto como um quociente de $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}$. Assim,

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

Pela Proposição (1.6.1), segue que $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$ é finito. Portanto, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)$ é finito. ∎

Proposição 1.6.3 *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Pelo Teorema (1.5.2), temos que $\mathfrak{b} = \prod_{i \in I} \mathfrak{p}_i^{\alpha_i}$, onde os $\mathfrak{p}_i's$ são ideais primos não nulos de $\mathcal{O}_{\mathbb{K}}$ e $\alpha_i \geq 0$, $i \in I$. Como $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind, segue que os ideais $\mathfrak{p}_i, i \in I$, são maximais. Seja $\mathfrak{p}_i = \mathfrak{m}$, para algum $i \in I$. Por indução sobre o número de fatores, é suficiente provar que

$$N(\mathfrak{am}) = N(\mathfrak{a})N(\mathfrak{m}). \tag{1.6}$$

Segue da definição de norma que a igualdade (1.6) se verifica se

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right).\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}\right). \tag{1.7}$$

Temos que o homomorfismo $\phi : \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}} \longrightarrow \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}$, definido por $\phi(x + \mathfrak{am}) = x + \mathfrak{a}$, é sobrejetor e $Ker(\phi) = \dfrac{\mathfrak{a}}{\mathfrak{am}}$. Assim, pelo Teorema do Isomorfismo temos que, $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}}/\dfrac{\mathfrak{a}}{\mathfrak{am}} \simeq \mathcal{O}_{\mathbb{K}}/\mathfrak{a}$. Logo,

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) \cdot \#\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right). \tag{1.8}$$

Das Equações (1.7) e (1.8), podemos concluir que (1.6) se verifica se $\#\left(\dfrac{\mathcal{O}}{\mathfrak{m}}\right) = \#\left(\dfrac{\mathfrak{a}}{\mathfrak{am}}\right)$.

Agora, temos que $\dfrac{\mathfrak{a}}{\mathfrak{am}}$ é um espaço vetorial sobre $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}$ mediante as operações

$$+ : \frac{\mathfrak{a}}{\mathfrak{am}} \times \frac{\mathfrak{a}}{\mathfrak{am}} \longrightarrow \frac{\mathfrak{a}}{\mathfrak{am}} \qquad \cdot : \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}} \times \frac{\mathfrak{a}}{\mathfrak{am}} \longrightarrow \frac{\mathfrak{a}}{\mathfrak{am}}$$
$$(x + \mathfrak{am}, y + \mathfrak{am}) \longmapsto (x + y) + \mathfrak{am} \qquad (x + \mathfrak{m}, y + \mathfrak{am}) \longmapsto (\alpha x) + \mathfrak{am}.$$

Temos que os $\mathcal{O}_{\mathbb{K}}$-submódulos de $\dfrac{\mathfrak{a}}{\mathfrak{am}}$ são ideais e são do tipo $\dfrac{\mathfrak{b}}{\mathfrak{am}}$, onde $\mathfrak{b}$ é um ideal tal que $\mathfrak{am} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Mas, como todo ideal num domínio de Dedekind admite inverso, segue que $\mathfrak{a}^{-1}\mathfrak{am} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a}$, ou seja, $\mathfrak{m} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_{\mathbb{K}}$. Como $\mathfrak{m}$ é maximal segue que $\mathfrak{m} = \mathfrak{a}^{-1}\mathfrak{b}$ ou $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_{\mathbb{K}}$. Assim, $\mathfrak{am} = \mathfrak{b}$ ou $\mathfrak{b} = \mathfrak{a}$. Portanto, não existe $\mathfrak{b}$ tal que $\mathfrak{am} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Assim, os $\mathcal{O}_{\mathbb{K}}$-submódulos de $\dfrac{\mathfrak{a}}{\mathfrak{am}}$, ou os subespaços do espaço vetorial $\dfrac{\mathfrak{a}}{\mathfrak{am}}$ são apenas os triviais. Portanto, $dim_{\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}} \dfrac{\mathfrak{a}}{\mathfrak{am}} = 1$ e então $\#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\dfrac{\mathfrak{a}}{\mathfrak{am}}\right)$. ■

Proposição 1.6.4 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão finita e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Então,*
i) $N(\mathfrak{a}) \in \mathfrak{a}$, onde $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{K}}$ é um ideal.
ii) Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{a}) = 1$ se, e somente se, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$.

Demonstração: i) Como $N(\mathfrak{a}) = \#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)$, segue que o grupo aditivo de $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}$ tem ordem $m = N(\mathfrak{a})$. Assim, $m\bar{1} = \bar{0}$, sendo $\bar{1}$ e $\bar{0}$, respectivamente, a unidade e o zero do anel $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$. Como, $\bar{m} = m\bar{1} = \bar{0}$ segue que $m + \mathfrak{a} = 0 + \mathfrak{a}$ e, portanto, $m \in \mathfrak{a}$. Logo, $N(\mathfrak{a}) \in \mathfrak{a}$. Para a prova de ii) temos que $N(\mathfrak{a}) = 1$ se, e somente se, $\#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) = 1$ se, e somente se, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$. ■

unesp

1.7 Anel de frações

Nesta seção veremos os conceitos dos anéis de frações enfocando suas principais propriedades, veremos também que o anel de frações de um anel de Dedekind também é um anel de Dedekind.

Definição 1.7.1 *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e S um subconjunto de $A-\{0\}$, que é fechado na multiplicação e $1 \in S$. Chamamos de* **anel de frações** *de A ao conjunto de todos os elementos de $\mathbb{K}$ que são escritos da forma $\frac{a}{s}$, com $a \in A$ e $s \in S$.*

Notação: $S^{-1}A$

Proposição 1.7.1 *Se $\mathbb{K}$ é um corpo de números e A é o anel de inteiros de $\mathbb{K}$, então:*
1) $S^{-1}A$ é um anel comutativo.
2) $A \subset S^{-1}A$.
3) Se $S = A - \{0\}$, então $S^{-1}A = \mathbb{K}$.
4) Se $S = \{1\}$ ou S é formado somente pelas unidades de A, então $S^{-1}A = A$.

Demonstração: 1) Se $x, y \in S^{-1}A$, então $x = \frac{a_1}{s_1}$ e $y = \frac{a_2}{s_2}$, com $a_1, a_2 \in A$ e $s_1 s_2 \in S$. Assim, $xy = \frac{a_1 a_2}{s_1 s_2} = \frac{a_2 a_1}{s_2 s_1} = yx$.
2) Se $x \in A$, então $x = \frac{x}{1}$, com $x \in A$ e $1 \in S$. Assim, $x = \frac{x}{1} \in S^{-1}A$.
3) Temos que $\mathbb{K} = \left\{\frac{a}{b}; a, b \in A \text{ e } b \neq 0\right\} = \left\{\frac{a}{b}; a \in A \text{ e } b \in A - \{0\}\right\} = S^{-1}A$.
4) Se $S = \{1\}$ temos que $S^{-1}A = \left\{\frac{a}{b}; a \in A \text{ e } b \in S = \{1\}\right\} = \left\{\frac{a}{1}; a \in A\right\} = A$. Agora, se S é formado somente pelas unidades de A então

$$S^{-1}A = \left\{\frac{a}{s}; a \in A \text{ e } s \in S\right\} = \left\{as^{-1}; a \in A \text{ e } s^{-1} \in S\right\} \subset A.$$

Portanto, $S^{-1}A = A$. ∎

Proposição 1.7.2 *Sejam A um domínio, S um subconjunto de $A - \{0\}$ fechado na multiplicação com $1 \in S$ e $A' = S^{-1}A$.*
i) Se $\mathfrak{b}' \subseteq A'$ é um ideal, então $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ e a função $\varphi(\mathfrak{b}') = \mathfrak{b}' \cap A$ é uma injeção crescente do conjunto dos ideais de A' no conjunto dos ideais de A, com relação a inclusão.
ii) A aplicação $\varphi(\mathfrak{p}') = \mathfrak{p}' \cap A$ é uma bijeção crescente do conjunto dos ideais primos de A' no conjunto dos ideais primos $\mathfrak{p}$ de A tal que $\mathfrak{p} \cap S = \emptyset$ e a aplicação inversa é dada por $\phi(\mathfrak{p}) = \mathfrak{p}A'$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: i) Primeiramente vamos mostrar que $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$. Como $\mathfrak{b}' \cap A \subseteq \mathfrak{b}'$ segue que $(\mathfrak{b}' \cap A)A' \subseteq \mathfrak{b}'A' = \mathfrak{b}'$. Por outro lado, se $x \in \mathfrak{b}' \subseteq A'$, então $x = \frac{a}{s}$, com $a \in A$ e $s \in S$. Como $\mathfrak{b}'$ é um ideal de A' e $A \subseteq A'$ segue que $sx \in \mathfrak{b}'$. Assim, $sx = a \in \mathfrak{b}' \cap A$ e, então $x = a\frac{1}{s} \in (\mathfrak{b}' \cap A)A'$, ou seja, $\mathfrak{b}' \subseteq (\mathfrak{b}' \cap A)A'$. Portanto, $\mathfrak{b}' = (\mathfrak{b}' \cap A)A'$. Também φ é uma injeção crescente, uma vez que se $\varphi(\mathfrak{b}'_1) = \varphi(\mathfrak{b}'_2)$ então $\mathfrak{b}'_1 \cap A = \mathfrak{b}'_2 \cap A$. Assim,

$$(\mathfrak{b}'_1 \cap A)A' = (\mathfrak{b}'_2 \cap A)A'$$

e isto implica que

$$\mathfrak{b}'_1 = \mathfrak{b}'_2.$$

Se $\mathfrak{b}'_1 \subseteq \mathfrak{b}'_2$ então $\mathfrak{b}'_1 \cap A \subseteq \mathfrak{b}'_2 \cap A$. Portanto, $\varphi(\mathfrak{b}'_1) \subseteq \varphi(\mathfrak{b}'_2)$. Para $ii)$ temos que φ está bem definida, pois por $i)$ φ é uma injeção crescente e pelo Lema (1.5.1) se $\mathfrak{p}' \subset A'$ é um ideal primo e como $A \subset A'$, segue que $\mathfrak{p}' \cap A$ é ideal primo de A. Falta mostrar que $\mathfrak{p} \cap S = \emptyset$. Suponhamos que exista $s \in \mathfrak{p} \cap S$. Então $s \in \mathfrak{p}$ e $s \in S$. Como $\mathfrak{p} \subseteq \mathfrak{p}'$ então $s \in \mathfrak{p}'$ e $\frac{1}{s} \in A'$ e portanto $1 = s\frac{1}{s} \in \mathfrak{p}'A' = \mathfrak{p}'$. Assim, $\mathfrak{p}' = A'$, o que é um absurdo, pois $\mathfrak{p}'$ é ideal primo de A'. Portanto, $\mathfrak{p} \cap S = \emptyset$ e φ está bem definida. Agora, vamos mostrar que $\phi(\mathfrak{p}) = \mathfrak{p}A'$ está bem definida. Seja $\mathfrak{p} \subset A$ um ideal primo tal que $\mathfrak{p} \cap S = \emptyset$. Assim, $\phi(\mathfrak{p}) = \mathfrak{p}A' \subset A'$. Temos que $\mathfrak{p}A' = \left\{\frac{p}{s} : p \in \mathfrak{p} \ e \ s \in S\right\}$, uma vez que se $x \in A'$, então

$$x = \sum_{i=1}^{n} p_i \frac{a_i}{s_i}, \quad com \ p_i \in \mathfrak{p}, a_i \in \mathfrak{p}A' \text{ e } s_i \in S.$$

Assim,

$$x = \frac{b_1 p_1 + \cdots + b_n p_n}{s}.$$

Logo, $x = \frac{p}{s}$ com $p \in \mathfrak{p}$ e $s \in S$, o que prova nossa afirmação. Agora, sejam $x = \frac{a}{s} \in A'$ e $y = \frac{b}{t} \in A'$ tal que $xy = \frac{ab}{st} \in \mathfrak{p}A'$. Assim,

$$\frac{ab}{st} = \frac{p}{u}, \ com \ p \in \mathfrak{p} \text{ e } u \in S.$$

Logo, $abu = pst \in \mathfrak{p}$. Como $u \in S$ e $u \notin \mathfrak{p}$ e como $\mathfrak{p}$ é primo segue que $ab \in \mathfrak{p}$. Assim, $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ e, portanto, $\frac{a}{s} \in \mathfrak{p}A'$ ou $\frac{b}{t} \in \mathfrak{p}A'$. Portanto, $\mathfrak{p}A'$ é ideal primo. Mostremos que $\mathfrak{p}A' \cap A = \mathfrak{p}$. Como $\mathfrak{p} \subseteq A$ e $\mathfrak{p} \subseteq \mathfrak{p}A'$ segue que $\mathfrak{p} \subseteq \mathfrak{p}A' \cap A$. Por outro lado, se $x \in \mathfrak{p}A' \cap A$ então $x \in \mathfrak{p}A'$ e $x \in A$. Assim, $x = \frac{p}{s}$, com $p \in \mathfrak{p}$ e $s \in S$, ou seja, o $sx \in \mathfrak{p}$. Como $s \notin \mathfrak{p}$, segue que $x \in \mathfrak{p}$, pois $\mathfrak{p}$ é ideal primo. Portanto, $\mathfrak{p}A' \cap A = \mathfrak{p}$. Finalmente, temos que $(\varphi \circ \phi)(\mathfrak{p}) = \varphi(\phi(\mathfrak{p})) = \varphi(\mathfrak{p}A') = \mathfrak{p}A' \cap A = \mathfrak{p}$ e $(\phi \circ \varphi)(\mathfrak{p}') = \phi(\varphi(\mathfrak{p}')) = \phi(\mathfrak{p}' \cap A) = (\mathfrak{p}' \cap A)A' = \mathfrak{p}'$. Portanto, $\varphi = \phi^{-1}$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Corolário 1.7.1 *Com as mesmas notações da Proposição (1.7.2), se A é um anel noetheriano, então A' é um anel noetheriano.*

Demonstração: Considere a aplicação $\varphi : \{ideais\ de\ A'\} \longrightarrow \{ideais\ de\ A\}$ definida por $\varphi(\mathfrak{b}') = \mathfrak{b}' \cap A$. Se $(\mathfrak{b}'_n)_{n>0}$ é uma sequência crescente de ideais de A', então pela Proposição (1.7.2) segue que $(\varphi(\mathfrak{b}'_n))_{n>0}$ é sequência crescente de ideais em A. Como A é noetheriano, segue que existe $n_0 \in \mathbb{N}$ tal que $\varphi(\mathfrak{b}'_n) = \varphi(\mathfrak{b}'_{n+1}), \forall n \geq n_0$, isto é, a sequência é estacionária. Como φ é injetora, temos que $\mathfrak{b}'_n = \mathfrak{b}'_{n+1}, \forall n \geq n_0$. Assim, $(\mathfrak{b}'_n)_{n>0}$ é estacionária. Portanto, A' é noetheriano. ∎

Corolário 1.7.2 *Se A é um domínio de Dedekind, $\mathfrak{p} \subset A$, um ideal primo, $S = A - \mathfrak{p}$ e $\mathcal{I}$ um ideal de A tal que $\mathcal{I} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, onde $\mathfrak{p}_i$, para $i = 1, \ldots, r$ são ideais primos de A, então a decomposição de $A'\mathcal{I}$ em ideais primos de $A' = S^{-1}A$ é dado por $A'\mathcal{I} = \prod_{\mathfrak{p}_i \cap S = \emptyset} (A'\mathfrak{p}_i)^{e_i}$.*

Demonstração: Se $\mathfrak{p}'$ é um ideal primo não nulo de A', então pela Proposição (1.7.2), segue que $\mathfrak{p}' \cap A = \mathfrak{p}$ é um ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$. Também, $\mathfrak{p} \neq \emptyset$, pois $\mathfrak{p}' = A'\mathfrak{p}$. Assim, $\mathfrak{p}$ é um ideal maximal de A. Pela Proposição (1.7.2), segue que $\mathfrak{p}'$ é um ideal maximal de A'. Como $\mathcal{I} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ segue que $A'\mathcal{I} = A'\left(\prod_{i=1}^{r} \mathfrak{p}_i\right)^{e_i} = \prod_{i=1}^{r} \left(A'\mathfrak{p}_i\right)^{e_i} = \prod_{\mathfrak{p}_i \cap S = \emptyset} \left(A'\mathfrak{p}_i\right)^{e_i}$. Finalmente, se $\mathfrak{p}_i \cap S \neq \emptyset$, então $A'\mathfrak{p}_i = A'$ e se $\mathfrak{p}_i \cap S = \emptyset$, então $A'\mathfrak{p}_i$ é um ideal primo de A', para $i = 1, \ldots, r$. ∎

Proposição 1.7.3 *Se $\mathcal{I}$ é um ideal de um anel A, então $\mathcal{I} = \bigcap_i A'_i\mathcal{I}$, onde $A'_i = S'_iA, S'_i = A - \mathfrak{p}_i$ e $\mathfrak{p}_i$ um ideal maximal de A.*

Demonstração: O resultado é verdadeiro quando A é um corpo, pois os únicos ideais de A são os triviais. Suponha que A não é corpo. Se $x \in \bigcap_i A'_i\mathcal{I}$, então $x = \frac{a_i}{b_i}$, com $a_i \in \mathcal{I}, b_i \in A$ e $b_i \notin \mathfrak{p}_i$, para todo i. Seja $\mathcal{B}$ o ideal de A gerado pelos elementos b_i. Como $b_i \notin \mathfrak{p}_i$, segue que $\mathcal{B} \not\subseteq \mathfrak{p}_i$, para todo ideal maximal $\mathfrak{p}_i$. Assim, $\mathcal{B} = A$, pois sabemos que todo ideal de A, diferente de A, está contido em um ideal maximal. Assim, 1 pode ser expresso em termos dos geradores de $\mathcal{B} = A$, isto é, existem elementos $c_{i1}, \ldots, c_{im} \in A$ tal que $1 = \sum_{k=1}^{m} c_{ik}b_{ik}$. Assim, $x = \sum_{k=1}^{m} c_{ik}(b_{ik}x) = \sum_{k=1}^{m} c_{ik}a_{ik} \in \mathcal{I}$. Portanto, $\bigcap_i A'_i\mathcal{I} \subset \mathcal{I}$. Como $\mathcal{I} \subset \bigcap_i A'_i\mathcal{I}$ segue que $\mathcal{I} = \bigcap_i A'_i\mathcal{I}$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Proposição 1.7.4 *Seja B um domínio, $A \subset B$ subanel e $S \subset A$ um subconjunto, com $1 \in S$ e S fechado para o produto. Se $\mathcal{O}_B$ é o anel de inteiros de A em B, então $\mathcal{O}_B$ é o anel de inteiros de A' em B.*

Demonstração: Se $x \in \mathcal{O}_B$, então $x = \frac{b}{s}$ com $b \in \mathcal{O}_B$ e $s \in S$. Como $\mathcal{O}_B$ é inteiro sobre A, segue que

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0, \tag{1.9}$$

onde $a_i \in A$, para $i = 0, 1, \ldots, n-1$, não são todos nulos. Dividindo (1.9) por s^n obtemos que

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0.$$

Como $\frac{a_i}{s} \in A'$ e não são todos nulos, segue que $x = \frac{b}{s}$ é inteiro sobre A'. Agora vamos mostrar que todo elemento de B que é inteiro sobre A' pertence a $\mathcal{O}_B$. Para isso, se $x \in B$ é inteiro sobre A', então

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + e\frac{a_0}{s_0} = 0, \tag{1.10}$$

com $\frac{a_i}{s_i} \in A'$, para $i = 0, 1, \ldots, n-1$, não todos nulos. Multiplicando (1.10) por s^n, com $s = s_0 s_1 \ldots s_{n-1}$, obtemos que $(sx)^n + a_{n-1}(sx)^{n-1} + \cdots + b_0 = 0$, onde $b_i \in A$, para $i = 0, 1, \ldots, n-1$, não são todos nulos. Logo, $sx \in \mathcal{O}_B$ e assim $sx = b$, com $b \in \mathcal{O}_B$. Portanto, $x = \frac{b}{s}$ onde $b \in \mathcal{O}_B$ e $s \in S$. Portanto, $x \in \mathcal{O}_B$. ∎

Corolário 1.7.3 *Se A é um anel integralmente fechado então $A' = S^{-1}S$ é integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações do anel A e seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre A. Como A é integralmente fechado, temos que $A = \mathcal{O}_{\mathbb{K}}$, e assim pela Proposição (1.7.4), $A' = \mathcal{O}_{\mathbb{K}}{}'$.

∎

Teorema 1.7.1 *Se A é um anel de Dedekind, então $A' = S^{-1}S$ é um anel de Dedekind.*

Demonstração: Temos pelos Corolários (1.7.1) e (1.7.3), que A' é um anel noetheriano e integralmente fechado, respectivamente. Deste modo, falta mostrar que todo ideal primo não nulo de A' é maximal. Assim, se $\mathfrak{p}' \subset A'$ é um ideal primo não nulo então, pelo Lema (1.5.1), segue que $\mathfrak{p}' \cap A$ é um ideal primo de A e, portanto, maximal. Pela Proposição (1.7.2), segue que se $\mathfrak{p}' \subseteq \mathcal{M}' \subseteq A'$, então $\varphi(\mathfrak{p}') \subseteq \varphi(\mathcal{M}') \subseteq \varphi(A')$. Como A é Dedekind,

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

segue que $\varphi(\mathfrak{p}')$ é maximal e, portanto, $\varphi(\mathfrak{p}') = \varphi(\mathcal{M}')$ ou $\varphi(\mathcal{M}') = \varphi(A')$. Logo, $\mathfrak{p}' = \mathcal{M}'$ ou $\mathcal{M}' = A'$. Portanto, $\mathfrak{p}'$ é maximal. ∎

Proposição 1.7.5 *Se A é um domínio de Dedekind e $S \subset A$ é um subconjunto tal que $S = A - \mathfrak{p}$, onde $\mathfrak{p} \subset A$ é um ideal primo então A' é principal, ou seja, existe $p \in A'$ tal que os ideais de A' são da forma $\langle p^n \rangle$, onde $n \in \mathbb{N}$.*

Demonstração: Temos que $\mathfrak{p} \subset A$ é o único ideal primo não nulo de A tal que $\mathfrak{p} \cap S = \emptyset$, pois se existisse um outro ideal primo $\mathfrak{p}_1 \subset A$ tal que $\mathfrak{p}_1 \cap S = \emptyset$, teríamos que $\mathfrak{p}_1 \subset \mathfrak{p}$. Como A é Dedekind, segue que $\mathfrak{p}_1 = \mathfrak{p}$. Pela Proposição (1.7.2), temos que $\mathfrak{p}A' = \mathfrak{b}$ é o único ideal primo de A'. Mas como A' é Dedekind, segue que todo ideal de A' é do tipo $\mathfrak{b}^n$ onde $n \in \mathbb{N}$. Assim,

$$\cdots \subseteq \mathfrak{b}^n \subseteq \mathfrak{b}^{n-1} \subseteq \cdots \subseteq \mathfrak{b}^2 \subseteq \mathfrak{b} \subseteq A'.$$

Se $p \in \mathfrak{b} - \mathfrak{b}^2$ então $\langle p \rangle$ é ideal de A'. Assim, $\langle p \rangle = \mathfrak{b}^{n_0}$, para algum $n_0 \in \mathbb{N}$, e $\langle p \rangle \not\subset \mathfrak{b}^2$. Logo, $n_0 = 1$ e, portanto, $\langle p \rangle = \mathfrak{b}$. Portanto, A' é principal e todos os seus ideais são da forma $\langle p^n \rangle$, com $n \in \mathbb{N}$. ∎

Teorema 1.7.2 *Seja A um domínio, $S \subset A$ um subconjunto tal que $0 \notin S$, $1 \in S$ e fechado no produto. Se $\mathcal{M}$ é um ideal maximal de A tal que $\mathcal{M} \cap S = \emptyset$, então $A'/\mathcal{M}A' \simeq A/\mathcal{M}$.*

Demonstração: Sendo $\mathcal{M}$ um ideal maximal de A, segue que $\mathcal{M}$ também é um ideal primo de A. Assim, pela Proposição (1.7.2), segue que $\mathcal{M}A'$ é um ideal primo de A'. Considere a aplicação $\varphi : A \xrightarrow{i} A' \xrightarrow{\pi} A'/\mathcal{M}A'$, onde i é a inclusão e π é a projeção. Temos que $\ker(\varphi) = \mathcal{M}A' \cap A$, pois $\varphi(x) = \bar{0}$ se, e somente se, $x + \mathcal{M}A' = \bar{0}$ se, e somente se, $x \in \mathcal{M}A'$ e $x \in A$. Portanto, $\ker(\varphi) = \mathcal{M}A' \cap A = \mathcal{M}$, onde a última igualdade segue da Proposição 1.7.2. Falta mostrar que φ é sobrejetora. Para isso, se $\bar{x} \in A'/\mathcal{M}A'$, então, $\bar{x} = x + \mathcal{M}A'$, com $x = \frac{a}{s}, a \in A$ e $s \in S$. Como $\mathcal{M} \cap S = \emptyset$, segue que $s \notin \mathcal{M}$ e como $\mathcal{M}$ é maximal segue que $A/\mathcal{M}$ é um corpo. Logo, $\bar{s} = s + \mathcal{M} \neq 0$ é inversível, ou seja, existe $\bar{b} \in A/\mathcal{M}$ tal que $\bar{s}\bar{b} = \bar{1}$. Assim, $sb - 1 \in \mathcal{M}$. Deste modo, $\frac{a}{s} - ab = \frac{a}{s}(1 - sb) \in \mathcal{M}A'$. Logo, $\varphi(ab) = ab + \mathcal{M}A' = x + \mathcal{M}A'$ se, e somente se, $x - ab \in \mathcal{M}A'$. Portanto, existe $ab \in A$ tal que $\varphi(ab) = x + \mathcal{M}A'$. Assim, $A'/\mathcal{M}A' \simeq A/\mathcal{M}$.

∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Capítulo 2

Corpos quadráticos e ciclotômicos

Neste capítulo apresentamos os conceitos de corpos quadráticos e de corpos ciclotômicos, utilizando os resultados vistos no Capítulo 1. Essas duas classes de corpos serão muito utilizadas nos próximos capítulos, como base para construção de reticulados. Também apresentamos a decomposição de um ideal primo em uma extensão através do Teorema de Kummer. Deste modo, na Seção 2.1 veremos corpos quadráticos, na Seção 2.2 veremos os corpos ciclotômicos e finalmente na Seção 2.3 veremos a decomposição de ideais primos em uma extensão. Os resultados aqui relatados podem der encontrados nas referências [2], [3], [4], [5], [6], [7] e [8].

2.1 Corpos quadráticos

O objetivo desta seção é introduzir o conceito de corpos quadráticos, bem como a caracterização de seu anel de inteiros, base integral e discriminante.

Definição 2.1.1 *Um corpo de números é uma extensão finita de* $\mathbb{Q}$. *Um* **corpo quadrático** *é uma extensão de grau* 2 *de* $\mathbb{Q}$.

Proposição 2.1.1 *Um corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$, *onde* d *é um inteiro livre de quadrados.*

Demonstração: Se $\mathbb{K}$ é um corpo quadrático, então todo elemento $\alpha \in \mathbb{K}$ tal que $\alpha \notin \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$. Pelo Teorema do Elemento Primitivo temos que $\mathbb{K} = \mathbb{Q}[\alpha]$ para algum $\alpha \in \mathbb{K}$. Seja $p(x) = x^2 + bx + c$ o polinômio minimal de α. Resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$, temos que $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Desta maneira, $\mathbb{K} = \mathbb{Q}[\alpha] = \mathbb{Q}\left[\sqrt{b^2 - 4c}\right]$, e observando que $b^2 - 4c$ é um número racional da forma $\frac{u}{v} = \frac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, temos que

$\mathbb{Q}[\sqrt{b^2-4c}] = \mathbb{Q}(\sqrt{uv})$. Como $uv \in \mathbb{Z}$, temos que uv é fatorado em produtos de primos. Assim, $\mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$, onde d é inteiro livre de quadrados. ∎

Observação 2.1.1

1. *O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $x^2 - d$. O conjugado de $\sqrt{d}$ é -$\sqrt{d}$, ou seja, existe um automorfismo $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$, tal que $\sigma(a+b\sqrt{d}) = a - b\sqrt{d}$.*

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

Lema 2.1.1 *Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados, sobre $\mathbb{Z}$. Se $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$, então $2a \in \mathbb{Z}$ e $2b \in \mathbb{Z}$.*

Demonstração: Pela Observação (2.1.1), existe um automorfismo σ de $\mathbb{K}$ tal que $\sigma(\alpha) = \sigma(a+b\sqrt{d}) = a - b\sqrt{d}$. Como $\sigma(\alpha)$ também é raiz da mesma equação de dependência integral de α, segue que $\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$. Como α e $\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$, pelo Corolário (1.2.2), segue que $\alpha + \sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$ e $\alpha\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$. Além disso, $\alpha + \sigma(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$. Pela Proposição (1.2.5) temos que $\mathbb{Z}$ é integralmente fechado e, portanto,

$$2a \in \mathbb{Z} \text{ e } a^2 - db^2 \in \mathbb{Z}. \tag{2.1}$$

Por (2.1) temos que $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Como $2a \in \mathbb{Z}$, segue que $d(2b)^2 \in \mathbb{Z}$. Se $2b \notin \mathbb{Z}$, o seu denominador tem um fator primo p e este fator aparece como p^2 no denominador de $d(2b)^2$. Sendo d livre de quadrados, segue que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Portanto, $2b \in \mathbb{Z}$. ∎

A seguir determinamos o anel dos inteiros algébricos de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados.

Teorema 2.1.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com $d \in \mathbb{Z}$ livre de quadrados, ou seja, $d \not\equiv 0 (mod\ 4)$.*
a) Se $d \equiv 2 (mod\ 4)$ ou $d \equiv 3 (mod\ 4)$, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$, consiste de todos os elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, ou seja, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.
b) Se $d \equiv 1 (mod\ 4)$, então o anel de 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, ou seja, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$. Pelo Lema (2.1.1) temos que

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

De (2.1) temos que

$$u^2 - dv^2 \in 4\mathbb{Z}.$$

a) Se $d \equiv 2$ ou $d \equiv 3(mod\ 4)$, então u e v são pares, pois se v fosse ímpar, teríamos $v^2 \equiv 1(mod\ 4)$. Como $u^2 - dv^2 \in 4\mathbb{Z}$ segue que $u^2 - d(4k+1) \in 4\mathbb{Z}$ o que implica que $u^2 - d \in 4\mathbb{Z}$, assim, $u^2 \equiv d(mod\ 4)$. Portanto, $d \equiv 1(mod\ 4)$ ou $d \equiv 0(mod\ 4)$, o que contradiz a hipótese. Sendo v par, temos que $v^2 \equiv 0(mod\ 4)$ e, portanto $u^2 \in 4\mathbb{Z}$. Assim u também é par. Logo $a, b \in \mathbb{Z}$ e $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ e, portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio

$$x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x].$$

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

b) Se $d \equiv 1(mod\ 4)$, então u e v tem a mesma paridade. Se u e v são pares então $a, b \in \mathbb{Z}$, e portanto $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = \frac{u}{2} + \frac{v\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. 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 $a, b \in \mathbb{Z}$, então α é raiz do polinômio $x^2 - (2a+b)x + \left(a^2 + ab - \frac{(1-d)b^2}{4}\right) \in \mathbb{Z}[x]$,

pois $d \equiv 1(mod\ 4)$. Assim, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_{\mathbb{K}}$. ∎

Exemplo 2.1.1 *Considere* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. *Como* $5 \equiv 1(mod\ 4)$, *segue que* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Observação 2.1.2 *Como os* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *com* $d \in \mathbb{Z}$ *livre de quadrados, em* $\mathbb{C}$ *são* σ_1 *e* σ_2, *onde* $\sigma_1(\sqrt{d}) = \sqrt{d}$ *e* $\sigma_2(\sqrt{d}) = -\sqrt{d}$, *segue que o discriminante absoluto de um corpo quadrático é obtido do seguinte modo:*

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

unesp

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

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

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

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

Exemplo 2.1.2 *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{7})$, *então* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\sqrt{7}\right]$. *Assim,* $\{1, \sqrt{7}\}$ *é uma base integral de* $\mathcal{O}_{\mathbb{K}}$ *e o discriminante absoluto de* $\mathbb{K}$ *é* 28. *Os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são* $\sigma_1(a+b\sqrt{7}) = a+b\sqrt{7}$ *e* $\sigma_2(a+b\sqrt{7}) = a-b\sqrt{7}$. *Logo,* $Tr(a+b\sqrt{7}) = \sum_{i=1}^{2} \sigma_i(a+b\sqrt{7}) = 2a$ *e* $N(a+b\sqrt{7}) = \prod_{i=1}^{2} \sigma_i(a+b\sqrt{7}) = a^2 + 7b^2$.

2.2 Corpos ciclotômicos

Nesta seção apresentamos os corpos ciclotômicos juntamente com suas principais propriedades. Esses corpos desempenham um papel fundamental na Teoria Algébrica dos Números, uma vez que é possível determinar claramente seu anel de inteiros algébricos e, conseqüentemente, seu discriminante.

Definição 2.2.1 *Seja* $\mathbb{K}$ *um corpo. Um elemento* $\xi \in \mathbb{K}$ *tal que* $\xi^n = 1$ *é chamado uma* **raiz n-ésima da unidade**. *Dizemos que* ξ *é uma raiz n-ésima primitiva da unidade se* $\xi^n = 1$ *e* $\xi^m \neq 1$ *para* $1 < m < n$.

Definição 2.2.2 *Um* **corpo ciclotômico** *é um corpo gerado por uma raiz n-ésima da unidade.*

Segue da Definição (2.2.1) que as raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$. Seja $U = \{\xi^{r_1}, \xi^{r_2}, \ldots, \xi^{r_n}\}$, o conjunto de todas as raízes distintas de $x^n - 1$ em $\mathbb{K}$. Como $(\xi^i\xi^j)^n = (\xi^i)^n(\xi^j)^n = (\xi^n)^i(\xi^n)^j = 1$ e $\left(\frac{\xi^i}{\xi^j}\right)^n = \frac{(\xi^i)^n}{(\xi^j)^n} = \frac{(\xi^n)^i}{(\xi^n)^j} = 1$, segue que o conjunto U é um grupo multiplicativo. Como todo grupo multiplicativo finito num corpo é cíclico, segue que U é um grupo cíclico, cujo gerador é ξ. Logo $U = \{\xi^n = 1, \xi, \ldots, \xi^{n-1}\}$.

unesp

Mas ξ não é o único gerador, uma vez que as raízes n-ésimas primitivas da unidade são também geradores de U, isto é, os elementos ξ^k, com $mdc(k,n)=1$, para $k=1,2,\ldots,n$. O número das raízes n-ésimas primitivas da unidade é dado por

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

onde φ é a função de Euler. Dado n um inteiro positivo, definimos ξ_n como sendo $e^{\frac{2\pi i}{n}}$ e o corpo $\mathbb{Q}(\xi_n)$ é chamado de n-ésimo corpo ciclotômico.

Definição 2.2.3 *O polinômio* $\phi_n(x) = \prod_{j=1, mdc(j,n)=1}^{n} (x - \xi_j^i)$ *é chamado de* n**-ésimo polinômio ciclotômico**.

Lema 2.2.1 *Se n é um inteiro positivo, então* $x^n - 1 = \prod_{d|n} \phi_d(x)$.

Demonstração: Sendo $f(x) = x^n - 1$, suas raízes são $1, \omega, \omega^2, \ldots, \omega^{n-1}$. Logo $x^n - 1 = (x-1)(x-\omega)\ldots(x-\omega^{n-1})$. Analisando os períodos de cada raiz de $f(x)$, e escrevendo todas de mesmo período como um polinômio da forma $\phi_d(x) = \prod_{\text{período de } \omega = d} (x - \omega)$, segue que $x^n - 1 = \prod_{d|n} \phi_d(x)$. ∎

Como consequência do Lema (2.2.1) temos que

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d<n} \phi_d(x)}. \tag{2.2}$$

Assim, $\phi_1(x) = x - 1$, $\phi_2(x) = \dfrac{x^2-1}{\phi_1(x)} = \dfrac{x^2-1}{x-1} = x + 1$, $\phi_3(x) = \dfrac{x^3-1}{\phi_1(x)} = \dfrac{x^3-1}{x-1} = x^2 + x + 1$, $\phi_4(x) = \dfrac{x^4-1}{\phi_1(x)\phi_2(x)} = \dfrac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = x^2 + 1$. Quando $n = p$, onde p é um número primo, segue que

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1. \tag{2.3}$$

que é chamado de **p-ésimo polinômio ciclotômico**. Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, de acordo com o Lema (2.2.1), temos que

$$x^{p^r} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x)\phi_{p^r}(x) \;\; e$$
$$x^{p^{r-1}} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x).$$

Logo $\phi_{p^r}(x) = \dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$. Este polinômio é chamado de **p^r-ésimo polinômio ciclotômico**.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Teorema 2.2.1 *Se ξ_n é uma raiz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\xi_n) : \mathbb{Q})] = \varphi(n)$.

Demonstração: Seja $f(x)$ o polinômio minimal de ξ_n sobre $\mathbb{Q}$. Logo, $x^n - 1 = f(x)h(x)$, com $h(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss, segue que $f(x), h(x) \in \mathbb{Z}[x]$. Se p é um número primo tal que $p \nmid n$, então, ξ_n^p é uma raiz n-ésima primitiva da unidade. Logo, $(\xi_n^p)^n - 1 = f(\xi_n^p)h(\xi_n^p)$, ou seja, $0 = f(\xi_n^p)h(\xi_n^p)$. Assim, se ξ_n^p não for raiz de $f(x)$, então ξ_n^p é raiz de $h(x)$, e portanto, ξ_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 pequeno Teorema de Fermat, temos 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, $\bar{h}(\xi_n)^p = \bar{0}$, pois ξ_n é raiz de $f(x)$. E, recursivamente, chegamos que $\bar{h}(\xi_n) = 0$. 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 $\lambda \in \mathbb{Z}_p, n\lambda^{n-1} = \bar{0}$. 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, ξ_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, $\partial(\phi_n(x)) = \partial(f(x)) = \varphi(n)$. ∎

Observação 2.2.1 *Existe um único polinômio minimal $f(x)$ tal que $f(\xi_n) = 0$. Pelo Teorema (2.2.1) temos que $\partial(f(x)) = \partial(\phi_n(x))$, e que $\phi_n(\xi_n) = 0$. Assim, $f(x) = \phi_n(x)$, e portanto, $\phi_n(x)$ é irredutível.*

Lema 2.2.2 *Se p é um número primo e ξ é uma raiz p-ésima primitiva da unidade então:*

1) $Tr(\xi^j) = -1$, *para* $j = 1, \ldots, p-1$.

2) $Tr(1 - \xi^j) = p$, *para* $j = 1, \ldots, p-1$.

3) $N(\xi - 1) = (-1)^{p-1}p$ *e* $N(1 - \xi) = p$.

4) $p = (1 - \xi)(1 - \xi^2)\ldots(1 - \xi^{p-1})$.

Demonstração: 1) O polinômio ciclotômico de ξ é dado por $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Como ξ^j são raízes de $f(x)$, segue que $Tr(\xi^j) = -1$, para $j = 1, \ldots, p-1$.

2) Como $[\mathbb{Q}[\xi] : \mathbb{Q}] = p-1$ temos que $Tr(1) = p-1$. Portanto, $Tr(1-\xi^j) = Tr(1) - Tr(\xi^j) = p - 1 + 1 = p$, para $j = 1, \ldots, p-1$.

3) Como $\xi - 1$ é uma raiz do polinômio $f(y) = y^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} y^{j-1}$ segue que,

$N(\xi - 1) = (-1)^{p-1}p$ e

unesp

$$N(1-\xi) = N((-1)(\xi-1)) = N(-1)N(\xi-1) = (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p.$$

4) Como $x^{p-1}+x^{p-2}+\cdots+x+1 = (x-\xi)(x-\xi^2)\ldots(x-\xi^{p-1})$, temos para $x=1$ que $(1-\xi)(1-\xi^2)\ldots(1-\xi^{p-1}) = p$. ∎

Sejam p um número primo e ξ_p uma raiz p-ésima da unidade. Como em ϕ_p o coeficiente de a_{p-2} do termo x^{p-2} é igual a 1, segue que

$$\begin{cases} Tr_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1) = [\mathbb{Q}(\xi_p):\mathbb{Q}].1 = p-1, \quad \text{e} \\ Tr_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(\xi_p^j) = -a_{p-2} = -1, \quad \text{para} \quad j = 1,2,\ldots,p-1. \end{cases}$$

Consequentemente,

$$Tr_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1-\xi_p^j) = Tr_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1) - Tr_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(\xi_p^j) = p, \text{para j} = 1,\ldots,p-1.$$

Os elementos $1-\xi_p^j$, para $j=1,\ldots,p-1$, são todos os conjugados de $1-\xi_p^k$, para $k=1,\ldots,p-1$. Assim, da Definição (2.2.3), segue que $N_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1-\xi_p^j) = \phi_p(1) = p$, para $j=1,\ldots,p-1$.

Lema 2.2.3 *Se $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\xi_p)$ então:*
i) $(1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.
ii) $Tr_{\mathbb{K}|\mathbb{Q}}((1-\xi_p)y) \in p\mathbb{Z}, \forall\, y \in \mathcal{O}_{\mathbb{K}}$.

Demonstração: i) O p-ésimo polinômio ciclotômico de ξ_p é $\phi_p(x) = x^{p-1}+\cdots+x+1 = (x-\xi_p)(x-\xi_p^2)\cdots(x-\xi_p^{p-1})$. Como $N_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1-\xi_p^k) = (1-\xi_p)(1-\xi_p^2)\ldots(1-\xi_p^{p-1}) = p$, segue que $\phi_p(1) = (1-\xi_p)(1-\xi_p^2)\ldots(1-\xi_p^{p-1}) = p$. Como $1-\xi_p^j \in \mathcal{O}_{\mathbb{K}}$, para $j=1,\ldots,p-1$, segue que $p \in (1-\xi_p)\mathcal{O}_{\mathbb{K}}$. Portanto, $p\mathbb{Z} \subset (1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$. Para mostrar a outra inclusão, vamos supor por absurdo que $p\mathbb{Z}$ está contido propriamente em $(1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, então $(1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Como $1 \in \mathbb{Z}$ segue que $1 = (1-\xi_p)a$, para algum $a \in \mathcal{O}_{\mathbb{K}}$. Logo, $1-\xi_p$ é inversível em $\mathcal{O}_{\mathbb{K}}$, e assim $1-\xi_p^j$ são inversíveis em $\mathcal{O}_{\mathbb{K}}$, para $j=2,\ldots,p-1$. Assim, $(1-\xi_p)(1-\xi_p^2)\ldots(1-\xi_p^{p-1})$ é inversível em $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$, isto é, p é inversível em $\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$, o que é um absurdo. Portanto, $(1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.
ii) Cada conjugado $y_i(1-\xi_p^i)$ de $y(1-\xi_p)$ é um múltiplo de $1-\xi_p^i$ em $\mathcal{O}_{\mathbb{K}}$, para $i=1,2,\ldots,p-1$. Como $1-\xi_p^i = (1-\xi_p)(1+\xi_p+\cdots+\xi_p^{i-1})$ segue que $1-\xi_p^i$ é um múltiplo de $1-\xi_p$ em $\mathcal{O}_{\mathbb{K}}$. Sendo o traço a soma dos conjugados, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(y(1-\xi_p)) = y_1(1-\xi_p)+y_2(1-\xi_p^2)+\cdots+y_{p-1}(1-\xi_p^{p-1}) = \alpha(1-\xi_p)$, com $\alpha \in \mathcal{O}_{\mathbb{K}}$. Portanto, $Tr(y(1-\xi_p)) \in \mathcal{O}_{\mathbb{K}}(1-\xi_p)$. Como, pela Proposição (1.2.5), $\mathbb{Z}$ é integralmente fechado, segue pelo Corolário (1.3.1) que $Tr(y(1-\xi_p)) \in \mathbb{Z}$. Assim, $Tr(y(1-\xi_p)) \in \mathcal{O}_{\mathbb{K}}(1-\xi_p) \cap \mathbb{Z} = p\mathbb{Z}$, onde a igualdade segue de (i). ∎

unesp

Teorema 2.2.2 *Se p é um número primo e ξ_p é uma raiz p-ésima primitiva da unidade, então $\mathbb{Z}[\xi_p]$ é o anel dos inteiros de $\mathbb{Q}[\xi_p]$ e $\{1, \xi, \ldots, \xi^{p-2}\}$ é uma base de $\mathbb{Z}[\xi_p]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Seja $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de $\mathbb{Q}[\xi_p]$. Temos que $\mathbb{Z}[\xi_p] \subset \mathcal{O}_{\mathbb{L}}$. Agora, vamos provar que $\mathcal{O}_{\mathbb{L}} \subset \mathbb{Z}[\xi_p]$. Considere $\alpha \in \mathcal{O}_{\mathbb{L}} \subset \mathbb{Q}[\xi_p]$. Assim,

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2},$$

com $a_i \in \mathbb{Q}$. Logo, $\alpha(1-\xi) = a_0(1-\xi) + a_1(\xi - \xi^2) + \cdots + a_{p-2}(\xi^{p-2} - \xi^{p-1})$. Assim, segue do Lema (2.2.3) que

$$Tr(\alpha(1-\xi)) = a_0 Tr(1-\xi) + a_1 Tr(\xi - \xi^2) + \cdots + a_{p-2} Tr(\xi^{p-2} - \xi^{p-1}) \in p\mathbb{Z}.$$

Portanto, $a_0 Tr(1-\xi) = a_0 p \in p\mathbb{Z}$ e $a_0 \in \mathbb{Z}$. De modo análogo temos que $a_i \in \mathbb{Z}$, para $i = 1, \ldots, n$, pois $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_{\mathbb{L}}$. assim,

$$(\alpha - a_0)\xi^{-1} = a_1 + a_2\xi + \cdots + a_{p-2}\xi^{p-3}.$$

Multiplicando por $1-\xi$ temos que $(\alpha - a_0)\xi^{-1}(1-\xi) = a_1(1-\xi) + a_2\xi(1-\xi) + \cdots + a_{p-2}\xi^{p-3}(1-\xi)$ e assim

$$Tr((\alpha - a_0)\xi^{-1}(1-\xi)) = a_1 Tr(1-\xi) + a_2 Tr(\xi - \xi^2) + \cdots + a_{p-2} Tr(\xi^{p-3} - \xi^{p-2}).$$

Logo, $a_1 Tr(1-\xi) = a_1 p \in p\mathbb{Z}$ e $a_1 \in \mathbb{Z}$. Prosseguindo, analogamente temos que $a_i \in \mathbb{Z}$, para $i = 1, \ldots, n$. Assim, $\alpha \in \mathbb{Z}$ e, portanto, $\mathbb{Z}[\xi_p] = \mathcal{O}_{\mathbb{L}}$. ∎

Proposição 2.2.1 *O discriminante absoluto de $\mathbb{K} = \mathbb{Q}(\xi_p)$ é dado por*

$$D_{\mathbb{K}} = D(1, \xi_p, \ldots, \xi_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

Demonstração: Sejam p um número primo e ξ_p uma raiz p-ésima da unidade. Vimos que $\{1, \xi_p, \ldots, \xi_p^{p-2}\}$ é uma base integral de $\mathbb{Z}[\xi_p]$. Pela Proposição (1.4.4) temos que $D(1, \xi_p, \ldots, \xi_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N(\phi_p'(\xi_p))$. Vamos mostrar então que $N(\phi_p'(\xi_p)) = p^{p-2}$. Como o p-ésimo polinômio ciclotômico é dado por $\phi_p(x) = \dfrac{x^p - 1}{x - 1}$, segue da derivação de ambos os lados que $\phi_p'(x) = \dfrac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2}$. Substituindo x por ξ_p, temos que $\phi_p'(\xi_p) = \dfrac{(\xi_p - 1)p\xi_p^{p-1} - (\xi_p^p - 1)}{(\xi_p - 1)^2}$. Como $\xi_p^p = 1$, segue que $\phi_p'(\xi_p) = \dfrac{p\xi_p^{-1}(\xi_p - 1)}{(\xi_p - 1)^2}$, ou seja,

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$\phi'_p(\xi_p) = \dfrac{p}{(\xi_p - 1)\xi_p}$, e isto implica que $\phi'_p(\xi_p) = \dfrac{-p}{(1-\xi_p)\xi_p}$. Aplicando a norma e usando sua linearidade, obtemos que

$$N(\phi'_p(\xi_p)) = \frac{N(-p)}{N(1-\xi_p)N(\xi_p)} = \frac{(-p)^{p-1}}{p.1} = \frac{p^{p-1}}{p} = p^{p-2}.$$

Portanto, $D(1, \xi_p, \ldots, \xi_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$. ∎

2.3 Ramificação de ideais

Nesta seção veremos a decomposição de ideais primos em uma extensão juntamente com suas principais propriedades.

Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$. Pelo Teorema (1.5.1) segue que $\mathcal{O}_{\mathbb{L}}$ é Dedekind. Seja $\mathfrak{p}$ um ideal primo não nulo de A. Pelo Teorema (1.5.2) temos que o ideal estendido $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ de $\mathcal{O}_{\mathbb{L}}$, é expresso de forma única como $\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, onde os $\mathfrak{q}_i$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e os e_i são elementos de $\mathbb{Z}$, para $i = 1, \ldots, g$.

Proposição 2.3.1 *Os ideais primos $\mathfrak{q}_i$ de $\mathcal{O}_{\mathbb{L}}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathfrak{q}_i \cap A = \mathfrak{p}$, para $i = 1, \ldots, g$.*

Demonstração: Seja $\mathfrak{b}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Então $\mathfrak{b} \cap A = \mathfrak{p}$ se, e somente se, $\mathfrak{b} \supset \mathfrak{p}\mathcal{O}_{\mathbb{L}}$. De fato, se $\mathfrak{b} \cap A = \mathfrak{p}$, então $\mathfrak{p} \subset \mathfrak{b}$ e, portanto, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} \subset \mathfrak{b}\mathcal{O}_{\mathbb{L}} = \mathfrak{b}$. Por outro lado, se $\mathfrak{b} \supset \mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, pelo Lema (1.5.1) segue que $\mathfrak{b} \supset \mathfrak{q}_i$, para algum i. Como $\mathfrak{q}_i$ maximal, pois $\mathcal{O}_{\mathbb{L}}$ é Dedekind, segue que $\mathfrak{q}_i = \mathfrak{b}$. Como $\mathfrak{b} \subset \mathcal{O}_{\mathbb{L}}$ e $A \subset \mathcal{O}_{\mathbb{L}}$, pelo Lema (1.5.1), segue que $\mathfrak{b} \cap A$ é um ideal primo de A e também $\mathfrak{b} \cap A \subsetneq A$, pois $1 \notin \mathfrak{b}$. Agora, como $\mathfrak{p} \subset \mathfrak{b}$ e $\mathfrak{p} \subset A$, segue que $\mathfrak{p} \subset A \cap \mathfrak{b}$. Como A é Dedekind, então $\mathfrak{p} = A \cap \mathfrak{b}$, pois $\mathfrak{p}$ é maximal. Portanto, $\mathfrak{p} = A \cap \mathfrak{q}_i$. Assim, $\mathfrak{b}$ está na fatoração de $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathfrak{b} \cap A = \mathfrak{p}$. ∎

Definição 2.3.1 *Se $\mathfrak{p} = A \cap \mathfrak{b}$, dizemos que $\mathfrak{b}$ está acima de $\mathfrak{p}$.*

Lema 2.3.1 *Com as notações anteriores temos que*
1) $\dfrac{A}{\mathfrak{p}}$ e $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ são corpos e que $\dfrac{A}{\mathfrak{p}}$ pode ser identificado como um subcorpo de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$.
2) Como $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado, então $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ é um espaço vetorial de dimensão finita sobre $\dfrac{A}{\mathfrak{p}}$, para $i = 1, \ldots, n$.

unesp

Demonstração: 1) Como A e $\mathcal{O}_{\mathbb{L}}$ são anéis de Dedekind, segue que $\frac{A}{\mathfrak{p}}$ e $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$, para $i = 1, \ldots, g$, são corpos. Agora, considere $A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$, onde i é a inclusão e π é a projeção. Temos que $\ker(\pi \circ i) = \mathfrak{q}_i \cap A = \mathfrak{p}$ e assim, $\frac{A}{\mathfrak{p}} \simeq Im(\pi \circ i)$. Portanto, $\frac{A}{\mathfrak{p}}$ pode ser identificado como um subcorpo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$.

2) Considerando as operações

$$\begin{aligned} \oplus : \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} \times \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} &\longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} \\ (\bar{x}, \bar{y}) &\longmapsto \bar{x} + \bar{y} \end{aligned}$$

$$\begin{aligned} \otimes : \frac{A}{\mathfrak{p}} \times \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} &\longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} \\ (\bar{a}, \bar{x}) &\longmapsto \bar{a}\bar{x} \end{aligned}$$

temos que $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ é um espaço vetorial sobre $\frac{A}{\mathfrak{p}}$ e $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ tem dimensão finita, pois sendo $\{x_1, \ldots, x_n\}$ os geradores de $\mathcal{O}_{\mathbb{L}}$ sobre A, e $b \in \mathcal{O}_{\mathbb{L}}$, então $b = a_1x_1 + \cdots + a_nx_n$ com $a_i \in A, i = 1, \ldots, n$. Assim, $\bar{b} = \bar{a}_1\bar{x}_1 + \cdots + \bar{a}_n\bar{x}_n$, com $\bar{a}_i = a_i + \mathfrak{p}$. Portanto, $\{\bar{x}_1, \ldots, \bar{x}_n\}$ gera $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ como um espaço vetorial sobre $\frac{A}{\mathfrak{p}}$. ∎

Definição 2.3.2 *O grau* $f_i = f(\mathfrak{q}_i|\mathfrak{p})$ *da extensão* $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$ *sobre* $\frac{A}{\mathfrak{p}}$ *é chamado de* **grau de inércia** *de* $\mathcal{O}_{\mathbb{L}}$ *sobre A, e o expoente* $e_i = e(\mathfrak{q}_i|\mathfrak{p})$ *é chamado de* **índice de ramificação** *de* $\mathfrak{q}_i$ *sobre A.*

Definição 2.3.3 *Dizemos que* $\mathfrak{p}$ *é:*

a) **totalmente decomposto em** $\mathbb{L}$*(ou em* $\mathcal{O}_{\mathbb{L}}$*) quando* $e = f = 1$*, para todo ideal primo* $\mathfrak{q}$ *que está acima de* $\mathfrak{p}$*.*

b) **inerte em** $\mathbb{L}$ *(ou em* $\mathcal{O}_{\mathbb{L}}$*) quando* $e = 1$ *e* $f = n$*, para todo ideal primo* $\mathfrak{q}$ *que está acima de* $\mathfrak{p}$*.*

c) **totalmente ramificado em** $\mathbb{L}$ *(ou em* $\mathcal{O}_{\mathbb{L}}$ *quando* $e = n$ *e* $f = 1$*, para todo ideal primo* $\mathfrak{q}$ *que está acima de* $\mathfrak{p}$*.*

d) **ramificado em** $\mathbb{L}$ *(ou em* $\mathcal{O}_{\mathbb{L}}$*) se existir um ideal primo* $\mathfrak{q}_i$ *de* $\mathcal{O}_{\mathbb{L}}$ *que está acima de* $\mathfrak{p}$ *tal que* $e_i > 1$ *para algum i.*

Lema 2.3.2 *Com as notações acima temos que*

1) $\mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap A = \mathfrak{p}$

2) $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}$ *é um espaço vetorial de dimensão finita sobre* $\frac{A}{\mathfrak{p}}$*.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: 1) Como $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{p} \subset A$ segue que $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap A$. Por outro lado,

$$\mathfrak{p} \cap \mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i} \subset \mathfrak{q}_i,$$

para $i = 1, \ldots, g$. Logo, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap A \subset \mathfrak{q}_i \cap A = \mathfrak{p}$. Portanto, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap A = \mathfrak{p}$.

Para 2) considere

$$A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}},$$

onde i é a inclusão e π é a projeção. Temos que $\ker(\pi \circ i) = \mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap A = \mathfrak{p}$ e assim, $\frac{A}{\mathfrak{p}} \simeq Im(\pi \circ i)$. Portanto, $\frac{A}{\mathfrak{p}}$ pode ser identificado com um subcorpo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}$. Como $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado, segue analogamente ao item 2) do Lema (2.3.1), que $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}$ é um espaço vetorial de dimensão finita sobre $\frac{A}{\mathfrak{p}}$. ∎

Proposição 2.3.2 *Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{p}) = p^f$, onde f é o grau de inércia de $\mathfrak{p}$.*

Demonstração: Pelo Lema (2.3.2) segue que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ é um espaço vetorial sobre $\mathbb{Z}_p$ de dimensão f. Portanto, $N(\mathfrak{p}) = \#(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}})p^f$. ∎

Lema 2.3.3 *A sequência de ideais*

$$\mathcal{O}_{\mathbb{L}} \supset \mathfrak{q}_1 \supset \mathfrak{q}_1^2 \supset \cdots \supset \mathfrak{q}_1^{e_1} \supset \mathfrak{q}_1^{e_1}\mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \supset \cdots \supset \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g} = \mathfrak{p}\mathcal{O}_{\mathbb{L}}$$

é maximal.

Demonstração: Dois elementos desta sequência é da forma $\mathfrak{q}$ e $\mathfrak{q}\mathfrak{q}_i$, onde $\mathfrak{q}$ é um produto de ideais $\mathfrak{q}_j$. Se existir $\mathfrak{b}$ tal que $\mathfrak{q}\mathfrak{q}_i \subset \mathfrak{b} \subset \mathfrak{q}$ segue, pelo Lema (1.5.3) que $\mathfrak{b}$ divide $\mathfrak{q}\mathfrak{q}_i$. Assim, existe $\mathcal{C}_1 \subset \mathcal{O}_{\mathbb{L}}$ tal que $\mathfrak{q}\mathfrak{q}_i = \mathfrak{b}\mathcal{C}_1$. De modo análogo, $\mathfrak{q}$ divide $\mathfrak{b}$, ou seja, existe $\mathcal{C}_2 \subset \mathcal{O}_{\mathbb{L}}$ tal que $\mathfrak{b} = \mathfrak{q}\mathcal{C}_2$. Logo, $\mathfrak{q}\mathfrak{q}_i = \mathfrak{q}\mathcal{C}_1\mathcal{C}_2$, ou seja, $\mathfrak{q}_i = \mathcal{C}_1\mathcal{C}_2$. Como $\mathfrak{q}_i$ é primo, segue que $\mathfrak{q}_i = \mathcal{C}_1$ ou $\mathfrak{q}_i = \mathcal{C}_2$. Se $\mathfrak{q}_i = \mathcal{C}_1$, então $\mathfrak{b} = \mathfrak{q}$, e se $\mathfrak{q}_i = \mathcal{C}_2$ então $\mathfrak{b} = \mathfrak{q}\mathfrak{q}_i$. Portanto, não existe ideal não trivial entre $\mathfrak{q}\mathfrak{q}_i$ e $\mathfrak{q}$. ∎

Teorema 2.3.1 *(Teorema da Igualdade Fundamental)* $\sum_{i=1}^{g} e_i f_i = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathfrak{p}}\right] = n.$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Vamos provar a primeira igualdade. Pela demonstração do Lema (2.3.1), temos que $\frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i}$ é um espaço vetorial sobre $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$, e pelo Lema (2.3.3) temos que seus subespaços são os triviais. Assim, $\dim_{\mathcal{O}_{\mathbb{L}}/\mathfrak{q}_i} \frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i} = 1$ e $\#\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} = \#\frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i}$. Como $\left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i} : \frac{A}{\mathfrak{p}}\right] = f_i$ e $\left[\frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i} : \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}\right] = 1$ segue que $\left[\frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i} : \frac{A}{\mathfrak{p}}\right] = f_i$. Dado um índice i, observemos que existem exatamente e_i elementos consecutivos na sequência dos ideais com o quociente da forma $\frac{\mathfrak{q}}{\mathfrak{q}\mathfrak{q}_i}$, ou seja, de dimensão f_i sobre $\frac{A}{\mathfrak{p}}$. A dimensão total de $\left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathfrak{p}}\right]$ é igual a soma das dimensões dos quocientes, ou seja,

$$\left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} : \frac{A}{\mathfrak{p}}\right] = e_1 f_1 + \cdots + e_g f_g = \sum_{i=1}^{g} e_i f_i.$$

Agora vamos provar a segunda igualdade. Se A é principal, pelo Corolário (1.3.3) temos que $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n. Se $\{x_1, \ldots, x_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre A, temos que $\{x_1 + \mathfrak{p}\mathcal{O}_{\mathbb{L}}, \ldots, x_n + \mathfrak{p}\mathcal{O}_{\mathbb{L}}\}$ é uma base de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}$ sobre $\frac{A}{\mathfrak{p}}$. De fato, se $\bar{b} \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}$ temos que $\bar{b} = b + \mathfrak{p}\mathcal{O}_{\mathbb{L}}$ e, então

$$\begin{aligned}(a_1x_1 + \cdots + a_nx_n) + \mathfrak{p}\mathcal{O}_{\mathbb{L}} &= (a_1x_1 + \mathfrak{p}\mathcal{O}_{\mathbb{L}}) + \cdots + (a_nx_n + \mathfrak{p}\mathcal{O}_{\mathbb{L}}) \\ &= (a_1 + \mathfrak{p})(x_1 + \mathfrak{p}\mathcal{O}_{\mathbb{L}}) + \cdots + (a_n + \mathfrak{p})(x_n + \mathfrak{p}\mathcal{O}_{\mathbb{L}}) \\ &= \bar{a_1}\bar{x_1} + \cdots + \bar{a_n}\bar{x_n},\end{aligned}$$

com $\bar{a_i} \in A/\mathfrak{p}$, $i = 1, \ldots, n$. Agora, se $\bar{a_1}\bar{x_1} + \cdots + \bar{a_n}\bar{x_n} = \bar{0}$ então,

$$a_1x_1 + \cdots + a_nx_n = \sum_{j=1}^{s} b_jp_j \text{ com } b_j \in \mathcal{O}_{\mathbb{L}} \text{ e } p_j \in \mathfrak{p}, \quad para \quad j = 1, \ldots, s.$$

Como $\{x_1, \ldots, x_n\}$ gera $\mathcal{O}_{\mathbb{L}}$ sobre A, segue que $b_j = \sum_{i=1}^{n} c_{ij}x_i$, com $c_{ij} \in A$, para $j = 1, \ldots, n$. Assim,

$$\sum_{i=1}^{n} a_ix_i = \sum_{j=1}^{s} \left(\sum_{i=1}^{n} c_{ij}x_i\right) p_j = \sum_{i=1}^{n} \left(\sum_{j=1}^{s} c_{ij}p_j\right) x_i.$$

Como $\{x_1, \ldots, x_n\}$ é linearmente independente, segue que $a_i = \sum_{j=1}^{s} c_{ij}p_j \in \mathfrak{p}$, ou seja, $\bar{a_i} = \bar{0}$, para $i = 1, \ldots, n$. A demonstração para o caso geral é feita por redução ao caso anterior. Temos que A é um anel de Dedekind. Se $\mathfrak{p}$ é um ideal primo não nulo de A e se $S = A - \mathfrak{p}$, temos pela Proposição (1.7.5), que $S^{-1}A$ é um anel principal e pela Proposição (1.7.4), que $S^{-1}\mathcal{O}_{\mathbb{L}}$ é anel dos inteiros de $\mathbb{L}$ sobre $S^{-1}A$ e $S^{-1}\mathcal{O}_{\mathbb{L}}$ é um $S^{-1}A$-módulo livre. Daí, pelo caso anterior, temos que $\left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{S^{-1}A}{S^{-1}A\mathfrak{p}}\right] = n$. Considerando a fatoração do ideal

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$\mathfrak{p}S^{-1}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g}(S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{q}_i)^{e_i}$ e como $\mathfrak{q}_i \cap A = \mathfrak{p}$, $\mathfrak{q}_i \cap S = \emptyset$ e $S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{q}_i$ são ideais primos não nulos de $S^{-1}\mathcal{O}_{\mathbb{L}}$, temos pela primeira parte que

$$\left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}S^{-1}\mathcal{O}_{\mathbb{L}}} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A}\right] = \sum_{i=1}^{g} e_i \left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{q}_i} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A}\right].$$

Porém, pelo Teorema (1.7.2), temos que $\frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \simeq \frac{A}{\mathfrak{p}}$ e $\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{q}_i} \simeq \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i}$. Portanto, $n = \left[\frac{S^{-1}\mathcal{O}_{\mathbb{L}}}{S^{-1}\mathcal{O}_{\mathbb{L}}\mathfrak{q}_i} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A}\right] = \sum_{i=1}^{g} e_i f_i$. ■

Proposição 2.3.3 *Com as notações anteriores, temos que* $\mathcal{O}_{\mathbb{L}}/\mathfrak{p}\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^{g} \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i^{e_i}}$.

Demonstração: Temos que $\mathfrak{q}_i$ é o único ideal maximal de $\mathcal{O}_{\mathbb{L}}$ que contém $\mathfrak{q}_i^{e_i}$, pois se existir $\mathcal{M}$ um outro ideal maximal, tal que $\mathcal{M} \supset \mathfrak{q}_i^{e_i}$, temos, pelo Lema (1.5.1), que $\mathcal{M} \supset \mathfrak{q}_i$, para algum i. Como $\mathfrak{q}_i$ é maximal segue que $\mathcal{M} = \mathfrak{q}_i$. Agora vamos mostrar que $\mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$, para $i \neq j$. Suponhamos que $\mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} \subsetneq \mathcal{O}_{\mathbb{L}}$. Assim, existe um ideal maximal $\mathcal{M}$ de $\mathcal{O}_{\mathbb{L}}$, tal que $\mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} \subset \mathcal{M} \subset \mathcal{O}_{\mathbb{L}}$. Como $\mathfrak{q}_i^{e_i} \subset \mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j}$, segue que $\mathfrak{q}_i^{e_i} \subset \mathcal{M}$, ou seja, $\mathfrak{q}_i \subset \mathcal{M}$, e como $\mathfrak{q}_i$ é maximal, segue que $\mathfrak{q}_i = \mathcal{M}$. De modo análogo, como $\mathfrak{q}_j^{e_j} \subset \mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j}$, segue que $\mathfrak{q}_j^{e_j} \subset \mathcal{M}$, ou seja, $\mathfrak{q}_j \subset \mathcal{M}$ e como $\mathfrak{q}_j$ é maximal, segue que $\mathfrak{q}_j = \mathcal{M}$. Assim, $\mathfrak{q}_i = \mathfrak{q}_j$, o que é um absurdo. Portanto, $\mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$. Então pelo Lema (1.1.2), segue que $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} \simeq \prod_{i=1}^{g} \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{q}_i^{e_i}}$. ■

Lema 2.3.4 *Seja A um domínio de Dedekind. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, ideais primos distintos e não nulos de A, e sejam $x_1, \ldots, x_r \in A$ e $e_1, \ldots, e_r$ inteiros positivos. Então existe um elemento $x \in A$ tal que $x - x_i \in \mathfrak{p}_i^{e_i}$ e $x - x_i \notin \mathfrak{p}_i^{e_i+1}$, para $i = 1, \ldots, r$.*

Demonstração: Para $i = 1, \ldots, r$ temos que $\mathfrak{p}_i^{e_i} \supsetneq \mathfrak{p}_i^{e_i+1}$. Assim, existe um elemento $a_i \in \mathfrak{p}_i^{e_i}$, $a_i \notin \mathfrak{p}_i^{e_i+1}$. Pela Proposição (2.3.3), existe $x \in A$ tal que $x - (x_i + a_i) \in \mathfrak{p}_i^{e_i+1}$, para $i = 1, \ldots, r$. Assim, $x - x_i = [x - (x_i + a_i)] + a_i \in \mathfrak{p}_i^{e_i}$, mas $x - x_i \notin \mathfrak{p}_i^{e_i+1}$, pois $a_i \notin \mathfrak{p}_i^{e_i+1}$. ■

Proposição 2.3.4 *Se A é um domínio de Dedekind que possui somente um número finito de ideais primos então A é principal.*

Demonstração: Pelo Teorema (1.5.2) temos que todo ideal não nulo de A é um produto finito de ideais primos não nulos de A. Assim, é suficiente mostrar que os ideais primos de

unesp

A são principais. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ os ideais primos não nulos de A. Pela Lema (2.3.4), para $h = 1, \ldots, r$, existe $y_h \in A$ tal que $y_h \in \mathfrak{p}_h$, $y_h \notin \mathfrak{p}_h^2$ e $y_h \notin \mathfrak{p}_j$, para $j \neq h$, onde consideramos $x_1 = \cdots = x_r = 0$, $e_h = 1$, e $e_j = 0$, para $j \neq h$. Assim, $\mathfrak{p}_h$ divide Ay_h, $\mathfrak{p}_h^2$ não divide Ay_h e $\mathfrak{p}_j$ não divide Ay_h, para $j \neq h$. Logo, a decomposição de Ay_h em ideais primos é $Ay_h = \mathfrak{p}_h$. Portanto, cada ideal $\mathfrak{p}_h$ é principal.

■

Teorema 2.3.2 *Seja $\mathbb{K} \subseteq \mathbb{L}$ corpos de números. Sejam $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ os anéis dos inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Um ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$ ramifica se, e somente se, $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{p}\mathcal{O}_\mathbb{L}}$ não é reduzido.*

Demonstração: Suponhamos que $\mathfrak{p}$ ramifica. Seja $\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, onde $\mathfrak{q}_i \cap \mathcal{O}_\mathbb{K} = \mathfrak{p}$, para $i = 1, \ldots, g$. Como $\mathfrak{p}$ ramifica, existe $k \in \mathbb{N}$ tal que $e_k > 1$. Temos que $\mathfrak{p}\mathcal{O}_\mathbb{L} \subsetneq \mathfrak{q}_j$, para todo $j = 1, \ldots, g$, pois se $\mathfrak{p}\mathcal{O}_\mathbb{L} = \mathfrak{q}_j$ teríamos que $e_j = 1$ para todo j, o que é contra a hipótese. Assim, para cada $j = 1, \ldots, g$, seja $a_j \in \mathfrak{q}_j - \mathfrak{p}\mathcal{O}_\mathbb{L}$. Seja $\bar{x} = a_1 \ldots a_g + \mathfrak{p}\mathcal{O}_\mathbb{L} \neq \bar{0}$. Se $r = e_1 \ldots e_g$, então

$$\bar{x}^r = (a_1 \ldots a_g)^r + \mathfrak{p}\mathcal{O}_\mathbb{L} = a_1^r \ldots a_k^r \ldots a_g^r + \mathfrak{p}\mathcal{O}_\mathbb{L} = \bar{0}.$$

Portanto, $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{p}\mathcal{O}_\mathbb{L}}$ não é reduzido. Reciprocamente, como $a_1 \in \mathfrak{q}_1$, segue que $(a_1^{e_2 e_3 \ldots e_g})^{e_1} \in \mathfrak{q}_1^{e_1}$ e como $\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$, segue que $\mathcal{O}_\mathbb{L}/\mathfrak{p}\mathcal{O}_\mathbb{L} \simeq \prod_{i=1}^{g} \dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{q}_i^{e_i}}$. Sendo $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{p}\mathcal{O}_\mathbb{L}}$ não reduzido temos que existe $\bar{x} = (x_1 + \mathfrak{q}_1^{e_1}, x_2 + \mathfrak{q}_2^{e_2}, \ldots, x_g + \mathfrak{q}_g^{e_g}) \neq \bar{0}$ nilpotente. Assim, existe j_0 tal que $x_{j_0} \notin \mathfrak{q}_{j_0}^{e_{j_0}}$ e existe $n \in \mathbb{N}$ tal que $\bar{x}^n = \bar{0}$. Portanto, $x_i^n \in \mathfrak{q}_i^{e_i}$, para $i = 1, \ldots, g$. Se $e_{j_0} = 1$, então $x_{j_0}^n \in \mathfrak{q}_{j_0}$ e assim, $x_{j_0} \in \mathfrak{q}_{j_0}$, o que é uma contradição. Portanto, $e_{j_0} > 1$. ■

Corolário 2.3.1 *Com as hipóteses do Teorema (2.3.2), $\mathfrak{p}$ ramifica se, e somente se,*

$$D_{(\mathcal{O}_\mathbb{L}/\mathfrak{p}\mathcal{O}_\mathbb{L})/(\mathcal{O}_\mathbb{K}/\mathfrak{p})} = \{0\}.$$

Demonstração: Temos, pelo Teorema (2.3.2), que $\mathfrak{p}$ ramifica se, e somente se, $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{p}\mathcal{O}_\mathbb{L}}$ não é reduzido, e pelo Lema (1.4.3) temos que $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{p}\mathcal{O}_\mathbb{L}}$ não é reduzido se, e somente se, $D_{(\mathcal{O}_\mathbb{L}/\mathfrak{p}\mathcal{O}_\mathbb{L})/(\mathcal{O}_\mathbb{K}/\mathfrak{p})} = \{0\}$. ■

Teorema 2.3.3 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos de números. Sejam $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ os anéis de inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Um ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$ ramifica se, e somente se, $\mathfrak{p} \supset D_{\mathcal{O}_\mathbb{L}/\mathcal{O}_\mathbb{K}}$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Suponhamos que $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ ramifica. Sejam $S = \mathcal{O}_{\mathbb{K}} - \mathfrak{p}$, $\mathcal{O}_{\mathbb{K}}{}' = S^{-1}\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}_{\mathbb{L}}{}' = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_{\mathbb{K}}{}'$. Pela Proposição (1.7.5), temos que $\mathcal{O}_{\mathbb{K}}{}'$ é principal e assim pelo Corolário (1.3.3), temos que $\mathcal{O}_{\mathbb{L}}{}'$ é um $\mathcal{O}_{\mathbb{K}}{}'$-módulo livre. Pelo Teorema (1.7.2), temos que $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} \simeq \frac{\mathcal{O}_{\mathbb{K}}{}'}{\mathfrak{p}'}$ e $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} \simeq \frac{\mathcal{O}_{\mathbb{L}}{}'}{\mathfrak{p}'\mathcal{O}_{\mathbb{L}}{}'}$. Seja $\{e_1, \ldots, e_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}{}'$ sobre $\mathcal{O}_{\mathbb{K}}{}'$. Pelo Corolário (2.3.1), temos que $D_{(\mathcal{O}_{\mathbb{L}}/\mathfrak{p}\mathcal{O}_{\mathbb{L}})/(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})} = \{0\}$. Assim, $\bar{0} = \overline{D(e_1, \ldots, e_n)} \in \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} = \frac{\mathcal{O}_{\mathbb{K}}{}'}{\mathfrak{p}'}$, e portanto $D(e_1, \ldots, e_n) \in \mathfrak{p}'$. Agora, se $\{x_1, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}}$, então $x_i = \sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathcal{O}_{\mathbb{K}}{}', i = 1, \ldots, n$, pois $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{L}}{}'$. Logo, $D(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}}$ e $D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n) \in \mathcal{O}_{\mathbb{K}}{}'\mathfrak{p}' \subset \mathfrak{p}'$. Assim, $D(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}} \cap \mathfrak{p}' = \mathfrak{p}$. Portanto, $D_{\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}} = \langle D(x_1, \ldots, x_n) \rangle \subset \mathfrak{p}$. Reciprocamente, se $D_{\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}} \subset \mathfrak{p}$ e se $\{e_1, \ldots, e_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}{}'$ sobre $\mathcal{O}_{\mathbb{K}}{}'$, então para $i = 1, \ldots, n$, temos que $e_i = \frac{y_i}{s}$, com $y_i \in \mathcal{O}_{\mathbb{L}}$ e $s \in S$. Assim,

$$\begin{aligned} D(e_1, \ldots, e_n) &= \det(Tr(e_i e_j)) = \det\left(Tr\left(\frac{y_i y_j}{s^2}\right)\right) \\ &= \frac{1}{s^{2n}} \det(Tr(y_i y_j)) = s^{-2n} D(y_1, \ldots, y_n) \in \mathcal{O}_{\mathbb{K}}{}' D_{\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}} \subseteq \mathcal{O}_{\mathbb{K}}{}'\mathfrak{p} = \mathfrak{p}' \end{aligned}$$

ou seja, $D(e_1, \ldots, e_n) \in \mathfrak{p}'$. Assim, $\overline{D(e_1, \ldots, e_n)} = \bar{0}$ em $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}'$ e portanto, $D_{(\mathcal{O}_{\mathbb{L}}/\mathfrak{p}\mathcal{O}_{\mathbb{L}})/(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})} = \{0\}$. Pelo Corolário (2.3.1), segue que $\mathfrak{p}$ ramifica. ∎

Corolário 2.3.2 *Com as hipóteses do Teorema (2.3.3), temos que existe somente um número finito de ideais primos de $\mathcal{O}_{\mathbb{K}}$ que ramifica em $\mathcal{O}_{\mathbb{L}}$.*

Demonstração: Pelo Teorema (2.3.3) temos que $\mathfrak{p}$ ramifica se, e somente se, $\mathfrak{p} \supset D_{\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{L}}} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$. Além disso, os $\mathfrak{p}_i$, para $i = 1, \ldots, g$, são os únicos ideais primos de $\mathcal{O}_{\mathbb{K}}$ que contém $D_{\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{L}}}$, uma vez que se $\mathfrak{m}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathfrak{m} \supset D_{\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{L}}} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, pelo Lema (1.5.1) segue que $\mathfrak{m} \supset \mathfrak{p}_i$, para algum $i = 1, \ldots, g$. Como $\mathfrak{p}_i$ é ideal maximal segue que $\mathfrak{m} = \mathfrak{p}_i$, o que prova o Corolário. ∎

Exemplo 2.3.1 *Sejam $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*
a) Se $d \equiv 2$ ou $3 (mod\ 4)$, então $\mathbb{Z}(\sqrt{d})$ é o anel de inteiros de $\mathbb{K}$ e $D(1, \sqrt{d}) = 4d$. Assim, os primos que se ramificam em $\mathbb{K}$ são 2 e os divisores de d.
b) Se $d \equiv 1 (mod\ 4)$, então $\mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ é o anel de inteiros de $\mathbb{K}$ e $D\left(1, \frac{1+\sqrt{d}}{2}\right) = d$. Assim, os primos que ramificam em $\mathbb{K}$ são os divisores de d.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Proposição 2.3.5 *Seja ξ_n uma raiz n-ésima primitiva da unidade. Então p ramifica em $\mathbb{Q}(\xi_n)$ se, e somente se, p divide n.*

Demonstração: Suponhamos que $p \mid n$, então $\mathbb{Q}(\xi_p) \subseteq \mathbb{Q}(\xi_n)$. Como p ramifica em $\mathbb{Q}(\xi_p)$, segue que p ramifica em $\mathbb{Q}(\xi_n)$. Reciprocamente, seja $n = \prod p_i^{m_i}$ e suponhamos por absurdo que $p \nmid n$. Então p não ramifica em cada $\mathbb{Q}(\xi_{p_i^{m_i}})$, já que p não divide o discriminante $D_{\mathbb{Q}(\xi_{p_i^{m_i}})}$. Agora, como $\mathbb{Q}(\xi_n)$ é a composição de $\mathbb{Q}(\xi_{p_i^{m_i}})$, segue que p não ramifica em $\mathbb{Q}(\xi_n)$, completando a demonstração. ■

Exemplo 2.3.2 *Pela Proposição (2.2.1), temos que $D(1, \xi, \ldots, \xi^{p-2}) = \pm p^{p-2}$. Assim, p é o único primo que ramifica em $\mathbb{Q}(\xi)$.*

Lema 2.3.5 *Se n e p são números primos ímpares tal que $p \equiv 1 (mod\ n)$, então existe um corpo cíclico $\mathbb{K}$ de grau n tal que p é o único primo que ramifica em $\mathbb{K}$.*

Demonstração: Seja $G = Gal(\mathbb{Q}(\xi_p)|\mathbb{Q})$, gerado por σ, e H subgrupo cíclico de G, gerado por σ^n, de ordem $\frac{p-1}{n}$. Note que $\frac{p-1}{n}$ é um número inteiro, uma vez que $p \equiv 1 (mod\ n)$. Seja $\mathbb{K}$ o subcorpo fixo por H. Temos que a extensão $\mathbb{K}|\mathbb{Q}$ é de Galois, pois $\mathbb{Q}(\xi_p)|\mathbb{Q}$ é cíclico. Consequentemente, $\mathbb{K}$ herda a propriedade de $\mathbb{Q}(\xi_p)$ de que p é o único primo que ramifica.
■

Teorema 2.3.4 *(Kummer) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita separável de $\mathbb{K}$ de grau n e $\mathcal{O}_\mathbb{L}$ o anel de inteiros de $\mathbb{L}$ sobre A. Assuma que $\mathcal{O}_\mathbb{L} = A[\alpha]$ para algum elemento α. Seja $f(x)$ o polinômio irredutível de α sobre $\mathbb{K}$ e $\mathfrak{p}$ um ideal primo não nulo de A. Seja $\overline{f}(x)$ a redução de $f(x)$ e $\mathfrak{p}$, e seja*

$$\overline{f}(x) = \overline{q}_1(x)^{e_1} \ldots \overline{q}_r(x)^{e_r}$$

a fatoração de $\overline{f}(x)$ em potências de fatores irredutíveis sobre $\overline{A} = A/\mathfrak{p}$, com coeficiente dominante 1. Então

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_r^{e_r} \tag{2.4}$$

é a fatoração de $\mathfrak{p}$ em $\mathcal{O}_\mathbb{L}$, de modo que e_i é o índice de ramificação de $\mathfrak{b}_i$ sobre $\mathfrak{p}$, e temos que

$$\mathfrak{b}_i = \mathfrak{p}\mathcal{O}_\mathbb{L} + q_i(\alpha)\mathcal{O}_\mathbb{L}, \tag{2.5}$$

se $q_i(x) \in A[x]$ é um polinômio com coeficiente dominante 1 cuja redução módulo $\mathfrak{p}$ é $\overline{q}_i(x)$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Sejam $\overline{q}(x)$ um fator irredutível de $\overline{f}(x)$, $\overline{\alpha}$ uma raiz de $\overline{q}(x)$, e $\mathfrak{b}$ o ideal primo de $\mathcal{O}_{\mathbb{L}}$ que é o núcleo da função

$$A[\alpha] \longrightarrow \overline{A}[\overline{\alpha}].$$

Temos que $\mathfrak{p}\mathcal{O}_{\mathbb{L}} + q(\alpha)\mathcal{O}_{\mathbb{L}}$ está contido em $\mathfrak{b}$. Por outro lado, seja $g(\alpha) \in \mathfrak{b}$ onde $g(x) \in A[x]$. Então $\overline{g}(x) = \overline{q(x)h(x)}$ para algum $\overline{h}(x) \in \overline{A}[x]$ e, portanto, $g(x) - q(x)h(x)$, que é um polinômio com coeficientes em A, uma vez que tem coeficientes em $\mathfrak{p}$. Isto prova a inclusão contrária, provando (2.5). Para provar (2.4), seja e_i' o índice de ramificação de $\mathfrak{b}_i$, tal que

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{b}_1^{e_1'} \dots \mathfrak{b}_r^{e_r'},$$

e seja d_i o grau de $\overline{q}_i$. Como $f(\alpha) = 0$, e como

$$f(x) - q_1(x)^{e_1} \dots q_r(x)^{e_r} \in \mathfrak{p}A[x],$$

segue que

$$q_1(\alpha)^{e_1} \dots q_r(\alpha)^{e_r} \in \mathfrak{p}\mathcal{O}_{\mathbb{L}}. \tag{2.6}$$

Por outro lado, temos que

$$\mathfrak{b}_i^{e_i} \subset \mathfrak{p}\mathcal{O}_{\mathbb{L}} + q_i(\alpha)^{e_i}\mathcal{O}_{\mathbb{L}},$$

consequentemente usando a Equação (2.6) temos que

$$\mathfrak{b}_1^{e_1} \dots \mathfrak{b}_r^{e_r} \subset \mathfrak{p}\mathcal{O}_{\mathbb{L}} + q_1(\alpha)^{e_1} \dots q_r(\alpha)^{e_r}\mathcal{O}_{\mathbb{L}} \subset \mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{b}_1^{e_1'} \dots \mathfrak{b}_r^{e_r'}.$$

Isto prova que $e_i \geq e_i'$ para todo i. Mas sabemos que

$$\sum e_i d_i = \partial f = [\mathbb{L} : \mathbb{K}] = \sum e_i' d_i.$$

Assim $e_i = e_i'$ para todo i, o que prova (2.4). ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Capítulo 3

Codiferente e diferente

Neste capítulo introduzimos os conceitos de codiferente e diferente, enfocando suas principais propriedades. Deste modo, na Seção 3.1 veremos o conceito de codiferente em uma extensão juntamente com suas principais propriedades e na Seção 3.2 veremos o diferente a partir do anel de inteiros de uma extensão. Os resultados aqui apresentados podem ser encontrados em [9] e [10].

3.1 Codiferente

Sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A. Seja $\mathbb{L}_1$ o espaço dual de $\mathbb{L}$. Pelo Corolário (1.3.2), temos que existe um isomorfismo $\varphi : \mathbb{L} \longrightarrow \mathbb{L}_1$ tal que $\varphi(x) = S_x$, onde $x \in \mathbb{L}$ e $S_x(y) = Tr_{\mathbb{L}|\mathbb{K}}(xy)$, para $y \in \mathbb{L}$. Seja $\{x_1, \ldots, x_n\}$ uma $\mathbb{K}$-base de $\mathbb{L}$ e seja $\{x_1^*, \ldots, x_n^*\}$ um conjunto de elementos de $\mathbb{L}$ tal que $\{\varphi_{x_1^*}, \ldots, \varphi_{x_n^*}\}$ seja uma base dual de $\{x_1^*, \ldots, x_n^*\}$, isto é, $\varphi_{x_i^*}(x_j) = Tr(x_i^* x_j) = \delta_{ij}$, onde $\delta_{ii} = 1$ e $\delta_{ij} = 0$ se $i \neq j$. Assim, $\{x_1^*, \ldots, x_n^*\}$ é também uma base de $\mathbb{L}$, chamada de base complementar de $\{x_1, \ldots, x_n\}$.

Proposição 3.1.1 *Com as notações acima, temos que* $D_{\mathbb{L}}(x_1, \ldots, x_n) D_{\mathbb{L}}(x_1^*, \ldots, x_n^*) = 1$.

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

$$X = (\sigma_i(x_j))_{ij} \text{ e } X^* = (\sigma_i(x_j^*))_{ij},$$

e denotando X^t para a matriz transposta de X, temos que $(X^*)^t X = (Tr(x_i^* x_j))_{ij}$. Assim, $\det(X^*)^t \det(X) = 1$. Pela Proposição (1.4.3), temos que

$$D_{\mathbb{L}}(x_1, \ldots, x_n) = \det(X)^2 \text{ e } D_{\mathbb{L}}(x_1^*, \ldots, x_n^*) = \det(X^*)^2.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Portanto, $D_{\mathbb{L}}(x_1,\ldots,x_n)D_{\mathbb{L}}(x_1^*,\ldots,x_n^*)=1$. ■

Definição 3.1.1 *Seja M um subconjunto de $\mathbb{L}$. O conjunto $M^*=\{x\in\mathbb{L}: Tr(xy)\in A, \forall\, y\in M\}$ é definido como o* **codiferente** *de M sobre $\mathbb{K}$, que também é chamado de dual ou complementar de M.*

Exemplo 3.1.1 *Se $A=\mathbb{Z}$, $\mathbb{K}=\mathbb{Q}$, $\mathbb{L}=\mathbb{Q}(\sqrt{2})$ e $M=\mathcal{O}_{\mathbb{L}}=\mathbb{Z}[\sqrt{2}]$, então, $\mathcal{O}_{\mathbb{L}}^*=\frac{1}{2\sqrt{2}}\mathcal{O}_{\mathbb{L}}$. De fato:*
Pela Definição (3.1.1) temos que $\mathcal{O}_{\mathbb{L}}^*=\{x\in\mathbb{Q}(\sqrt{2}): Tr(xy)\in\mathbb{Z}, \forall y\in\mathbb{Z}[\sqrt{2}]\}$. Sejam $x=a+b\sqrt{2}$, $a,b\in\mathbb{Q}$ e $y=c+d\sqrt{2}$, $c,d\in\mathbb{Z}$, então, $Tr(xy)=2ac+4bd\in\mathbb{Z}$. Como vale para todo $y\in\mathbb{Z}[\sqrt{2}]$, em particular

- *se $d=0$, e $c=1$, então $2a=m\in\mathbb{Z}$. Logo, $a=m/2$.*
- *se $d=1$ e $c=0$, então $4b=n\in\mathbb{Z}$. Logo, $b=n/4$.*

Assim, $x=\frac{m}{2}+\frac{n}{4}\sqrt{2}$, $m,n\in\mathbb{Z}$. Portanto, $\mathcal{O}_{\mathbb{L}}^*=\frac{1}{2\sqrt{2}}\mathcal{O}_{\mathbb{L}}$.

Exemplo 3.1.2 *Considere $A=\mathbb{Z}$, $\mathbb{K}=\mathbb{Q}$, $\mathbb{L}=\mathbb{Q}(\sqrt{7})$ e $M=\mathcal{O}_{\mathbb{L}}=\mathbb{Z}[\sqrt{7}]$.*
$\mathcal{O}_{\mathbb{L}}^*=\{x\in\mathbb{Q}(\sqrt{\not{7}}): Tr(xy)\in\mathbb{Z}, \forall y\in\mathbb{Z}[\sqrt{7}]\}$. Sejam $x=a+b\sqrt{7}$, $a,b\in\mathbb{Q}$ e $y=c+d\sqrt{7}$, $c,d\in\mathbb{Z}$, então $Tr(xy)=2ac+14bd$. Como vale para todo $y\in\mathbb{Z}[\sqrt{7}]$, em particular

- *se $d=0$, e $c=1$, então $2a=m\in\mathbb{Z}$. Logo, $a=m/2$.*
- *se $d=1$ e $c=0$, então $14b=n\in\mathbb{Z}$. Logo, $b=n/14$.*

Assim, $x=\frac{m}{2}+\frac{n}{14}\sqrt{7}$, $m,n\in\mathbb{Z}$. Portanto, $\mathcal{O}_{\mathbb{L}}^*=\frac{1}{2\sqrt{7}}\mathcal{O}_{\mathbb{L}}$.

Proposição 3.1.2 *Sejam M um subconjunto de $\mathbb{L}$ e M^* o codiferente de M sobre $\mathbb{K}$. Então*

1. *Se $\mathcal{O}_{\mathbb{L}}M\subseteq M$ então M^* é um módulo sobre $\mathcal{O}_{\mathbb{L}}$.*
2. *Se $M_1\subseteq M_2\subseteq\mathbb{L}$ então $M_2^*\subseteq M_1^*\subseteq\mathbb{L}$.*
3. *$\mathcal{O}_{\mathbb{L}}\subseteq\mathcal{O}_{\mathbb{L}}^*$.*

Demonstração: 1) Assumimos que $\mathcal{O}_{\mathbb{L}}M\subseteq M$. Se $b\in\mathcal{O}_{\mathbb{L}}$, $x\in M^*$e $y\in M$ temos que

$$Tr((bx)y)=Tr(x(by))\in A,$$

pois $by\in M$. Assim, $bx\in M^*$. Portanto, M^* é um $\mathcal{O}_{\mathbb{L}}$-módulo.
2) Suponhamos que $M_1\subseteq M_2$. Se $x_2\in M_2^*$, então, $x_2\in\mathbb{L}$ 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, $x_2\in M_1^*$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Portanto, $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.

3) Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre A, e integralmente fechado segue pelo Corolário (1.3.1) que $Tr(\mathcal{O}_{\mathbb{L}}) \subset A$. Assim, se $x, y \in \mathcal{O}_{\mathbb{L}}$ então $Tr(xy) \in A$, e deste modo $x \in \mathcal{O}_{\mathbb{L}}^*$. Portanto, $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$. ∎

Proposição 3.1.3 *Com as mesmas hipóteses da Proposição (3.1.2) segue que:*

1. *M^* é um A-módulo.*
2. *Se M é um A-módulo livre com base $\{x_1, \ldots, x_n\}$ então M^* é um A-módulo livre com base $\{x_1^*, \ldots, x_n^*\}$ e $M^{**} = M$.*

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 $a \in A$ e $x \in M^*$ e se $y \in M$, temos que

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

Assim, $ax \in M^*$. Portanto, M^* é um A-módulo.

2) Seja $\{x_1, \ldots, x_n\}$ uma base de M e seja $\{x_1^*, \ldots, x_n^*\}$ uma base de $\mathbb{L}$ 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

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

Pela linearidade 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 $a_i \in \mathbb{K}$, para $i = 1, \ldots, n$, então,

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

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 e $M^{**} = M$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Teorema 3.1.1 *Se* $\mathbb{L} = \mathbb{K}[\alpha]$, *onde* α *é inteiro sobre* A *e* $g(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in A[X]$ *o polinômio minimal de* α *sobre* $\mathbb{K}$, *então* $Tr\left(\frac{\alpha^i}{g'(\alpha)}\right) = 0$, *para* $i = 1, \ldots, n-2$, *e* $Tr\left(\frac{\alpha^{n-1}}{g'(\alpha)}\right) = 1$.

Demonstração: Sejam $\alpha = \alpha_1, \ldots, \alpha_n$ os conjugados de α sobre $\mathbb{K}$, onde são necessariamente distintos e pertencem a uma extensão finita de Galois sobre $\mathbb{K}$. Temos que $Tr\left(\frac{\alpha^i}{g'(\alpha)}\right) = \sum_{k=1}^{n} \frac{\alpha_k^i}{g'(\alpha_k)}$, para $i = 1, \cdots, n-1$. Como $g(x)$ é o polinômio minimal de α, segue que $g(x) = \prod_{k=1}^{n}(x - \alpha_k)$. Assim,

$$\frac{1}{g(x)} = \prod_{k=1}^{n} \frac{1}{x - \alpha_k}$$

e podemos expressar este produto como a soma $\sum_{k=1}^{n} \frac{a_k}{x - \alpha_k}$, para certos elementos a_k. Sendo $\frac{1}{g(x)} = \sum_{k=1}^{n} \frac{a_k}{x - \alpha_k}$, temos que

$$1 = \sum_{k=1}^{n} \frac{a_k g(x)}{x - \alpha_k} = \sum_{k=1}^{n} a_k \left(\prod_{i \neq k} (x - \alpha_i) \right),$$

para $i = 1, \ldots, n$. Assim, para $j = 1, \ldots, n$ temos que

$$1 = \sum_{k=1}^{n} a_k \left(\prod_{i \neq k} (\alpha_j - \alpha_i) \right) = a_j \prod_{i \neq j} (\alpha_j - \alpha_i).$$

Logo, $a_j = \frac{1}{\prod_{i \neq j}(\alpha_j - \alpha_i)} = \frac{1}{g'(\alpha_j)}$, para $j = 1, 2, \ldots, n$ e $\frac{1}{g(x)} = \sum_{k=1}^{n} \frac{1}{g'(\alpha_k)(x - \alpha_k)}$. Pelo algoritmo da divisão longa de Euclides, temos que

$$\frac{1}{g(x)} = \frac{1}{x^n} + c_1 \frac{1}{x^{n+1}} + c_2 \frac{1}{x^{n+2}} + c_3 \frac{1}{x^{n+3}} + \cdots$$

e

$$\sum_{k=1}^{n} \frac{1}{g'(\alpha_k)(x - \alpha_k)} = \sum_{k=1}^{n} \frac{1}{g'(\alpha_k)} \left[\frac{1}{x} + \frac{\alpha_k}{x^2} + \frac{\alpha_k^2}{x^3} + \frac{\alpha_k^3}{x^4} + \cdots \right].$$

Assim, temos que $\sum_{k=1}^{n} \frac{1}{g'(\alpha_k)} \left[\frac{1}{x} + \frac{\alpha_k}{x^2} + \frac{\alpha_k^2}{x^3} + \cdots \right] = \frac{1}{x^n} + c_1 \frac{1}{x^{n+1}} + \cdots$. Comparando esta última igualdade, temos que $\sum_{k=1}^{n} \left(\frac{\alpha_k^i}{g'(\alpha_k)} \right) = 0$, para $i = 1, \ldots, n-2$ e $\sum_{k=1}^{n} \left(\frac{\alpha_k^{n-1}}{g'(\alpha_k)} \right) = 1$. ■

unesp

Corolário 3.1.1 *O conjunto* $B = \left\{ \frac{1}{g'(\alpha)}, \frac{\alpha}{g'(\alpha)}, \ldots, \frac{\alpha^{n-1}}{g'(\alpha)} \right\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$.

Demonstração: Se

$$y = \sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right) = 0,$$

com $a_j \in \mathbb{K}$, para $j = 1, \ldots, n-1$, então $0 = Tr_{\mathbb{L}|\mathbb{K}}(y) = Tr\left(\sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right) \right) = a_{n-1}$.

Tomando $y\alpha = \sum_{j=1}^{n-2} a_j \left(\frac{\alpha^{j+1}}{g'(\alpha)} \right)$, temos que

$$0 = Tr_{\mathbb{L}|\mathbb{K}}(y\alpha) = Tr_{\mathbb{L}|\mathbb{K}}\left(\sum_{j=1}^{n-2} a_j \left(\frac{\alpha^{j+1}}{g'(\alpha)} \right) \right) = a_{n-2}.$$

De modo análogo, obtemos $a_j = 0$, para todo $j = 1, \ldots, n-1$, e assim B é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. ∎

O próximo Teorema nos fornece um critério para determinar $A[\alpha]^*$.

Teorema 3.1.2 *Com as mesmas definições do Teorema (3.1.1) segue que* $A[\alpha]^* = \frac{1}{g'(\alpha)} A[\alpha]$.

Demonstração: Tomando $y = \sum_{i=0}^{n-1} a_i \alpha^i \in A[\alpha]$ temos que

$$Tr\left(\frac{\alpha^j y}{g'(\alpha)} \right) = \sum_{i=0}^{n-1} a_i Tr\left(\frac{\alpha^{j+i}}{g'(\alpha)} \right) = a_{n-1-j} \in A,$$

e assim, $\frac{\alpha^j}{g'(\alpha)} \in A[\alpha]^*$, para todo $j = 0, \ldots, n-1$. Portanto, $A[\alpha]\frac{1}{g'(\alpha)} \subseteq A[\alpha]^*$. Para mostrar a outra inclusão, seja $y \in A[\alpha]^*$, pelo Corolário (3.1.1), temos que $y = \sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right)$, com $a_j \in \mathbb{K}$ *para* $j = 0, \ldots, n-1$ forma uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim,

$$Tr_{\mathbb{L}|\mathbb{K}}(y) = \sum_{j=0}^{n-1} a_j Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^j}{g'(\alpha)} \right) = a_{n-1} \in A,$$

pois $y \in A[\alpha]^*$. Analogamente,

$$\begin{aligned} Tr_{\mathbb{L}|\mathbb{K}}(y\alpha) &= \sum_{j=0}^{n-1} a_j Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{j+1}}{g'(\alpha)} \right) \\ &= a_{n-2} + a_{n-1} Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^n}{g'(\alpha)} \right) = a_{n-2} - a_{n-1}\left(\sum_{i=0}^{n} c_i Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{n-i}}{g'(\alpha)} \right) \right) \end{aligned}$$

unesp

$$= a_{n-2} - a_{n-1}c_1,$$

pois $\alpha^n = -(c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n)$, com $c_i \in A$. Como $a_{n-2} - a_{n-1}c_1 \in A$ segue que $a_{n-2} \in A$. De modo análogo, $a_i \in A$, para todo $i = 1, \ldots, n-1$. Portanto, $A[\alpha]^* = \dfrac{1}{g'(\alpha)}A[\alpha]$, e isto conclui a demonstração. ∎

Exemplo 3.1.3 *Seja* $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. *O polinômio minimal de* $\sqrt{2}$ *sobre* $\mathbb{Q}$ *é* $g(x) = x^2 - 2$ *e pelo Teorema (3.1.2) segue que* $\mathbb{Z}[\sqrt{2}]^* = \frac{1}{2\sqrt{2}}\mathbb{Z}[\sqrt{2}]$

Proposição 3.1.4 *Se* $\mathbb{L} = \mathbb{K}[\alpha]$, *onde* α *é inteiro sobre* $\mathbb{K}$, *então* $\mathcal{O}_{\mathbb{L}}^*$ *é um* $\mathcal{O}_{\mathbb{L}}$*-módulo finitamente gerado.*

Demonstração: Pelo Teorema (1.2.1) temos que $A[\alpha]$ é um A-módulo livre de posto finito. Pela Proposição (3.1.3) item 2) temos que $A[\alpha]^*$ é um A-módulo finitamente gerado. Como $A[\alpha] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}}^* \subseteq A[\alpha]^*$. Como A é Noetheriano, pois é Dedekind, segue pelo Corolário (1.1.2) que $\mathcal{O}_{\mathbb{L}}^*$ é um A-módulo Noetheriano e assim, $\mathcal{O}_L^*$ também é finitamente gerado. Pela Proposição (1.1.2), segue que $\mathcal{O}_{\mathbb{L}}^*$ é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado. ∎

Corolário 3.1.2 $\mathcal{O}_{\mathbb{L}}^*$ *é um ideal fracionário de* $\mathbb{L}$.

Demonstração: Pela Proposição (3.1.3) temos que $\mathcal{O}_{\mathbb{L}}^*$ é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado. Assim, $d\mathcal{O}_{\mathbb{L}}^* \subseteq \mathcal{O}_{\mathbb{L}}$, onde d é fator comum entre os numeradores dos geradores de $\mathcal{O}_{\mathbb{L}}^*$, o que prova o Corolário. ∎

3.2 Diferente

Nesta seção veremos o conceito de diferente juntamente com suas principais propriedades. Para isso, sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau n, $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A e $\mathcal{O}_{\mathbb{L}}^*$ o codiferente de $\mathcal{O}_{\mathbb{L}}$.

Definição 3.2.1 *O ideal de* $\mathcal{O}_{\mathbb{L}}$ *igual ao inverso do ideal fracionário* $\mathcal{O}_{\mathbb{L}}^*$ *é chamado* **diferente** *de* $\mathcal{O}_{\mathbb{L}}$ *sobre* A *(ou de* $\mathbb{L}$ *sobre* $\mathbb{K}$*) e denotado por* $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ *(ou* $\Delta(\mathbb{L}|\mathbb{K})$*). Em particular, se* $\mathbb{K} = \mathbb{Q}$, *o diferente de* $\mathcal{O}_{\mathbb{L}}$ *sobre* $\mathbb{Z}$ *é chamado de diferente absoluto.*

Observação 3.2.1 *Como* $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$ *segue que* $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ *é um ideal inteiro de* $\mathcal{O}_{\mathbb{L}}$. *Sendo* $\mathcal{O}_{\mathbb{L}}$ *um domínio de Dedekind, pelo Teorema (1.5.2) temos que* $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ *pode ser escrito de modo único como* $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \prod_{i=1}^{g} \mathfrak{p}_i^{s_i}$, *onde* $\mathfrak{p}_i's$ *são ideais primos de* $\mathcal{O}_{\mathbb{L}}$ *e* $s_i \geq 0$ *são inteiros, para* $i = 1, \ldots, g$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Proposição 3.2.1 *Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde $\alpha \in \mathcal{O}_{\mathbb{L}}$ e se $g(x) \in A[x]$ é o polinômio minimal de α sobre $\mathbb{K}$, então $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \mathcal{O}_{\mathbb{L}} g'(\alpha)$ se, e somente se, $\mathcal{O}_{\mathbb{L}} = A[\alpha]$.*

Demonstração: Se $\mathcal{O}_{\mathbb{L}} = A[\alpha]$, temos pelo Teorema (3.1.2), que $\mathcal{O}_{\mathbb{L}}{}^{*} = \frac{1}{g'(\alpha)}\mathcal{O}_{\mathbb{L}}$. Assim $\Delta(\mathcal{O}_{\mathbb{L}}|A) = (\mathcal{O}_{\mathbb{L}}^{*})^{-1} = \left(\frac{1}{g'(\alpha)}\mathcal{O}_{\mathbb{L}}\right)^{-1} = g'(\alpha)\mathcal{O}_{\mathbb{L}}$. Reciprocamente, se $z \in \mathcal{O}_{\mathbb{L}}$, então, existe um polinômio $h(x) \in \mathbb{K}[x]$, de grau menor que $n = [\mathbb{L} : \mathbb{K}]$, tal que $z = h(\alpha)$. Na demonstração do Teorema (3.1.1), vimos que

$$1 = \sum_{k=1}^{n} \frac{g(x)}{g'(\alpha_k)(x - \alpha_k)} = \sum_{k=1}^{n} \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i},$$

onde $\alpha = \alpha_1, \ldots, \alpha_n$, são os conjugados de α sobre $\mathbb{K}$. O polinômio $h_1(x) = \sum_{k=1}^{n} h(\alpha_k) \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i}$ tem grau menor que n e $h_1(\alpha_j) = \sum_{k=1}^{n} h(\alpha_k) \prod_{i \neq k} \frac{\alpha_j - \alpha_i}{\alpha_k - \alpha_i} = h(\alpha_j)$, pois se $k \neq j$ temos que $\prod_{i \neq k} \frac{\alpha_j - \alpha_i}{\alpha_k - \alpha_i} = 0$. Assim, $h(x) = h_1(x)$, pois o polinômio $h(x) - h_1(x)$ tem n raízes. Mas,

$$Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{zg(x)}{g'(\alpha)(x - \alpha)}\right) = Tr_{\mathbb{L}|\mathbb{K}}\left(z \prod_{i \neq k} \frac{x - \alpha_i}{\alpha - \alpha_i}\right) = \sum_{k=1}^{n} h(\alpha_k) \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i} = h(x).$$

Como os coeficientes de $\frac{g(x)}{x - \alpha}$ pertencem a $\mathbb{L}$ e são inteiros sobre A, segue que $\frac{g(x)}{x - \alpha} \in \mathcal{O}_{\mathbb{L}}[x]$, e como $\frac{z}{g'(\alpha)} \in \mathcal{O}_{\mathbb{L}}{}^{*}$ segue que $h(x) = Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{zg(x)}{g'(\alpha_k)(x - \alpha)}\right) \in A[x]$. Assim, $z = h(\alpha) \in A[\alpha]$, e portanto, $\mathcal{O}_{\mathbb{L}} = A[\alpha]$. ∎

Exemplo 3.2.1 *Sejam $A = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. Pelo Exemplo (3.1.1) temos que $\mathcal{O}_{\mathbb{L}}{}^{*} = \frac{1}{2\sqrt{2}}\mathcal{O}_{\mathbb{L}}$. Assim, $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = (\mathcal{O}_{\mathbb{L}}{}^{*})^{-1} = 2\sqrt{2}\mathbb{Z}[\sqrt{2}]$.*

Exemplo 3.2.2 *Sejam $A = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\xi_3)$, onde ξ_3 é raiz cúbica da unidade. O polinômio minimal de ξ_3 é $g(x) = x^2 + x + 1$. Pela Proposição (3.2.1) temos que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = g'(\xi_3)\mathcal{O}_{\mathbb{L}} = (2\xi_3 + 1)\mathbb{Z}[\xi_3]$.*

Observação 3.2.2

1. *Para corpos quadráticos $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados, temos:*

   - *Se $d \equiv 2 (mod\ 4)$ ou $d \equiv 3 (mod\ 4)$, pelo Teorema (2.1.1), temos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}]$ e pela Proposição (3.2.1) temos que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = \mathbb{Z}[\sqrt{d}]g'(\sqrt{d})$, onde $g(x)$ é o polinômio minimal de $\sqrt{d}$ sobre $\mathbb{Q}$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

- *Se $d \equiv 1 (mod\ 4)$, pelo Teorema (2.1.1), temos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e pela Proposição (3.2.1) temos que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]g'(\frac{1+\sqrt{d}}{2})$, onde $g(x)$ é o polinômio minimal de $\frac{1+\sqrt{d}}{2}$ sobre $\mathbb{Q}$.*

2. *Se ξ_m é uma raiz m-ésima primitiva da unidade, então pela Proposição (3.2.1) temos que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = \mathbb{Z}[\xi_m]g(\xi_m)$, onde $g(x)$ é o polinômio minimal de ξ_m sobre $\mathbb{Q}$.*

Exemplo 3.2.3 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\frac{1+\sqrt{5}}{2})$. Pela Observação (3.2.2), $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]g'(\frac{1+\sqrt{5}}{2})$, onde $g(x)$ é o polinômio minimal de $\frac{1+\sqrt{5}}{2}$ sobre $\mathbb{Q}$. Fazendo as contas obtemos $\Delta(\mathcal{O}_{\mathbb{L}}|\mathbb{Z}) = \mathbb{Z}[\frac{1+\sqrt{5}}{5}]\sqrt{5}$.*

Proposição 3.2.2 *Seja $\mathcal{B}$ um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$. Então $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{B}) \subseteq A$ se, e somente se, $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{L}}^* = \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$.*

Demonstração: Se $\mathcal{B} \subset \mathcal{O}_{\mathbb{L}}^*$ então $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{B}) \subseteq A$. Por outro lado, se $x \in \mathcal{O}_{\mathbb{L}}$ e $y \in \mathcal{B}$, temos que $xy \in \mathcal{O}_{\mathbb{L}}\mathcal{B} = \mathcal{B}$. Como $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{B}) \subseteq A$, segue $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A$. Portanto, $\mathcal{B} \subset \mathcal{O}_{\mathbb{L}}^*$. ∎

Lema 3.2.1 *Sejam $\mathcal{A}$, $\mathcal{B}$ ideais fracionários de $\mathbb{L}$. Se para todo $\mathcal{M}$ ideal fracionário de $\mathbb{L}$ tem-se que $\mathcal{M} \subseteq \mathcal{A}$ se, e somente se, $\mathcal{M} \subseteq \mathcal{B}$, então $\mathcal{A} = \mathcal{B}$.*

Demonstração: Se $x \in \mathcal{A}$ então $\mathcal{M} = \langle x \rangle \subset \mathcal{A}$. Assim, $\mathcal{M} \subset \mathcal{B}$, ou seja, $x \in \mathcal{B}$. Logo, $\mathcal{A} \subseteq \mathcal{B}$. De modo análogo, temos que $\mathcal{B} \subseteq \mathcal{A}$. Portanto, $\mathcal{A} = \mathcal{B}$. ∎

Proposição 3.2.3 *Seja $\mathbb{N}$ uma extensão separável de $\mathbb{L}$ de grau finito. Se $\mathcal{O}_{\mathbb{N}}$ e $\mathcal{O}_{\mathbb{L}}$ e A são os anéis de inteiros de $\mathbb{N}$, $\mathbb{L}$ e $\mathbb{K}$, respectivamenete, então*

$$\Delta(\mathcal{O}_{\mathbb{N}}|A) = \mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{N}}|\mathcal{O}_{\mathbb{L}}).$$

Demonstração: Seja $\mathcal{M}$ um ideal fracionário de $\mathcal{O}_{\mathbb{N}}$ tal que $\mathcal{M} \subseteq \Delta(\mathcal{O}_{\mathbb{N}}|\mathcal{O}_{\mathbb{L}})^{-1}$. Pela Proposição (3.2.2), temos que $Tr_{\mathbb{N}|\mathbb{L}}(\mathcal{M}) \subseteq \mathcal{O}_{\mathbb{L}}$. Assim,

$$\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1} \supseteq \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}Tr_{\mathbb{N}|\mathbb{L}}(\mathcal{M}).$$

Como $\mathcal{M} = \mathcal{M}\mathcal{O}_{\mathbb{N}}$ segue que $\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1} \supseteq Tr_{\mathbb{N}|\mathbb{L}}(\mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M})$. Temos também que

$$A \supseteq Tr_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}) \supseteq Tr_{\mathbb{L}|\mathbb{K}}(Tr_{\mathbb{N}|\mathbb{L}}(\mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1})\mathcal{M}) = Tr_{\mathbb{N}|\mathbb{K}}(\mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M}).$$

Novamente, pela Proposição (3.2.2), temos que

$$\mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M} \subseteq \Delta(\mathcal{O}_{\mathbb{N}}|A)^{-1} \text{ e que } \mathcal{M} \subseteq T_{\mathbb{N}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{N}}|A)^{-1}).$$

Pelo Lema (3.2.1) segue que $\Delta(\mathcal{O}_{\mathbb{N}}|\mathcal{O}_{\mathbb{L}})^{-1} = \mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{N}}|A)^{-1}$. Portanto, $\Delta(\mathcal{O}_{\mathbb{N}}|A) = \mathcal{O}_{\mathbb{N}}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{N}}|\mathcal{O}_{\mathbb{L}})$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Definição 3.2.2 *Sejam $\mathbb{K}$ um corpo de números, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n, e $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$ os anéis de inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$, $S = \mathcal{O}_{\mathbb{K}} - \mathfrak{p}$, $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. O diferente $\Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}})$ é chamado de* **diferente de $\mathbb{L}|\mathbb{K}$ sobre $\mathfrak{p}$** *e é denotado por $\Delta_{\mathfrak{p}}(\mathbb{L}|\mathbb{K})$.*

Proposição 3.2.4 *Com as notações da Definição (3.2.2), temos que $\mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}) = \Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}})$.*

Demonstração: Se $x \in \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$ então x é da forma $\frac{y}{s}$, com $y \in \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$ e $s \in S$. Seja $z \in (\mathcal{O}'_{\mathbb{L}})^*$, onde $(\mathcal{O}'_{\mathbb{L}})^*$ é o codiferente do $\mathcal{O}'_{\mathbb{K}}$-módulo $\mathcal{O}'_{\mathbb{L}}$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(z\mathcal{O}'_{\mathbb{L}}) \subset \mathcal{O}'_{\mathbb{K}}$. Sendo $\mathcal{O}_{\mathbb{L}}$ um $\mathcal{O}_{\mathbb{K}}$-módulo finitamente gerado, então considere $\{t_1, \ldots, t_m\}$ um sistema de geradores. Seja $Tr_{\mathbb{L}|\mathbb{K}}(zt_i) = \frac{a_i}{s_i}$, com $a_i \in \mathcal{O}_{\mathbb{K}}$ e $s_i \in S$. Se $s_0 = s_1 \ldots s_m \in S$ então

$$Tr_{\mathbb{L}|\mathbb{K}}(zs_0t_i) = s_0 Tr_{\mathbb{L}|\mathbb{K}}(zt_i) \in \mathcal{O}_{\mathbb{K}},$$

para $i = 1, 2, \ldots, n$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(zs_0\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{O}_{\mathbb{K}}$ e portanto $zs_0 \in \mathcal{O}^*_{\mathbb{L}}$, isto é, $yzs_0 \in \mathcal{O}_{\mathbb{L}}$, pois $y \in \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$. Logo,

$$xz = \frac{yz}{s} = \frac{yzs_0}{ss_0} \in \mathcal{O}'_{\mathbb{L}}$$

o que implica que $x \in \Delta(\mathcal{O}'_{\mathbb{L}}|A')$. Assim, $\mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}) \subseteq \Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}})$. Por outro lado, seja $x \in \Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}})$. Sendo $\mathcal{O}^*_{\mathbb{L}}$ um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}^*_{\mathbb{L}}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo finitamente gerado. Seja $\{z_1, \ldots, z_m\}$ um sistema de geradores do $\mathcal{O}_{\mathbb{K}}$-módulo $\mathcal{O}^*_{\mathbb{L}}$. Temos que $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{O}_{\mathbb{K}}$, para $i = 1, \ldots, n$. Como $S \subseteq \mathbb{K}$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}'_{\mathbb{L}}) \subseteq \mathcal{O}'_{\mathbb{K}}$, ou seja, $z_i \in (\mathcal{O}'_{\mathbb{L}})^*$. Assim,

$$xz_i \in \mathcal{O}'_{\mathbb{L}}, \text{ ou seja } xz_i = \frac{b_i}{s_i} \text{ com } b_i \in \mathbb{L} \text{ e } s_i \in S.$$

Se $s = s_1 \ldots s_m \in S$, então $sxz_i \in \mathcal{O}_{\mathbb{L}}$, para todo $i = 1, \ldots, m$ e assim $sx\mathcal{O}^*_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}$. Portanto $sx \in \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$ e $x \in \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$. Logo, $\Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}}) \subseteq \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$. Portanto, $\mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}) = \Delta(\mathcal{O}'_{\mathbb{L}}|\mathcal{O}'_{\mathbb{K}})$. ∎

Lema 3.2.2 *Sejam $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, $S = \mathcal{O}_{\mathbb{K}} - \mathfrak{p}$, $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Se $\{x'_1, \ldots, x'_n\}$ é uma base do $\mathcal{O}'_{\mathbb{K}}$-módulo $\mathcal{O}'_{\mathbb{L}}$ então $\mathcal{O}'_{\mathbb{K}}D_{\mathbb{L}|\mathbb{K}}(x'_1, \ldots, x'_n) = \mathcal{O}'_{\mathbb{K}}N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$.*

Demonstração: Pelo Teorema (1.7.1) temos que $\mathcal{O}'_{\mathbb{L}}$ é um domínio de Dedekind. Pela Proposição (1.7.2), temos que $\mathcal{O}'_{\mathbb{L}}$ tem somente um número finito de ideais primos e pela Proposição (2.3.4) temos que $\mathcal{O}'_{\mathbb{L}}$ é um domínio de ideais principais. Se $(\mathcal{O}'_{\mathbb{L}})^*$ é o codiferente

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

do $\mathcal{O}'_{\mathbb{K}}$-módulo $\mathcal{O}'_{\mathbb{L}}$ livre temos que $(\mathcal{O}'_{\mathbb{L}})^*$ é um ideal fracionário de $\mathcal{O}'_{\mathbb{L}}$. Logo, existe $y \in \mathbb{L}$, $y \neq 0$, tal que $(\mathcal{O}'_{\mathbb{L}})^* = \mathcal{O}_{\mathbb{L}}{}'y$. Assim, pela Proposição (3.2.4), temos que

$$\mathcal{O}'_{\mathbb{L}} y^{-1} = \Delta(\mathcal{O}_{\mathbb{L}}{}'|\mathcal{O}'_{\mathbb{K}}) = \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}).$$

Se $\{x'_1, \ldots, x'_n\}$ é uma base de $\mathcal{O}'_{\mathbb{K}}$-módulo $\mathcal{O}'_{\mathbb{L}}$ então $\{yx'_1, \ldots, yx'_n\}$ é uma base de $(\mathcal{O}'_{\mathbb{L}})^*$. Pela Proposição (3.1.2), temos que $(\mathcal{O}'_{\mathbb{L}})^*$ tem uma base complementar $\{(x'_1)^*, \ldots, (x'_n)^*\}$ sobre $\mathcal{O}'_{\mathbb{K}}$. Pela Proposição (1.1.2) e pelo Lema (1.4.2), temos que

$$D_{\mathbb{L}/\mathbb{K}}((x'_1)^*, \ldots, (x'_n)^*) = D_{(\mathcal{O}_{\mathbb{L}}{}')^*/\mathcal{O}'_{\mathbb{K}}}((x'_1)^*, \ldots, (x'_n)^*)$$

e $D_{\mathbb{L}/\mathbb{K}}(yx'_1, \ldots, yx'_n) = D_{((\mathcal{O}'_{\mathbb{L}})^*/\mathcal{O}'_{\mathbb{K}})}(y(x'_1)^*, \ldots, y(x'_n)^*)$ são elementos associados de $\mathcal{O}'_{\mathbb{K}}$. Mas

$$D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n) D_{\mathbb{L}/\mathbb{K}}((x'_1)^*, \ldots, (x'_n)^*) = 1$$

e $D_{\mathbb{L}/\mathbb{K}}(yx'_1, \cdots, yx'_n) = [N(y)]^2 \; D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n)$. Portanto, $[N(y)]^2[D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n)]^2$ é uma unidade de $\mathcal{O}'_{\mathbb{K}}$. Portanto, $\mathcal{O}'_{\mathbb{K}} D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n) = \mathcal{O}'_{\mathbb{K}} N(y^{-1})$. Seja $y = \dfrac{z}{a}$ onde $z \in \mathcal{O}_{\mathbb{K}}$, $a \in S$. Como $\mathcal{O}'_{\mathbb{L}} y^{-1} = \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$ segue que

$$\mathcal{O}'_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}} a) = \mathcal{O}'_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}} z \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})).$$

Logo, $\mathcal{O}_{\mathbb{L}} a = \mathcal{O}_{\mathbb{L}} z \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})$. Assim, $N(\mathcal{O}_{\mathbb{L}} a) = N(\mathcal{O}_{\mathbb{L}} z) N(\Delta(\mathcal{O}_{\mathbb{L}}|A))$, e portanto $a^n \mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}} N(z) N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$. Assim, $a^n \mathcal{O}'_{\mathbb{K}} = \mathcal{O}'_{\mathbb{K}} N(z) N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$ e portanto $N(a)\mathcal{O}'_{\mathbb{K}} N(z^{-1})$ $= \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$. Logo, $N(az^{-1})\mathcal{O}'_{\mathbb{K}} = \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$, e assim,

$$N(y^{-1})\mathcal{O}'_{\mathbb{K}} = \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})).$$

Portanto, $\mathcal{O}'_{\mathbb{K}} D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n) = \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$. ∎

Teorema 3.2.1 *Com as mesmas notações do Lema (3.2.2), temos que* $N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})) = D_{\mathbb{L}/\mathbb{K}}$.

Demonstração: Sejam $\{x_1, \ldots, x_n\}$ uma $\mathbb{K}$-base de $\mathbb{L}$ contida em $\mathcal{O}_{\mathbb{L}}$ e $\{x'_1, \ldots, x'_n\}$ uma base do $\mathcal{O}'_{\mathbb{K}}$-módulo $\mathcal{O}'_{\mathbb{L}}$. Assim $x_j = \sum_{i=1}^{n} a'_{ij} x'_i$, com $a'_{ij} \in \mathcal{O}'_{\mathbb{K}}$, para $j = 1, \ldots, n$. Assim, $D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) \in \mathcal{O}'_{\mathbb{K}} D_{\mathbb{L}/\mathbb{K}}(x'_1, \ldots, x'_n)$. Pelo Lema (3.2.2), temos que

$$D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) \subseteq \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})),$$

e isto implica que $D_{\mathbb{L}/\mathbb{K}} \subseteq \bigcap \mathcal{O}'_{\mathbb{K}} N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}))$. Pela Proposição (1.7.3), temos que

$$D_{\mathbb{L}/\mathbb{K}} \subseteq N(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}})).$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Reciprocamente, sejam $D_{\mathbb{L}|\mathbb{K}} = \mathfrak{p}^s\mathcal{A}$ e $N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K})) = \mathfrak{p}^{s'}\mathcal{B}$, onde $\mathcal{A}, \mathcal{B}$ são ideais de $\mathcal{O}_\mathbb{K}$, não múltiplos de $\mathfrak{p}$. Devemos mostrar que $s \leq s'$, pois se é verdadeiro para todo ideal primo $\mathfrak{p} \neq 0$ de $\mathcal{O}_\mathbb{K}$, temos que $D_{\mathbb{L}/\mathbb{K}}$ divide $N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K}))$, ou seja, $N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K})) \subseteq D_{\mathbb{L}|\mathbb{K}}$. Para todo ideal primo $\mathfrak{p} \neq 0$ de $\mathcal{O}_\mathbb{K}$, escolhemos uma base $\{x_1', \ldots, x_n'\}$ do $\mathcal{O}_\mathbb{K}'$-módulo $\mathcal{O}_\mathbb{L}'$. Multiplicando por um elemento conveniente de S temos que cada $x_i' \in \mathcal{O}_\mathbb{L}$. Seja $\mathcal{O}_\mathbb{K}D_{\mathbb{L}/\mathbb{K}}(x_1', \ldots, x_n') = \mathfrak{p}^r\mathcal{I}$, onde $\mathcal{I}$ é um ideal $\mathcal{O}_\mathbb{K}$ não múltiplo de $\mathfrak{p}$. Pelo Corolário (1.7.2), temos que

$$\mathcal{O}_\mathbb{K}'D_{\mathbb{L}/\mathbb{K}}(x_1', \ldots, x_n') = (\mathcal{O}_\mathbb{K}'\mathfrak{p})^r$$

e pelo Lema (3.2.2), temos que $\mathcal{O}_\mathbb{K}'D_{\mathbb{L}/\mathbb{K}}(x_1', \ldots, x_n') = \mathcal{O}_\mathbb{K}'N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K})) = (\mathcal{O}_\mathbb{K}'\mathfrak{p})^{s'}$. Assim, $s' = r$. Como $D_{\mathbb{L}/\mathbb{K}} \supset \mathcal{O}_\mathbb{K}D_{\mathbb{L}/\mathbb{K}}(x_1', \ldots, x_n') = \mathfrak{p}^{s'}\mathcal{I}$ segue que $D_{\mathbb{L}/\mathbb{K}}$ divide $\mathfrak{p}^{s'}\mathcal{I}$, e então $s \leq s'$. Assim,

$$N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K})) \subseteq D_{\mathbb{L}/\mathbb{K}}.$$

Portanto, $N(\Delta(\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K})) = D_{\mathbb{L}/\mathbb{K}}$. ■

Proposição 3.2.5 *Se $\mathbb{K}$ é uma extensão cíclica de grau primo $n > 2$ e $p > n$ é o único primo que ramifica em $\mathbb{K}$, então o discriminante de $\mathbb{K}$ é $D_\mathbb{K} = p^{n-1}$.*

Demonstração: Como p é totalmente ramificado em $\mathbb{K}$ segue que $p\mathcal{O}_\mathbb{K} = \mathfrak{p}^n$. Como $p \nmid n$, segue que $\mathfrak{p}^{n-1} \mid \Delta(\mathcal{O}_\mathbb{K}|\mathbb{Q})$, mas $\mathfrak{p}^n \nmid \Delta(\mathcal{O}_\mathbb{K}|\mathbb{Q})$. Agora, como $\Delta(\mathcal{O}_\mathbb{K}|\mathbb{Q}) = \mathfrak{p}^{n-1}$ e $N(\Delta(\mathcal{O}_\mathbb{K}|\mathbb{Q})) = |D_\mathbb{K}|$ segue que $N(\Delta(\mathcal{O}_\mathbb{K}|\mathbb{Q})) = |D_\mathbb{K}| = p^{n-1}$. ■

unesp

Capítulo 4

Reticulados e ideais reticulados

Intuitivamente, entende-se por reticulado um subconjunto discreto do $\mathbb{R}^n$ que tem a estrutura de um $\mathbb{Z}$-módulo de posto finito n. Neste capítulo apresentamos as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e homomorfismo canônico. Através do homomorfismo canônico obtemos um método para gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel de inteiros do corpo de números. Apresentamos também o conceito de ideais reticulados. Usando esta teoria, veremos formas de se obter reticulados rotacionados no $\mathbb{R}^n$ que são tão bons quanto os já conhecidos. Os resultados aqui mencionados podem ser encontrados nas referências [8], [9], [11], [12], [13], [14] e [15].

4.1 Reticulados

Nesta seção apresentamos o conceito de reticulado, enfocando suas principais propriedades.

Definição 4.1.1 *Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subset \mathbb{K}$ um anel e $v_1, \ldots, v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$, com $m \leq n$. Chama-se* **reticulado** *com base $\beta = \{v_1, \ldots, v_m\}$ ao conjunto de elementos de V da forma*

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \text{ com } a_i \in A \right\},$$

que será denotado por $\mathcal{H}_\beta$.

Definição 4.1.2 *Seja $\mathcal{H}_\beta \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = \{v_1, \ldots, v_m\}$. O conjunto*

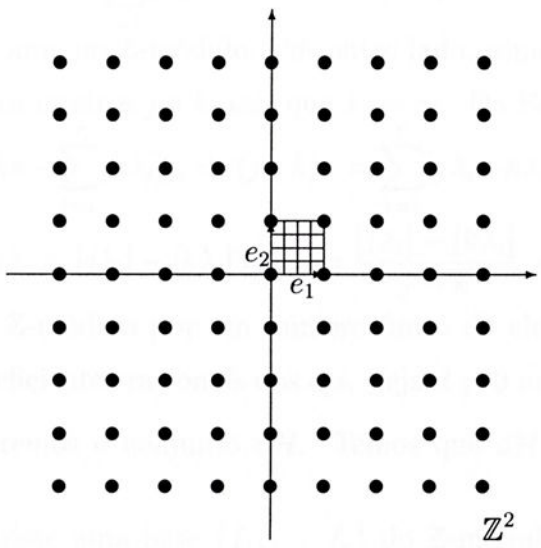
$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^{m} \lambda_i v_i, 0 \leq \lambda_i < 1 \right\},$$

unesp

é chamado de **região fundamental** *de $\mathcal{H}_\beta$, com relação a base $\{v_1, \ldots, v_m\}$.*

Se $\mathcal{H}_\beta$ é um reticulado com base $\beta = \{v_1, \ldots, v_m\}$ e se $e_1, \ldots, e_m$ são elementos quaisquer de $\mathcal{H}_\beta$, então $e_i = \sum_{j=1}^{m} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Uma condição necessária e suficiente para que $\{e_1, \ldots, e_m\}$ seja uma base de $\mathcal{H}_\beta$ é que $det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Exemplo 4.1.1 *$\mathcal{H}_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.*



Definição 4.1.3 *Um subconjunto $\mathcal{H}$ do $\mathbb{R}^n$ é* **discreto** *se para qualquer subconjunto compacto (fechado e limitado) K do $\mathbb{R}^n$, tivermos $\mathcal{H} \cap \mathcal{K}$ finito.*

Exemplo 4.1.2 *$\mathbb{Z}^n$ é um exemplo de subconjunto discreto do $\mathbb{R}^n$.*

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

Teorema 4.1.1 *Se $\mathcal{H}$ é um subgrupo discreto do $\mathbb{R}^n$, então $\mathcal{H}$ é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

Demonstração: Seja $\beta = \{e_1, \ldots, e_r\}$ um conjunto de vetores de $\mathcal{H}$ que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível, com $r \leq n$. Considere 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, $\mathcal{P}_\beta \cap \mathcal{H}$ é finito, pois $\mathcal{H}$ é discreto. Se

unesp

$x \in \mathcal{H}$, então pela maximalidade de r, segue que $\{x, e_1, \ldots, e_r\}$ é linearmente dependente. Logo, existem $\lambda_i \in \mathbb{R}$, para $i = 1, \ldots, r$, não todos nulos, tal que $x = \sum_{i=1}^{r} \lambda_i e_i$. Para cada $j \in \mathbb{N}$, seja

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \in \mathcal{H}, \tag{4.1}$$

onde $[k]$ denota o maior inteiro menor ou igual a k. Assim, $x_j = j\sum_{i=1}^{r} \lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i \in \mathcal{P}_e \cap \mathcal{H}$. Dessa forma, tomando $j = 1$ na Equação (4.1), temos que $x_1 = x - \sum_{i=1}^{r} [\lambda_i] e_i$, ou seja, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$. Assim, como $x_1 \in \mathcal{P}_e \cap \mathcal{H}$ e este é finito, segue que $\mathcal{H}$ é finitamente gerado como um $\mathbb{Z}$-módulo. Por outro lado, como $\mathcal{P}_e \cap \mathcal{H}$ é finito e como $\mathbb{N}$ é infinito, segue que existem inteiros j e k, tais que $x_j = x_k$. Da Equação (4.1), segue que $x_j = x_k \Rightarrow jx - \sum_{i=1}^{r} [j\lambda_i] e_i = kx - \sum_{i=1}^{r} [k\lambda_i] e_i \Rightarrow (j-k)x = \sum_{i=1}^{r} [j\lambda_i - k\lambda_i] e_i \Rightarrow (j-k) \sum_{i=1}^{r} \lambda_i e_i = \sum_{i=1}^{r} ([j\lambda_i] - [k\lambda_i]) e_i \Rightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \Rightarrow \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{j-k}$, ou seja, $\lambda_i \in \mathbb{Q}$. Assim, como $\mathcal{H}$ é gerado como um $\mathbb{Z}$-módulo por um número finito de elementos, segue que são combinações lineares com coeficientes racionais dos $e_i's$. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto $d\mathcal{H}$. Temos que $d\mathcal{H} \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Daí, pelo Teorema (1.1.1) segue que existe uma base $\{f_1, \ldots, f_r\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z} e_i$ e inteiros α_i, tal que $\{\alpha_1 f_1, \ldots, \alpha_r f_r\}$ gera $d\mathcal{H}$ sobre $\mathbb{Z}$. Como o $\mathbb{Z}$-módulo $d\mathcal{H}$ tem o mesmo posto de $\mathcal{H}$ e como $\sum_{i=1}^{r} \mathbb{Z} e_i \subset \mathcal{H}$, segue que o posto de $d\mathcal{H} \leq r$. Pela maximalidade de r, decorre que o posto de $d\mathcal{H}$ é r e os $\alpha_i's$ são não nulos pois, caso contrário $d\mathcal{H}$ não teria posto r. Assim os $f_i's$ são linearmente independentes sobre $\mathbb{R}$ e, consequentemente, $\mathcal{H}$ também é gerado por r vetores linearmente independentes sobre $\mathbb{R}$. ∎

Observação 4.1.1 *Segue do Teorema (4.1.1) que qualquer subgrupo discreto do $\mathbb{R}$ é um reticulado.*

Definição 4.1.4 *Seja $\mathcal{H} \subset \mathbb{R}^n$ um reticulado, $v = \{v_1, \ldots, v_n\}$ uma base de $\mathcal{H}$ e $\mathcal{P}_v$ a região fundamental. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \ldots, n$, definimos o* **volume da região**

fundamental $\mathcal{P}_v$ *como o módulo do determinante da matriz*

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

que denotamos por $Vol(\mathcal{P}_v)$.

Proposição 4.1.1 *O volume da região fundamental* $Vol(\mathcal{P}_v)$ *independe da base* v *de* $\mathcal{H}$.

Demonstração: Se $\{f_1, \ldots, f_n\}$ é outra base de $\mathcal{H}$, então $f_i = \sum_{i=1}^{n} \alpha_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Assim, $\text{Vol}(\mathcal{P}_f) = |det(\alpha_{ij})|\ \text{Vol}(\mathcal{P}_v)$. Como a matriz de mudança de base (a_{ij}) é inversível, segue que $det(a_{ij}) = \pm 1$. Portanto, $\text{Vol}(\mathcal{P}_f) = \text{Vol}(\mathcal{P}_v)$. ∎

Note que, sendo β' uma outra base de $\mathcal{H}_\beta$, segue que $\text{Vol}(\mathcal{H}_\beta) = \text{Vol}(\mathcal{H}_{\beta'})$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido definir o volume de $\mathcal{H}_\beta$ como sendo o volume de uma região fundamental.

Definição 4.1.5

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 interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

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

3. *Dado um empacotamento no* $\mathbb{R}^n$, *associado a um reticulado* $\mathcal{H}_\beta$, *com* $\mathbb{Z}$*-base* $\{v_1, \ldots, v_n\}$, *definimos a* **densidade de empacotamento** *como sendo a proporção do espaço* $\mathbb{R}^n$ *coberto pela união das esferas.*

Estamos interessados no empacotamento associado a um reticulado $\mathcal{H}_\beta$ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado $\mathcal{H}_\beta$ é um conjunto finito, de onde segue que o número $\mathcal{H}_{\beta_{min}} = \min\{|\lambda|; \lambda \in \mathcal{H}_\beta, \lambda \neq 0\}$ está bem definido e $(\mathcal{H}_{\beta_{min}})^2$ é chamado de **norma mínima**. Observamos que $\rho = \frac{\mathcal{H}_{\beta_{min}}}{2}$ é o maior raio para o qual é

unesp

possível distribuir esferas centradas nos pontos de $\mathcal{H}_\beta$ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.
Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de $\mathcal{H}_\beta$ é dada por

$$\Delta(\mathcal{H}_\beta) = \frac{\text{volume da região coberta pelas esferas}}{\text{volume da região fundamental}} = \frac{\text{Vol}(\mathcal{B}(\rho))}{\text{Vol}(\mathcal{H}_\beta)} = \frac{\text{Vol}(\mathcal{B}(1))\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$

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

$$\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$

Exemplo 4.1.3 *Se $\mathcal{H}_\beta = \mathbb{Z}^2$ com base $(1,0)$ e $(0,2)$, temos que $\rho = 1/2$, $Vol(\mathcal{B}(1)) = \pi 1 = \pi$, o volume do reticulado é $Vol(\mathcal{H}_\beta) = 1 \times 2 = 2$, a densidade de empacotamento é*

$$\Delta(\mathcal{H}_\beta) = Vol(\mathcal{B}(1)).\frac{\rho^2}{Vol(\mathcal{H}_\beta)} = \pi\frac{1}{4}.\frac{1}{2} = \frac{\pi}{8}$$

e a densidade de centro é $\delta(\mathcal{H}_\beta) = 1/8$.

Um dos problemas de empacotamento esférico de um reticulado $\mathcal{H}_\beta$ do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade.

4.2 Homomorfismo canônico

Nesta seção apresentamos o método de Minkowiski para a geração de reticulados via ideais do anel de inteiros de um corpo de números.

Seja $\mathbb{K}$ um corpo de números de grau n. Existem n monomorfismos distintos $\sigma_j : \mathbb{K} \longrightarrow \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$, diz-se que σ_j é **real**, caso contrário, σ_j é dito **imaginário**. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um **corpo totalmente real** e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um **corpo totalmente imaginário**. Se $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$ temos que $\alpha \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_j = \sigma_k$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos reordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ sejam os monomorfismos imaginários. Assim, $n = r_1 + 2r_2$ e para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1+2r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2},$$

é um homomorfismo injetivo de anéis, chamado de **homomorfismo canônico** ou **homomorfismo de Minkowiski**, de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, e este homomorfismo também pode ser visto como

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

onde $\Re$ representa a parte real e $\Im$ representa a parte imaginária do número complexo.

Exemplo 4.2.1 *Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, 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, $r_1 = 0$ e $r_2 = 1$. 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 4.2.2 *Sejam o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\xi_3)$, onde $\xi_3 = e^{\frac{2\pi i}{3}}$ e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Como $\mathbb{K}$ é um corpo totalmente complexo, temos que $r_1 = 0$ e $r_2 = 1$. Os 2 monomorfismos são dados por $\sigma_1(\xi_3) = \xi_3$, $\sigma_2(\xi_3) = \xi_3^2 = \xi_3^{-1}$. Se $x = a + b\xi_3 \in \mathbb{K}$, com a, $b \in \mathbb{Q}$, temos que $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x))$.*

Exemplo 4.2.3 *Considere agora o corpo ciclotômico totalmente complexo $\mathbb{K} = \mathbb{Q}(\xi_7)$, onde $\xi_7 = e^{\frac{2\pi i}{7}}$. O grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ é dado por $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, onde $\sigma_j(\xi_7) = \xi_7^j$. Se $x = a_0 + a_1\xi_7 + a_2\xi_7^2 + a_3\xi_7^3 + a_4\xi_7^4 + a_5\xi_7^5 + a_6\xi_7^6 \in \mathbb{K}$, com $a_i \in \mathbb{Q}$ para $i = 1, 2, \ldots, 6$, temos que $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \Re\sigma_2(x), \Im\sigma_2(x), \Re\sigma_3(x), \Im\sigma_3(x))$, pois $r_1 = 0$ e $r_2 = 3$.*

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal nos resultados que seguem.

Proposição 4.2.1 *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*

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

onde r_2 é o número de pares de monomorfismos imaginários.

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

$$(\sigma_1(x_j), \ldots, \sigma_{r_1}(x_j), \Re\sigma_{r_1+1}(x_j), \Im\sigma_{r_1+1}(x_j), \ldots, \Re\sigma_{r_1+r_2}(x_j), \Im\sigma_{r_1+r_2}(x_j)). \tag{4.2}$$

Agora calculamos o determinante D da matriz que tem a j-ésima coluna dada pela Equação (4.2) fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z+\overline{z})$, $\Im(z) = \frac{1}{2i}(z-\overline{z})$ para z em $\mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)$-ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)$-ésima coluna da sua posterior, para $l = 1, \ldots, r_2$. Assim,

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

$$D = \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2} . M_1,$$

onde

$$M_1 = \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)} & \ldots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \ldots & \sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)} & \ldots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)} & \ldots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)} & \ldots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$D = \left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2} 2^{r_2}.M_2$$

onde

$$M_2 = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_j) & \dots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)} & \dots & \sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)} & \dots & \sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)} & \dots & \sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)} & \dots & \sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}.$$

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

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

$$D = (2i)^{-r_2}\det(\sigma_j(x_k)).$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Portanto, $D = (2i)^{-r_2}\det(\sigma_j(x_k))$, para $j, k = 1, \ldots, n$. Como $(x_j)_{1\leq j\leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue da Proposição (1.4.3), 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 $\{x_1, \ldots, x_n\}$ ser uma $\mathbb{Z}$-base de M, temos $m = \sum_{j=1}^{n} a_j x_j$, 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, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}$. Logo, $Vol(\sigma_{\mathbb{K}}(M)) = |D| = 2^{-r_2}|\det_{1\leq j,k\leq n}(\sigma_j(x_k))|$. ■

Exemplo 4.2.4 *Tome* $\mathbb{K} = \mathbb{Q}(\sqrt{7})$, *e* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{7}\,]$ *o seu anel dos inteiros com* $\mathbb{Z}$*-base* $\{1, \sqrt{7}\}$. *Como* $\mathbb{K}$ *é totalmente real, segue que* $r_2 = 0$, *e portanto*

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

Assim, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{7}\,]) \subseteq \mathbb{R}^2$ *é um reticulado de posto* 2 *do* $\mathbb{R}^2$, *cujo volume é* $2\sqrt{7}$.

Exemplo 4.2.5 *Tome* $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, *e* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ *o seu anel dos inteiros com* $\mathbb{Z}$*-base* $\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$. *Como* $\mathbb{K}$ *é totalmente imaginário, então* $r_2 = 1$, *e portanto*

$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2}\left|\det \begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix}\right| = \frac{1}{2}\sqrt{7}.$$

Assim, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{R}^2$ *é um reticulado de posto 2 de* $\mathbb{R}^2$ *com volume* $\frac{1}{2}\sqrt{7}$.

Exemplo 4.2.6 *Tome* $\mathbb{K} = \mathbb{Q}(\xi_6)$, *onde* $\xi_6 = e^{\frac{2\pi i}{6}}$ *e* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_6]$ *o seu anel dos inteiros com* $\mathbb{Z}$*-base* $\{1, \xi_6\}$. *Como* $\mathbb{K}$ *é totalmente imaginário, segue que* $r_2 = 1$, *e portanto*

$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2}\left|\det \begin{pmatrix} 1 & \xi_6 \\ 1 & \overline{\xi_6} \end{pmatrix}\right| = \frac{1}{2}\left|\frac{1}{2} - \frac{i\sqrt{3}}{2} - \left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right| = \frac{1}{2}\sqrt{3}.$$

A imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\xi_6])$ *é um reticulado de posto* 2 *no* $\mathbb{R}^2$, *cujo volume é* $\frac{\sqrt{3}}{2}$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Proposição 4.2.2 *Seja $\mathbb{K}$ um corpo de números de grau n. Se $D_{\mathbb{K}}$ é o discriminante absoluto 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, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathfrak{a})$ são reticulados, com respectivos volumes,*

$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} \text{ e } Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a}),$$

onde r_2 é o número de pares de monomorfismos imaginários e $N(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$.

Demonstração: Pelo Corolário (1.3.4) temos que $\mathfrak{a}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n. Assim pela Proposição (4.2.1), temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ e $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|\det(\sigma_i(x_k))|$, onde $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. Pela Proposição (1.4.3) temos que $D_{\mathbb{K}} = \det(\sigma_i(x_k))^2$, e assim, $|D_{\mathbb{K}}|^{\frac{1}{2}} = |\det(\sigma_i(x_k))|$ e, portanto, $Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}$. Para a segunda fórmula, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de índice $N(\mathfrak{a})$ uma vez que $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}$ é isomorfo a $\frac{\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})}{\sigma_{\mathbb{K}}(\mathfrak{a})}$. Além disso, como um domínio fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de $N(\mathfrak{a})$ cópias de um domínio fundamental de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, segue que $Vol(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})$.

■

Se $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, a matriz geradora de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

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

Como $\mathfrak{a}$ é um $\mathbb{Z}$-módulo livre de posto n sobre $\mathcal{O}_{\mathbb{K}}$, existe uma base $\{x_1, x_2, \ldots, x_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros positivos $\{q_1, q_2, \ldots, q_n\}$ tais que $\{x_1q_1, x_2q_2, \ldots x_nq_n\}$ é uma base de $\mathfrak{a}$. Assim, a matriz geradora de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é dada por

$$G_1 = \begin{pmatrix} q_1\sigma_1(x_1) & \cdots & q_1\sigma_{r_1}(x_1) & q_1\Re\sigma_{r_1+1}(x_1) & q_1\Im\sigma_{r_1+1}(x_1) & \cdots & q_1\Re\sigma_{r_1+r_2}(x_1) & q_1\Im\sigma_{r_1+r_2}(x_1) \\ q_2\sigma_1(x_2) & \cdots & q_2\sigma_{r_1}(x_2) & q_2\Re\sigma_{r_1+1}(x_2) & q_2\Im\sigma_{r_1+1}(x_2) & \cdots & q_2\Re\sigma_{r_1+r_2}(x_2) & q_2\Im\sigma_{r_1+r_2}(x_2) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ q_n\sigma_1(x_n) & \cdots & q_n\sigma_{r_1}(x_n) & q_n\Re\sigma_{r_1+1}(x_n) & q_n\Im\sigma_{r_1+1}(x_n) & \cdots & q_n\Re\sigma_{r_1+r_2}(x_n) & q_n\Im\sigma_{r_1+r_2}(x_n) \end{pmatrix}.$$

Em consequência das Proposições (4.2.1) e (4.2.2), temos que a densidade de centro destes reticulados é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{a})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{a})}, \tag{4.3}$$

unesp

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

Proposição 4.2.3 *Se $\mathbb{K}$ é um corpo de números e $x \in \mathbb{K}$, então*

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

onde

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

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

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

Como

$$\Re(\sigma_k(x))^2 + \Im(\sigma_k(x))^2 = \sigma_k(x)\overline{\sigma_k(x)} = \sigma_k(x\overline{x}), \quad \text{para} r_1 + 1 \leq k \leq r_1 + r_2,$$

segue que

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

Se $r_1 = 0$, então

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

pois sendo $\overline{\sigma}$ a conjugação complexa, temos que $\sigma_{r_2+j}(x\overline{x}) = (\overline{\sigma} \circ \sigma_j)(x\overline{x}) = \sigma_j(x\overline{x})$, para $j = 1, \ldots, r_2$. Logo,

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

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

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

Se $r_2 = 0$, então

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

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

e como $\sigma_i(x) = (\overline{\sigma} \circ \sigma_i)(x) = \sigma_i(\overline{x})$ segue que $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = (\sigma_i(x))^2$ e assim, $|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x\overline{x}) + \cdots + \sigma_{r_1}(x\overline{x})$. Portanto,

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

e isto conclui a demonstração. ■

Observação 4.2.1 *Se $\mathbb{K}$ é um corpo de números e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, podemos reescrever o raio de empacotamento do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ da seguinte forma:*

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{1}{2} min\{|\sigma_{\mathbb{K}}(x)|,\ x \in \mathfrak{a},\ x \neq 0\} = \frac{1}{2} min\left\{\sqrt{c_{\mathbb{K}} Tr(x\overline{x})},\ x \in \mathfrak{a},\ x \neq 0\right\}.$$

Fazendo $t_{\mathfrak{a}} = min\{Tr(x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$ temos que:

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

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{\sqrt{t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\sqrt{\frac{t_{\mathfrak{a}}}{4}}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.$$

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

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{2^{\frac{n}{2}}\left(\frac{\sqrt{\frac{1}{2}t_{\mathfrak{a}}}}{2}\right)^n}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{2^{\frac{n}{2}} t_{\mathfrak{a}}^{\frac{n}{2}}}{2^{\frac{3n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{2^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{(\sqrt{4})^n}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \frac{\frac{t_{\mathfrak{a}}^{\frac{n}{2}}}{4^{\frac{n}{2}}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})} = \\ &= \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|D_{\mathbb{K}}|^{\frac{1}{2}} N(\mathfrak{a})}.\end{aligned}$$

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

Exemplo 4.2.7 *Se $\mathbb{K} = \mathbb{Q}(i)$ então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$ e $D_{\mathbb{K}} = -4$. Se $x = a + bi \in \mathcal{O}_{\mathbb{K}}$, então $x\overline{x} = (a+bi)(a-bi) = a^2 - abi + abi + b^2 = a^2 + b^2$, $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = 2(a^2+b^2)$ e $t_{\mathcal{O}_{\mathbb{K}}} = 2$, para $a = 1$ e $b = 0$. Assim*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{\left(\frac{2}{4}\right)}{\sqrt{4}} = \frac{\left(\frac{1}{2}\right)}{2} = \frac{1}{4} = 0,25.$$

unesp

4.3 Ideais reticulados

Nesta seção veremos o conceito de ideais reticulados e suas principais propriedades.

Definição 4.3.1 *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.*

Definição 4.3.2 *Seja* $\{v_1, v_2, \ldots, v_n\}$ *uma base de* L*. A matriz que representa a forma bilinear* b *é dada por* $(b(v_i, v_j))_{i,j=1}^{n}$*. O* **determinante** *de* b *é o determinante da matriz de* b *em alguma base de* L*.*

Sobre os números reais, b pode ser diagonalizada, e é isomorfa à soma ortogonal de r cópias de $\langle 1 \rangle$ e s cópias de $\langle -1 \rangle$, para inteiros não negativos r e s.

Definição 4.3.3 *A* **assinatura** *de* b *é denotada por* $sign(b)$ *e é definida pelo par* $sign(b) = (r, s)$*.*

Definição 4.3.4 *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 4.3.1 *Com as notações da Definição (4.3.4) temos que* $[\mathbb{K} : \mathbb{F}] \geq 2$.

Demonstração: Seja $\mathbb{K}$ um corpo de números de grau n e seja G o grupo de Galois de $\mathbb{K}$, ou seja, o grupo dos automorfismos de $\mathbb{K}$ em $\mathbb{C}$

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \{id\} \\ | & & | \\ \mathbb{F} & \longrightarrow & H = \{id, \phi\}, pois\ \phi^2 = id \\ \vdots & & \vdots \\ \mathbb{Q} & \longrightarrow & G \end{array}$$

Pelo Teorema da Correspodência de Galois, segue que $[\mathbb{K} : \mathbb{F}] = (H : \{id\}) = o(H)$. Temos que $H = \{id, \phi\}$, logo $o(H) = 1$, se $\phi = id$, ou $o(H) = 2$, se $\phi \neq id$. Portanto, $o(H) \leq 2$ e consequentemente, $[\mathbb{K} : \mathbb{F}] \leq 2$. ∎

unesp

Definição 4.3.5 *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 é* **ímpar**.

Definição 4.3.6 *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.*

Definição 4.3.7 *Seja $\mathcal{I}$ um ideal de $\mathbb{K}$ e seja $\alpha \in \mathbb{F}$ tal que $\alpha\mathcal{I}\phi(\mathcal{I}) \subset \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Z})^{-1}$. Um ideal reticulado é um reticulado inteiro $(\mathcal{I}, b)$, onde $b : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}$ é tal que $b(x, y) = Tr(\alpha x\phi(y))$. Dizemos que $(\mathcal{I}, b)$ é um* **$\mathcal{O}_{\mathbb{K}}$-reticulado**, *ou que é obtido por uma construção traço escalonada.*

Note que a condição $\alpha\mathcal{I}\phi(\mathcal{I}) \subset \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Z})^{-1}$ garante que o reticulado seja inteiro e a escolha de $\alpha \in \mathbb{F}$ garante que a forma traço seja simétrica.

$$b(x, y) = Tr(\alpha x\phi(y)) = \phi(Tr(\phi(\alpha)\phi(x)y)) = b(y, x),$$

onde a última igualdade vale já que $Tr(z) \in \mathbb{Z}$ para todo $z \in \mathbb{K}$.

Definição 4.3.8 *Quando $\alpha = 1$, dizemos que $(\mathcal{I}, b)$ é obtido por uma construção traço ou que é do* **tipo traço**.

Proposição 4.3.2 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ seu anel de 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: Temos que $b(x, x) = Tr(\alpha x\phi(x)) = Tr(\alpha x\bar{x}) = Tr(\gamma + \bar{\gamma})(\alpha x\bar{x}) = Tr(\gamma\alpha x\bar{x}) + \overline{Tr(\gamma\alpha x\bar{x})} = 2\Re Tr(\gamma\alpha x\bar{x})$. ∎

Proposição 4.3.3 *Sejam $\mathbb{K}$ um corpo de números, ϕ uma involução sobre $\mathbb{K}$ e $\mathbb{F}$ o corpo fixo da involução. Suponha que $\mathbb{F}$ é totalmente real e $\mathbb{K}$ é totalmente imaginário. Se $I \subset \mathcal{O}_{\mathbb{K}}$ e (I, b) é um $\mathcal{O}_{\mathbb{K}}$-reticulado do tipo traço, então $min(\mathcal{I}, b) \geq [\mathbb{K} : \mathbb{Q}]$.*

Demonstração: Temos que $b(x, x) = Tr(x\phi(x))$. Seja $n = [\mathbb{K} : \mathbb{Q}]$. Pela desigualdade entre as médias aritmética e geométrica, temos que

$$\frac{\sum_{i=1}^{n} \sigma(x\phi(x))}{n} \geq [\prod_{i=1}^{n} \sigma(x\phi(x))]^{1/n}.$$

Logo,

$$Tr(x\phi(x)) \geq nN(x\phi(x))^{1/n}.$$

Como $x \in \mathrm{I} \subset \mathcal{O}_{\mathbb{K}}$, segue que $N(x\phi(x)) \geq 1$. Portanto $min(\mathrm{I}, b) \geq [\mathbb{K} : \mathbb{Q}]$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

4.4 Perturbação do homomorfismo canônico

Nesta seção apresentamos uma perturbação do homomorfismo canônico e a geração de reticulados a partir dela.

Definição 4.4.1 *O homomorfismo* $\sigma_\alpha(x) : \mathbb{K} \longrightarrow \mathbb{R}^n$ *definido por*

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)),$$
$$\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))),$$

onde $\alpha_i = \sigma_i(\alpha) > 0$, *para* $i = 1, \ldots, n$, *onde* $n = r_1 + r_2$.

é uma **perturbação do homomorfismo canônico**.

Proposição 4.4.1 *Seja* $L \subseteq \mathcal{O}_\mathbb{K}$ *um* $\mathbb{Z}$*-módulo livre de rank* n *com* $\mathbb{Z}$*-base* $\{w_1, \ldots, w_n\}$. *Então a imagem de* $\sigma_\alpha(L)$ *em* $\mathbb{R}^n$ *é um reticulado cuja base é* $\{\sigma_\alpha(w_1), \ldots, \sigma_\alpha(w_n)\}$.

Demonstração: Análoga a Proposição (4.2.1). ∎

Definição 4.4.2 *Se* $\{w_1, \ldots, w_n\}$ *é uma* $\mathbb{Z}$*-base de* L, *então o reticulado* $\sigma_\alpha(L)$ *tem matriz geradora* M *dada por*

$$M = \begin{pmatrix} A & B \end{pmatrix},$$

onde

$$A = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \sqrt{\alpha_2}\sigma_2(w_1) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \sqrt{\alpha_2}\sigma_2(w_2) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \sqrt{\alpha_2}\sigma_2(w_n) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_n) \end{pmatrix}$$

e

$$B = \begin{pmatrix} \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_1) & \cdots & \sqrt{2\alpha_r 1 + r_2}\Re\sigma_{r1+r_2}(w_1) & \sqrt{2\alpha_{r1+r_2}}\Im\sigma_{r_1+r_2}(w_1) \\ \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_2) & \cdots & \sqrt{2\alpha_{r1+r_2}}\Re\sigma_{r1+r_2}(w_2) & \sqrt{2\alpha_{r1+r_2}}\Im\sigma_{r1+r_2}(w_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_n) & \cdots & \sqrt{2\alpha_{r1+r_2}}\Re\sigma_{r1+r_2}(w_n) & \sqrt{2\alpha_{r1+r_2}}\Im\sigma_{r1+r_2}(w_n) \end{pmatrix}.$$

Observação 4.4.1 *A matriz de Gram é dada por* $G = MM^t = (g_{ij})_{i,j=1}^n$, *onde*

$$g_{ij} = \sum_{k=1}^{r_2} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) +$$
$$\sum_{k=1}^{r_2} 2\sqrt{\alpha_{r_1+k}}[\Re(\sigma_{r_1+k}(w_i))\Re(\sigma_{r_1+k}(w_j)) + \Im(\sigma_{r_1+k}(w_i))\Im(\sigma_{r_1+k}(w_j))]$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$\begin{aligned} &= \sum_{k=1}^{r_2} \alpha_k \sigma_k(w_i w_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k} \Re(\sigma_{r_1+k}(w_i)(\sigma_{r_1+k})(\overline{w_j})) \\ &= \sum_{k=1}^{r_1} \alpha_k \sigma_k(w_i w_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k} \sigma_{r_1+k}(w_i \overline{w_j}) + \sum_{k=1}^{r_2} \alpha_{r_1+k} \overline{\sigma_{r_1+k}(w_i \overline{w_j})} \\ &= Tr(\alpha w_i \overline{w_j}). \end{aligned}$$

A segunda igualdade vale pois a conjugação complexa comuta com todos σ_i, para todo $i = 1, \ldots, n$. Como a matriz de Gram é do tipo traço, temos que a matriz geradora M define um ideal reticulado. O determinante do reticulado Λ é o determinante da matriz G, ou seja, $det(\Lambda) = det(G)$.

Note que o principal fator que define o homomorfismo canônico e a perturbação do homomorfismo de $\mathbb{K}$ em $\mathbb{R}^n$ é uma $\mathbb{Z}$-base de n elementos. Como todo ideal $\mathcal{I}$ de $\mathcal{O}_\mathbb{K}$ possui uma $\mathbb{Z}$-base de n elementos, podemos construir reticulados a partir de $\mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$ (ou $\mathcal{I} = \mathcal{O}_\mathbb{K}$).

Proposição 4.4.2 *Se $(\mathcal{I}, b)$ é um ideal reticulado, então $|det(b)| = |D_\mathbb{K}| N(I)^2 N(\alpha)$.*

Demonstração: Como $\mathcal{I}$ é um $\mathbb{Z}$-módulo livre de rank n sobre $\mathcal{O}_\mathbb{K}$, pelo Teorema (1.2.1) existe uma base $\{u_1, \ldots, u_n\}$ de $\mathcal{O}_\mathbb{K}$ e inteiros positivos $q_1, \ldots, q_n$ tais que $\{u_1 q_1, \ldots, u_n q_n\}$ é uma base para $\mathcal{I}$. Expressando a matriz geradora de $(\mathcal{I}, b)$ nesta base temos que

$$|det(b)| = |D_\mathbb{K}| N(I)^2 N(\alpha),$$

e isto conclui a demonstração. ∎

A concepção de ideais reticulados tem duas vantagens. Uma delas é poder ver um reticulado em $\mathbb{R}^n$ dado por uma matriz geradora, e a outra é que os pontos do reticulado são imagens de inteiros algébricos através do homomorfismo canônico aplicado em $\mathcal{O}_\mathbb{K}$. Deste modo, este processo enfatiza a correspondência entre os pontos $x \in \Lambda \subseteq \mathbb{R}^n$ e os inteiros algébricos. Usando a matriz geradora dada na Definição (4.4.2), um ponto do reticulado pode ser expresso como

$$\begin{aligned} x &= (x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+2r_2}) \\ &= (\sum_{i=1}^{n} \lambda_i \sqrt{\alpha_1} \sigma_1(w_i), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{2\alpha_{r_1+1}} \Re(\sigma_{r_1+1}(w_i)), \ldots, \sum_{i=1}^{n} \lambda_i \sqrt{2\alpha_{r_1+2r_2}} \Im(\sigma_{r_1+2r_2}(w_i))), \\ &\quad \lambda_i \in \mathbb{Z}, \quad i = 1, \ldots, n. \\ &= (\sqrt{\alpha_1} \sigma_1(\sum_{i=1}^{n} \lambda_i w_i), \ldots, \sqrt{2\alpha_{r_1+1}} \Re(\sigma_{r_1+1}(\sum_{i=1}^{n} \lambda_i w_i), \ldots, \sqrt{2\alpha_{r_1+2r_2}} \Im(\sigma_{r_1+2r_2}(\sum_{i=1}^{n} \lambda_i w_i)). \end{aligned}$$

Portanto,

$$x = (\sqrt{\alpha_1} \sigma_1(y), \ldots, \sqrt{2\alpha_{r_1+1}} \Re(\sigma_{r_1+1}(y), \ldots, \sqrt{2\alpha_{r_1+2r_2}} \Im(\sigma_{r_1+2r_2}(y)) = \sigma_\alpha(y),$$

para algum inteiro algébrico $y = \sum_{i=1}^{n} \lambda_i w_i \in \mathcal{I}$. Esta correspondência entre um vetor $x \in \mathbb{R}^n$ e um inteiro algébrico y de $\mathcal{O}_{\mathbb{K}}$ facilita o cálculo de algumas propriedades de reticulados que em geral são difíceis de se calcular.

Existem outras perturbações do homomorfismo canônico, que podem ser definidas de maneira análoga a esta que apresentamos e também geram reticulados em $\mathbb{R}^n$.

Definição 4.4.3 *Seja $\{w_1, \ldots, w_n\}$ uma $\mathbb{Z}-$base do ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Considere o homomorfismo $\sigma'_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por*

$$\sigma'_\alpha(x) = (\sqrt{\alpha_1}w_1, \ldots, \sqrt{\alpha_{r_1}}w_{r_1}, \sqrt{\alpha_{r_1+1}}\Re(w_{r_1+1}), \sqrt{\alpha_{r_1+1}}\Im(w_{r_1+1}), \ldots, \sqrt{\alpha_{r_1+2r_2}}\Re(w_{r_1+2r_2}), \sqrt{\alpha_{r_1+2r_2}}\Im(w_{r_1+2r_2})),$$

onde $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{K}$ é totalmente positivo, ou seja, $\sigma_i(\alpha) = \alpha_i$ é real e positivo para todo i. Esta é uma outra perturbação do homomorfismo canônico.

A matriz geradora do reticulado $\sigma'_\alpha(\mathcal{I})$ é dada por

$$M' = \begin{pmatrix} A' & B' \end{pmatrix},$$

onde

$$A' = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \sqrt{\alpha_2}\sigma_2(w_1) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \sqrt{\alpha_2}\sigma_2(w_2) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \sqrt{\alpha_2}\sigma_2(w_n) & \cdots & \sqrt{\alpha_{r1}}\sigma_{r1}(w_n) \end{pmatrix}$$

e

$$B' = \begin{pmatrix} \Re\sigma_{r_1+1}(w_1) & \sqrt{\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_1) & \cdots & \sqrt{\alpha_{r_1+2r_2}}\Re\sigma_{r_1+2r_2}(w_1) & \sqrt{\alpha_{r_1+2r_2}}\Im\sigma_{r_1+2r_2}(w_1) \\ \Re\sigma_{r_1+1}(w_2) & \sqrt{\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_2) & \cdots & \sqrt{\alpha_{r_1+2r_2}}\Re\sigma_{r_1+2r_2}(w_2) & \sqrt{\alpha_{r_1+2r_2}}\Im\sigma_{r_1+2r_2}(w_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \Re\sigma_{r_1+1}(w_n) & \sqrt{\alpha_{r_1+1}}\Im\sigma_{r_1+1}(w_n) & \cdots & \sqrt{\alpha_{r_2}}\Re\sigma_{r_1+2r_2}(w_n) & \sqrt{\alpha_{r_1+2r_2}}\Im\sigma_{r_1+2r_2}(w_n) \end{pmatrix}.$$

Todas as definições e resultados relacionados com os reticulados obtidos por esta perturbação são análogos aos da perturbação descrita anteriormente.

4.5 Diversidade e distância produto mínima

Nesta seção veremos os conceitos de diversidade e da distância produto de um reticulado. Além disso, veremos que a distância produto mínima de um reticulado pode ser obtida através do determinante do reticulado e do discriminante do corpo.

Definição 4.5.1 *Dados dois vetores $x, y \in \mathbb{R}^n$, definimos a* **diversidade** *(ou a distância de Hamming) de x e y como $div(x, y) = \#\{i, x_i \neq y_i \;\; i = 1, \ldots, n\}$.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Definição 4.5.2 *Dado um subconjunto $S \subseteq \mathbb{R}^n$, a* **diversidade** *ou a distância mínima de Hamming de S é $min\{div(x,y) \mid x \neq y, x, y \in S\}$.*

Todo reticulado Λ é um subconjunto do $\mathbb{R}^n$, então podemos estender essa definição a reticulados. Como reticulados tem estrutura de grupo, isto é, a soma de quaisquer dois pontos de Λ está em Λ, podemos reformular definição de distância de Hamming entre dois vetores. Assim, definimos a distância de Hamming de x a origem, ou seja, a distância de Hamming de x é o número de coordenadas não nulas de x.

Definição 4.5.3 *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 $div(\Lambda) = min\{div(x); x \in \Lambda,\ x \neq 0\}$.*

Proposição 4.5.1 *Um ideal reticulado $\Lambda = (\mathcal{I}, b)$ tem diversidade $div(\Lambda) = r_1 + r_2$.*

Demonstração: Seja $x \neq 0$ um ponto arbitrário de Λ,
$x = (\sqrt{\alpha_1}\sigma_1(y), \ldots, \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(y), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(y)) = \sigma_\alpha(y)$, com $y \in \mathcal{I} \subseteq \mathcal{O}_\mathbb{K}$. Como $x \neq 0$, segue que $y \neq 0$ e os primeiros r_1 coeficientes de x são não nulos. 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. Assim, a $div(\Lambda) \geq r_1 + r_2$. Aplicando o homomorfismo canônico a $y = 1$ temos exatamente $r_1 + r_2$ coeficientes não nulos. Portanto $div(\Lambda) = r_1 + r_2$.

■

Proposição 4.5.2 *Um ideal reticulado $\Lambda = (\mathcal{I}, b)$ pode ser imerso no $\mathbb{R}^n$, com*
i) diversidade n se $\mathbb{K}$ é totalmente real.
ii) diversidade $\frac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.

Demonstração: Seja $\Lambda = (\mathcal{I}, b)$ um ideal reticulado. Assim, $b : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$ é definido por $b(x,y) = Tr(\alpha x \phi(y))$, para todo $x, y \in \mathcal{I}$, onde $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_\mathbb{K}$ e $\sigma_i(\alpha)$ é real e positivo para todo $i = 1, 2, \ldots, r_1 + r_2$. Seja $\{w_1, \ldots, w_n\}$ uma base de $\mathcal{I}$. Seja $M = (\sigma_\alpha(w_i))_{i=1,\ldots,n}$. Assim, M é uma matriz geradora de $\sigma_\alpha(\mathcal{I})$ e $MM^t = (Tr(w_i\sigma(w_j)))_{i,j}$, o que implica que $\sigma_\alpha(\mathcal{I})$ com o produto escalar usual é isomorfo a Λ. Pela Proposição (4.5.1) temos que Λ tem diversidade n se $\mathbb{K}$ é totalmente real, e diversidade $\frac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.

■

Definição 4.5.4 *Seja Λ um reticulado em $\mathbb{R}^n$, com diversidade $l \leq n$ e $x, y \in \Lambda$. Definimos*

1. *A* **distância l-produto** *entre x e y por $d_p^l(x,y) = \prod_{i=1}^{n} |x_i - y_i|$.*
2. *A* **distância l-produto mínima** *de Λ por $d_{p,min}^l(\Lambda) = min\{d^l(x,y) \mid x \neq y, x, y \in \Lambda\}$.*

Definição 4.5.5 *Equivalentemente, podemos considerar a distância l-produto de $x \in \Lambda$ a origem.*

1. *A* **distância l-produto** *de x é $d_p^l(x) = \prod_{i=1}^{n} |x_i|$.*
2. *A* **distância l-produto mínima** *de Λ é $d_{p,min}^l(\Lambda) = min\{d_p^l(x) \mid x \neq 0, x \in \Lambda\}$.*

Definição 4.5.6 *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $x = (x_1, \ldots, x_n) \in \Lambda$.*

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

Definição 4.5.7 *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ uma extensão de $\mathbb{Q}$ de grau n, e $\mathcal{D} \subset \mathbb{K}$ um anel. Dizemos que $\mathcal{D}$ é uma* **ordem** *de $\mathbb{K}$ se é um $\mathbb{Z}$-módulo livre finitamente gerado de rank máximo n. Sendo $\mathcal{O}_\mathbb{K}$ um anel de $\mathbb{K}$ tal que $\mathcal{O}_\mathbb{K} \subset \mathbb{K}$ e tem rank máximo, chamamos $\mathcal{O}_\mathbb{K}$ de ordem máxima de $\mathbb{K}$.*

Teorema 4.5.1 *Sejam $\mathbb{K}$ um corpo de números totalmente real com discriminante $D_\mathbb{K}$, $\mathcal{D}$ uma ordem de $\mathbb{K}$ e $\mathcal{I}$ um ideal principal de $\mathcal{D}$. A distância produto mínima de um ideal reticulado definido sobre $\mathcal{I}$ é*

$$d_{p,min}(\Lambda) = \frac{1}{[\mathcal{O}_\mathbb{K} : \mathcal{D}]} \sqrt{\frac{det(\Lambda)}{D_\mathbb{K}}},$$

onde $det(\Lambda) = det(G)$, sendo Λ um reticulado em $\mathbb{R}^n$ e G sua matriz de Gram.

Demonstração: Seja $(\mathcal{I}, b)$ um ideal reticulado, onde $b : \mathcal{I} \times \mathcal{I} \to$ é tal que $b(x,y) = Tr(\alpha xy)$, onde α é totalmente real e positivo em $\mathbb{K}$. Indique por $d_p(b)$ a distância produto de b. Temos

$$d_p(b) = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_j} \sigma_i(v_i) \right|$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$
\begin{aligned}
&= \prod_{j=1}^{n} \left| \sqrt{\alpha_j} \sigma_j \sum_{i=1}^{n} \lambda_i v_i \right| \\
&= \prod_{j=1}^{n} |\sqrt{\alpha_j}| \prod_{j=1}^{n} \sigma_i (\sum_{i=1}^{n} \lambda_i v_i) \\
&= \sqrt{N(\alpha)} \left| N(\sum_{i=1}^{n} \lambda_i v_i) \right|.
\end{aligned}
$$

Como $det(b) = N(\alpha)N(\mathcal{I})^2 disc(\mathcal{D})$, segue que $\sqrt{N(\alpha)} = \frac{\sqrt{det(\Lambda)}}{\sqrt{disc(\mathcal{D})}N(\mathcal{I})}$, onde $disc(\mathcal{D})$ é o discriminante da ordem $\mathcal{D}$.

Logo concluímos que

$$d_{p,min}(b) = \sqrt{N(\alpha)} min_{x \in \mathcal{I}} N(x) = \sqrt{N(\alpha)} N(\mathcal{I}) = \frac{1}{[\mathcal{O}_{\mathbb{K}} : \mathcal{D}]} \sqrt{\frac{det(\Lambda)}{D_{\mathbb{K}}}}.$$

■

Lema 4.5.1 *Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, então $min_{x \neq 0 \in \mathcal{I}} N(x) = N(\mathcal{I})$.*

Demonstração: Como $\mathcal{I}$ é um ideal principal, segue que $\mathcal{I} = \langle a \rangle$, com $a \in \mathcal{I}$, e $N(\mathcal{I}) = |N(a)|$. Se $x \in \mathcal{I}$, $x \neq 0$, então $x = ay$ para algum $y \in \mathcal{O}_{\mathbb{K}}$. Assim,

$$|N(x)| = |N(a)||N(y)| \geq N(\mathcal{I})$$

e a igualdade é verdadeira se, e somente se, $N(y) = \pm 1$, se, e somente se, y é uma unidade. Portanto, o mínimo é atingido para $x = ay$, onde y é uma unidade. ■

Quando $\mathcal{I}$ é principal, a distância produto mínima de um ideal reticulado $(\mathcal{I}, b)$ pode ser calculada conforme o seguinte resultado.

Corolário 4.5.1 *Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$. A distância produto mínima de um ideal reticulado definido sobre $\mathcal{I}$, é dado por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(\Lambda)}{D_{\mathbb{K}}}}.$$

Demonstração: Sejam $\{w_1, \ldots, w_n\}$ uma base de $\mathcal{I}$ e $x = \sum_{i=1}^{n} \lambda_i w_i$ para $\lambda_i \in \mathbb{Z}$, com $i = 1, \ldots, n$. Da matriz da Definição (4.4.2) temos que

$$d_p(x) = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_j} \sigma_j(w_i) \right|$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$
\begin{aligned}
&= \prod_{j=1}^{n} \left| \sqrt{\alpha_j} \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \\
&= \prod_{j=1}^{n} |\sqrt{\alpha_j}| \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \\
&= \sqrt{N(\alpha)} \left| N \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right|.
\end{aligned}
$$

Pela Proposição (4.4.2) temos que $\det(\Lambda) = N(\alpha) D_{\mathbb{K}} N(\mathcal{I})^2$. Assim $N(\alpha) = \dfrac{\det(\Lambda)}{N(\mathcal{I})^2 D_{\mathbb{K}}}$. Pelo Lema (4.5.1), segue que

$$
\begin{aligned}
d_{p,min}(\Lambda) &= \sqrt{N(\alpha)} min_{x \in \mathcal{I}} N(x) \\
&= \sqrt{\frac{\det(\Lambda)}{D_{\mathbb{K}}}} \frac{min_{x \in \mathcal{I}} N(x)}{N(\mathcal{I})} = \sqrt{\frac{\det(\Lambda)}{D_{\mathbb{K}}}}.
\end{aligned}
$$

■

4.6 O canal Rayleigh com desvanecimento

O rápido crescimento da comunicação sem fio requer um aumento na capacidade e melhoria no desempenho dos sistemas de transmissão. Os canais de comunicação móvel são agrupados em dois tipos: canal via satélite e canal terrestre.

O canal de comunicação terrestre é caracterizado pelo efeito de múltiplos percursos de propagação. Tal efeito pode alterar de maneira significativa a amplitude do sinal, mesmo para uma pequena variação na distância ou orientação entre o transmissor e o receptor, comportamento que é comumente rotulado como desvanecimento. Limitações nas perdas de propagação, variação no tempo, ruído, inferência e desvanecimento fazem com que, nestes sistemas, a transmissão de dados com altas taxas de transmissão não seja uma tarefa fácil.

Para se alcançar essas altas taxas de transmissão de dados é necessário aumentar a capacidade do canal de comunicações móveis. Quando o desvanecimento compromete substancialmente a qualidade da transmissão, o aumento da capacidade do canal ou equivalentemente, a diminuição da taxa de erro é extremamente difícil.

Uma alternativa mais simples para aumentar a capacidade do canal com desvanecimento é utilizar técnicas de diversidade. Estas técnicas geralmente fornecem ao receptor réplicas da informação transmitida que experimentam desvanecimentos descorrelacionados. Neste caso, se uma componente do sinal estiver sobre um desvanecimento profundo, algumas das outras componentes terão uma grande probabilidade de sofrer uma atenuação mais leve.

A função densidade de probabilidade de Rayleigh caracteriza o desvanecimento percebido

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

em uma comunicação móvel onde não há predominância direta entre a antena transmissora e a receptora. Esse desvanecimento indica que existe uma maior probabilidade da amplitude da envoltória do sinal recebido estar abaixo de um valor médio.

Os códigos projetados para canais com desvanecimento Rayleigh levam em conta dois parâmetros fundamentais: o ganho de diversidade, isto é, aumento de distância mínima, que descreve a diminuição exponencial da taxa de erro na decodificação em função da relação sinal-ruído na curva de desempenho e o ganho de codificação que resulta em deslocamentos à esquerda dessa curva. Os melhores valores para estes parâmetros foram obtidos maximizando-se, respectivamente, o posto mínimo e a média geométrica mínima dos autovalores, de um conjunto de matrizes complexas formadas pelas diferenças entre palavras-código tomadas duas a duas.

A principal desvantagem destes códigos é que são extremamente difíceis de se projetar, pois os critérios utilizados na sua construção baseiam-se em operações no domínio complexo das modulações em banda básica e não no domínio binário ou discreto no qual os códigos de canal são tradicionalmente projetados. Uma grande capacidade computacional é necessária para acompanhar a busca, codificação e decodificação destes códigos.

Vejamos algumas características desse canal.

- A probabilidade de erro de símbolo com alta relação sinal-ruído satisfaz,

$$P_e(\Lambda) \leq \frac{1}{2} \sum_{l=L}^{n} \frac{1}{\left(\frac{\eta}{8} \frac{E_b}{N_0}\right)^l d_p^{(l)}(x,y)^2}, \tag{4.4}$$

  onde onde E_b é a energia média por bit, $\eta = \dfrac{2m}{n}$ é a eficiência espectral e $d_p^{(l)}(x,y)^2$ é a distância l-produto normalizada de x a y, quando esses pontos diferem em l componentes e é dada por

$$d_p^{(l)}(x,y)^2 = \frac{\prod_{x_i \neq y_i} (x_i - y_i)^2}{\left(\frac{E}{n}\right)^l}, \tag{4.5}$$

  onde $E = E(||x||^2)$ é a energia média por ponto da constelação S.

- Constelações eficientes, ou seja, aquelas em que a probabilidade de erro é mínima, podem ser obtidas através de reticulados com diversidade máxima $L = min(l)$, menor energia média da constelação E e maior distância produto mínima $d_{p,min} = min(d_p^{(L)}(x,y))$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

- Usando corpos de números totalmente reais e com discriminante absoluto mínimo, a grande vantagem é que eles apresentam diversidade máxima.

  Isso nos leva a investigar códigos reticulados sobre corpos de números totalmente reais, que tenham discriminante mínimo.

Observação 4.6.1 *Uma pergunta que pode surgir é porque os reticulados gerados desta forma não são eficientes para um canal aditivo.*

O canal de comunicação via satélite é um canal AWGN (Additive White Gaussian Noise) onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal. O termo AWGN é utilizado em modulamentos matemáticos para caracterizar aqueles canais onde o tipo de ruído responsável por degradar a comunicação é um ruído branco adicionado ao sinal. Este tipo de ruído é um dos mais "bem comportados" e a teoria acerca do desenvolvimento de receptores ótimos para a utilização em canais AWGN já se tornou clássica.

O ruído branco é um sinal aleatório e tem um modelamento matemático que o considera como possuindo largura de faixa infinita, média nula e correlação nula entre suas amplitudes tomadas a instantes de tempo distintos, ou seja, o valor da amplitude do ruído em um determinado instante independe daquele observado em outro instante de tempo qualquer. O termo gaussiano se deve ao fato desse tipo de ruído possuir uma função densidade de probabilidade gaussiana com média nula, com desvio padrão igual à sua tensão rms e variância igual à potência dissipada de um resistor de 1W.

No canal gaussiano, usando esquemas convencionais de modulação e codificação de canal apropriada, pode-se reduzir a probabilidade de erro e bit de 10^{-2} a 10^{-3} por meio de um aumento da relação sinal-ruído de somente 1 ou 2 dB.

Para o canal Gaussiano temos:

- *A probabilidade de erro de símbolo é limitada superiormente por*

$$P_e(\Lambda) \leq \frac{\tau}{2} erfc\left(\frac{d_{E\,min}/2}{\sqrt{2N_0}}\right), \tag{4.6}$$

  onde τ é o número de vizinhos, $erfc$ é a função erro, N_0 é a variância gaussiana e $d_{E\,min}$ é a distância mínima Euclidiana do reticulado Λ. O ganho de codificação do reticulado Λ é dado por

$$\gamma = \frac{d^2_{E\,min}}{Vol(\Lambda)^{2/n}}.$$

unesp

- *Constelações eficientes podem ser obtidas através de reticulados com alta densidade de empacotamento. Assim, constelações com boas propriedades de simetria podem ser obtidas.*

- *Usando corpos de números totalmente reais e com discriminante absoluto mínimo a grande desvantagem é que a densidade de empacotamento esférico é baixa.*

- *Usando corpos de números totalmente complexos e com discriminante absoluto mínimo a grande vantagem é que é possível obter reticulados com alta densidade de empacotamento.*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Capítulo 5

Construções de ideais reticulados

Na seção 4.6 vimos alguns critérios para construção de códigos reticulados para o canal Rayleigh com desvanecimento e neste capítulo, usando esses critérios, veremos algumas construções de ideais reticulados.

A diversidade da modulação, a distância produto mínima e ter estrutura conhecida são parâmetros que podem otimizar essas construções. Além disso, temos que em termos de reticulados algébricos, estes parâmetros são dados por fórmulas explícitas relacionadas com a estrutura dos corpos de números. A diversidade depende da assinatura do corpo, enquanto que a distância produto mínima está relacionada com o discriminante. Deste modo, para se construir reticulados eficientes devemos satisfazer as seguintes condições:

1. Maximizar a diversidade, ou seja, considerar corpos de números totalmente reais.
2. Maximizar a distância produto mínima, ou seja, procurar corpos de números com discriminante mínimo.
3. Garantir fácil rotulamento e boa estrutura, ou seja, construir $\mathbb{Z}^n$-reticulados.

Dizemos que um reticulado Λ se realiza como $\mathbb{Z}^n$-reticulado se a matriz da forma traço for a matriz identidade. Equivalentemente, dizemos que a forma traço é isomorfa à forma unidade.

Neste capítulo apresentamos 5 algoritmos de construções de $\mathbb{Z}^n$-reticulados rotacionados que satisfazem os critérios acima mencionados. Tais construções são:

1. Construção quadrática: usando o anel de inteiros do corpo quadrático construímos $\mathbb{Z}^2$-reticulados rotacionados.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

2. Construção ciclotômica: usando o anel de inteiros do subcorpo maximal real de $\mathbb{Q}(\xi_p)$, construímos $\mathbb{Z}^n$-reticulados rotacionados em dimensão $n = \frac{p-1}{2}$, $p \geq 5$ um número primo.

3. Construção cíclica: usando o inverso do diferente de um corpo cíclico de grau primo ímpar construímos $\mathbb{Z}^n$-reticulados rotacionados de dimensão prima.

4. Construção mista: combina as construções ciclotômica e cíclica, resultando em reticulados de outras dimensões.

5. Método de Krüskemper: usando os autovalores de uma matriz simétrica $n \times n$ construímos reticulados de dimensão n.

Os resultados aqui apresentados podem ser encontrados em [9], [12], [13], [14], [15], [16], [17], [18], [19], [20] e [21]. Gostaria de ressaltar que os reticulados dos Exemplos (5.3.1), (5.3.2), (5.4.2), (5.5.1), (5.5.2) e (5.6.2) foram construídos no decorrer deste trabalho.

5.1 Ideais reticulados via corpos totalmente reais

Nesta seção apresentamos a matriz geradora de ideais reticulados obtidos via corpos totalmente reais.

Para maximizar a diversidade de um reticulado devemos considerar corpos de números totalmente reais, consideramos $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números totalmente real, $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros e $\mathcal{I}$ um ideal de $\mathcal{O}_{\mathbb{K}}$.

Definição 5.1.1 *Se $\{w_1, w_2, \ldots, w_n\}$ for uma $\mathbb{Z}$-base de $\mathcal{I}$, a matriz M, geradora do reticulado $\Lambda = \sigma_\alpha(\mathcal{I}) = \{x = \lambda M | \lambda \in \mathbb{Z}^n\}$ é dada por*

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \sqrt{\alpha_2}\sigma_2(w_1) & \cdots & \sqrt{\alpha_n}\sigma_n(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \sqrt{\alpha_2}\sigma_2(w_2) & \cdots & \sqrt{\alpha_n}\sigma_n(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \sqrt{\alpha_2}\sigma_2(w_n) & \cdots & \sqrt{\alpha_n}\sigma_n(w_n) \end{pmatrix} = (\sigma_i(w_j))_{i,j=1}^n \begin{pmatrix} \sqrt{\alpha_1} & & 0 \\ \vdots & \ddots & \vdots \\ 0 & & \sqrt{\alpha_n} \end{pmatrix},$$

onde $\alpha_j = \sigma_j(\alpha)$, para $j = 1, 2, \cdots, n$.

A matriz Gram é dada por $G = MM^t = (g_{ij})_{i,j=1}^n$, onde

$$g_{ij} = \sum_{k=1}^{n} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j)$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$= \sum_{k=1}^{n} \alpha_k \sigma_k(w_i w_j) = Tr(\alpha w_i w_j).$$

5.2 Construção quadrática

Nesta seção veremos a construção de ideais reticulados via corpos quadráticos. Deste modo, seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados, um corpo quadrático.

Seja $(\mathcal{I}, b)$ um ideal reticulado. Uma condição necessária, mas não suficiente, para que Λ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$, uma versão escalar de $\mathbb{Z}^n$, é que $det(\Lambda) = c^n$, pois a matriz de Gram de $(\sqrt{c})\mathbb{Z}$ é cI_n, onde c é um número inteiro. Pela Proposição (4.4.2) temos que $N(\mathcal{I})^2 N(\alpha) D_{\mathbb{K}} = c^n$ e se $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, então $N(\alpha) D_{\mathbb{K}} = c^n$. Como nosso objetivo é encontrar reticulados contidos em $\mathbb{Z}^n$, devemos construir reticulados cujas matrizes de Gram sejam a matriz identidade, ou seja, precisamos encontrar um elemento $\alpha \in \mathbb{K}$ que satisfaça a condição acima.

Exemplo 5.2.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro positivo livre de quadrados. Seja $\{1, \omega\}$ uma base integral de $\mathcal{O}_{\mathbb{K}}$. A correspondente matriz geradora do reticulado é dada por*

$$N = \begin{pmatrix} 1 & 1 \\ \sigma_1(\omega) & \sigma_2(\omega) \end{pmatrix},$$

e $|det(N)| = \sqrt{D_{\mathbb{K}}}$. Se existir um inteiro α totalmente positivo tal que $N(\alpha) = \dfrac{1}{(det(N))^2}$, então obtemos o reticulado rotacionado com a seguinte matriz geradora

$$M = N \cdot \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{pmatrix}.$$

O próximo lema fornece uma condição para a existência do elemento α.

Lema 5.2.1 *Sejam m uma dada norma algébrica em $\mathbb{K}$ e $\mu \in \mathbb{K}$. Se $N(\mu) = 1$, então existe um elemento α totalmente real e positivo com norma algébrica m.*

Demonstração: Seja β um elemento de $\mathbb{K}$ com $N(\beta) = m$. Se $\sigma_i(\beta) > 0$, para $i = 1, 2$, tomamos $\alpha = \beta$. Se $\sigma_1(\beta) > 0$ e $\sigma_2(\beta) < 0$, tomamos $\alpha = \dfrac{\beta}{\mu}$. Se $\sigma_i(\beta) < 0$, para $i = 1, 2$ tomamos $\alpha = \beta$. Se $\sigma_1(\beta) < 0$ e $\sigma_2(\beta) > 0$, tomamos $\alpha = \dfrac{\beta}{\mu}$. ∎

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Uma família de corpos quadráticos com tal propriedade é dada por $\mathbb{K} = \mathbb{Q}(\sqrt{p})$, onde p é primo tal que $p \equiv 1(mod\ 4)$. Mas podemos obter reticulados rotacionados via outros corpos quadráticos.

Exemplo 5.2.2 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. *Pelo Teorema (2.1.1), temos que* $D_{\mathbb{K}} = 5$. *Como* $\mathbb{K}$ *é totalmente real, segue que as imersões são* $\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$ *e* $\sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}$, *onde* $a, b \in \mathbb{Q}$. *Uma condição para obter* $\mathbb{Z}^2$ *é encontrar um elemento* α *tal que* $D_{\mathbb{K}}N(\alpha)=5N(\alpha) = c^2, c \in \mathbb{Z}$. *Assim, uma possibilidade é encontrar um elemento* $\alpha \in \mathbb{K}$ *tal que* $N(\alpha) = 5$. *Sejam* $\alpha = 2 + \frac{1-\sqrt{5}}{2}$ *e* $\{1, \frac{1+\sqrt{5}}{2}\}$ *uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. *A matriz geradora* M *do reticulado* $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ *é dada por*

$$\begin{aligned} M &= \begin{pmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} \cdot \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\frac{1+\sqrt{5}}{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} \end{aligned}$$

e a matriz $G = MM^T$ *é dada por*

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})) \\ \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})^2) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})^2) \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

A matriz G *fornece uma versão escalar de* $\mathbb{Z}^2$. *Assim, depois da normalização, temos que* $\mathbb{Z}^2$ *pode ser obtido a partir de* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, *com matriz geradora dada por* $R = \frac{1}{\sqrt{5}}M$. *Pelo Corolário (4.5.1) a distância produto mínima deste reticulado é dada por*

$$d_{p,min}(\Lambda) = \frac{1}{\sqrt{D_{\mathbb{K}}}} = \frac{1}{\sqrt{5}}.$$

Exemplo 5.2.3 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. *Pela Teorema (2.1.1), temos que* $D_{\mathbb{K}} = 8$. *Como* $\mathbb{K}$ *é totalmente real, segue que as imersões são* $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ *e* $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$, *onde* $a, b \in \mathbb{Q}$. *Uma condição para obter* $\mathbb{Z}^2$ *é encontrar um elemento* α *tal que* $D_{\mathbb{K}}N(\alpha)=8N(\alpha) = c^2, c \in \mathbb{Z}$. *Assim, uma possibilidade é encontrar um elemento* $\alpha \in \mathbb{K}$ *tal que* $N(\alpha) = 2$. *Sejam* $\alpha = \sqrt{2} - 2$ *e* $\{1, 1 + \sqrt{2}\}$ *uma* $\mathbb{Z}$*-base do ideal* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. *A matriz geradora* M *do reticulado* $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ *é dada por*

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(1 + \sqrt{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(1 + \sqrt{2}) \end{pmatrix}$$

e a matriz $G = MM^T$ *é dada por*

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha(1+\sqrt{2})) + \sigma_2(\alpha(1+\sqrt{2})) \\ \sigma_1(\alpha(1+\sqrt{2})) + \sigma_2(\alpha(1+\sqrt{2})) & \sigma_1(\alpha(1+\sqrt{2})^2) + \sigma_2(\alpha(1+\sqrt{2})^2) \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

A matriz G *fornece uma versão escalar de* $\mathbb{Z}^2$. *Assim, depois da normalização, temos que* $\mathbb{Z}^2$ *pode ser construído a partir de* $\mathcal{O}_{\mathbb{K}}$, *com matriz geradora dada por* $R = \frac{1}{2}M$. *Pelo Corolário (4.5.1) segue que a distância produto mínima deste reticulado é dada por*

$$d_{p,min}(\Lambda) = \frac{1}{\sqrt{D_{\mathbb{K}}}} = \frac{1}{\sqrt{8}}.$$

A seguir faremos as construções ciclotômica e cíclica, que são realizações particulares de $\mathbb{Z}^n$-reticulados como ideais reticulados, em pequenas dimensões. No caso ciclotômico, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ e $\alpha = (1-\xi)(1-\xi^{-1})$, onde ξ é uma raiz primitiva da unidade. No caso cíclico, $\mathcal{I} = \mathcal{A}$, onde $\mathcal{A}^2 = \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})^{-1}$ e $\alpha = 1$.

5.3 Construção ciclotômica em dimensão $n = \frac{p-1}{2}$

Nesta seção veremos a construção de reticulados via o anel de inteiros do subcorpo maximal real de um corpo ciclotômico.

Sejam $\mathbb{Q}(\xi_p)$ um corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\xi_p + \xi_p^{-1})$ o subcorpo real maximal de $\mathbb{Q}(\xi_p)$, onde $p \geq 5$ é um número primo e ξ_p é uma raiz p-ésima primitiva da unidade. Temos que o grau de $\mathbb{Q}(\xi_p)$ sobre $\mathbb{Q}$, é $p-1$ e o grau de $\mathbb{Q}(\xi_p)$ sobre $\mathbb{K}$ é 2, cujo polinômio minimal de ξ_p sobre $\mathbb{K}$ é dado por $x^2 - (\xi_p + \xi_p^{-1})x + 1$. Assim, o corpo $\mathbb{K}$ é totalmente real e é chamado de **subcorpo maximal real** do corpo ciclotômico $\mathbb{Q}(\xi_p)$.

$$p-1 \left\{ \begin{array}{l} \mathbb{Q}(\xi_p) \\ |2 \\ \mathbb{Q}(\xi_p + \xi_p^{-1}) \\ |\frac{p-1}{2} \\ \mathbb{Q} \end{array} \right.$$

O discriminante de $\mathbb{K}$ é dado por $D_{\mathbb{K}} = p^{\frac{p-3}{2}}$.

Proposição 5.3.1 *O conjunto* $\left\{\xi_p + \xi_p^{-1}, \xi_p^2 + \xi_p^{-2}, \ldots, \xi_p^{\frac{p-1}{2}} + \xi_p^{\frac{1-p}{2}}\right\}$ *é uma base de* $\mathbb{Z}[\xi_p + \xi_p^{-1}]$ *sobre* $\mathbb{Q}$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Temos que o conjunto $\left\{\xi_p+\xi_p^{-1}, \xi_p^2+\xi_p^{-2}, \ldots, \xi_p^{\frac{p-1}{2}}+\xi_p^{\frac{1-p}{2}}\right\} \subseteq \mathbb{Z}[\xi_p+\xi_p^{-1}]$. Assim, falta mostrar que esse conjunto é linearmente independente e gera $\mathbb{Z}[\xi_p+\xi_p^{-1}]$. Seja $\beta \in \mathbb{Z}[\xi_p+\xi_p^{-1}]$, então $\beta = a_0+a_1(\xi_p+\xi_p^{-1})+a_2(\xi_p+\xi_p^{-1})^2+\cdots+a_{\frac{p-1}{2}}(\xi_p+\xi_p^{-1})^{\frac{p-1}{2}}$. Desenvolvendo as potências de $(\xi_p+\xi_p^{-1})$, temos que $\beta = b_0+b_1(\xi_p+\xi_p^{-1})+b_2(\xi_p^2+\xi_p^{-2})+\cdots+b_{\frac{p-1}{2}}(\xi_p^{\frac{p-1}{2}}+\xi_p^{-\frac{1-p}{2}})$. Portanto, $\left\{\xi_p+\xi_p^{-1}, \xi_p^2+\xi_p^{-2}, \ldots, \xi_p^{\frac{p-1}{2}}+\xi_p^{\frac{1-p}{2}}\right\}$ gera $\mathbb{Z}[\xi_p+\xi_p^{-1}]$. Sejam $a_1, a_2, \ldots, a_{\frac{p-1}{2}} \in \mathbb{Q}$ tais que

$$a_1(\xi_p+\xi_p^{-1})+a_2(\xi_p^2+\xi_p^{-2})+\cdots+a_{\frac{p-1}{2}}(\xi_p^{\frac{p-1}{2}}+\xi_p^{\frac{1-p}{2}})=0.$$

Assim,

$$a_1\xi_p+a_1\xi_p^{-1}+a_2\xi_p^2+\cdots+a_{\frac{p-1}{2}}\xi_p^{\frac{p-1}{2}}+a_{\frac{p-1}{2}}\xi_p^{\frac{1-p}{2}}=0.$$

Como $\{1, \xi_p, \ldots, \xi_{p-2}\}$ é uma base de $\mathbb{Z}[\xi_p]$ sobre $\mathbb{Q}$, segue que é linearmente independente e portanto, $a_1 = a_2 = \cdots = a_{\frac{p-1}{2}} = 0$. Portanto, $\left\{\xi_p+\xi_p^{-1}, \xi_p^2+\xi_p^{-2}, \ldots, \xi_p^{\frac{p-1}{2}}+\xi_p^{\frac{1-p}{2}}\right\}$ é uma base de $\mathbb{Z}[\xi_p+\xi_p^{-1}]$ sobre $\mathbb{Q}$. ∎

Proposição 5.3.2 *O anel de inteiros de* $\mathbb{K} = \mathbb{Q}(\xi_p+\xi_p{}^{-1})$ *é dado por* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_p+\xi_p{}^{-1}]$.

Demonstração: Pelo Teorema (2.2.2) temos que o anel de inteiros de $\mathbb{Q}(\xi_p)$ é $\mathbb{Z}[\xi_p]$. Como ξ_p é um inteiro , segue que ξ_p^{-1} também o é. Pelo Corolário (1.2.2) segue que $\xi_p+\xi_p^{-1}$ é um inteiro e portanto, $\mathbb{Z}[\xi_p+\xi_p^{-1}] \subseteq \mathcal{O}_{\mathbb{K}}$. Reciprocamente, se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_1(\xi_p+\xi_p^{-1})+a_2(\xi_p^2+\xi_p^{-2})+\cdots+a_{\frac{p-1}{2}}(\xi_p^{\frac{p-1}{2}}+\xi_p^{\frac{1-p}{2}}),$$

onde $a_1, a_2, \ldots, a_{\frac{p-1}{2}} \in \mathbb{Q}$.

Multiplicando α por $\xi_p^{\frac{p-1}{2}}$, obtemos que

$$\xi_p^{\frac{p-1}{2}}\alpha = a_1\xi_p^{\frac{p+1}{2}}+a_1\xi_p^{\frac{p-3}{2}}+a_2\xi_p^{\frac{p+3}{2}}+a_2\xi_p^{\frac{p-5}{2}}+\cdots+a_{\frac{p-1}{2}}\xi_p^{p-1}+a_{\frac{p-1}{2}}.$$

Assim, $\xi_p^{\frac{p-1}{2}}\alpha \in \mathbb{Q}(\xi_p)$ e é um inteiro algébrico. Logo, $\xi_p^{\frac{p-1}{2}}\alpha \in \mathbb{Z}[\xi_p]$. Assim, $a_i \in \mathbb{Z}$, para $i = 1, \ldots, n$ e portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi_p+\xi_p^{-1}]$. ∎

Definição 5.3.1 *Os n monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$, *que são dados por*

$$\sigma_k(e_j) = \xi_p{}^{kj}+\xi_p{}^{-kj} = 2\cos(\frac{2\pi kj}{p}).$$

Na Seção 5.2 vimos que uma condição necessária para obtenção de um $\mathbb{Z}^n$-ideal reticulado é encontrar um elemento α tal que

$$N(\alpha)D_{\mathbb{K}} = c^n$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$N(\alpha)p^{\frac{p-3}{2}} = p^{\frac{p-1}{2}}.$$

Precisamos encontrar então $\alpha \in \mathbb{K}$ tal que $N(\alpha) = p$. Temos que $p\mathbb{Z}[\xi_p] = (1-\xi_p)^{p-1}\mathbb{Z}[\xi_p]$ em $\mathbb{Q}(\xi_p)$ e $N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(1-\xi_p) = p$. Usando a transitividade da norma,

$$\begin{aligned} N_{\mathbb{Q}(\xi_p)|\mathbb{Q}}(1-\xi_p) &= N_{\mathbb{K}|\mathbb{Q}}(N_{\mathbb{Q}(\xi_p)|\mathbb{K}}(1-\xi_p)) \\ &= N_{\mathbb{K}|\mathbb{Q}}((1-\xi_p)(1-\xi_p^{-1})). \end{aligned}$$

Consequentemente, $\alpha = (1-\xi_p)(1-\xi_p{}^{-1})$ é um elemento de $\mathbb{Z}[\xi_p + \xi_p^{-1}]$ cuja norma é p.

Vimos que $\{e_j = \xi_p^j + \xi_p^{-j}\}_{j=1}^n$ é uma base de $\mathbb{Z}[\xi_p + \xi_p^{-1}]$. Uma outra base é dada por $\{e_i'\}_{i=1}^n$, onde $e_n' = e_n$ e $e_j' = e_j + e_{j+1}'$, para $j = 1, \ldots, n-1$.

O próximo Teorema nos fornece como o reticulado é construído.

Teorema 5.3.1 *Se* $\alpha = (1-\xi_p)(1-\xi_p{}^{-1}) = 2 - (\xi_p + \xi_p^{-1})$, *então* $\frac{1}{p}Tr(\alpha e_i' e_j') = \delta_{ij}$, *onde* δ_{ij} *é o delta de Kronecker.*

Demonstração: Para simplificar a notação consideremos $\xi = \xi_p$. Primeiramente, vamos calcular a matriz $(Tr(\alpha e_i e_j))$, onde $\{e_j = \xi^j + \xi^{-j}\}_{j=1}^n$ é a base integral usual de $\mathbb{K} = \mathbb{Q}(\xi_p + \xi_p{}^{-1})$. A partir dessa matriz encontramos a nova base $\{e_j'\}_{j=1}^n$, onde a matriz $\frac{1}{p}(Tr(\alpha e_i' e_j'))$ é exatamente a matriz identidade. Denotemos por $\sigma_k(\xi)$ e por $\alpha_j = \sigma_j(\alpha)$, os conjugados de ξ e α respectivamente , de acordo com a Definição (5.3.1). Note que

$$Tr(\xi^k + \xi^{-k}) = \sum_{j=1}^n \sigma_j(\xi^k + \xi^{-k}) = -1, \quad para \quad k = 1, \ldots, n. \tag{5.1}$$

Usando a Equação (5.1) temos que

$$\begin{aligned} Tr(\alpha(\xi^k + \xi^{-k})) &= \sum_{j=1}^n \sigma_j(\alpha)\sigma_j(\xi^k + \xi^{-k}) \\ &= \sum_{j=1}^n \alpha_j \sigma_j(\xi^k + \xi^{-k}) \\ &= \sum_{j=1}^n (2 - \sigma_j(\xi^k - \xi^{-k}))\sigma_j(\xi^k + \xi^{-k}) \\ &= -2 - \sum_{j=1}^n \sigma_j(\xi^{k+1} + \xi^{-k-1} + \xi^{-k+1} + \xi^{k-1}) \\ &= \begin{cases} -2 + 1 - 2n = -p, & \text{se } k = \pm 1 (mod\ p) \\ -2 + 1 + 1 = 0, & \text{caso contrário.} \end{cases} \end{aligned} \tag{5.2}$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Seja $b(x,y) = Tr(\alpha xy)$. Usando as Equações (5.1) e (5.2), vamos calcular $b(e_i, e_j)$, para $i = j$ e $i \neq j$. Temos que

$$\begin{aligned} b(e_i,e_i) &= Tr(\alpha e_i^2) \\ &= \sum_{j=1}^{n} \alpha_j \sigma_j(\xi^{2i} + \xi^{-2i} + 2) \\ &= \sum_{j=1}^{n} \alpha_j \sigma_j(\xi^{2i} + \xi^{-2i}) + 2\sum_{j=1}^{n} 2 - \sigma_j(\xi + \xi^{-1}) \\ &= \begin{cases} p, & \text{se } i = n, \text{ ou } \textit{seja}, \ 2i \equiv -1 (mod\ p) \\ 2p, & \text{caso contrário,} \end{cases} \end{aligned}$$

$$\begin{aligned} b(e_i,e_j) &= Tr(\alpha e_i e_j) \\ &= \sum_{j=1}^{n} (\alpha_j \sigma_j(\xi^{i+j} + \xi^{-(i+j)})) + \sum_{j=1}^{n} (\alpha_j \sigma_j(\xi^{i-j} + \xi^{-(i-j)})) \\ &= \begin{cases} -p, & \text{se } |i-j| = 1 \\ 0, & \text{caso contrário.} \end{cases} \end{aligned}$$

Seja $B(x,y) = \frac{1}{p} Tr(\alpha xy)$. Dessa forma, a matriz de B na base $\{e_1, \ldots, e_n\}$ é dada por

$$\begin{pmatrix} 2 & -1 & 0 & \cdots & \cdots & 0 \\ -1 & 2 & -1 & \cdots & \vdots & \vdots \\ 0 & -1 & 2 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & -1 & 0 \\ \vdots & \vdots & \vdots & -1 & 2 & -1 \\ 0 & \cdots & \cdots & 0 & -1 & 1 \end{pmatrix}. \tag{5.3}$$

Na nova base $\{e_1', \cdots, e_n'\}$, a matriz em (5.3) é a matriz de Gram do reticulado $\mathbb{Z}^n$. ■

Em outras palavras, o ideal reticulado $\Lambda = (\mathcal{O}_{\mathbb{K}}, \frac{1}{p} b_\alpha)$, com $\alpha = (1-\xi)(1-\xi^{-1})$ é isomorfo ao reticulado $\mathbb{Z}^n$.

Como os n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são dados por

$$\sigma_k(e_j) = \xi_p^{kj} + \xi_p^{-kj} = 2cos(\frac{2\pi kj}{p}),$$

segue que o reticulado gerado pelo anel de inteiros de $\mathbb{K}$ tem $N_{n\times n}$ como matriz geradora, cujos elementos são da forma $N_{kj} = 2cos(\frac{2\pi kj}{p})$. O elemento α pode ser representado por uma matriz diagonal dada por

$$A = diag(\sqrt{\sigma_k(\alpha)}).$$

A matriz mudança de base de $\{e_j\}$ para $\{e'_j\}$ é dada por

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

Assim, o $\mathbb{Z}^n$-reticulado rotacionado tem como matriz geradora

$$R = \frac{1}{\sqrt{p}} TNA$$

Note que a matriz NA é igual a matriz M da Definição (5.1.1).

Seguindo os passos desse algoritmo, pode-se construir $\mathbb{Z}^n$-reticulados rotacionados para $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$.

Proposição 5.3.3 *Se Λ é um ideal reticulado de dimensão n, então $d_{p,min}(\Lambda) = p^{-\frac{n-1}{2}}$.*

Demonstração: Pelo Corolário (4.5.1) temos que a distância produto mínima de Λ é dada por $\frac{1}{\sqrt{D_{\mathbb{K}}}}$, uma vez que $det(\Lambda) = 1$. Como o discriminante de $\mathbb{K}$ é $D_{\mathbb{K}} = p^{\frac{p-3}{2}} = p^{n-1}$, segue que $d_{p,min}(\Lambda) = p^{-\frac{n-1}{2}}$. ∎

A Tabela 5.1 fornece a $d_{p,min}(\Lambda)$ para a construção ciclotômica em algumas dimensões.

Exemplo 5.3.1 *Se $p = 5$, então $\mathbb{K} = \mathbb{Q}(\xi_5 + \xi_5^{-1})$ e $D_{\mathbb{K}} = 5$.*

$$4 \begin{pmatrix} \mathbb{Q}(\xi_5) \\ |2 \\ \mathbb{Q}(\xi_5 + \xi_5^{-1}) \\ |2 \\ \mathbb{Q} \end{pmatrix}$$

Assim, se $\Lambda \subseteq \mathbb{R}^2$ então $d_{p,min}(\Lambda) = \frac{1}{\sqrt{5}}$. O $\mathbb{Z}^2$-reticulado rotacionado tem como matriz geradora

$$R = \frac{1}{\sqrt{5}} TNA$$

onde

$$N = \begin{pmatrix} 2cos(\frac{2\pi}{5}) & 2cos(\frac{4\pi}{5}) \\ 2cos(\frac{4\pi}{5}) & 2cos(\frac{8\pi}{5}) \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad e$$

T. 1502/06
Biblioteca de Biociências, Letras e Ciências Exatas - UNESP - S. J. Rio Preto
BIBLIOTECA

$$A = \begin{pmatrix} \sqrt{2 - 2cos(\frac{2\pi}{5})} & 0 \\ 0 & \sqrt{2 - 2cos(\frac{4\pi}{5})} \end{pmatrix}.$$

Logo,

$$R = \begin{pmatrix} -0,5257 & -0,85065 \\ -0,85065 & 0,5257 \end{pmatrix}.$$

Tabela 5.1: Distância Produto Mínima para a Construção Ciclotômica

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
29	14	$\frac{1}{\sqrt{29^{13}}}$	0,209425
31	15	$\frac{1}{31^7}$	0,201386
37	18	$\frac{1}{\sqrt{37^{17}}}$	0,181744
41	20	$\frac{1}{\sqrt{41^{19}}}$	0,171367
43	21	$\frac{1}{43^{10}}$	0,166785
47	23	$\frac{1}{47^{11}}$	0,158599
53	26	$\frac{1}{\sqrt{53^{25}}}$	0,148259
59	29	$\frac{1}{59^{14}}$	0,139670
61	30	$\frac{1}{\sqrt{61^{29}}}$	0,137116

Exemplo 5.3.2 *Se $p = 7$, então $\Lambda \subseteq \mathbb{R}^3$ e $d_{p,min}(\Lambda) = \frac{1}{7}$. O $\mathbb{Z}^3$-reticulado rotacionado tem como matriz geradora*

$$R = \frac{1}{\sqrt{7}} TNA,$$

onde

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 2cos(\frac{2\pi}{7}) & 2cos(\frac{4\pi}{7}) & 2cos(\frac{6\pi}{7}) \\ 2cos(\frac{4\pi}{7}) & 2cos(\frac{8\pi}{7}) & 2cos(\frac{12\pi}{7}) \\ 2cos(\frac{6\pi}{7}) & 2cos(\frac{12\pi}{7}) & 2cos(\frac{18\pi}{7}) \end{pmatrix}, \quad A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix},$$

e $\alpha_1 = \sqrt{2 - 2cos(\frac{2\pi}{7})}$, $\alpha_2 = \sqrt{2 - 2cos(\frac{4\pi}{7})}$ *e* $\alpha_3 = \sqrt{2 - 2cos(\frac{6\pi}{7})}$.

Assim,

$$R = \begin{pmatrix} -0,32798 & -0,591 & -0,73696 \\ -0,73696 & -0,32798 & 0,591 \\ -1,5636 & 0,73696 & -0,32798 \end{pmatrix}$$

5.4 Construção cíclica

Nesta seção veremos a construção cíclica de ideais reticulados via o ideal $\mathcal{A}$ de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{A}^2 = \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})^{-1}$.

Seja $\mathbb{K}$ uma extensão cíclica de $\mathbb{Q}$ de grau primo $n > 2$. Uma vez que toda extensão de Galois de grau ímpar é totalmente real, veremos a construção de $\mathbb{Z}^n$-reticulados rotacionados com diversidade $L = n$. A construção dada em [17], mostra que sempre existe uma forma traço sobre $\mathcal{A}$, que é isomorfa à forma unidade por escalonamento de fatores.

Seja p um primo ímpar. Dependendo quais primos p ramificam em $\mathcal{O}_{\mathbb{K}}$, obtemos três classes diferentes de reticulados.

- Caso I: Quando $p > n$ é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$.
- Caso II: Quando $p = n$ é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$;
- Caso III: Quando existem pelo menos dois primos p_1 e p_2 que ramificam em $\mathcal{O}_{\mathbb{K}}$.

Essas três construções resultam em reticulados de dimensão prima, e que não são construídos no caso ciclotômico. Para uma dada dimensão prima n, veremos que sempre podemos selecionar um primo ímpar p satisfazendo as condições dos casos I ou II, ou dois primos p_1 e p_2 que satisfaça o caso III. Além disso, temos que não é necessário conhecer explicitamente o corpo $\mathbb{K}$, e que o conhecimento de p (ou p_1 e p_2) e n é suficiente para construir o reticulado. Veremos também que se n e p são dois primos ímpares, segue que sempre existe um corpo cíclico $\mathbb{K}$ onde p se ramifica. O objetivo é obter, para uma dada dimensão, a construção que fornece a maior distância produto mínima.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

5.4.1 Caso I: Somente $p > n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$

Nesta subseção veremos a construção de ideais reticulados quando somente $p > n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$. Para isso, suponhamos que o primo $p > n$ é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$. Assim, como $\mathbb{K}$ é cíclico, pelo Teorema de Kronecker-Weber, podemos mergulhar $\mathbb{K}$ no corpo ciclotômico $\mathbb{Q}(\xi)$, onde $\xi = \xi_p$ é uma raiz p-ésima primitiva da unidade.

Se $G = Gal(\mathbb{Q}(\xi)|\mathbb{Q})$, é o grupo de Galois de $\mathbb{Q}(\xi)$ sobre $\mathbb{Q}$, então, G é cíclico de ordem $p-1$, uma vez que $o(G) = \varphi(p) = p-1$, onde φ é a função de Euler. Seja σ o gerador de G. Como $[\mathbb{Q}(\xi) : \mathbb{K}] = \frac{p-1}{n}$, segue que o elemento σ^n é o gerador do grupo cíclico $H = Gal(\mathbb{Q}(\xi)|\mathbb{K})$.

Pela Correrspondência de Galois temos o seguinte diagrama

$$\begin{array}{ccc} \mathbb{Q}(\xi_p) & \longrightarrow & \{id\} \\ |\frac{p-1}{n} & & | \\ \mathbb{K} & \longrightarrow & H = \langle \sigma^n \rangle \\ |n & & | \\ \mathbb{Q} & \longrightarrow & G = \langle \sigma \rangle \end{array}$$

Seja r um elemento primitivo $(mod\ p)$, ou seja, $r^{p-1} \equiv 1(mod\ p)$ e $p-1$ é o menor inteiro positivo com esta propriedade. Sejam $\alpha = \prod_{k=0}^{m-1}(1-\xi^{r^k})$, onde $m = \frac{p-1}{2}$ e λ tal que $\lambda(r-1) \equiv 1(mod\ p)$. Assim $r^m \equiv -1(mod\ p)$, e pela definição de r temos, $\sigma(\xi) = \xi^r$.

Lema 5.4.1 $\sigma(\alpha) = -\xi^{p-1}\alpha$.

Demonstração: Temos que

$$\begin{aligned} \sigma(\alpha) &= \sigma(\prod_{k=0}^{m-1}(1-\xi^{r^k})) \\ &= \prod_{k=0}^{m-1}\sigma(1-\xi^{r^k}) = \prod_{k=0}^{m-1}\sigma(1) - \sigma(\xi^{r^k}) \\ &= \prod_{k=0}^{m-1}(1-\xi^{r^{k+1}}) = (1-\xi)^{-1}(1-\xi)\left[\prod_{k=0}^{m-2}(1-\xi^{r^{k+1}})\right](1-\xi^{r^m}) \\ &= (1-\xi)^{-1}(1-\xi^{r^m})(1-\xi)\prod_{k=0}^{m-2}(1-\xi^{r^{k+1}}) \\ &= (1-\xi)^{-1}(1-\xi^{-1})\alpha = -\xi^{p-1}\alpha \end{aligned}$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

e a útima igualdade segue de

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

e $\xi^{p-1} + \xi^{p-2} + \cdots + \xi + 1 = 0$. ■

Lema 5.4.2 $\sigma(\xi^\lambda \alpha) = -\xi^\lambda \alpha$.

Demonstração: Usando o Lema (5.4.1) e a definição de λ, temos que

$$\sigma(\xi^\lambda \alpha) = \sigma(\xi^\lambda)\sigma(\alpha) = \xi^{\lambda+1}(-\xi^{p-1}\alpha) = -\xi^{\lambda+p}\alpha = -\xi^\lambda \xi^p \alpha = -\xi^\lambda \alpha,$$

uma vez que $\xi^p = 1$. ■

Lema 5.4.3 $(\xi^\lambda \alpha)^2 = (-1)^m p$.

Demonstração: O polinômio ciclotômico de ξ_p, é dado por

$$\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{k=0}^{p-2}(x - \sigma^k(\xi)).$$

Para $x = 1$ temos que

$$\begin{aligned} p &= \prod_{k=0}^{p-2}(1-\xi^{r^k}) = \prod_{k=0}^{m-1}(1-\xi^{r^k}) \prod_{j=0}^{m-1}(1-\xi^{-r^j}) \\ &= \alpha(1-\xi^{-1})(1-\xi^{-r})(1-\xi^{-r^2})\cdots(1-\xi^{-r^{m-1}}) \\ &= \alpha(-1)^m(\xi^{-1}-1)(\xi^{-r}-1)\cdots(\xi^{-r^{m-1}}-1) \\ &= (-1)^m\alpha(1-\xi)\xi^{-1}(1-\xi^r)\xi^{-r}\cdots(1-\xi^{r^{m-1}})\xi^{-r^{m-1}} \\ &= (-1)^m\alpha^2\prod_{j=0}^{m-1}(\xi^{-r^j}) = (-1)^m\alpha^2\xi^{2\lambda} = (-1)^m(\alpha\xi^\lambda)^2. \end{aligned}$$

A última igualdade vale uma vez que

$$\xi^{-1-r-\cdots-r^{m-1}} = \xi^{\frac{1-r^m}{r-1}},$$

e λ é o inverso de $r-1$ módulo p. ■

Lema 5.4.4 *Se* $\omega_{d,t} = \xi^{r^{nd}+r^t}$, *onde* d *e* t *são inteiros tais que* $t \in \{0,1,\ldots,n-1\}$ *e* $d \in \left\{1,2,\ldots,\frac{(p-1)}{n}\right\}$, *então* $\omega_{d,t} = 1 \iff t = 0$ *e* $d = \frac{p-1}{2n}$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Demonstração: Temos que

$$\begin{aligned}
\omega_{d,t} = 1 &\iff r^{nd} + r^t \equiv 0(mod\ p) \\
&\iff r^{nd} \equiv -r^t(mod\ p) \\
&\iff r^{nd} \equiv r^m r^t(mod\ p), \quad \text{pois} \quad r^m \equiv -1(mod\ p) \\
&\iff r^{nd} \equiv r^{m+t}(mod\ p) \\
&\iff nd = m + t - k_1(p-1), \quad \text{pois} \quad r^{p-1} \equiv 1(mod\ p) \\
&\iff t = nd - m + k_1(p-1).
\end{aligned}$$

então t é um múltiplo de n que pertence ao conjunto $\{0, 1, \ldots, n-1\}$, portanto $t = 0$. Considerando então $t = 0$, temos que

$$\begin{aligned}
r^{nd} \equiv r^m(mod\ p) &\iff nd = k_2 m,\ k_2 \text{ ímpar} \\
&\iff d = k_2 \frac{m}{n} \\
&\iff d = k_2 \left(\frac{p-1}{2n} \right).
\end{aligned}$$

Como k_2 é ímpar, podemos tomar $k_2 = 1$ e portanto $d = \dfrac{p-1}{2n}$. ∎

Lema 5.4.5 *Se* $z = \xi^\lambda \alpha(1-\xi)$ *e* $x = Tr_{\mathbb{Q}(\xi)|\mathbb{K}}(z) = \displaystyle\sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z)$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m} p \sum_c (-1)^c \sum_{a,j} (-1)^j \xi^{r^{a+cn} + r^{a+t+jn}},$$

para $a = 0, 1, \ldots, n-1$, *e* $c, j = 1, 2, \ldots, \dfrac{p-1}{n}$.

Demonstração:

$$\begin{aligned}
Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) &= \sum_{a=0}^{n-1} \sigma^a(x\sigma^t(x)) \\
&= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\
&= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(\xi^\lambda \alpha(1-\xi))\sigma^{a+t+jn}(\xi^\lambda \alpha(1-\xi)) \\
&= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} (-1)^{a+cn} \xi^\lambda \alpha(1-\xi^{r^{a+cn}})(-1)^{a+t+jn} \xi^\lambda \alpha(1-\xi^{r^{a+t+jn}})
\end{aligned}$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$= (-1)^t \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} (-1)^{2a}(-1)^c(-1)^j(\xi^\lambda\alpha)^2(1-\xi^{r^{a+cn}})(1-\xi^{r^{a+t+jn}})$$

$$= (-1)^{t+m} p \sum_{c=1}^{\frac{p-1}{n}} (-1)^c \sum_{a=0}^{n-1} \beta_a,$$

em que

$$\beta_a = \sum_{j=1}^{\frac{p-1}{n}} (-1)^j (1-\xi^{r^{a+cn}}) - \sum_j (-1)^j (\xi^{r^{a+t+jn}} - \xi^{r^{a+cn}+r^{a+t+jn}}),$$

onde a quarta igualdade vale pelo Lema (5.4.2) e a onde a quarta igualdade vale pelo Lema (5.4.2) e a última igualdade vale pelo Lema (5.4.3). Note que o primeiro somatório em j é zero, pois existem tantos $1's$ como $-1's$. Usando o mesmo pincípio, o termo ξ^{r^a+t+jn} também desaparece no segundo somatório em j. Assim, considerando a soma em c temos que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m} p \sum_c (-1)^c \sum_{a,j} (-1)^j \xi^{r^{a+cn}+r^{a+t+jn}}.$$

■

A seguinte proposição fornece um método para a construção do reticulado.

Proposição 5.4.1 *Seja* $z = \xi^\lambda\alpha(1-\xi)$. *Se* $x = Tr_{\mathbb{Q}(\xi)|\mathbb{K}}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z)$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = \delta_{0,t}p^2, \quad para \quad t = 0, \ldots, n-1,$$

onde $\delta_{0,t}$ *é o delta de Kronecker.*

Demonstração: Pelo Lema (5.4.5) temos que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m} p \sum_c (-1)^c \sum_{a,j} (-1)^j \xi^{r^{a+cn}+r^{a+t+jn}}.$$

Podemos verificar também que

$$\sum_{c=1}^{\frac{p-1}{n}} (-1)^c \sum_{a,j} (-1)^j \xi^{r^{a+cn}+r^{a+t+jn}} = \sum_{d=1}^{\frac{p-1}{n}} (-1)^d \sum_{a,k} \xi^{(r^{nd}+r^t)r^{a+kn}}.$$

Trocando todos os índices de todos os termos do somatório, verificamos que eles percorrem o mesmo conjunto de expoentes de $\xi(mod\ p)$. Note ainda que r^{a+kn}, para $a = 0, 1, \ldots, n-1$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

e $k = 1, 2, \ldots, \frac{p-1}{n}$ assume os valores $s = 1, 2, \ldots, p-1$. Denotando portanto $\omega_{d,t} = \xi^{r^{nd}+t^t}$, temos

$$\sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{a,k} \xi^{(r^{nd}+r^t)r^{a+kn}} = \sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{s}^{p-1} \omega_{d,t}^s. \tag{5.4}$$

Pelo Lema (5.4.4),

$$\sum_{s}^{p-1} \omega_{d,t}^s = \begin{cases} p-1 \text{ se } t=0 \text{ e } d = \dfrac{p-1}{2} \\ -1 \text{ caso contrário.} \end{cases}$$

Na Equação (5.4), quando $t \neq 0$ temos

$$(-1)^{t+m} p \sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{s}^{p-1} \omega_{d,t}^s = (-1)^{t+m} p \sum_{d=1}^{\frac{p-1}{n}}(-1)^d(-1) = 0.$$

Quando $t = 0$, temos

$$\begin{aligned}(-1)^{t+m} p \sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{s}^{p-1} \omega_{d,t}^s &= (-1)^m \sum_{d=1, d\neq\frac{p-1}{2}}^{\frac{p-1}{n}} (-1)^d(-1) + (-1)^m p(-1)^{\frac{p-1}{2n}}(p-1) \\ &= p + p(p-1) = p^2\end{aligned}$$

A última igualdade vale já que $(-1)^{m+\frac{p-1}{2n}} = 1$ (pois o expoente é sempre par) e também

$$(-1)^m \sum_{d=1, d\neq\frac{p-1}{2}}^{\frac{p-1}{n}} (-1)^d(-1) = \begin{cases} (-1)^{m+1}(-1) = 1, \text{ se } p \equiv 1(mod\ 4) \ (m \text{ par}) \\ (-1)^{m+1}(-1) = 1, \text{ se } p \equiv 3(mod\ 4) \ (m \text{ ímpar}). \end{cases}$$

Isto prova que

$$(-1)^{t+m} p \sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{a,k} \xi^{(r^{nd}+r^t)r^{a+kn}} = \begin{cases} 0, \text{ se } t \neq 0 \\ p^2, \text{ se } t = 0. \end{cases}$$

■

A Proposição (5.4.1) fornece um método de encontrar o elemento x, tal que a matriz $\frac{1}{p^2} Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x))$ seja a matriz identidade. Assim, o algoritmo para obter a matriz geradora do reticulado é dado da seguinte forma:

1. Escolha uma dimensão prima n.
2. Encontre p tal que $p \equiv 1(mod\ n)$.
3. Encontre r e λ de acordo com suas definições.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

4. Escreva α e z em relação a base $\{1, \xi, \ldots, \xi^{p-2}\}$ do corpo ciclotômico.

5. Calcule x e seus conjugados usando o fato que $\sigma(\xi) = \xi^r$ e $\sigma^n(\xi) = \xi^{r^n}$.

6. Calcule a matriz geradora do reticulado M, cuja a primeira coluna é dada por $\sigma^i(x)$, para $i = 0, \ldots, n-1$, e as demais colunas são as mudanças cíclicas da primeira, ou seja,

$$M = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{n-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(x) & x & \cdots & \sigma^{n-2}(x) \end{pmatrix}$$

   Para obtermos valores numéricos de M, precisamos substituir ξ por $e^{\frac{2\pi i}{p}}$.

7. Calcule a matriz geradora do $\mathbb{Z}^n$-reticulado rotacionado dada por $R = \frac{1}{p}M$.

Tabela 5.2: Parâmetros para o Caso I

n	p	r	λ
3*	7	3	4
3	13	2	1
5*	11	2	1
5	31	3	16
7	29	2	1
11*	23	5	6
11	67	2	1
13	53	2	1
17	103	5	26
19	191	19	138
23*	47	5	12
29*	59	2	1

Alguns parâmetros para o caso I são dados na Tabela (5.2). Os reticulados marcados com asterisco coincidem, para um certo p, com algum reticulado obtido via construção ciclotômica, onde $\mathbb{K} = \mathbb{Q}(\xi_p + \xi_p^{-1})$. Note que o valor de p não é único, e que qualquer escolha de p satisfazendo $p \equiv 1 (mod\ n)$ fornece um corpo bem definido $\mathbb{K}$.

unesp

Exemplo 5.4.1 *Seja* $n = 3$. *Temos que* $13 \equiv 1 (mod\ 3)$. *Estes dois parâmetros determinam um corpo cíclico* $\mathbb{K}$ *de* $\mathbb{Q}(\xi_{13})$. *Para simplificar a notação usaremos* $\xi = \xi_{13}$. *Não precisamos conhecer explicitamente o corpo* $\mathbb{K}$, *mas neste caso* $\mathbb{K} = \mathbb{Q}(\theta)$, *onde* $\theta^3 - \theta^2 - 4\theta - 1 = 0$. *Seu discriminante é* 13^2 *e portanto somente* $p = 13$ *se ramifica em* $\mathbb{K}$. *Calculando* r *e* λ *obtemos que* $r = 2$ *e* $\lambda = 1$. *Uma base de* $\mathbb{Q}(\xi_{13})$ *é* $\{1, \xi, \ldots, \xi^{11}\}$. *Calculando* $\alpha = \prod_{k=0}^{5}(1 - \xi^{2^k})$ *e* $z = \xi\alpha(1 - \xi)$ *obtemos*

$$\begin{aligned} \alpha &= -1 + \xi - \xi^2 - \xi^3 - \xi^4 + \xi^5 + \xi^6 + \xi^7 - \xi^8 - \xi^9 - \xi^{10} + \xi^{11}, \\ z &= 3 + \xi + 4\xi^2 + 2\xi^4 + 4\xi^5 + 2\xi^6 + 2\xi^7 + 2\xi^8 + 2\xi^{10} + 4\xi^{11}. \end{aligned}$$

Pela Proposição (5.4.1), seja

$$x = \sum_{j=1}^{4} \sigma^{jn}(z) = \sigma^1(z) + \sigma^3(z) + \sigma^6(z) + \sigma^9(z),$$

onde $\sigma^k(\xi) = \xi^{2^k}$. *Fazendo os cálculos obtemos*

$$x = 5 + 3\xi^2 + 3\xi^3 - \xi^4 - \xi^6 - \xi^7 - \xi^9 + 3\xi^{10} + 3\xi^{11}.$$

Calculando os conjugados de x *temos que*

$$\begin{aligned} \sigma(x) &= 6 + \xi^2 + \xi^3 + 4\xi^4 + 4\xi^6 + 4\xi^7 + 4\xi^9 + \xi^{10} + \xi^{11} \\ \sigma^2(x) &= 2 - 4\xi^2 - 4\xi^3 - 3\xi^4 - 3\xi^6 - 3\xi^7 - 3\xi^9 - 4\xi^{10} - 4\xi^{11} \end{aligned}$$

Assim,

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) \\ \sigma(x) & \sigma^2(x) & x \\ \sigma^2(x) & x & \sigma(x) \end{pmatrix}.$$

Substituindo x *por* $\xi = e^{\frac{2\pi i}{2}}$ *temos que*

$$M = \begin{pmatrix} 11,78268 & -3,22712 & 4,44444 \\ -3,22712 & 4,44444 & 11,78268 \\ 4,44444 & 11,78268 & -3,22712 \end{pmatrix}.$$

Normalizando M *por* $\frac{1}{13}$ *obtemos*

$$R = \frac{1}{13}M = \begin{pmatrix} 0,90636 & -0,24824 & 0,34188 \\ -0,24824 & 0,34188 & 0,90636 \\ 0,34188 & 0,90636 & -0,24824 \end{pmatrix}.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Note que $RR^t = I_3$. *Portanto,* R *é matriz geradora de um* $\mathbb{Z}^3$*-reticulado rotacionado. Pelo Corolário (4.5.1), a distância produto mínima do reticulado é* $d_{p,min}(\Lambda) = \frac{1}{13}$.

Exemplo 5.4.2 *Seja* $n = 5$. *Temos que* $11 \equiv 1 (mod\ 5)$. *Estes dois parâmetros determinam um corpo cíclico* $\mathbb{K}$ *de* $\mathbb{Q}(\xi_{11})$. *Novamente, para simplificar a notação usaremos* $\xi = \xi_{11}$. *Não precisamos conhecer explicitamente o corpo* $\mathbb{K}$, *mas seu discriminante é* 11^4 *e portanto somente* $p = 11$ *se ramifica em* $\mathbb{K}$. *Calculando* r *e* λ *obtemos que* $r = 2$ *e* $\lambda = 1$. *Uma base de* $\mathbb{Q}(\xi_{11})$ *é* $\{1, \xi, \ldots, \xi^9\}$. *Calculando* $\alpha = \prod_{k=0}^{4}(1 - \xi^{2^k})$ *e* $z = \xi\alpha(1 - \xi)$ *obtemos*

$$\begin{aligned} \alpha &= -1 + \xi - \xi^2 - \xi^3 - \xi^4 + \xi^5 + \xi^6 + \xi^7 - \xi^8 + \xi^9, \\ z &= 3 - 3\xi - 4\xi^3 - 2\xi^4 - 2\xi^5 - 2\xi^7 - 2\xi^8 - 4\xi^9. \end{aligned}$$

Pela Proposição (5.4.1), seja

$$x = \sum_{j=1}^{2} \sigma^{jn}(z) = \sigma^5(z) + \sigma^{10}(z),$$

onde $\sigma^k(\xi) = \xi^{2^k}$. *Fazendo os cálculos obtemos*

$$x = -3 - \xi^2 - 3\xi^3 - \xi^4 + \xi^5 + \xi^6 - \xi^7 - 3\xi^8 - \xi^9.$$

Calculando os conjugados de x *temos que*

$$\begin{aligned} \sigma(x) &= -4 - \xi^2 - 2\xi^3 - 2\xi^4 - 4\xi^5 - 4\xi^6 - 2\xi^7 - 2\xi^8 - \xi^9 \\ \sigma^2(x) &= 4\xi^2 + 2\xi^3 + 3\xi^4 + 2\xi^5 + 2\xi^6 + 3\xi^7 + 2\xi^8 + 4\xi^9 \\ \sigma^3(x) &= -2 - 2\xi^2 + \xi^3 + 2\xi^4 + 2\xi^7 + \xi^8 - 2\xi^9 \\ \sigma^4(x) &= -2 + 2\xi^3 - 2\xi^4 + \xi^5 + \xi^6 - 2\xi^7 + 2\xi^8 \end{aligned}$$

Assim,

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \sigma^3(x) & \sigma^4(x) \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & \sigma^4(x) & x \\ \sigma^2(x) & \sigma^3(x) & \sigma^4(x) & x & \sigma(x) \\ \sigma^3(x) & \sigma^4(x) & x & \sigma(x) & \sigma^2(x) \\ \sigma^4(x) & x & \sigma(x) & \sigma^2(x) & \sigma^3(x) \end{pmatrix}.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Substituindo x *por* $\xi = e^{\frac{2\pi i}{2}}$ *temos que*

$$M = \begin{pmatrix} -3,58621 & 6,03381 & -5,01310 & -6,56567 & -1,86881 \\ 6,03381 & -5,01310 & -6,56567 & -1,86881 & -3,58621 \\ -5,01310 & -6,56567 & -1,86881 & -3,58621 & 6,03381 \\ -6,56567 & -1,86881 & -3,58621 & 6,03381 & -5,01310 \\ -1,86881 & -3,58621 & 6,03381 & -5,01310 & -6,56567 \end{pmatrix}.$$

Normalizando M *por* $\frac{1}{11}$ *obtemos*

$$R = \frac{1}{11}M = \begin{pmatrix} -0,326019 & 0,5485278 & -0,455736 & -0,596878 & -0,169892 \\ 0,548528 & -0,455736 & -0,596878 & -0,169892 & -0,326019 \\ -0,455736 & -0,596878 & -0,169892 & -0,326019 & 0,548528 \\ -0,596878 & -0,169892 & -0,326019 & 0,548528 & -0,455736 \\ -0,169892 & -0,326019 & 0,548528 & -0,455736 & -0,596879 \end{pmatrix}.$$

Note que $RR^t = I_5$. *Portanto,* R *é matriz geradora de um* $\mathbb{Z}^3$*-reticulado rotacionado. Pelo Corolário (4.5.1), a distância produto mínima do reticulado é* $d_{p,min}(\Lambda) = \frac{1}{11^2}$.

5.4.2 Caso II: Somente $p = n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$

Nesta subseção veremos a construção de ideais reticulados quando somente $p = n$ se ramifica em $\mathcal{O}_{\mathbb{K}}$. Para isso, suponhamos que somente o primo $p = n$ se ramifica em $\mathbb{K}$. Assim, pelo Teorema de Kronecker-Weber, podemos mergulhar $\mathbb{K}$ em $\mathbb{Q}(\xi_{n^2})$, onde $\mu = \xi_{n^2}$ é uma raiz n^2-ésima primitiva da unidade. Seja σ o gerador do grupo $Gal(\mathbb{Q}(\mu)|\mathbb{Q})$. Se r é um elemento tal que $r^{n(n-1)} \equiv 1 (mod\ n^2)$ e $n(n-1)$ é o menor inteiro com esta propriedade, então σ é definido como $\sigma(\mu) = \mu^r$. Além disso, temos que

$$\begin{array}{l} \mathbb{Q}(\xi_{n^2}) \\ |n-1 \\ \mathbb{K} \\ |n \\ \mathbb{Q} \end{array}$$

Proposição 5.4.2 *Se* $T = Tr_{\mathbb{Q}(\mu)|\mathbb{K}}(\mu) = \sum_{j=1}^{n-1} \sigma^{nj}(\mu)$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T)) = \delta_{0,t}n^2, \quad para \quad t = 0, \ldots, n-1,$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

onde $\delta_{0,t}$ é o delta de Kronecker.

Demonstração:

$$\begin{aligned}
Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T)) &= \sum_{a=0}^{n-1}\sigma^a((1+T)\sigma^t(1+T)) \\
&= \sum_{a=0}^{n-1}\sigma^a(1+T)\sigma^{a+t}(1+T) \\
&= \sum_{a=0}^{n-1}(1+\sigma^a(T))(1+\sigma^{a+t}(T)) \\
&= \sum_{a=0}^{n-1}[1+\sigma^{a+t}(T)+\sigma^a(T)+\sigma^a(T)+\sigma^{a+t}(T)] \\
&= n+\sum_{a=0}^{n-1}\sum_{j=1}^{n-1}\sigma^{a+t+nj}(\mu)+\sum_{a=0}^{n-1}\sum_{j=1}^{n-1}\sigma^{a+nj}(\mu) \ + \\
&\quad + \sum_{j,k=1}^{n-1}\sigma^{a+nj}(\mu)\sigma^{a+t+kn}(\mu) \\
Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T)) &= n+\sum_{a=0}^{n-1}\sum_{j=1}^{n-1}\mu^{r^{a+t+nj}}+\sum_{a=0}^{n-1}\sum_{j=1}^{n-1}\mu^{r^{a+nj}}+\sum_{j,k=1}^{n-1}\mu^{r^{a+nj}+r^{a+t+kn}} \\
&= n+\sum_{s=0}^{n(n-1)-1}\mu^{r^{s+t}}+\sum_{s=0}^{n(n-1)-1}\mu^{r^s}+\sum_{a=0}^{n-1}\sum_{d,c=1}^{n-1}\mu^{r^{a+nd+nc}+r^{a+t+cn}}.
\end{aligned}$$

A última igualdade é verdadeira pois o conjunto dos valores $a+nj$ para $a=0,1,\ldots,n-1$ e $j=1,2,\ldots,n-1$ são os mesmos para $s=0,1,\ldots,n(n-1)$. A mudança de variáveis é feita como na Proposição (5.4.1). Como

$$Tr_{\mathbb{Q}(\mu)|\mathbb{Q}}(\mu)=\sum_{s=0}^{n(n-1)-1}\sigma^s(\mu)=\sum_{s=0}^{n(n-1)-1}\mu^{r^s}=\sum_{s=0}^{n(n-1)-1}\mu^{r^{s+t}}=0, \quad \text{para} \quad t=0,\ldots,n-1,$$

obtemos

$$Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T))=n+\sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1}\mu^{(r^{nd}+r^t)r^s}=n+\sum_{d=1}^{n-1}Tr_{\mathbb{Q}(\mu)|\mathbb{Q}}(\omega_{d,t}), \qquad (5.5)$$

onde $\omega_{d,t}=\mu^{r^{nd}+r^t}$. A expressão $Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T))$ em (5.5) pode tomar três valores diferentes, que dependem de $\omega_{d,t}$:

1. Se $\omega_{d,t}=1$, então $Tr_{\mathbb{Q}(\mu)|\mathbb{K}}(\omega_{d,t})=n(n-1)$;

2. Se $\omega_{d,t}$ é uma raiz n^2-ésima primitiva da unidade, então $Tr_{\mathbb{Q}(\mu)|\mathbb{K}}(\omega_{d,t})=0$;

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

3. Se $\omega_{d,t}$ é uma raiz da unidade, a qual não é primitiva, temos que $\omega_{d,t}$ é da forma $\mu^{k_1 n}$, para $k_1 = 1, \ldots, n-1$, a qual é uma raiz n-ésima da unidade, então, $Tr_{\mathbb{Q}(\mu)|\mathbb{K}}(\omega_{d,t}) = -n$.

Para concluir a demonstração,consideraremos dois casos, $t = 0$ e $t \neq 0$. Em cada caso determinaremos se $\omega_{d,t}$ é primitivo ou não.

• $t = 0$

Temos que $\omega_{d,t} = 1$ somente neste caso. De fato,

$$\begin{aligned} r^{nd} + r^t &\equiv 0 \ (mod\ n^2) \\ &\iff t = nd - n\frac{(n-1)}{2} + k_2 n(n-1) \\ &\iff t = 0. \end{aligned}$$

Substituindo então $t = 0$, temos que

$$r^{nd} \equiv -1 \ (mod\ n^2) \Longrightarrow d = \frac{n-1}{2}.$$

Quando $d \neq \frac{n-1}{2}$, $\omega_{d,t}$ é uma raiz primitiva da unidade. Suponha que $\omega_{d,t}$ não é primitiva, então,

$$r^{nd} + 1 \equiv 0 \ (mod\ n^2) \Longrightarrow r^{nd} + 1 \equiv 0 \ (mod\ n) \Longrightarrow d = \frac{n-1}{2} + k_3\frac{n-1}{n}.$$

Como $d \geq n-1$, k_3 deve ser igual a 0, e portanto $\omega_{d,t} = 1$. Assim,

$$n + \sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1} \mu^{(r^{nd}+r^t)r^s} = n + n(n-1) = n^2, \quad \text{para} \quad t = 0.$$

• $t \neq 0$

Vamos determinar as raízes primitivas da unidade.

$$r^{nd} + r^t \equiv 0 \ (mod\ n) \Longrightarrow d = \frac{t - k_4}{n} + \frac{n-1}{2} + k_4$$

k_4 deve ser igual a t (como $d \geq n-1$, k_4 não pode ser igual a $t + k_5$). Assim, existe somente um d tal que $\omega_{d,t}$ não é primitivo. Logo,

$$n + \sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1} \mu^{(r^{nd}+r^t)r^s} = n - n = 0.$$

■

A Proposição (5.4.2) fornece um método de encontrar o elemento T, tal que a matriz $\frac{1}{p^2}Tr_{\mathbb{K}|\mathbb{Q}}((1+T)\sigma^t(1+T))$ seja isomorfa à matriz identidade. Assim, o algoritmo para obter a matriz geradora do reticulado é dado da seguinte forma:

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

1. Escolha uma dimensão prima n.

2. Calcule r tal que $r^{n(n-1)} \equiv 1(mod\ n^2)$ e que $n(n-1)$ seja o menor inteiro positivo k tal que $r^k \equiv 1(mod\ n^2)$.

3. Calcule $1+T$ e seus conjugados na base $\{1, \xi, \xi^2, \ldots, \xi^{p^{r-1}(p-1)-1}\}$, do corpo ciclotômico usando o fato que $\sigma(\mu) = \mu^r$ e $\sigma^n(\mu) = \mu^{r^n}$.

4. Calcule a matriz geradora do reticulado M que é dada por

$$\begin{pmatrix} (1+T) & \sigma(1+T) & \cdots & \sigma^{n-1}(1+T) \\ \sigma(1+T) & \sigma^2(1+T) & \cdots & (1+T) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(1+T) & (1+T) & \cdots & \sigma^{n-2}(1+T) \end{pmatrix}.$$

5. Calcule a matriz geradora do $\mathbb{Z}^n$-reticulado rotacionado $R = \frac{1}{n}M$.

Exemplo 5.4.3 *Escolha* $n = 3$. *Assim,* $\mathbb{Q}(\mu) = \mathbb{Q}(\xi_9)$, *cuja base é* $\{1, \xi_9, \xi_9^2, \xi_9^3, \xi_9^4, \xi_9^5\} = \{1, \mu, \mu^2, \mu^3, \mu^4, \mu^5\}$. *Neste caso,* $\mathbb{K} = \mathbb{Q}(\theta)$, *onde* $\theta^3 - 3\theta - 1 = 0$. *Pela definição de* r *temos* $r = 2$. *Calculando* T *na base de* $\mathbb{Q}(\mu)$ *temos que,*

$$T = \sum_{j=1}^{2} \sigma^{3j}(\mu) = \sigma(\mu) + \sigma^3(\mu) = \mu + \mu^8 = \mu - \mu^2 - \mu^5.$$

Logo,

$$\begin{aligned} 1+T &= 1 + \mu - \mu^2 - \mu^5, \\ \sigma(1+T) &= 1 - \mu + \mu^2 - \mu^4 \quad e \\ \sigma^2(1+T) &= 1 + \mu^4 + \mu^5. \end{aligned}$$

Assim,

$$M = \begin{pmatrix} 2,532092453 & 1,347299934 & -0,8793924 \\ 1,347299934 & -0,8793924 & 2,532092453 \\ -0,8793924 & 2,532092453 & 1,347299934 \end{pmatrix}.$$

Finalmente,

$$R = \frac{1}{3}M = \begin{pmatrix} 0,84402 & -0,29312 & 0,44909 \\ 0,44909 & 0,84402 & -0,29312 \\ -0,29312 & 0,44909 & 0,84402 \end{pmatrix}.$$

A distância produto mínima do reticulado é $d_{p,min}(\Lambda) = \frac{1}{3^2}$, *uma vez que* $D_{\mathbb{K}} = 3^4$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Tabela 5.3: Parâmetros para o Caso II

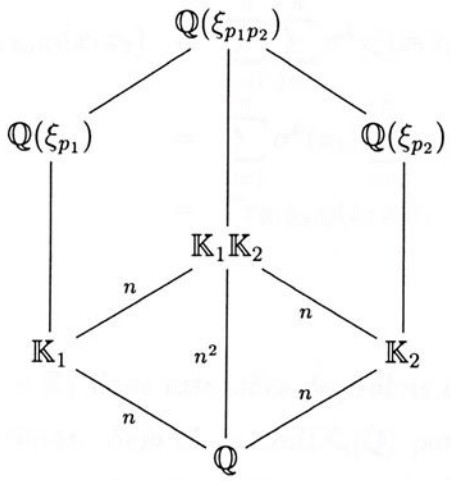
n	n^2	$D_{\mathbb{K}}$	$d_{p,min}(\Lambda)$	$\sqrt[n]{d_{p,min(\Lambda)}}$
3	9	9^2	$\frac{1}{9}$	0,480749856
5	25	5^8	$\frac{1}{5^4}$	0,275945932
7	49	7^{12}	$\frac{1}{7^6}$	0,188638463

5.4.3 Caso III: Pelo menos dois primos se ramificam em $\mathcal{O}_{\mathbb{K}}$

Nesta subseção veremos uma construção de ideais reticulados quando pelo menos dois primos se ramificam em $\mathcal{O}_{\mathbb{K}}$. Para isso, suponhamos que existam pelo menos dois primos que se ramificam em $\mathbb{K}$. Para obter o corpo $\mathbb{K}$ usaremos dois corpos, onde somente um primo se ramifica em cada um deles.

Lema 5.4.6 *Seja n um primo ímpar. Sejam dois primos ímpares distintos p_1 e p_2 tais que $p_i \equiv 1(mod\ n)$, mas $p_i \not\equiv 1(mod\ n^2)$ para $i = 1, 2$. Se $\mathbb{K}$ é um corpo cíclico de grau n onde p_1 e p_2 se ramificam, então $\mathbb{K}$ está contido na composição de dois corpos $\mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_i$ é um corpo cíclico de grau n que somente p_i se ramifica, para $i = 1, 2$.*

Demonstração: Se p_1 e p_2 são dois primos distintos , tais que $p_i \equiv 1(mod\ n)$ e $p_i \not\equiv 1(mod\ n^2)$, para $i = 1, 2$, então existem corpos $\mathbb{K}_i \subseteq \mathbb{Q}(\xi_p)$ tal que $[\mathbb{K}_i : \mathbb{Q}] = n$, para $i = 1, 2$. Assim, temos o seguinte diagrama



Seja $\mathbb{K}$ um corpo cíclico de grau n, onde p_1 e p_2 ramificam. Deste modo, $\mathbb{K}$ é uma subextensão de $\mathbb{Q}(\xi_{p_1p_2})$. Mostraremos que $\mathbb{K} \subseteq \mathbb{K}_1\mathbb{K}_2$ usando o Teorema da Correspondência de Galois. Seja $G = Gal(\mathbb{Q}(\xi_{p_1p_2})|\mathbb{Q})$. Do fato que $Gal(\mathbb{Q}(\xi_{p_1})|\mathbb{Q}) = \dfrac{\mathbb{Z}}{(p_1-1)\mathbb{Z}}$ e

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$Gal(\mathbb{Q}(\xi_{p_2})|\mathbb{Q}) = \dfrac{\mathbb{Z}}{(p_2-1)\mathbb{Z}}$, segue que

$$\begin{aligned} G &\cong \tfrac{\mathbb{Z}}{(p_1-1)\mathbb{Z}} \times \tfrac{\mathbb{Z}}{(p_2-1)\mathbb{Z}} \\ &\cong C_n \times C_n \times \tfrac{\mathbb{Z}}{(\frac{p_1-1}{n})\mathbb{Z}} \times \tfrac{\mathbb{Z}}{(\frac{p_2-1}{n})\mathbb{Z}}. \end{aligned}$$

Temos também que G é um grupo abeliano de ordem $(p_1-1)(p_2-1)$. Do fato que um grupo abeliano tem decomposição única em subgrupos de Sylow e, segue que G é o produto direto de um n-subgrupo de Sylow e de p_i-subgrupos de Sylow, onde $mdc(p_i, n) = 1$, para $i = 1, 2$. Se $H = Gal(\mathbb{Q}(\xi_{p_1p_2})|\mathbb{K}_1\mathbb{K}_2)$, então H é um subgrupo de G de ordem $(\frac{p_1-1}{n})(\frac{p_2-1}{n})$. Como $mdc(o(H), n) = 1$, segue que H corresponde ao produto direto de p_i-subgrupos de G, onde $mdc(p_i, n) = 1$, para $i = 1, 2$. Seja $I = Gal(\mathbb{Q}(\xi_{p_1p_2})|\mathbb{K})$. Como I é um subgrupo de G e como I ter ordem $\dfrac{(p_1-1)(p_2-1)}{n} = n\dfrac{p_1-1}{n}\dfrac{p_2-1}{n}$, segue que I contém um subgrupo J de ordem $\dfrac{(p_1-1)}{n}\dfrac{(p_2-1)}{n}$. Usando o mesmo raciocínio, temos que J é também um produto direto de p_i-subgrupos de Sylow de G, com $mdc(p_i, n) = 1$, para $i = 1, 2$. Logo $H = J \subseteq I$ e pelo Teorema da Correspondência de Galois segue que $\mathbb{K} \subseteq \mathbb{K}_1\mathbb{K}_2$. ∎

Observação 5.4.1 *Se p_1 ou p_2 é igual a n o mesmo resultado é obtido substituindo $\mathbb{Q}(\xi p_1 p_2)$ por $\mathbb{Q}(\xi p_1 n^2)$.*

Lema 5.4.7 *Se $x_1 \in \mathbb{K}_1$ e $x_2 \in \mathbb{K}_2$ temos que $Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(x_1x_2) = Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(x_1x_2)$.*

Demonstração:

$$\begin{aligned} Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(x_1x_2) &= \sum_{k=1}^{n}\sum_{j=1}^{n}\sigma^k\tau^j(x_1x_2) \\ &= \sum_{k=1}^{n}\sigma^k(x_1)\sum_{j=1}^{n}\tau^j(x_2) \\ &= Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(x_1x_2). \end{aligned}$$

∎

Proposição 5.4.3 *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ duas extensões de Galois de $\mathbb{Q}$, disjuntas, cujos discriminantes são relativamente primos. Seja $G_i = Gal(\mathbb{K}_i|\mathbb{Q})$ para $i = 1, 2$, onde $G_1 = \langle\sigma\rangle$ e $G_2 = \langle\tau\rangle$ são cíclicos de ordem n. Seja $\mathbb{K} \subseteq \mathbb{K}_1\mathbb{K}_2$ outra extensão cíclica de grau n. Se existir $x_i \in \mathbb{K}_i$, para $i = 1, 2$, satisfazendo:*

1. *$Tr_{\mathbb{K}_1|\mathbb{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p_1^2$, para $t = 0, \ldots, n-1$;*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

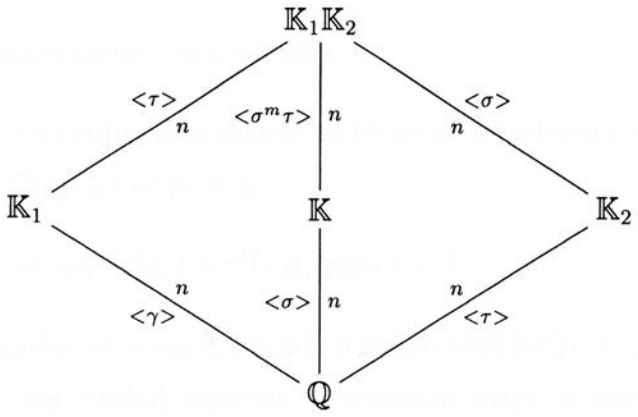
2. $Tr_{\mathbb{K}_2|\mathbb{Q}}(x_2\tau^t(x_2)) = \delta_{0,t}p_2^2$, *para* $t = 0, \ldots, n-1$.

então existe $x = Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{K}}(x_1x_2) \in \mathbb{K}$, *tal que*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\gamma^t(x)) = \delta_{0,t}p_1^2p_2^2, \quad para \quad t = 0, \ldots, n-1,$$

onde $\langle\gamma\rangle = Gal(\mathbb{K}|\mathbb{Q})$.

Demonstração: Seja $1 \leq m \leq n-1$ tal que $\langle\sigma^m\tau\rangle = Gal(\mathbb{K}_1\mathbb{K}_2|\mathbb{Q})$ e $\gamma = \sigma^{-m}\tau$ é um gerador do $Gal(\mathbb{K}|\mathbb{Q})$. Deste modo temos o seguinte diagrama



Assim, se

$$x = \sum_{b=0}^{n-1}(\sigma^m\tau)^b(x_1x_2),$$

então,

$$\begin{aligned} x\gamma^t(x) &= \sum_{b,c=0}^{n-1}\sigma^{mb}(x_1)\tau^b(x_2)\sigma^{-mt}\tau^t\sigma^{mc}(x_1)\sigma^{-mt}\tau^t\tau^c(x_2) \\ &= \sum_{b,c=0}^{n-1}\sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\tau^b(x_2\tau^{t-b+c}(x_2)), \end{aligned}$$

logo,

$$\begin{aligned} nTr_{\mathbb{K}|\mathbb{Q}}(x\gamma^t(x)) &= Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(x\gamma^t(x)) \\ &= \sum_{b,c=0}^{n-1}Tr_{\mathbb{K}_1\mathbb{K}_2|\mathbb{Q}}(\sigma^{mb}\tau^b[(x_1\sigma^{m(c-t-b)}(x_1))(x_2\tau^{c+t-b}(x_2))]) \\ &= \sum_{b,c=0}^{n-1}Tr_{\mathbb{K}_1|\mathbb{Q}}(x_1\sigma^{m(c-t-b)}(x_1))Tr_{\mathbb{K}_2|\mathbb{Q}}(x_2\tau^{c+t-b}(x_2)). \qquad (5.6) \end{aligned}$$

Por hipótese, temos que os termos da soma na Equação (5.6) são diferentes de zero somente quando $m(c-b-t) = 0$ e $c+t-b = 0$. Mas isto é equivalente a dizer que $t = 0$ e $c = b$.

unesp

Isto significa que na Equação (5.6) é não nulo se, e somente se, $t = 0$, se, e somente se, (5.6) é igual a $np_1^2p_2^2$. ■

Segue da Proposição (5.4.3) que se conhecermos dois primos p_1 e p_2 que ramificam em um corpo cíclico $\mathbb{K}$ de grau n, então podemos encontrar um elemento $x \in \mathbb{K}$ tal que sua forma traço é isomorfa a matriz identidade. Além disso, não precisamos conhecer explicitamente $\mathbb{K}$ para construirmos o reticulado. Assim, o algoritmo para a construção do reticulado é dado por:

1. Escolha uma dimensão prima n.
2. Escolha p_1 e p_2 satisfazendo as hipóteses.
3. Calcule x_1, x_2 e seus conjugados usando as técnicas anteriores e mergulhe $\mathbb{K}$ em $\mathbb{Q}(\xi_{p_1p_2})$ se $p_2 > n$ ou em $\mathbb{Q}(\xi_{p_1n^2})$ se $p_2 = n$.
4. Calcule x com base em $\sigma^t(x_1)$ e $\tau^t(x_2)$, para $t = 0, \ldots, n-1$.
5. Calcule os conjugados de x em $\mathbb{K}$ usando o grupo $Gal(\mathbb{K}|\mathbb{Q})$. O grupo cíclico $Gal(\mathbb{K}|\mathbb{Q})$ de ordem n deve ser cuidadosamente selecionado entre os subgrupos de ordem n do grupo $Gal(\mathbb{K}_1\mathbb{K}_2|\mathbb{Q})$.
6. Calcule a matriz R.

Exemplo 5.4.4 *Consideramos dois casos já calculados anteriormente. Para isso, seja a dimensão prima $n = 3$ e os primos $p_1 = 13$ e $p_2 = 3$. Seja $\xi = \xi_{13\times 3^2} = \xi_{117} = \xi$. Na base de $\mathbb{Q}(\xi)$, de grau 72, temos por exemplo que*

$$\begin{aligned} x_1 \;=\; & (5,0,0,1,0,0,0,0,0,0,0,0,-3,0,0,0,0,3,0,0,-3,0,0,\\ & 0,0,0,3,0,0,0,0,0,0,0,0,-1,0,0,0,0,0,1,0,0,0,0,0,0,\\ & 0,0,0,-3,0,0,-1,0,0,0,0,0,-3,0,0,-1,0,0,0,0,0,0,0,0) \end{aligned}$$

da mesma forma calculamos $x_2 \in \mathbb{Q}(\xi)$.

Pela Proposição (5.4.3), temos que

$$x = x_1x_2 + \sigma(x_1)\tau(x_2) + \sigma^2(x_1)\tau^2(x_2).$$

Fazendo os cálculos,

$$x \;=\; (13,5,-9,0,-2,7,0,2,0,0,7,-9,0,-3,7,0,0,2,0,0,-2,0,-2,2,$$

unesp

$$0,-5,3,0,7,-9,0,0,0,0,-5,2,0,7,-7,0,5,-7,0,0,7,0,2,-7,$$
$$0,0,-7,0,-4,7,0,7,0,0,-2,-2,0,0,9,0,0,-3,0,0,-7,0,-5,2)$$

Os conjugados de x são calculados a partir do gerador do $Gal(\mathbb{K}|\mathbb{Q})$ é γ, definido por $\gamma(\xi) = \xi^{40}$.

Finalmente,

$$R = \begin{pmatrix} 0,55329 & 0,76837 & -0,32166 \\ -0,32166 & 0,55329 & 0,76837 \\ 0,76837 & -0,32166 & 0,55329 \end{pmatrix}.$$

5.4.4 Distância produto mínima via a construção cíclica

Nesta seção veremos uma comparação entre os três casos de construções via a construção cíclica.

Sejam $\mathbb{K}$ uma extensão cíclica de $\mathbb{Q}$ de grau primo $n > 2$ e $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{A}^2 = \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})^{-1}$. Como o ideal $\mathcal{A}$ é principal, segue que em todos os casos e dimensões consideradas, podemos calcular a distância produto mínima usando o Corolário (4.5.1), que é dado por $d_{p,min}(\Lambda) = \frac{1}{\sqrt{D_{\mathbb{K}}}}$. A Tabela (5.4) apresenta alguns valores da $d_{p,min}(\Lambda)$ dos reticulados obtidos via os os casos I e II.

Exemplo 5.4.5 *Através do Exemplo (5.4.1) temos para $n = 3$, $p = 13$, $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta^3 - \theta^2 - 4\theta - 1 = 0$, que o discriminante de $\mathbb{K}$ é $D_{\mathbb{K}} = 13^2$. Logo, $d_{p,min}(\Lambda) = \dfrac{1}{\sqrt{D_{\mathbb{K}}}} = \dfrac{1}{13}$.*

Exemplo 5.4.6 *No Exemplo(5.4.3) para $n = 3$, $N = 9$ e $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta^3 - 3\theta - 1 = 0$, que $D_{\mathbb{K}} = 3^4$, e portanto, $d_{p,min}(\Lambda) = \frac{1}{9}$.*

Para cada dimensão prima n, vimos construções de reticulados de diversidade máxima. O desempenho do reticulado é avaliado pela distância produto mínima. Por exemplo, para $n = 5$, podemos construir os seguintes reticulados, dependendo da escolha do primo p.

1. No caso I, onde somente 11 se ramifica em $\mathbb{K}$, temos que $d_{p,min}(\Lambda) = 1/121$;
2. No caso I, onde somente 31 se ramifica em $\mathbb{K}$ temos que $d_{p,min}(\Lambda) = 1/961$;
3. No caso II, onde somente 5 se ramifica em $\mathbb{K}$ temos que $d_{p,min}(\Lambda) = 1/625$;
4. No caso III, onde 11 e 31 se ramificam em $\mathbb{K}$, temos que $d_{p,min}(\Lambda) = 1/(121 \times 961)$;
5. No caso III, onde 11 e 5 se ramificam em $\mathbb{K}$, temos $d_{p,min}(\Lambda) = 1/(121 \times 625)$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Tabela 5.4: Algumas distâncias produto mínima para os casos I e II, onde N é tal que $\mathbb{K} \subseteq \mathbb{Q}(\xi_N)$

n	N	$D_{\mathbb{K}}$	$d_{p,min}(\Lambda)$	$\sqrt[n]{d_{p,min(\Lambda)}}$
3	7	7^2	$\frac{1}{7}$	0,522757958
3	13	13^2	$\frac{1}{13}$	0,425290370
5	11	11^2	$\frac{1}{11}$	0,383215375
5	31	31^4	$\frac{1}{31^2}$	0,253195115
7	29	29^6	$\frac{1}{29^3}$	0,236188093
11	23	23^{10}	$\frac{1}{23^5}$	0,240454440
11	67	67^{10}	$\frac{1}{67^5}$	0,147899259
13	53	53^{12}	$\frac{1}{53^6}$	0,160022248
17	103	103^{16}	$\frac{1}{103^8}$	0,112923019
19	191	191^{18}	$\frac{1}{191^9}$	0,083082682
23	47	47^{22}	$\frac{1}{47^{11}}$	0,158599211
29	59	59^{28}	$\frac{1}{59^{14}}$	0,139670898
3	9	9^2	$\frac{1}{9}$	0,480749856
5	25	5^8	$\frac{1}{5^4}$	0,265945932
7	49	7^{12}	$\frac{1}{7^6}$	0,188638463

Como nosso objetivo é maximizar a distância produto mínima, neste exemplo, a melhor escolha é a primeira construção, isto é, quando somente um primo se ramifica, tamando este o menor possível. Consideremos o seguinte resultado.

De modo geral, para maximizar a distância produto mínima devemos tomar o menor $p > n$ que se ramifica em $\mathbb{K}$. Como vimos, no caso I, $D_{\mathbb{K}} = p^{n-1}$, já no caso III, $D_{\mathbb{K}} = (p_1 p_2)^{n-1}$. Logo o caso I é sempre melhor que o caso III.

Proposição 5.4.4 *Se $n > 2$ é uma dimensão prima então a construção do Caso I, com o menor primo possível p, maximiza a distância produto mínima.*

Demonstração: Pela Proposição (3.2.5), temos que, $D_{\mathbb{K}} = p^{n-1}$. Seguindo o mesmo raciocínio daquela demonstração, como p é totalmente ramificado em $\mathbb{K}$, segue que $\mathfrak{p}^n \mid \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})$, mas $\mathfrak{p}^k \nmid \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})$, para $k > n$. Considerando a transitividade do diferente

$$\Delta(\mathbb{Z}[\xi]|\mathbb{Q}) = \Delta(\mathbb{Z}[\xi]|\mathbb{K})\Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q}) \tag{5.7}$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

e fazendo $\mathfrak{p} = (1-\xi)\mathbb{Z}[\xi]$, $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p} \cap \mathcal{O}_{\mathbb{K}}$. Note que $\mathfrak{p}_{\mathbb{K}}\mathbb{Z}[\xi] = \mathfrak{p}^{n-1}$, pois p é totalmente ramificado. Isto mostra que $\Delta(\mathbb{Z}[\xi]|\mathbb{Q}) = \mathfrak{p}^{n(2n-3)}$ e que $\Delta(\mathbb{Z}[\xi]|\mathbb{K}) = \mathfrak{p}^{n-2}$. De (5.7) temos que

$$\Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q}) = \mathfrak{p}^{2(n-1)^2} = (\mathfrak{p}^{n-1})^{2(n-1)} = \mathfrak{p}_{\mathbb{K}}^{2(n-1)}$$

Então temos $D_{\mathbb{K}} = N_{\mathbb{K}|\mathbb{Q}}(\mathfrak{p}_{\mathbb{K}}^{2(n-1)}) = p^{2(n-1)}$. Disto segue que quanto maior $n^2 > p$, a distância mínima é menor que no caso onde $p > n$. ∎

5.5 Construção mista

Nesta seção veremos uma técnica de construção de ideais reticulados que combina as construções ciclotômica e cíclica, resultando em $\mathbb{Z}^n$-reticulados rotacionados em outras dimensões.

Proposição 5.5.1 *Seja $\mathbb{K}$ a composição de N extensões de Galois $\mathbb{K}_j$ de grau n_j, isto é, $\mathbb{K}$ é o menor corpo que contém todos os $\mathbb{K}_j$. Suponhamos que $mdc(D_{\mathbb{K}_i}, D_{\mathbb{K}_j}) = 1$ para todo $i \neq j$. Se existir um α_j tal que a forma traço sobre $\mathbb{K}_j$, $Tr(\alpha_j xy)$, é isomorfo a forma identidade de grau n_j, para $j = 1, \ldots, N$, então a forma traço sobre $\mathbb{K}$,*

$$Tr(\alpha_1 xy) \otimes Tr(\alpha_2 xy) \otimes \cdots \otimes Tr(\alpha_N xy)$$

é isomorfo à forma unidade $\langle 1, 1, \ldots, 1\rangle$ de grau $n = \prod_{j=1}^{N} n_j$.

Demonstração: Consideremos o caso $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$. Sejam $\{\omega_1, \ldots, \omega_{n_1}\}$ e $\{\omega_1', \ldots, \omega_{n_2}'\}$ as bases integrais de $\mathbb{K}_1$ e $\mathbb{K}_2$, respectivamente. Como $\mathbb{K}_1$ e $\mathbb{K}_2$ são extensões de Galois sobre $\mathbb{Q}$ com discriminantes coprimos, segue que $\{\omega_j\omega_k' | j = 1, \ldots, n_1, k = 1, \ldots, n_2\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$. Usando o fato de que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha_1\omega_j\omega_i\alpha_2\omega_l'\omega_k') = Tr_{\mathbb{K}_1|\mathbb{Q}}(\alpha_1\omega_j\omega_i)Tr_{\mathbb{K}_2|\mathbb{Q}}(\alpha_2\omega_l'\omega_k'))$$

temos que existe $\alpha \in \mathbb{K}$ tal que $Tr(\alpha xy) = Tr_{\mathbb{K}_1|\mathbb{Q}}(\alpha_1 xy) \otimes Tr_{\mathbb{K}_2|\mathbb{Q}}(\alpha_2 xy)$. Por indução sobre N concluímos a demonstração. ∎

Com base na Proposição (5.5.1), temos que a matriz geradora do reticulado pode ser obtida como o produto tensorial das matrizes geradoras $R^{(j)}$ das correspondentes formas traço, para $j = 1, \ldots, N$, ou seja

$$R = R^{(1)} \otimes R^{(2)} \otimes \cdots \otimes R^{(N)}.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Corolário 5.5.1 *Sejam $m = p_1 \dots p_N$ um produto de N primos distintos, $\xi_j = e^{\frac{2\pi i}{p_j}}$ para $j = 1, \dots, N$, e $\mathbb{K}$ a composição dos $\mathbb{K}_j = \mathbb{Q}(\xi_j + \xi_j^{-1})$, para $j = 1, \dots, N$, isto é, $\mathbb{K}$ é o menor corpo que contém todos os $\mathbb{K}_j$. Se $\alpha_j = (1 - \xi_j)(1 - \xi_j^{-1})$ então*

$$\frac{1}{p_1} Tr(\alpha_1 xy) \otimes \cdots \otimes \frac{1}{p_N} Tr(\alpha_N xy)$$

é isomorfo à forma unidade $\langle 1, \dots, 1 \rangle$ de grau $n = \prod_{j=1}^{N} \frac{(p_j - 1)}{2}$

Demonstração: Segue diretamente da Proposição (5.5.1). ∎

Observação 5.5.1 *O Corolário (5.5.1) genenereliza a construção ciclotômica para $\mathbb{Q}(\xi_m)$, onde m é produto de primos e livre de quadrados. Podemos construir $\mathbb{Z}^n$ reticulados rotacionados em dimensões, como $n = 10, 12, 16, 22, 24, 27, 28$. Para as dimensões 4 e 25 temos que*

1. *Para $n = 4$, podemos construir um reticulado combinando dois reticulados rotacionados de dimensão 2, usando o Caso III da construção cíclica.*
2. *Para $n = 25$, podemos construir um reticulado combinando dois $\mathbb{Z}^n$-reticulados rotacionados de dimensão 5, usando o Caso I e o Caso II da construção cíclica.*

Proposição 5.5.2 *Se $\mathbb{K}$ é uma composição de duas extensões de Galois de graus n_1 e n_2, respectivamente, cujos discriminantes sejam primos entre si, então o discriminante de $\mathbb{K}$ é $D_{\mathbb{K}} = D_{\mathbb{K}_1}^{m_1} D_{\mathbb{K}_2}^{m_2}$, onde $m_j = [\mathbb{K}|\mathbb{K}_j] = n/n_j$, para $j = 1, 2$.*

Demonstração: Pela Proposição (3.2.3) temos que

$$\Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q}) = \Delta(\mathcal{O}_{\mathbb{K}_1}|\mathbb{Q})\Delta(\mathcal{O}_{\mathbb{K}_2}|\mathbb{Q}).$$

Assim,

$$\begin{aligned} N(\Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})) &= N_{\mathbb{K}|\mathbb{Q}}(\Delta(\mathcal{O}_{\mathbb{K}_1}|\mathbb{Q}))N_{\mathbb{K}|\mathbb{Q}}(\Delta(\mathcal{O}_{\mathbb{K}_2}|\mathbb{Q})) \\ &= N_{\mathbb{K}_1/\mathbb{Q}}(\Delta(\mathcal{O}_{\mathbb{K}_1}|\mathbb{Q}))^{m_1} N_{\mathbb{K}_2/\mathbb{Q}}(\Delta(\mathcal{O}_{\mathbb{K}_2}|\mathbb{Q}))^{m_2} = D_{\mathbb{K}_1}^{m_1} D_{\mathbb{K}_2}^{m_2} \end{aligned}$$

uma vez que $N(\Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Q})) = D_{\mathbb{K}}$. ∎

Como conseqüência direta temos que

$$d_{p,min}(\Lambda) = \frac{1}{\sqrt{D_{\mathbb{K}_1} D_{\mathbb{K}_2}}}$$

Alguns valores numéricos de $d_{p,min}(\Lambda)$ são dados na Tabela 5.5

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Exemplo 5.5.1 *Se $m = 5 \times 7$, temos que $n_1 = 2$, $n_2 = 3$ e $n = 2.3 = 6$. Sejam $\xi_{p_j} = e^{\frac{2\pi i}{p_j}}$, para $j = 1, 2$ e $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_1 = \mathbb{Q}(\xi_5 + \xi_5^{-1})$ e $\mathbb{K}_2 = \mathbb{Q}(\xi_7 + \xi_7^{-1})$. A matriz geradora do reticulado é dada por $R = R^{(1)} \otimes R^{(2)}$, onde $R^{(1)} = \frac{1}{\sqrt{5}} T_1 N_1 A_1$ e $R^{(2)} = \frac{1}{\sqrt{7}} T_2 N_2 A_2$. Notemos que a matriz $R^{(1)}$ foi construída no Exemplo (5.3.1) e é dada por*

$$R^{(1)} = \begin{pmatrix} -0,52573 & -0,85065 \\ -0,85065 & 0,52573 \end{pmatrix}.$$

Para a construção de $R^{(2)}$, temos que

$$N_2 = \begin{pmatrix} 2cos(\frac{2\pi}{7}) & 2cos(\frac{4\pi}{7}) & 2cos(\frac{6\pi}{7}) \\ 2cos(\frac{4\pi}{7}) & 2cos(\frac{8\pi}{7}) & 2cos(\frac{12\pi}{7}) \\ 2cos(\frac{6\pi}{7}) & 2cos(\frac{12\pi}{7}) & 2cos(\frac{18\pi}{7}) \end{pmatrix} = \begin{pmatrix} 2cos(\frac{2\pi}{7}) & -2cos(\frac{3\pi}{7}) & -2cos(\frac{1\pi}{7}) \\ -2cos(\frac{3\pi}{7}) & -2cos(\frac{1\pi}{7}) & 2cos(\frac{2\pi}{7}) \\ -2cos(\frac{1\pi}{7}) & 2cos(\frac{2\pi}{7}) & -2cos(\frac{3\pi}{7}) \end{pmatrix},$$

$$T_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad e \quad A_2 = \begin{pmatrix} \sqrt{2 - (\xi_7 + \xi_7^{-1})} & 0 & 0 \\ 0 & \sqrt{2 - (\xi_7^2 + \xi_7^{-2})} & 0 \\ 0 & 0 & \sqrt{2 - (\xi_7^3 + \xi_7^{-3})} \end{pmatrix}$$

Assim,

$$R^{(2)} = \begin{pmatrix} -0,32798 & -0,591 & -0,73696 \\ -0,73696 & -0,32798 & 0,591 \\ -1,5636 & 0,73696 & -0,32798 \end{pmatrix}$$

Finalmente, temos que

$$R = \begin{pmatrix} -0.52573 & -0.85065 \\ -0.85065 & 0.52573 \end{pmatrix} \otimes \begin{pmatrix} -0,32798 & -0,591 & -0,73696 \\ -0,73696 & -0,32798 & 0,591 \\ -1,5636 & 0,73696 & -0,32798 \end{pmatrix}$$

Portanto, a distância produto mínima do reticulado é dada por $d_{p,min}(\Lambda) = \frac{1}{\sqrt{5^3 7^4}}$.

Exemplo 5.5.2 *Considere agora $m = 7 \times 11$. Logo, $n_1 = 3$, $n_2 = 5$, e $n = 3 \times 5 = 15$. Seja $\mathbb{K} = \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_j = \mathbb{Q}(\xi_{p_j} + \xi_{p_j}^{-1})$, para $j = 1, 2$. Como vimos, a matriz do reticulado é dada por $R = R^{(1)} \otimes R^{(2)}$. A matriz $R^{(1)}$, conforme o Exemplo (5.5.1), é dada por*

$$R^{(1)} = \begin{pmatrix} -0,32798 & -0,591 & -0,73696 \\ -0,73696 & -0,32798 & 0,591 \\ -1,5636 & 0,73696 & -0,32798 \end{pmatrix}.$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Para a construção da matriz $R^{(2)} = \frac{1}{\sqrt{11}} T_2 N_2 A_2$, *temos que*

$$N_2 = \begin{pmatrix} 2cos(\frac{2\pi}{11}) & 2cos(\frac{4\pi}{11}) & 2cos(\frac{6\pi}{11}) & 2cos(\frac{8\pi}{11}) & 2cos(\frac{10\pi}{11}) \\ 2cos(\frac{4\pi}{11}) & 2cos(\frac{8\pi}{11}) & 2cos(\frac{12\pi}{11}) & 2cos(\frac{16\pi}{11}) & 2cos(\frac{20\pi}{11}) \\ 2cos(\frac{6\pi}{11}) & 2cos(\frac{12\pi}{11}) & 2cos(\frac{18\pi}{11}) & 2cos(\frac{24\pi}{11}) & 2cos(\frac{30\pi}{11}) \\ 2cos(\frac{8\pi}{11}) & 2cos(\frac{16\pi}{11}) & 2cos(\frac{24\pi}{11}) & 2cos(\frac{32\pi}{11}) & 2cos(\frac{40\pi}{11}) \\ 2cos(\frac{10\pi}{11}) & 2cos(\frac{20\pi}{11}) & 2cos(\frac{30\pi}{11}) & 2cos(\frac{40\pi}{11}) & 2cos(\frac{50\pi}{11}) \end{pmatrix}$$

$$= \begin{pmatrix} 2cos(\frac{2\pi}{11}) & 2cos(\frac{4\pi}{11}) & -2cos(\frac{5\pi}{11}) & -2cos(\frac{3\pi}{11}) & -2cos(\frac{\pi}{11}) \\ 2cos(\frac{4\pi}{11}) & -2cos(\frac{3\pi}{11}) & -2cos(\frac{\pi}{11}) & -2cos(\frac{5\pi}{11}) & 2cos(\frac{2\pi}{11}) \\ -2cos(\frac{5\pi}{11}) & -2cos(\frac{\pi}{11}) & 2cos(\frac{4\pi}{11}) & 2cos(\frac{2\pi}{11}) & -2cos(\frac{3\pi}{11}) \\ -2cos(\frac{3\pi}{11}) & -2cos(\frac{5\pi}{11}) & 2cos(\frac{2\pi}{11}) & -2cos(\frac{\pi}{11}) & 2cos(\frac{4\pi}{11}) \\ -2cos(\frac{\pi}{11}) & 2cos(\frac{2\pi}{11}) & -2cos(\frac{3\pi}{11}) & 2cos(\frac{4\pi}{11}) & -2cos(\frac{5\pi}{11}) \end{pmatrix},$$

$$T_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 & 0 \\ 0 & 0 & 0 & \alpha_4 & 0 \\ 0 & 0 & 0 & 0 & \alpha_5 \end{pmatrix},$$

onde $\alpha_1 = \sqrt{2 - 2cos(\frac{2\pi}{11})}$, $\alpha_2 = \sqrt{2 - 2cos(\frac{4\pi}{11})}$, $\alpha_3 = \sqrt{2 + 2cos(\frac{5\pi}{11})}$, $\alpha_4 = \sqrt{2 + 2cos(\frac{3\pi}{11})}$ *e* $\alpha_5 = \sqrt{2 + 2cos(\frac{\pi}{11})}$. *Logo,*

$$R^{(2)} = \begin{pmatrix} -0,169891 & -0,32602 & -0,45573 & -0,54853 & -0,59688 \\ -0,45573 & -0,59688 & -0,32602 & 0,16989 & 0,54853 \\ -0,59688 & -0,16989 & 0,54853 & 0,32602 & -0,45573 \\ -0,54853 & 0,45573 & 0,16989 & -0,59688 & 0,32602 \\ -0,32602 & 0,54853 & -0,59688 & 0,45573 & -0,16989 \end{pmatrix}.$$

E, finalmente,

$$R = R^{(1)} \otimes R^{(2)}.$$

Portanto, a distância produto mínima do reticulado é dada por $d_{p,min}(\Lambda) = \frac{1}{\sqrt{7^{10}11^{12}}}$.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Tabela 5.5: Distância Produto Mínima para Construções Mistas

n	$d_{p,min}(\Lambda)$	$\sqrt[n]{d_{p,min}}(\Lambda)$
4	$\frac{1}{\sqrt{5.8}}$	0,39763536
6	$\frac{1}{\sqrt{5^3 7^4}}$	0,34958931
10	$\frac{1}{\sqrt{5^5 11^8}}$	0,25627156
12	$\frac{1}{\sqrt{5^6 13^{10}}}$	0,22967537
15	$\frac{1}{\sqrt{7^{10} 11^{12}}}$	0,20032888
16	$\frac{1}{\sqrt{5^8 17^{14}}}$	0,19361370
18	$\frac{1}{\sqrt{5^9 19^{16}}}$	0,18068519
22	$\frac{1}{\sqrt{5^{11} 23^{20}}}$	0,16080157
24	$\frac{1}{\sqrt{7^{16} 17^{21}}}$	0,15134889
25	$\frac{1}{\sqrt{5^{20} 11^{10}}}$	0,10574672
27	$\frac{1}{\sqrt{7^{18} 19^{24}}}$	0,14124260
28	$\frac{1}{\sqrt{5^{14} 29^{26}}}$	0,14005125
30	$\frac{1}{\sqrt{11^{24} 13^{25}}}$	0,13161332

Observação 5.5.2 *Vimos alguns $\mathbb{Z}^n$-reticulados rotacionados a partir da teoria de ideais reticulados. As construções foram baseadas em corpos ciclotômicos, corpos cíclicos e também pela combinação desses dois. Como os reticulados construídos possuem diversidade máxima, segue que o desempenho do reticulado é avaliado pela distância produto mínima que é dada por fórmulas explícitas, relacionadas com o discriminante do corpo. Como vimos na seção 5.4.4, na construção cíclica, conseguimos melhores reticulados quando somente um primo se ramifica em $\mathbb{K}$, sendo este o menor primo possível. A tabela (5.6) compara alguns valores da $\sqrt[n]{d_{p,min}(\Lambda)}$ para construções ciclotômicas, cíclicas e mistas. Analizando a tabela vemos que para uma dada dimensão não é possível fazer as três construções, ou seja, para cada dimensão existe uma construção (ou duas) apropriada. Além disso, quando é possível realizar duas construções não é possível comparar qual construção é melhor, pois o valor da distância produto mínima do reticulado é o mesmo. O que podemos concluir com certeza é que as contruções ciclotômicas, as cíclicas e as mistas facilitam a construção de $\mathbb{Z}^n$-reticulados em todas as dimensões.*

Tabela 5.6: Comparação dos valores da $\sqrt[n]{d_{p,min}(\Lambda)}$ para construções ciclotômicas, cíclicas e mistas

n	Construção Ciclotômica	Construção Cíclica	Construção Mista
2	0, 66874030	-	-
3	0, 52275795	0, 52275795	-
4	-	-	0.3976536
5	0, 38321537	0, 38321537	-
6	0, 34344479	-	0, 34958931
7	-	0, 23618809	-
8	0, 28952001	-	-
9	0, 27018738	-	-
10	-	-	0, 25627156
11	0, 24045444	0, 24045444	-
12	-	-	0, 22967537
13	-	0, 16002224 -	-
14	0, 20942547	-	-
15	0, 20138689	-	0, 20032888
16	-	-	0, 19361370
17	-	011292301	-
18	018174408	-	0, 18068519
19	-	0, 08308268	-
20	0, 17136718	-	-
21	0, 16678534	-	-
22	-	-	0, 16080157
23	0, 15859921	0, 15859921	-
24	-	-	0, 15134889
25	-	-	0, 10574672
26	0, 14825905	-	-
27	-	-	0, 14124260
28	-	-	0, 14005125
29	0, 13967089	0, 13967089	-
30	0, 13711677	-	0, 13711677

unesp

5.6 Método de Krüskemper

Krüskemper mostrou [19] que toda forma $\mathbb{Z}$-bilinear simétrica não degenerada pode ser compreendida como uma forma traço. Nesta seção veremos uma construção de ideais reticulados usando o método de Krüskemper. Deste, veremos que todo reticulado inteiro pode ser construído como um ideal reticulado sobre $\frac{\mathbb{Z}[X]}{\langle f(X)\rangle}$, onde $f(X) \in \mathbb{Z}[X]$ é um polinômio mônico irredutível.

Seja L um $\mathbb{Z}$-módulo livre finitamente gerado de rank n e seja $b : L \times L \longrightarrow \mathbb{Z}$ uma forma bilinear simétrica. Seja $f(x)$ um polinômio mônico irredutível de grau n e $\theta \in \mathbb{C}$ uma raiz de $f(x)$. Então $\frac{\mathbb{Z}[x]}{\langle f(x)\rangle} = \mathbb{Z}[\theta]$, cuja base é $\{1, \theta, \ldots, \theta^{n-1}\}$. Seja $\mathcal{I}$ um ideal de $\mathbb{Z}[\theta]$ e $\mathcal{I}^*$ o codiferente de $\mathcal{I}$.

Teorema 5.6.1 *Se A é uma matriz $n \times n$ cujo polinômio característico, χ_A, é irredutível e θ é uma raiz de χ_A, então o autovetor $(v_1, v_2, \ldots, v_n)$ associado a θ forma uma base de um ideal de $\mathbb{Z}[\theta]$.*

Demonstração: Como todas as raízes de χ_A são simples, os correspondentes autovetores são unicamente determinados. Da definição de autovetor temos que

$$\theta(v_1, v_2, \ldots, v_n) = A(v_1, v_2, \ldots, v_n). \tag{5.8}$$

Seja $v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_n)$ o cofator do i-ésimo elemento de uma coluna fixada da matriz $(A - \theta I_n)$. De (5.8) segue que

$$\theta^i(v_1, v_2, \ldots, v_n) = A^i(v_1, v_2, \ldots, v_n), \quad para \quad i = 1, \ldots, n.$$

Como $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ forma uma base de $\mathbb{Z}[\theta]$, segue que

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n, a_i \in \mathbb{Z}$$

gera um ideal de $\mathbb{Z}[\theta]$. ∎

Teorema 5.6.2 *(Taussky) Seja $b : L \times L \longrightarrow \mathbb{Z}$ uma forma bilinear simétrica e S a matriz que representa b sobre $\mathbb{Z}$. Seja $A \in M_n(\mathbb{Z})$ uma matriz cujo polinômio característico, χ_A, é irredutível e $S^{-1}AS = A^t$. Então S é a matriz de um ideal reticulado.*

Demonstração: Sejam $S = (s_{ij})_{i,j=1}^n \in M_n(\mathbb{Z})$ a matriz de b e $A \in M_n(\mathbb{Z})$uma matriz tal que χ_A é irredutível e $S^{-1}AS = A^t$. Provemos que b é uma forma traço escalonada. Seja

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

θ uma raiz de χ_A, assim, θ é um inteiro algébrico, pois χ_A é mônico com coeficientes em $\mathbb{Z}$. Pelo Teorema (5.6.1), existe um autovetor $v_\theta = (v_1, v_2, \ldots, v_n)^t$ de A associado a θ, com $v_i \in \mathbb{Z}[\theta]$, tal que $\{v_1, v_2, \ldots, v_n\}$ é uma $\mathbb{Z}$-base de um ideal de $\mathbb{Z}[\theta]$. Pela primeira prova do Teorema 1 de [21], existe um autovetor $v'_\theta = (v'_1, v'_2, \ldots, v'_n)^t$ de A^t associado a θ, com $v'_i \in \mathbb{Q}(\theta)$ e tal que

$$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v_i v_j) = \delta_{ij}, \forall i, j \tag{5.9}$$

Como $S^{-1}AS = A^t$, segue que $A^t S^{-1} v_\theta = S^{-1} A v_\theta$. Assim, v'_θ e $S^{-1}v_\theta$ são ambos autovetores de A^t associados a θ. Como $\chi_{A^t} = \chi_A$ é irredutível sobre $\mathbb{Q}$, então é separável, e portanto seus autovalores são distintos. Desta forma, os subespaços associados a θ tem dimensão 1. Isto implica que existe $\alpha \in \mathbb{Q}(\theta)$ tal que $v'_\theta = \alpha S^{-1} v_\theta$, isto é, $S v'_\theta = \alpha v_\theta$. Denote $S = (s_{ij})_{i,j}$, assim,

$$\sum_{j=1}^{n} s_{ij} v'_j = \alpha v_i, \forall i$$

então

$$\sum_{j=1}^{n} s_{ij} v'_j v_k = \alpha v_i v_k, \forall i, k,$$

logo,

$$\sum_{j=1}^{n} s_{ij} Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v'_j v_k) = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha v_i v_k).$$

Pela Equação (5.9), $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}$ segue que $s_{ik} = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha v_i v_k)$. Portanto, S é a matriz de uma forma traço escalonada. Definindo o ideal $\mathcal{I} = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \ldots \oplus \mathbb{Z}v_n$ concluímos a demonstração.

■

Teorema 5.6.3 *Seja (L, b) um reticulado inteiro. Então existe um inteiro algébrico θ e um ideal $\mathcal{I}$ de $\mathbb{Z}[\theta]$ e $\alpha \in (\mathcal{I}^2)^* \subseteq \mathbb{Q}(\theta)$ tal que b é isomorfa a*

$$\mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto Tr(\alpha xy).$$

Demostração: Pelo Teorema (5.6.2), basta mostrar que sempre existe uma matriz $A \in M_{n\times n}(\mathbb{Z})$ cujo polinômio característico χ_A é irredutível e totalmente real e que satisfaça $S^{-1}AS = A^t$. Considere a matriz $N = (X_{ij})$, onde $X_{ij} = X_{ji}$ são indeterminadas. Em [19] é mostrado que o polinômio característico de SN, χ_{SN} é irredutível. Pelo Teorema da

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

irredutibilidade de Hilbert, existe $x_{ij} = x_{ji} \in \mathbb{Q}$ tal que $\chi_{S(x_{ij})}$ é irredutível e totalmente real. Tome A definida por $A = S(x_{ij})$. Assim, $S^{-1}AS = A^t$. ∎

Baseado na demonstração do Teorema (5.6.3), obtemos um algoritmo que calcula $v_1, \ldots, v_n$ e α, tal que $\mathcal{I} = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n$ e o ideal reticulado

$$\mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$$
$$(x, y) \longmapsto Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha xy)$$

é isomorfo a forma unidade $\langle 1, ..., 1 \rangle$ de grau n. Tal algoritmo pode resumido nos seguintes passos:

1. Cáculo da matriz A.

   Primeiramente encontramos uma matriz simétrica A, com coeficientes em $\mathbb{Z}$, tal que seu polinômio característico, $\chi_A(x)$, seja irredutível sobre $\mathbb{Z}$ e só possua raízes reais. Esta matriz pode ser obtida aleatoriamente.

2. Cálculo do vetor v_θ.

   Seja θ uma raiz de $\chi_A(x)$. Considere

   $$v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_n).$$

   O vetor v_θ é dado por

   $$v_\theta = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

   onde, v_j é o j-ésimo cofator em uma dada coluna da matriz $(A - \theta I_n)$.

3. Calculo da matriz V.

   V é a matriz das coordenadas de $v_1, \ldots, v_n$ na base $\{1, \theta, \ldots, \theta^{n-1}\}$.

4. Calculo da matriz H.

   A matriz H é dada por

   $$H = \left(Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i+j-2})\right)_{i,j=1}^{n}.$$

5. Cálculo do vetor v'_θ.

   O vetor v'_θ é dado por

   $$v'_\theta = \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix},$$

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

onde $v_j' = \sum_{i=1}^{n} m_{ij}\theta^{i-j}$, e $(m_{ij})_{i,j=1}^{n} = H^{-1}(V^t)^{-1}$.

6. Cálculo de α.

   O elemento α é dado por $\alpha = \frac{v_i'}{v_i}$, para algum $i \in \{1, \ldots, n\}$. Observamos que o cálculo de α é feito somente para um valor de i.

7. Cálculo da matriz geradora do reticulado.

   A matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \cdots & \sqrt{\alpha_n}\sigma_n(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \cdots & \sqrt{\alpha_n}\sigma_n(v_2) \\ \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(v_n) & \cdots & \sqrt{\alpha_n}\sigma_n(v_n) \end{pmatrix}.$$

   Observamos que $MM^t = I_n$.

Exemplo 5.6.1 *Seja A uma matriz dada por*

$$A = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

O polinômio característico de A é $\chi_A(x) = x^4 - 6x^2 + 4$, que é irredutível sobre $\mathbb{Z}$. Uma vez que $v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_n)$, e escolhendo a coluna 1, obtemos que $v_j = (-1)^{1+j}\Delta_{1j}(A - \theta I_n)$. Fazendo os cálculos, obtemos que

$$v_\theta = \begin{pmatrix} -\theta^3 + 2\theta \\ -2\theta^2 + 2 \\ -2\theta \\ -2 \end{pmatrix}$$

Escrevendo v_θ na base $\{1, \theta, \ldots, \theta^{n-1}\}$, obtemos a matriz V, dada por

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

unesp

Como θ é raiz de $x^4 - 6x^2 + 4$, segue que

$$\begin{aligned} \theta^4 &= 6\theta^2 - 4, \\ \theta^5 &= 6\theta^3 - 4\theta \ e \\ \theta^6 &= 32\theta^2 - 24. \end{aligned}$$

Da Definição (1.3.2) temos que $Tr(1) = 4$ e $Tr(\theta) = 0$. Para calcular $Tr(\theta^2)$ e $Tr(\theta^3)$ também usaremos a Definição (1.3.2). Como o polinômio irredutível de θ^2 sobre $\mathbb{Q}$ é $x^2 - 6x + 4$, segue que

$$\begin{aligned} &Tr(\theta^2) = Tr_{\mathbb{Q}(\theta^2)|\mathbb{Q}}(Tr_{\mathbb{Q}(\theta)|\mathbb{Q}(\theta^2)}(\theta^2)) = Tr_{\mathbb{Q}(\theta^2)|\mathbb{Q}}(\theta^2.[\mathbb{Q}(\theta) : \mathbb{Q}(\theta^2)]) = 2Tr_{\mathbb{Q}(\theta^2)|\mathbb{Q}}(\theta^2) = 12. \\ &Tr(\theta^4) = Tr(6\theta^2 - 4) = 6Tr_{\mathbb{Q}(\theta^2)|\mathbb{Q}}(Tr_{\mathbb{Q}(\theta)|\mathbb{Q}(\theta^2)}(\theta^2)) - Tr(4) = 6.12 - 16 = 56. \\ &Tr(\theta^6) = Tr(32\theta^2 - 24) = 32Tr_{\mathbb{Q}(\theta^2)|\mathbb{Q}}(Tr_{\mathbb{Q}(\theta)|\mathbb{Q}(\theta^2)}(\theta^2)) - Tr(24) = 32.12 - 96 = 288. \end{aligned}$$

Como o polinômio irredutível de θ^3 sobre $\mathbb{Q}$ é $x^4 - 116x^2 + 484$, segue que

$$\begin{aligned} &Tr(\theta^3) = 0 \\ &Tr(\theta^5) = Tr(6\theta^3 - 4\theta) = 6Tr(\theta^3) - 4Tr(\theta) = 0. \end{aligned}$$

Deste modo, temos as seguintes matrizes

$$H = \begin{pmatrix} 4 & 0 & 12 & 0 \\ 0 & 12 & 0 & 56 \\ 12 & 0 & 56 & 0 \\ 0 & 56 & 0 & 288 \end{pmatrix}, \quad H^{-1} = \begin{pmatrix} \frac{7}{10} & 0 & -\frac{3}{20} & 0 \\ 0 & \frac{9}{10} & 0 & -\frac{7}{40} \\ -\frac{3}{20} & 0 & \frac{1}{20} & 0 \\ 0 & -\frac{7}{40} & 0 & \frac{3}{80} \end{pmatrix},$$

$$(V^t)^{-1} = \begin{pmatrix} 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & \frac{-1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} \\ -1 & 0 & -1 & 0 \end{pmatrix} \quad e \quad H^{-1}(V^t)^{-1} = \begin{pmatrix} 0 & \frac{3}{40} & 0 & -\frac{11}{40} \\ \frac{7}{40} & 0 & -\frac{11}{40} & 0 \\ 0 & -\frac{1}{40} & 0 & \frac{1}{20} \\ -\frac{3}{80} & 0 & \frac{1}{20} & 0 \end{pmatrix}.$$

Uma vez que $v_j' = \sum_{i=1}^{4} m_{ij}\theta^{i-1}$, temos que

$$v_\theta' = \begin{pmatrix} \frac{7}{40}\theta - \frac{3}{80}\theta^3 \\ \frac{3}{40}\theta - \frac{1}{40}\theta^2 \\ -\frac{11}{40}\theta + \frac{1}{20}\theta^3 \\ -\frac{11}{40}\theta + \frac{1}{20}\theta^2 \end{pmatrix}.$$

unesp

Escolhendo por exemplo $i = 4$ *temos* $\alpha = \frac{v_4'}{v_4} = \frac{11}{80}\theta - \frac{1}{40}\theta^2$. *Além disso, temos que o conjunto das raízes de* χ_A *é dado por* $\{-\frac{1}{2}\sqrt{10} - \frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{10} - \frac{1}{2}\sqrt{2}, -\frac{1}{2}\sqrt{10} + \frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{10} - \frac{1}{2}\sqrt{2}\}$. *Logo as imersões reais de* θ *são:* $\sigma_1(\theta) = -2,288245611$, $\sigma_2(\theta) = 2,288245611$, $\sigma_3(\theta) = -0,8740320490$ *e* $\sigma_4(\theta) = 0,8740320490$. *Assim, a matriz geradora do reticulado é dada por*

$$M = \begin{pmatrix} 0,60150 & -0,60150 & -0,37174 & 0,37174 \\ -0,68819 & -0,68819 & 0,16245 & 0,16245 \\ 0,37174 & -0,37174 & 0,60150 & -0,60150 \\ -0,16245 & -0,16245 & 0,6881 & -0,6881 \end{pmatrix}.$$

Exemplo 5.6.2 *Para a dimensão* $n = 2$, *seja a seguinte matriz*

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

O polinômio característico de A, *é dado por* $\chi_A(x) = x^2 - x - 1$, *que é irredutível sobre* $\mathbb{Z}$. *Escolhendo* $i = 2$ *e fazendo os cálculos obtemos que*

$$v_\theta = \begin{pmatrix} -1 \\ 1 - \theta \end{pmatrix}.$$

Logo,

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

Sendo θ *uma raiz de* $x^2 - x - 1$, *segue que* $\theta^2 = \theta + 1$. *Assim,* $Tr(1) = 3$ *e pela definição (1.3.2), temos que* $Tr(\theta) = 1$. *Assim,* $Tr(\theta^2) = Tr(\theta) + Tr(1) = 1 + 2 = 3$. *Deste modo, obtemos as seguintes matrizes*

$$H = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \quad H^{-1} = \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix},$$

$$(V^t)^{-1} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} \quad e \quad H^{-1}(V^t)^{-1} = \begin{pmatrix} -\frac{2}{5} & \frac{1}{5} \\ -\frac{1}{5} & -\frac{2}{5} \end{pmatrix}.$$

Como $v_j' = \sum_{i=1}^{2} m_{ij}\theta^{i-1}$, *segue que*

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

$$v'_\theta = \begin{pmatrix} -\frac{2}{5} - \frac{1}{5}\theta \\ \frac{1}{5} - \frac{2}{5}\theta \end{pmatrix}.$$

Escolhendo $i = 1$, *obtemos que* $\alpha = \frac{v'_1}{v_1} = \frac{2}{5} + \frac{\theta}{5}$ *e que o conjunto das raízes de* $\chi_A(x)$ *é dado por* $\{\frac{1}{2} + \frac{1}{2}\sqrt{5}, \frac{1}{2} - \frac{1}{2}\sqrt{5}\}$. *Deste modo, as imersões reais de* θ *são* $\sigma_1(\theta) = 1,61833989$ *e* $\sigma_2(\theta) = -0,61833989$. *Assim, a matriz geradora do reticulado é dada por*

$$M = \begin{pmatrix} -0,850686768 & -0,525672923 \\ -0,525672923 & 0,850686768 \end{pmatrix}.$$

Referências Bibliográficas

[1] **Shannon, C.E.** "*A Mathematical Theory of Communications.*" BSTJ 27, pp. 379-423 and 623-656, 1948

[2] **Samuel, P.** "*Algebraic Theory of Numbers.*" Hermana, Paris, 1967.

[3] **Stewart, I., Tall, D.** "*Algebric Number Theory.*" Chapman & Hall, New York,1987.

[4] **Marcus, D.A.** "*Numbers Fields.*" Springer-Verlag, 1977.

[5] **Ribenboim, P.** "*Algebraic Numbers.*" Wiley - Interscience, 1972.

[6] **Lang, S.** "*Algebraic Number Theory.*" Addison-Wesley Publishing Company, 1970.

[7] **Washington, L.C.** "*Introduction to Ciclotomic Fields.*" Springer-Verlag, 1982.

[8] **Endler, O.** "*Teoria dos Números Algébricos.*" IMPA, Rio de Janeiro, 1986.

[9] **Oliveira, C. M.** "*Discriminante, ramificação e diferente.*", Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto, 2005.

[10] **Swinnerton-Dyer, H. P. F.** "*A brief quide to algebraic number theory.*", Cambridge, U. K., Cambridge Univ. Press, 2001.

[11] **Alves, C.** "*Reticulados via corpos ciclotômicos.*", Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto, 2005.

[12] **Bayer, E. F.** "*Lattices and number fields.*" Contemporany Mathematics, vol. 241, 1999.

[13] **Boutros, J., Viterbo, E., Rastello, C. e Belfiori, J.C.** "*Good Lattice Constellations for both Rayleigh fading and Gaussian channels.*" IEEE Trans. Inform. Theory, Vol.42, N.2, March, 1996.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

[14] **Viterbo, E.** "*Algebraic number theory and its application to code design for Rayleigh fading channels.*", Notas, August, 2004.

[15] **Oggier, F.** "*Algebraic methods for channel coding.*" Dissertação de Doutorado, Ècole Polytechnique Fèdérale de Lausane, 2005.

[16] **Bayer, E. F., Oggier, F., Viterbo, E.** "*New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for Rayleigh fadind channel.*", IEEE Trans. Inform. Theory, Vol.50, N.4, April, 2004.

[17] **Erez, B.** "*The galois structure of trace form in extensions of odd prime degree.*", Journal of Algebra, Vol. 118, pp. 438-446, 1988.

[18] **Viterbo, E.** "*Best constructions of rotated cubic lattice constellations in small dimension for the Rayleigh fadind channel.*", to appear.

[19] **Krüskemper, M.** "*Algebraic construction of bilinear forms over $\mathbb{Z}$.*", Pub. Math. de Besancon, Théorie des nombres, 1996/97-1997/98.

[20] **Taussky, O.** "*On a theorem of Latmer and MacDuffee.*" Canadian J. Math., 1, pp. 300-302, 1949.

[21] **Taussky, O.** "*On matrix classes corresponding to an ideal and its inverse.*", Illinois J. Math., 1, pp. 108-113, 1957.

cm 1 2 3 4 5 6 7 unesp 1 12 13 14 15 16 17 18

Índice Remissivo

álgebra, 11
álgebra comutativa, 11

anel de Dedekind, 29
anel de frações, 35
anel de inteiros, 14
anel integralmente fechado, 14
anel inteiro sobre subanel, 14
anel Noetheriano, 6
anel reduzido, 10
assinatura de forma bilinear, 80

base de um módulo, 6
base integral, 26

canal Gaussiano, 90
canal Rayleigh com desvanecimento, 88
codiferente, 58
conjunto linearmente independente , 6
construção cíclica, 102
construção ciclotômica, 96
construção mista, 121
construção quadrática, 94
corpo ciclotômico, 43
corpo fixo, 80
corpo quadrático, 40

densidade de empacotamento, 71
determinante de forma bilinear , 80
determinante do reticulado Λ, 83
diferente, 62, 65
discriminante absoluto, 26
discriminante de n elementos, 23
discriminante de anel sobre subanel, 24
distância l-produto mínima, 86
distância de Hamming, 84
distância produto, 86
distância produto mínima, 86
diversidade de conjunto, 85
diversidade de elemento, 84
divisão de ideais fracionários, 32

elemento inteiro, 11
elemento nilpotente, 10
empacotamento esférico, 71
empacotamento reticulado, 71
equação de dependência integral, 11

grau de inércia, 49
grupo de classes de ideais , 32

homomorfismo canônico, 73
homomorfismo de Minkowiski, 73

ideal acima, 48
ideal fracionário, 30
ideal inerte em corpo, 49
ideal ramificado em corpo, 49
ideal reticulado, 81
ideal reticulado do tipo traço, 81

ideal totalmente decomposto em corpo , 49
ideal totalmente ramificado em corpo, 49
inteiro algébrico, 14
involução, 80

l-distância produto, 86

método de Krüskempe, 127
módulo, 5
módulo finitamente gerado, 6
módulo livre, 6
módulo Noetheriano, 6
matriz de Gram, 82

número algébrico, 14
norma de elemento, 17
norma de homorfismo, 17
norma de um ideal de $\mathcal{O}_{\mathbb{K}}$, 32

ordem, 86

perturbação do homomorfismo canônico, 82, 84
polinômio característico de elemento, 17
polinômio característico de homomorfismo, 17
polinômio ciclotômico, 44
posto de um módulo, 6

raiz n-ésima da unidade, 43
região fundamental, 69
reticulado, 68
reticulado inteiro, 80
reticulado inteiro ímpar, 81
reticulado inteiro par, 81
reticulado inteiro positivo, 81

sequência estacionária, 6
subconjunto compacto, 69
subconjunto discreto, 69
submódulo, 5

traço de elemento, 17
traço de homomorfismo, 17

volume da região fundamental, 70

cm 1 2 3 4 5 6 7 8 unesp 12 13 14 15 16 17 18 19