Universidade Estadual Paulista

Campus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Construções de Reticulados via Extensões Cíclicas de Grau Ímpar

Everton Luiz de Oliveira

Orientador: Prof. Dr. Antonio Aparecido de Andrade

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

São José do Rio Preto

Fevereiro - 2011

Everton Luiz de Oliveira

Construções de Reticulados via Extensões Cíclicas de Grau Ímpar

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

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
Professor Adjunto
UNESP – São José do Rio Preto
Orientador

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

Prof. Dr. Clotilzio Moreira dos Santos
Professor Assistente Doutor
UNESP – São José do Rio Preto

São José do Rio Preto, 28 de fevereiro de 2011.

Oliveira, Everton Luiz de.

Construções de reticulados via extensões cíclicas de grau ímpar / Everton Luiz de Oliveira. - São José do Rio Preto : [s.n.], 2011.

122 f. : il. ; 30 cm.

Orientador: Antonio Aparecido de Andrade

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas

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

CDU - 512.56

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

Aos que trouxeram força
durante os dias de
elaboração deste trabalho,
dedico. Em especial,
aos meus pais,
Claudio e Cleide.

Ficar, deixar...
como vir a ser, quiçá.
Onde for que há de ir
o que fica é o início
do que vir.
E assim, o que surge
em torno a ti
te espera reagir...
e ver... viver

Resumo

Neste trabalho, descrevemos construções cíclicas de reticulados algébricos $\mathbb{Z}^n$-rotacionados de dimensão ímpar. Essas construções são obtidas através da imersão no $\mathbb{R}^n$, via o homomorfismo canônico, de determinados $\mathbb{Z}$-módulos livres de posto finito contidos em subcorpos de extensões ciclotômicas do tipo $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^2})$, $\mathbb{Q}(\zeta_{pq})$ e $\mathbb{Q}(\zeta_{pq^2})$, com p e q primos ímpares. Caracterizamos os reticulados obtidos e apresentamos propriedades e aplicações na Teoria da Informação.

Palavras-Chave: Extensões cíclicas, ramificação de ideais, reticulados algébricos, anéis de grupo, reticulados $\mathbb{Z}^n$-rotacionados.

Abstract

In this work we describe cyclic constructions of rotated algebraic $\mathbb{Z}^n$-lattices of odd dimension. These constructions are obtained by immersion in $\mathbb{R}^n$ via the canonical homomorphism, of certain $\mathbb{Z}$-free modules of finite rank contained in subfield cyclotomic extensions of type $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^2})$, $\mathbb{Q}(\zeta_{pq})$ e $\mathbb{Q}(\zeta_{pq^2})$, with p and q odd prime. Featuring the obtained lattices and presenting properties and applications in Information Theory.

Keywords: Cyclic extension, ideal ramification, algebraic lattices, group rings, rotated $\mathbb{Z}^n$-lattices.

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

$\sum$: somatório

$\prod$: produtório

$\#B$: cardinalidade do conjunto B

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

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

$a|b$: a divide b

$a \equiv b(mod\ m)$: a congruente a b módulo m

δ_{ij}: delta de Kronecker

$Ker(f)$: núcleo da aplicação f

$Im(f)$: imagem da aplicação f

$\circ(G)$: ordem do grupo G

$H \leqslant G$: H é subgrupo de G

$H \lhd G$: H é subgrupo normal de G

A, R: anéis

$S^{-1}R$: anel de frações de R com respeito a S

RG: anel de grupo de G sobre R

$\mathcal{I}, \mathcal{J}, \mathcal{P}, \mathcal{M}$, ...: ideais

$\mathcal{I} + \mathcal{J}$: soma de ideais

$\mathcal{I}\mathcal{J}$: produto de ideais

$R/\mathcal{I}$: anel quociente

M, N: módulos

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

$\mathbb{K}\mathbb{L}$: corpo composto de $\mathbb{K}$ e $\mathbb{L}$

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

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

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

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

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

$\mathcal{O}_R(A)$: anel de inteiros de R sobre A

$\mathcal{O}_{\mathbb{K}}$: anel de inteiros do corpo de números $\mathbb{K}$

$\mathcal{D}(\alpha_1, \ldots, \alpha_n)$: discriminante de $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{K}$

$\mathcal{D}_{\mathbb{K}}$: discriminante do corpo de números $\mathbb{K}$

$\mathcal{D}(R/A)$: discriminante de R sobre A

$\Delta^{-1}_{\mathbb{K}/\mathbb{Q}}$: codiferente de $\mathbb{K}$ sobre $\mathbb{Q}$

$\mathbb{Z}_n$: grupo das classes residuais módulo n

$\mathbb{Z}_n^*$: grupo das classes residuais invertíveis módulo n

ζ_n: raiz n-ésima da unidade

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

$\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico

Λ: reticulado

$\mathcal{V}ol(\Lambda)$: volume do reticulado Λ

$div(\Lambda)$: diversidade do reticulado Λ

$d_{p,min}(\Lambda)$: distância produto mínima de Λ

$\sigma_{\mathbb{K}}$: homomorfismo canônico

σ_α: perturbação do homomorfismo canônico

$\sigma_{\mathbb{K}}(M), \sigma_\alpha(M)$: reticulados algébricos

$(\mathcal{I}, Tr_\alpha)$: reticulado ideal

(Tr_α): matriz da forma traço

Sumário

Introdução

O recente surgimento de novos canais de comunicação na Teoria da Informação influencia diretamente na importância de determinados reticulados. Em particular, há interesse pelo reticulado $\mathbb{Z}^n$ devido à aplicabilidade no canal Rayleigh Fading e, por esta razão, há uma busca por diferentes formas de obtenção de reticulados isomorfos à $\mathbb{Z}^n$, chamados $\mathbb{Z}^n$-reticulados. Neste trabalho, apresentamos a descrição de algumas famílias de $\mathbb{Z}^n$-reticulados através da Teoria Algébrica dos Números, utilizando determinados $\mathbb{Z}$-módulos de extensões cíclicas de grau ímpar (por vezes primo ímpar).

Originalmente, as estruturas que utilizamos provêm de construções algébricas desenvolvidas em décadas passadas. No ano de 1984, P. E. Conner e R. Perlis indagaram, em [10], sobre a existência de uma base, para um determinado ideal fracionário do anel de inteiros de um corpo de números, que faria a matriz da forma traço coincidir com a identidade. Quatro anos depois B. Erez exibiu tal base, em [20], para o caso particular em que o corpo de números é cíclico de grau primo ímpar, onde fez o estudo da forma traço, dividindo em alguns casos de ramificação. Entretanto, Erez utilizou-se de bases fornecidas pelas construções feitas em [21], por S. Ullom no final dos anos sessenta.

Estas bases geram estruturas algébricas, chamadas $\mathbb{Z}$-módulos, que podem ser imersas no $\mathbb{R}^n$ fornecendo reticulados algébricos. Além disso, como veremos na Seção (4.2), o fato da matriz da forma traço associada coincidir com a matriz identidade faz com que esses reticulados sejam isomorfos à $\mathbb{Z}^n$. Esse é o foco de nosso estudo nesse texto. Fazemos a obtenção de $\mathbb{Z}^n$-reticulados tomando como referência as construções desenvolvidas em [18] e [19], e utilizando as estruturas algébricas fornecidas por [20]. Organizamos o texto da seguinte maneira:

No Capítulo (1), percorremos os elementos fundamentais da Teoria Algébrica dos Números. Na Seção (1.1), é introduzida uma miscelânea de conceitos e resultados que serão utilizados no decorrer do texto, onde utilizamos as referências [1], [4], [5] e [6]. Na Seção (1.2), apresentamos os conceitos de traço e norma em corpos de números, juntamente com suas propriedades fundamentais, em que fizemos uso das referências [4] e [5]. Na Seção (1.3), é feita uma abordagem sobre módulos, utilizando [2] e [5] como referência. Na Seção (1.4), expomos alguns resultados sobre a estrutura de um anel de inteiros; fizemos uso das referências [4], [5] e [6]. Na Seção

(1.5), é apresentado o conceito de norma de um ideal e as propriedades que ela preserva, onde utilizamos a referência [5]. A Seção (1.6) é destinada ao conceito de discriminante em corpos de números e alguns resultados de importante aplicação relacionados a este parâmetro; fizemos uso das referências [4], [5] e [14]. Na Seção (1.7), são introduzidas as propriedades que definem anéis noetherianos e de Dedekind e verificamos que o anel de inteiros de um corpo de números as satisfaz, onde utilizamos as referências [5] e [6]. Por fim, na Seção (1.8), apresentamos uma estrutura de importante aplicação em reticulados ideais, chamada ideal fracionário, em que fizemos uso das referências [5] e [11].

No Capítulo (2), apresentamos resultados sobre anéis de frações e a fatoração de ideais, permitindo um estudo da ramificação de ideais primos (ou de números primos) através do discriminante. Como principal resultado, é caracterizada a ramificação de um número primo no anel de inteiros de um corpo de números, fornecendo valiosa ferramenta para as construções de reticulados deste trabalho. Utilizamos as referências [5] e [18].

No Capítulo (3), apresentamos três abordagens sobre reticulados: a Teoria dos Reticulados Clássica, Reticulados Algébricos e Reticulados Ideais. Na primeira, introduzimos o conceito de reticulado no $\mathbb{R}^n$, algumas propriedades e parâmetros de importante aplicação, como volume, diversidade e distância produto mínima, onde fizemos uso das referências [9], [11] e [12]. As outras duas abordagens descrevem maneiras de se obter reticulados no $\mathbb{R}^n$ através da Teoria Algébrica dos Números, fornecendo propriedades e fórmulas explícitas para alguns parâmetros desses reticulados, em que utilizamos as referências [5], [11], [12], [16] e [17].

No capítulo (4), descrevemos construções de famílias de reticulados algébricos de dimensão ímpar (por vezes prima ímpar), imergindo no $\mathbb{R}^n$, via homomorfismo canônico, determinados $\mathbb{Z}$-módulos livres de posto finito contidos em extensões cíclicas. Na seção (4.1), apresentamos uma construção inicial imergindo o anel de inteiros de uma extensão cíclica no $\mathbb{R}^n$, fornecendo alguns parâmetros dos reticulados obtidos. Na Seção (4.2), é introduzido o conceito de reticulado $\mathbb{Z}^n$-rotacionado e apresentamos uma condição suficiente para obtê-lo, onde utilizamos as referências [15] e [18]. Na seção (4.3), é apresentado o conceito de anel de grupo visando intermediar as abordagens feitas em [18] e [20], referências utilizadas para a Seção (4.4), na qual é feita a obtenção de reticulados $\mathbb{Z}^n$-rotacionados. Na Seção (4.4), fizemos uso também das referências [14] e [21] e na Seção (4.3), utilizamos as referências [8], [10] e [20]. Por fim, apresentamos uma conclusão do capítulo e expomos possíveis novas construções e generalizações de resultados na Teoria Algébrica dos Números.

Neste trabalho, quando citado um anel, ele é comutativo e possui unidade.

Capítulo 1

Teoria Algébrica dos Números

Neste capítulo, apresentamos uma introdução sobre a Teoria Algébrica dos Números. São abordados conceitos fundamentais, como traço e norma, anel de inteiros e discriminante de um corpo de números, norma de um ideal e as principais propriedades relacionadas a esses elementos. A demonstração de determinados resultados é omitida. Alguns por se tratarem de resultados clássicos e outros pela extensa demonstração. Todavia, inserimos a referência nos que seguem sem demonstração.

1.1 Conceitos preliminares

Nesta seção, introduzimos alguns conceitos e resultados fundamentais da Teoria de Galois e da Teoria Algébrica dos Números.

Definição 1.1.1 *Se $\mathbb{K}$ é um subcorpo de um corpo $\mathbb{L}$, dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, ou ainda, que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão. O grau da extensão $\mathbb{K} \subseteq \mathbb{L}$ é a dimensão de $\mathbb{L}$ como espaço vetorial sobre $\mathbb{K}$, e denotamos por $\dim_{\mathbb{K}} \mathbb{L} = [\mathbb{L} : \mathbb{K}]$. No caso em que $[\mathbb{L} : \mathbb{K}]$ é finito, dizemos que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita.*

Definição 1.1.2 *Uma extensão finita $\mathbb{K}$ do corpo $\mathbb{Q}$ dos números racionais é chamada de corpo de números. Se $[\mathbb{K} : \mathbb{Q}] = n$, dizemos que $\mathbb{K}$ é um corpo de números de grau n.*

Definição 1.1.3 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão e $Aut(\mathbb{L})$ o grupo dos automorfismos de $\mathbb{L}$. O conjunto*

$$Gal(\mathbb{L} : \mathbb{K}) = \{\sigma \in Aut(\mathbb{L});\ \sigma(x) = x,\ \forall x \in \mathbb{K}\}$$

é um subgrupo de $Aut(\mathbb{L})$, chamado de grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$.

Definição 1.1.4 *Uma extensão finita $\mathbb{K} \subseteq \mathbb{L}$ tal que $[\mathbb{L} : \mathbb{K}] = \circ(Gal(\mathbb{L} : \mathbb{K}))$ é chamada de extensão de Galois, ou galoisiana. Nesse caso, se $Gal(\mathbb{L} : \mathbb{K})$ é abeliano, dizemos que $\mathbb{K} \subseteq \mathbb{L}$ é abeliana e se $Gal(\mathbb{L} : \mathbb{K})$ é cíclico, dizemos que $\mathbb{K} \subseteq \mathbb{L}$ é cíclica.*

Teorema 1.1.1 *([1],Teo.12.1)(Teorema da Correspondência de Galois) Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão galoisiana contida num corpo algebricamente fechado.*

(i) Se H é um subgrupo de $Gal(\mathbb{L} : \mathbb{K})$, então existe um único corpo intermediário $\mathbb{M}$ de $\mathbb{K} \subset \mathbb{L}$ tal que $H = Gal(\mathbb{L} : \mathbb{M})$. Nesse caso, $\mathbb{M}$ é dito o corpo fixo de H.

(ii) Se $\mathbb{M}$ é um corpo intermediário de $\mathbb{K} \subset \mathbb{L}$, então $\mathbb{M} \subset \mathbb{L}$ é galoisiana e $Gal(\mathbb{L} : \mathbb{M})$ é o único subgrupo de $Gal(\mathbb{L} : \mathbb{K})$ que satisfaz

$$[\mathbb{M} : \mathbb{K}] = \frac{\circ(Gal(\mathbb{L} : \mathbb{K}))}{\circ(Gal(\mathbb{L} : \mathbb{M}))}.$$

(iii) Seja $\mathbb{M}$ um corpo intermediário de $\mathbb{K} \subset \mathbb{L}$. Temos que $\mathbb{K} \subset \mathbb{M}$ é galoisiana se, e somente se, $Gal(\mathbb{L} : \mathbb{M})$ é um subgrupo normal de $Gal(\mathbb{L} : \mathbb{K})$, e nesse caso

$$Gal(\mathbb{M} : \mathbb{K}) \simeq \frac{Gal(\mathbb{L} : \mathbb{K})}{Gal(\mathbb{L} : \mathbb{M})}.$$

Definição 1.1.5 *Seja n um inteiro positivo. Dizemos que ζ_n é uma raiz n-ésima da unidade se $\zeta_n^n = 1$, e que ζ_n é uma raiz n-ésima primitiva da unidade se $\zeta_n^n = 1$ e $\zeta_n^j \neq 1$, para todo $j = 1, \ldots, n-1$. Se ζ_n é primitiva, chamamos o polinômio*

$$\phi_n(x) = \prod_{\substack{j=1 \\ mdc(j,n)=1}}^{n} (x - \zeta_n^j)$$

de n-ésimo polinômio ciclotômico. O corpo $\mathbb{Q}(\zeta_n)$ é dito o n-ésimo corpo ciclotômico.

Observação 1.1.1 *Considere $\mathbb{Q}(\zeta_n)$ um corpo ciclotômico e $\mathbb{Z}_n^*$ o grupo das classes residuais invertíveis módulo n. Temos que*

$$Gal(\mathbb{Q}(\zeta_n) : \mathbb{Q}) = \{\sigma_i : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n);\ \sigma_i(\zeta_n) = \zeta_n^i,\ mdc(i,n) = 1,\ i = 1, \ldots, n\}.$$

Desse modo, $Gal(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \simeq \mathbb{Z}_n^*$ via o isomorfismo natural $\sigma_i \mapsto \bar{i}$.

Teorema 1.1.2 *([6],pág.44) O grupo $\mathbb{Z}_n^*$ é cíclico se, e somente se, $n = 2$, 4, p^r ou $2p^r$, com $r \geq 1$ e p um primo ímpar.*

Exemplo 1.1.1 *Se p é um primo ímpar, segue da Observação 1.1.1 e do Teorema 1.1.2 que o corpo ciclotômico $\mathbb{Q}(\zeta_p)$ é uma extensão cíclica de grau $p-1$ sobre $\mathbb{Q}$, cujo grupo de Galois é dado por $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{p-1}\}$, onde $\sigma_i : \zeta_p \mapsto \zeta_p^i$, para $i = 1, \ldots, p-1$. Além disso,*

o p-ésimo polinômio ciclotômico é dado por

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

Teorema 1.1.3 *([6],pág.273)(Teorema de Kronecker-Weber) Se $\mathbb{Q} \subseteq \mathbb{K}$ é uma extensão abeliana, então existe uma raíz n-ésima da unidade ζ_n, tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$.*

Definição 1.1.6 *Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão abeliana. O menor inteiro positivo m tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$ é chamado de condutor do corpo $\mathbb{K}$.*

Teorema 1.1.4 *([5],pág.34)(Teorema do Elemento Primitivo) Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão finita, então existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. O elemento α é chamado elemento primitivo.*

Corolário 1.1.1 *Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão finita de grau n e $\mathbb{F}$ é um corpo algebricamente fechado contendo $\mathbb{K}$, então existem exatamente n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{F}$.*

Demonstração: Pelo Teorema 1.1.4, temos que existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Como $\mathbb{K} \subset \mathbb{K}(\alpha)$ é finita de grau n, segue que o grau do polinômio minimal $p(x)$ de α sobre $\mathbb{K}$ é n. Desse modo, como $p(x)$ é irredutível, ele possui n raízes distintas $\alpha_1, \ldots, \alpha_n$ em $\mathbb{F}$. Portanto, para cada $i = 1, \ldots, n$, temos definido o $\mathbb{K}$-monomorfismo $\sigma_i : \mathbb{K}(\alpha) \to \mathbb{F}$, dado por $\sigma_i(\alpha) = \alpha_i$, como queríamos. ∎

Observação 1.1.2 *Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão galoisiana de grau n, segue pelo Teorema 1.1.4 que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$, desse modo*

$$Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\},$$

onde os σ_i's são exatamente os monomorfismos dados pelo Corolário 1.1.1.

Definição 1.1.7 *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$.*

(i) Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ dizemos que σ_i é um monomorfismo real. Caso contrário, dizemos que σ_i é um monomorfismo imaginário.

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

Teorema 1.1.5 *([6],pág.20)(Lema de Dedekind) Se $\mathbb{K} \subset \mathbb{L}$ é uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ num corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$, então $\{\sigma_1, \ldots, \sigma_n\}$ é linearmente independente sobre $\mathbb{F}$.*

1.2 Traço e norma

Introduzimos nesta seção os conceitos de traço e norma em corpos de números e apresentamos suas propriedades elementares.

Definição 1.2.1 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de grau n de corpos de números e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Definimos o traço e a norma de um elemento $\alpha \in \mathbb{L}$, com respeito a extensão $\mathbb{K} \subseteq \mathbb{L}$, como sendo respectivamente:*

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

Proposição 1.2.1 *Sejam $\mathbb{M} \subseteq \mathbb{K} \subseteq \mathbb{L}$ extensões de corpos de números, tal que $[\mathbb{L} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:*

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$
2. $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}/\mathbb{K}}(\alpha)$
3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$
4. $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = \mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha)\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\beta)$
5. $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha)$
6. $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(a) = a^n$
7. $Tr_{\mathbb{L}/\mathbb{M}}(\alpha) = Tr_{\mathbb{K}/\mathbb{M}}(Tr_{\mathbb{L}/\mathbb{K}}(\alpha))$
8. $\mathcal{N}_{\mathbb{L}/\mathbb{M}}(\alpha) = \mathcal{N}_{\mathbb{K}/\mathbb{M}}(\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha))$
9. $Tr_{\mathbb{L}/\mathbb{M}}(a) = nTr_{\mathbb{K}/\mathbb{M}}(a)$
10. $\mathcal{N}_{\mathbb{L}/\mathbb{M}}(a) = \mathcal{N}_{\mathbb{K}/\mathbb{M}}(a)^n$.

Observação 1.2.1 *Quando subentendida a extensão $\mathbb{K} \subseteq \mathbb{L}$ da qual $\alpha \in \mathbb{L}$, denotamos simplesmente $Tr(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $\mathcal{N}(\alpha) = \mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha)$.*

1.3 Módulos

Nesta seção, é apresentado o conceito de módulo e algumas de suas propriedades fundamentais.

Definição 1.3.1 *Seja R um anel. Um grupo abeliano aditivo $(M,+)$ munido de um produto escalar $\cdot : R \times M \to M$ é dito um R-módulo se satisfaz as seguintes propriedades:*

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

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

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

(iv) $1m = m$,

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

Definição 1.3.2 *Sejam R um anel e M um R-módulo. Um subgrupo N de M é chamado de um R-submódulo de M, se para todo $a \in R$ e $n \in N$ tivermos $an \in N$.*

Definição 1.3.3 *Sejam R um anel e M um R-módulo.*

(i) Dizemos que um subconjunto $\{x_1, \ldots, x_n\} \subset M$ é um gerador de M se todo elemento $m \in M$ é da forma $m = a_1x_1 + \ldots + a_nx_n$, com $a_i \in R$, para $i = 1, \ldots, n$.

(ii) O conjunto $\{x_1, \ldots, x_n\}$ é dito uma base de M se é formado por geradores linearmente independentes sobre R. Se M possui uma base, M é chamado de R-módulo livre e o número de elementos dessa base é chamado de posto de M.

Definição 1.3.4 *Sejam R um anel e M, N dois R-módulos. Dizemos que uma aplicação $\varphi : M \to N$ é um homomorfismo de R-módulos se satisfaz as seguintes condições*

(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$

(ii) $\varphi(ax) = a\varphi(x)$,

para todo $x, y \in M$ e $a \in R$. Se, além disso, a aplicação φ é injetiva (sobrejetiva), dizemos que φ é um monomorfismo (epimorfismo) de R-módulos, e se φ é bijetiva dizemos que é um isomorfismo de R-módulos.

Teorema 1.3.1 *([5],pág.21) Se R é um anel principal, M um R-módulo livre de posto n e N um R-submódulo de M, então:*

(i) N é livre de posto q, com $0 \leq q \leq n$.

(ii) Se $N \neq \{0\}$, então existem uma base $\{e_1, \ldots, e_n\}$ de M e elementos não nulos $a_1, \ldots, a_q \in R$ tal que $\{a_1e_1, \ldots, a_qe_q\}$ é uma base de N, de modo que a_i divide a_{i+1}, para $1 \leq i \leq q-1$.

Proposição 1.3.1 *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$ e $M \subseteq \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. Se $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $det(\sigma_i(x_j))_{i,j=1}^n \neq 0$.*

Demonstração: Se $det(\sigma_i(x_j))_{i,j=1}^n = 0$, então as colunas da matriz $(\sigma_i(x_j))_{i,j=1}^n$ são linearmente dependentes. Assim, existem $a_1, \ldots, a_n \in \mathbb{C}$, não todos nulos, tal que $\sum_{i=1}^n a_i\sigma_i(x_j) = 0$, para todo $j = 1, \ldots, n$. Desse modo, teremos $\sum_{i=1}^n a_i\sigma_i(x) = 0$, para todo $x \in M$, o que contradiz o Teorema 1.1.5 (Lema de Dedekind). Portanto, $det(\sigma_i(x_j))_{i,j=1}^n \neq 0$. ∎

1.4 Anel de inteiros

Nesta seção, introduzimos o conceito de anel de inteiros e apresentamos algumas propriedades relacionadas a sua estrutura.

Definição 1.4.1 *Sejam $A \subseteq R$ anéis. Dizemos que um elemento $\alpha \in R$ é inteiro sobre A se existe um polinômio mônico não-nulo $f(x)$ com coeficientes em A tal que $f(\alpha) = 0$, isto é, existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tal que*

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

Se todo elemento de R é inteiro sobre A, dizemos que R é inteiro sobre A.

Definição 1.4.2 *Sejam $A \subseteq R$ anéis. O conjunto de todos os elementos de R que são inteiros sobre A é um subanel de R, que denotamos por $\mathcal{O}_R(A)$. O anel $\mathcal{O}_R(A)$ é chamado de anel de inteiros de R sobre A.*

Se $\mathbb{K}$ é um corpo de números, o anel de inteiros $\mathcal{O}_{\mathbb{K}}(\mathbb{Z})$ de $\mathbb{K}$ sobre $\mathbb{Z}$ será denotado simplesmente por $\mathcal{O}_{\mathbb{K}}$, e chamado de anel de inteiros de $\mathbb{K}$.

Proposição 1.4.1 *([5],pág.38) Se $\mathbb{K}$ é um corpo de números e $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha)$ e $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ são números inteiros.*

Definição 1.4.3 *Sejam R um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que R é um anel integralmente fechado se $\mathcal{O}_{\mathbb{K}}(R) = R$.*

Proposição 1.4.2 *Se R é um domínio, $\mathbb{K}$ seu corpo de frações e $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita, então $\mathcal{O}_{\mathbb{L}}(R)$ é integralmente fechado.*

Demonstração: Seja $\mathbb{M}$ o corpo de frações de $\mathcal{O}_{\mathbb{L}}(R)$. Temos que $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$. Seja $x \in \mathbb{M}$ tal que x é inteiro sobre $\mathcal{O}_{\mathbb{L}}(R)$. Como $\mathcal{O}_{\mathbb{L}}(R)$ é inteiro sobre R, segue que x é inteiro sobre R. Assim, se $\mathcal{O}_{\mathbb{M}}$ é o conjunto dos elementos de $\mathbb{M}$ que são inteiros sobre $\mathcal{O}_{\mathbb{L}}(R)$, então $\mathcal{O}_{\mathbb{M}} \subset \mathcal{O}_{\mathbb{L}}(R)$. Mas, como $\mathcal{O}_{\mathbb{L}}(R) \subset \mathcal{O}_{\mathbb{M}}$, segue que $\mathcal{O}_{\mathbb{L}}(R) = \mathcal{O}_{\mathbb{M}}$. Portanto, $\mathcal{O}_{\mathbb{L}}(R)$ é integralmente fechado. ∎

Teorema 1.4.1 *([5],pág.40) Sejam R um anel principal, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$. Temos que:*

(i) $\mathcal{O}_{\mathbb{L}}(R)$ é um R-módulo livre de posto n;

(ii) Se $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{L}}(R)$, então $\mathcal{I}$ é um R-módulo livre de posto n.

1.5 Norma de um ideal

Considere $\mathbb{K}$ um corpo de números de grau n. Apresentamos o conceito de norma de um ideal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ e algumas propriedades que ela preserva.

Definição 1.5.1 *Seja $\mathcal{I}$ um ideal não-nulo do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. A norma do ideal $\mathcal{I}$ é definida como sendo a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/\mathcal{I}$, isto é,*

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

Proposição 1.5.1 *([5],Seç.3.5) Se $\langle\alpha\rangle$ é um ideal principal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, então*

$$\mathcal{N}(\langle\alpha\rangle) = |\mathcal{N}(\alpha)|.$$

Proposição 1.5.2 *([5],Seç.3.5) Se $\mathcal{I}, \mathcal{J}$ são ideais não-nulos de $\mathcal{O}_{\mathbb{K}}$, então*

$$\mathcal{N}(\mathcal{I}\mathcal{J}) = \mathcal{N}(\mathcal{I})\mathcal{N}(\mathcal{J}).$$

Proposição 1.5.3 *([5],Seç.3.5) Seja $\mathcal{I}$ um ideal não-nulo do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Se $\{w_1, \ldots, w_n\}$ for uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e $\{e_1w_1, \cdots, e_nw_n\}$ uma $\mathbb{Z}$-base de $\mathcal{I}$, onde $e_1, \ldots, e_n$ são inteiros não-nulos, então $\mathcal{N}(\mathcal{I}) = |e_1 \ldots e_n|$.*

1.6 Discriminante

Esta seção é destinada ao conceito de discriminante em corpos de números. Utilizamos este parâmetro no estudo da ramificação de ideais e dos reticulados algébricos.

Considere $\mathbb{K}$ um corpo de números de grau n.

Definição 1.6.1 *Sejam $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $\{\alpha_1, \ldots, \alpha_n\}$ um conjunto de elementos de $\mathbb{K}$. Definimos o discriminante desse conjunto por*

$$\mathcal{D}(\alpha_1, \ldots, \alpha_n) = det[(\sigma_i(\alpha_j))_{i,j=1}^{n}]^2.$$

Proposição 1.6.1 *Se* $\{\alpha_1, \ldots, \alpha_n\}$ *é um subconjunto de* $\mathbb{K}$*, então*

$$\mathcal{D}(\alpha_1, \ldots, \alpha_n) = det(Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j=1}^n.$$

Demonstração: Sejam $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Para cada $i, j = 1, \ldots, n$, temos que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Desse modo,

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

o que justifica a proposição. ■

Proposição 1.6.2 *Seja* $\{\alpha_1, \ldots, \alpha_n\}$ *um subconjunto de* $\mathbb{K}$*. Se* $\{\beta_1, \ldots, \beta_n\}$ *é um conjunto de elementos de* $\mathbb{K}$ *tal que* $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$*, com* $a_{ij} \in \mathbb{Q}$*, para* $j = 1, \ldots, n$*, então*

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

Demonstração: Se $\sigma_1, \ldots, \sigma_n$ são os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, então

$$\begin{aligned}
\mathcal{D}(\beta_1, \ldots, \beta_n) &= det(\sigma_k(\beta_j))^2 \\
&= det(\sigma_k(\sum_{i=1}^{n} a_{ij}\alpha_i))^2 \\
&= det(\sum_{i=1}^{n} a_{ij}\sigma_k(\alpha_i))^2 \\
&= det((a_{ij})(\sigma_k(\alpha_i)))^2 \\
&= det(a_{ij})^2 det(\sigma_k(\alpha_i))^2 \\
&= det(a_{ij})^2\mathcal{D}(\alpha_1, \ldots, \alpha_n),
\end{aligned}$$

o que conclui a demonstração. ■

Definição 1.6.2 *Seja* $\{\alpha_1, \ldots, \alpha_n\}$ *uma* $\mathbb{Z}$*-base do anel de inteiros* $\mathcal{O}_{\mathbb{K}}$*. Dizemos que o discriminante* $\mathcal{D}(\alpha_1, \ldots, \alpha_n)$ *é o discriminante do corpo de números* $\mathbb{K}$*, e denotamos por* $\mathcal{D}_{\mathbb{K}}$*.*

Os três seguintes resultados, demonstrados por José Othon D. Lopes em [14], fornecem valiosa ferramenta para as construções de reticulados do Capítulo 4.

Teorema 1.6.1 *([14],Cor.3.2) Se p é um primo ímpar e $\mathbb{K}$ é um subcorpo do corpo ciclotômico $\mathbb{Q}(\zeta_p)$, então*

$$|\mathcal{D}_{\mathbb{K}}| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Teorema 1.6.2 *([14],Cor.3.9) Se $\mathbb{K}$ é um corpo de números abeliano de grau primo p e condutor m, então*

$$|\mathcal{D}_{\mathbb{K}}| = m^{p-1}.$$

Teorema 1.6.3 *([14],Cor.3.5) Se p é um primo ímpar e $\mathbb{K}$ é um subcorpo do corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, com $[\mathbb{K}:\mathbb{Q}] = up^j$, onde u e p são relativamente primos, então*

$$|\mathcal{D}_{\mathbb{K}}| = p^{u[(j+2)p^j-(\frac{p^{j+1}-1}{p-1})]-1}.$$

Definição 1.6.3 *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos de números e $A \subset R$ anéis tal que $A \subset \mathbb{K}$ e $R \subset \mathbb{L}$, onde R é um A-módulo livre de posto n. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de R sobre A, definimos o discriminante de R sobre A, como sendo o ideal de A gerado por $\mathcal{D}(\alpha_1, \ldots, \alpha_n)$, e denotamos por $\mathcal{D}(R/A)$.*

Definição 1.6.4 *Seja R um anel. Um elemento $\alpha \in R$ é dito nilpotente se existe um inteiro positivo r tal que $\alpha^r = 0$. Dizemos que R é reduzido se o único elemento nilpotente de R é o zero.*

Proposição 1.6.3 *([5],pág.73) Sejam $\mathbb{K}$ um corpo finito de característica zero e R um anel tal que, R é um $\mathbb{K}$-módulo livre de posto finito com $\mathbb{K} \subset R$. Temos que $\mathcal{D}(R/\mathbb{K}) \neq \{0\}$ se, e somente se, R é reduzido.*

1.7 Anéis noetherianos e de Dedekind

Nesta seção, apresentamos as propriedades que definem anéis noetherianos e de Dedekind e verificamos que o anel de inteiros de um corpo de números satisfaz essas propriedades.

Definição 1.7.1 *Sejam R um anel e $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ uma sequência crescente de ideais de R. Dizemos que a sequência $(I_i)_{i\in\mathbb{N}}$ é estacionária se existir $n_o \in \mathbb{N}$ tal que $I_n = I_{n_o}$, para todo $n \geq n_o$.*

Definição 1.7.2 *Dizemos que um anel R é noetheriano se satisfaz uma das seguintes condições:*

(i) Todo ideal de R é finitamente gerado.

(ii) Toda sequência crescente de ideais de R é estacionária.

(iii) Toda família não-vazia de ideais de R contém um elemento maximal.

Definição 1.7.3 *Dizemos que um domínio R é um anel de Dedekind se é noetheriano, integralmente fechado e todo ideal primo não-nulo de R é maximal.*

Exemplo 1.7.1 *O anel $\mathbb{Z}$ é um anel de Dedekind.*

Teorema 1.7.1 *Se R é um anel de Dedekind, $\mathbb{K}$ é seu corpo de frações e $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita, então $\mathcal{O}_{\mathbb{L}}(R)$ é um anel de Dedekind.*

Demonstração: Pela Proposição 1.4.2, temos que $\mathcal{O}_{\mathbb{L}}(R)$ é integralmente fechado. Seja $\mathcal{P}$ um ideal primo não-nulo de $\mathcal{O}_{\mathbb{L}}(R)$. Assim, $\mathcal{P} \cap R$ é um ideal primo de R. Mostremos que $\mathcal{P} \cap R$ é não nulo. Seja $\alpha \in \mathcal{P} - \{0\}$. Como $\mathcal{P} \subset \mathcal{O}_{\mathbb{L}}(R)$, segue que existem $a_i \in R$, com $i = 0, \ldots, n-1$, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$, e suponha que n seja o grau mínimo com esta propriedade. Desse modo, $a_0 \neq 0$, pois caso contrário obteríamos uma equação de grau menor. Assim,

$$a_0 = \alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \ldots - a_1) \in \alpha\mathcal{O}_{\mathbb{L}}(R) \cap R \subset \mathcal{P} \cap R.$$

Portanto, $\mathcal{P} \cap R \neq \{0\}$. Como $\mathcal{P} \cap R$ é um ideal primo de R, que por sua vez é de Dedekind, segue que $\mathcal{P} \cap R$ é um ideal maximal de R e, assim, $R/(\mathcal{P} \cap R)$ é um corpo. Considere a aplicação

$$\varphi : R \xrightarrow{i} \mathcal{O}_{\mathbb{L}}(R) \xrightarrow{\pi} \frac{\mathcal{O}_{\mathbb{L}}(R)}{\mathcal{P}},$$

onde i é a inclusão e π a projeção. Como $\mathcal{O}_{\mathbb{L}}(R)$ é inteiro sobre R, segue que $\mathcal{O}_{\mathbb{L}}(R)/\mathcal{P}$ é inteiro sobre $R/(\mathcal{P} \cap R)$. Assim, como

$$\frac{R}{\mathcal{P} \cap R} \simeq Im(\varphi) \subset \frac{\mathcal{O}_{\mathbb{L}}(R)}{\mathcal{P}}$$

e $R/(\mathcal{P} \cap R)$ é um corpo, segue que $\mathcal{O}_{\mathbb{L}}(R)/\mathcal{P}$ é um corpo. Dessa forma, $\mathcal{P}$ é maximal. Portanto, como $\mathcal{O}_{\mathbb{L}}(R)$ é noetheriano, concluímos que é um anel de Dedekind (veja a Seção 3.2 de [5]). ■

Corolário 1.7.1 *Se $\mathbb{K}$ é um corpo de números, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind.*

Demonstração: Como $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, o qual é o corpo de frações de $\mathbb{Z}$, segue do Teorema 1.7.1 que $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind. ■

1.8 Ideais fracionários

Nesta seção, é introduzido o conceito de ideal fracionário de um domínio. O objetivo ao apresentar essa estrutura é a aplicação em reticulados ideais.

Definição 1.8.1 *Sejam R um domínio e $\mathbb{K}$ seu corpo de frações. Um R-submódulo $\mathcal{I}$ de $\mathbb{K}$ do qual existe $d \in R - \{0\}$ tal que $d\mathcal{I} \subset R$, é dito um ideal fracionário de R. Neste caso, $d\mathcal{I}$ é um ideal $\mathcal{J}$ de R e $\mathcal{I} = d^{-1}\mathcal{J}$.*

Observação 1.8.1 *Os ideais de um domínio R são exatamente os ideais fracionários que estão contidos em R. Se $\mathbb{K}$ é um corpo de números, um $\mathcal{O}_{\mathbb{K}}$-módulo $\mathcal{I} \subset \mathbb{K}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, se existe $d \in \mathcal{O}_{\mathbb{K}}$ não-nulo tal que $d\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$.*

Definição 1.8.2 *Sejam R um domínio e $\mathcal{I}$, $\mathcal{J}$ ideais fracionários de R. Definimos a soma $\mathcal{I} + \mathcal{J}$ como sendo o conjunto*

$$\mathcal{I} + \mathcal{J} = \{a + b;\ a \in \mathcal{I}, b \in \mathcal{J}\},$$

e o produto $\mathcal{I}\mathcal{J}$ como sendo

$$\mathcal{I}\mathcal{J} = \left\{ \sum_{i=1}^{n} a_i b_i;\ a_i \in \mathcal{I}, b_i \in \mathcal{J} \right\}.$$

De modo análogo, se M é um R-módulo definimos o produto $\mathcal{I}M$.

Definição 1.8.3 *Seja R um domínio. Um ideal fracionário $\mathcal{I}$ de R é inversível se existe um ideal fracionário $\mathcal{J}$ de R tal que $\mathcal{I}\mathcal{J} = R$.*

Definição 1.8.4 *Sejam R um domínio e $\mathcal{I}, \mathcal{J}$ ideais fracionários de R. Dizemos que $\mathcal{I}$ divide $\mathcal{J}$ se existe um ideal $\mathcal{M}$ de R tal que $\mathcal{J} = \mathcal{M}\mathcal{I}$.*

Proposição 1.8.1 *Sejam R um domínio e $\mathcal{I}, \mathcal{J}$ ideais fracionários inversíveis de R. Temos que $\mathcal{I}$ divide $\mathcal{J}$ se, e somente se, $\mathcal{J} \subset \mathcal{I}$.*

Demonstração: Se $\mathcal{I}$ divide $\mathcal{J}$, então existe um ideal $\mathcal{M}$ de R tal que $\mathcal{J} = \mathcal{M}\mathcal{I} \subset \mathcal{I}$. Agora, supondo que $\mathcal{J} \subset \mathcal{I}$, segue que $\mathcal{J}\mathcal{I}^{-1} \subset \mathcal{I}\mathcal{I}^{-1} = R$. Mas, desse modo $\mathcal{J}\mathcal{I}^{-1}$ é um ideal de R tal que $(\mathcal{J}\mathcal{I}^{-1})\mathcal{I} = \mathcal{J}$. Portanto, $\mathcal{I}$ divide $\mathcal{J}$. ∎

Proposição 1.8.2 *Se R é um domínio noetheriano, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de $\mathbb{K}$, então todo ideal fracionário $\mathcal{I}$ de $\mathcal{O}_{\mathbb{L}}(R)$ é um R-módulo finitamente gerado.*

Demonstração: Como $\mathcal{I}$ é um ideal fracionário de R, segue que existe $d \in R - \{0\}$ tal que $d\mathcal{I} \subseteq R$, e assim $\mathcal{I} \subseteq d^{-1}R$. A aplicação $\varphi : R \to d^{-1}R$, definida por $\varphi(x) = d^{-1}x$, para $x \in R$, é um isomorfismo. Logo, como R é noetheriano, segue que $d^{-1}R$ é noetheriano. Portanto, $\mathcal{I}$ é um R-módulo finitamente gerado. ■

Proposição 1.8.3 *Se R é um anel principal, $\mathbb{K}$ seu corpo de frações e $\mathbb{K} \subseteq \mathbb{L}$ finita de grau n, então todo ideal fracionário não-nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{L}}(R)$ é um R-módulo livre de posto n.*

Demonstração: Se $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}(R)$, então existe $d \in \mathcal{O}_{\mathbb{L}}(R) - \{0\}$ tal que $d\mathcal{I} \subset \mathcal{O}_{\mathbb{L}}(R)$. O ideal $\mathcal{J} := d\mathcal{I}$ de $\mathcal{O}_{\mathbb{L}}(R)$ é um R-módulo livre de posto n (veja Teorema 1.4.1). Seja $\{w_1, \ldots, w_n\}$ uma R-base de $\mathcal{J}$. Desse modo, $\{d^{-1}w_1, \ldots, d^{-1}w_n\}$ gera $\mathcal{I}$ sobre R. Agora, se $\sum_{i=1}^{n} a_i d^{-1} w_i = 0$, para $a_i \in R$, com $i = 1, \ldots, n$, então $d^{-1} \sum_{i=1}^{n} a_i w_i = \sum_{i=1}^{n} a_i d^{-1} w_i = 0$. Logo, $\sum_{i=1}^{n} a_i w_i = 0$, e como $\{w_1, \ldots, w_n\}$ é linearmente independente sobre R, segue que $a_i = 0$, para todo $i = 1, \ldots, n$. Portanto, $\mathcal{I}$ é um R-módulo livre de posto n. ■

Teorema 1.8.1 *([5],pág.50) Se R é um anel de Dedekind, então todo ideal fracionário não-nulo $\mathcal{I}$ de R pode ser unicamente expresso como um produto*

$$\mathcal{I} = \sum_{i=1}^{q} \mathcal{P}_i^{e_i}$$

de ideais $\mathcal{P}_i$ primos não-nulos de R, onde q e e_i, com $i = 1, \ldots, q$, são inteiros positivos.

Capítulo 2

Ramificação de Ideais

Neste capítulo, introduzimos resultados sobre anéis de frações e a fatoração de ideais primos, fornecendo condições para uma abordagem sobre ramificação de ideais primos via discriminante. O objetivo é apresentar o conceito de ramificação de um ideal primo (ou número primo) no anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números e caracterizar a ramificação de um número primo p, garantindo que p ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, p divide o discriminante de $\mathbb{K}$.

2.1 Anéis de frações

Nesta seção, apresentamos o conceito de anel de frações e alguns resultados relacionando-o com outros elementos, como anéis noetherianos e de Dedekind.

Definição 2.1.1 *Sejam R um domínio, $\mathbb{K}$ seu corpo de frações e $S \subset R - \{0\}$ fechado com relação à multiplicação, com $1 \in S$. Definimos o anel de frações $S^{-1}R$, de R com respeito a S, como sendo o conjunto*

$$S^{-1}R = \left\{ \frac{a}{s};\ a \in R, s \in S \right\} \subset \mathbb{K}.$$

Claramente $S^{-1}R$ é um anel comutativo, pois é um subanel de $\mathbb{K}$. Se $S = R - \{0\}$ então $S^{-1}R = \mathbb{K}$ e se $S = \{1\}$ teremos $S^{-1}R = R$.

Proposição 2.1.1 *Sejam R um domínio e S um subconjunto de $R - \{0\}$ fechado com relação à multiplicação, com $1 \in S$. Ao denotar $R' = S^{-1}R$, temos que:*

(i) Para qualquer ideal $\mathcal{I}'$ de R' tem-se que $(\mathcal{I}' \cap R)R' = \mathcal{I}'$. Assim, a aplicação $\mathcal{I}' \mapsto \mathcal{I}' \cap R$ é uma injeção (crescente) do conjunto dos ideais de R' no conjunto dos ideais de R.

(ii) A aplicação $\mathcal{P}' \mapsto \mathcal{P}' \cap R$ é uma bijeção do conjunto dos ideais primos de R' no conjunto dos ideais primos $\mathcal{P}$ de R, que satisfazem $\mathcal{P} \cap S = \emptyset$. A aplicação inversa é $\mathcal{P} \mapsto \mathcal{P}R'$.

Demonstração: (i) Seja $\mathcal{I}'$ um ideal de R'. Se $x \in (\mathcal{I}' \cap R)R'$, então $x = \sum_i a'_i r'_i$, com $a'_i \in \mathcal{I}' \cap R$ e $r'_i \in R'$. Logo $a'_i r'_i \in \mathcal{I}'$, e assim $x \in \mathcal{I}'$. Dessa forma, $(\mathcal{I}' \cap R)R' \subset \mathcal{I}'$. Seja,

agora, $x \in \mathcal{I}' \subset R' = S^{-1}R$, isto é, existem $a \in R$ e $s \in S$ tal que $x = a/s$. Logo, como $S \subset R \subset R'$ e $\mathcal{I}'$ é um ideal de R', segue que $a = xs \in \mathcal{I}'$ e, assim, $a \in \mathcal{I}' \cap R$. Desse modo, $x = a(\frac{1}{s}) \in (\mathcal{I}' \cap R)R'$, assim $\mathcal{I}' \subset (\mathcal{I}' \cap R)R'$. Portanto, $(\mathcal{I}' \cap R)R' = \mathcal{I}'$. Agora, se $\mathcal{I}'$ e $\mathcal{J}'$ são ideais de R' tal que $\mathcal{I}' \cap R = \mathcal{J}' \cap R$, então $\mathcal{I}' = (\mathcal{I}' \cap R)R' = (\mathcal{J}' \cap R)R' = \mathcal{J}'$, ou seja, a aplicação $\mathcal{I}' \mapsto \mathcal{I}' \cap R$ é injetora e, além disso, crescente, pois se $\mathcal{I}' \subset \mathcal{J}'$ então $\mathcal{I}' \cap R \subset \mathcal{J}' \cap R$.

(ii) Denotemos por $\varphi : \mathcal{P}' \mapsto \mathcal{P}' \cap R$ a aplicação definida no conjunto dos ideais primos de R' e por $\psi : \mathcal{P} \mapsto \mathcal{P}R'$ a aplicação definida no conjunto dos ideais primos de R que satisfazem $\mathcal{P} \cap S = \emptyset$. Mostremos que φ está bem definida. Seja $\mathcal{P}'$ um ideal primo de R'. Assim, $\mathcal{P}' \cap R$ é um ideal primo de R e, pondo $\mathcal{P} := \mathcal{P}' \cap R$, tem-se $\mathcal{P} \cap S = \emptyset$, pois se $x \in \mathcal{P} \cap S$ então $x \in \mathcal{P}'$ e $1 = (\frac{1}{x})x \in R'\mathcal{P}' = \mathcal{P}'$, o que é uma contradição. Portanto, φ está bem definida. Mostremos agora que ψ está bem definida. Seja $\mathcal{P}$ um ideal primo de R com $\mathcal{P} \cap S = \emptyset$. Devemos mostrar que $\mathcal{P}R'$ é um ideal primo de R'. Note que

$$\mathcal{P}R' = \left\{ \frac{p}{s};\ p \in \mathcal{P}, s \in S \right\} \subset R'.$$

Sejam a/s e b/t pertencentes a R' com $(a/s)(b/t) \in \mathcal{P}R'$. Assim, existem $p \in \mathcal{P}$ e $u \in S$ tal que $(a/s)(b/t) = p/u$. Logo $abu = pst \in \mathcal{P}$. Uma vez que $\mathcal{P} \cap S = \emptyset$, tem-se que $u \notin \mathcal{P}$. Logo $ab \in \mathcal{P}$ e, assim, $a \in \mathcal{P}$ ou $b \in \mathcal{P}$. Dessa forma $a/s \in \mathcal{P}R'$ ou $b/t \in \mathcal{P}R'$, ou seja, $\mathcal{P}R'$ é um ideal primo de R'. Portanto ψ está bem definida. Agora, mostremos que $\varphi \circ \psi = id$, isto é, $\mathcal{P}R' \cap R = \mathcal{P}$. Claramente $\mathcal{P} \subset \mathcal{P}R' \cap R$. Seja $x \in \mathcal{P}R' \cap R$. Assim existe $p \in \mathcal{P}$ e $s \in S$ tal que $x = p/s$. Logo $sx = p \in \mathcal{P}$. Como $\mathcal{P} \cap S = \emptyset$, segue que $s \notin \mathcal{P}$ e assim $x \in \mathcal{P}$. Portanto $\mathcal{P}R' \cap R = \mathcal{P}$. Mostremos agora que se $\mathcal{P}'$ é um ideal primo de R' então $(\mathcal{P}' \cap R)R' = \mathcal{P}'$, isto é, $\psi \circ \varphi = id$. Claramente $(\mathcal{P}' \cap R)R' \subset \mathcal{P}'$. Se $x \in \mathcal{P}' \subset R'$, então existe $a \in R$ e $s \in S$ tal que $x = \frac{a}{s} = a(\frac{1}{s})$. Assim, a ou $1/s$ pertence $\mathcal{P}'$. Mas, $1/s \notin \mathcal{P}'$, pois caso contrário teríamos que $1 \in \mathcal{P}'$. Assim, $a \in \mathcal{P}'$ e dessa forma $x = a/s \in (\mathcal{P}' \cap R)R'$. Portanto $(\mathcal{P}' \cap R)R' = \mathcal{P}'$. Concluímos, então, que φ é uma bijeção cuja inversa é ψ. ∎

Corolário 2.1.1 *Se R é um domínio noetheriano então todo anel de frações $R' = S^{-1}R$ é noetheriano.*

Demonstração: Seja $R' = S^{-1}R$ um anel de frações de R e considere a aplicação $\varphi : \mathcal{I}' \mapsto \mathcal{I}' \cap R$ definida no conjunto dos ideais de R' e aplicando no conjunto dos ideais de R. Seja $(\mathcal{I}'_n)_n$ uma sequência crescente de ideais de R'. Pelo ítem (i) da Proposição 2.1.1, tem-se que φ é crescente. Logo $(\varphi(\mathcal{I}'_n))_n$ é uma sequência crescente de ideais de R, que é noetheriano. Assim $(\varphi(\mathcal{I}'_n))_n$ é estacionária, isto é, existe n_o inteiro positivo tal que $\varphi(\mathcal{I}'_n) = \varphi(\mathcal{I}'_{n+1})$, para todo $n \geq n_o$. Ainda pelo ítem (i), tem-se que φ é injetiva, e assim $\mathcal{I}'_n = \mathcal{I}'_{n+1}$, para todo $n \geq n_o$, ou seja, $(\mathcal{I}'_n)_n$ é estacionária. Portanto, R' é noetheriano. ∎

Proposição 2.1.2 *Sejam R um domínio, A um subanel de R e $S \subset A - \{0\}$ fechado na multiplicação, com $1 \in S$. Se $B = \mathcal{O}_R(A)$, então o anel de inteiros de $S^{-1}R$ sobre $S^{-1}A$ é $S^{-1}B$.*

Demonstração: Denotemos por $A' = S^{-1}A$, $B' = S^{-1}B$ e $R' = S^{-1}R$. Mostremos que $B' = \mathcal{O}_{R'}(A')$. Se $\alpha \in B'$, então existem $b \in B$ e $s \in S$ tal que $\alpha = b/s$. Como b é inteiro sobre A, segue que existem $a_0, a_1, \ldots, a_{n-1} \in A$ tal que $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$. Multiplicando a igualdade por $1/(s^n)$ obtemos

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_1}{s^{n-1}}\left(\frac{b}{s}\right) + \frac{a_0}{s^n} = 0.$$

Como $a_i/s^{n-i} \in S^{-1}A = A'$, para todo $i = 0, \ldots, n-1$, segue que $\alpha = b/s$ é inteiro sobre A'. Além disso, como $B' \subset R'$, segue que $\alpha \in \mathcal{O}_{R'}(A')$. Portanto, $B' \subset \mathcal{O}_{R'}(A')$. Agora, se $\alpha \in \mathcal{O}_{R'}(A')$, então existem $a_i \in A$ e $s_i \in S$, com $i = 0, \ldots, n-1$, tal que

$$\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \ldots + \frac{a_1}{s_1}\alpha + \frac{a_0}{s_0} = 0. \tag{2.1.1}$$

Pondo $s = s_0 s_1 \ldots s_{n-1}$ e multiplicando a igualdade 2.1.1 por s^n, obtemos

$$(s\alpha)^n + a_{n-1}(s_0 \ldots s_{n-2})(s\alpha)^{n-1} + \ldots + a_0(s_1 \ldots s_{n-1})s^{n-1} = (s\alpha)^n + b_{n-1}(s\alpha)^{n-1} + \ldots + b_0 = 0,$$

em que $b_i = a_i(s_0 \ldots s_{i-1}s_{i+1} \ldots s_{n-1})s^{n-1-i} \in A$, para $i = 0, \ldots, n-1$. Como $\alpha \in R'$, segue que existem $r \in R$ e $t \in S$ tal que $\alpha = r/t$. Dessa forma,

$$\left(\frac{sr}{t}\right)^n + b_{n-1}\left(\frac{sr}{t}\right)^{n-1} + \ldots + b_0 = 0. \tag{2.1.2}$$

com $b_i \in A$, para $i = 0, 1, \ldots, n-1$. Multiplicando a igualdade 2.1.2 por t^n obtemos que $(sr)^n + b_{n-1}t(sr)^{n-1} + \ldots + b_0 t^n = 0$. Assim, $sr \in \mathcal{O}_R(A) = B$, ou seja, $sr = b \in B$, o que implica que $r = b/s \in S^{-1}B = B'$. Desse modo, como $1/t \in B'$, segue que $\alpha = r/t \in B'$. Assim, $\mathcal{O}_{R'}(A') \subset B'$, e portanto $\mathcal{O}_{R'}(A') = B'$. ∎

Corolário 2.1.2 *Se R é um anel integralmente fechado, então todo anel de frações $R' = S^{-1}R$ é integralmente fechado.*

Demonstração: Sejam $R' = S^{-1}R$ um anel de frações e $\mathbb{K}$ o corpo de frações de R. Por hipótese $R = \mathcal{O}_{\mathbb{K}}(R)$. Como $\mathbb{K}$ é um domínio e $R \subset \mathbb{K}$ é um subanel, segue da Proposição 2.1.2 que, $\mathcal{O}_{S^{-1}\mathbb{K}}(R') = S^{-1}R = R'$. Seja $\mathbb{K}'$ o corpo de frações de R'. Mostremos que $\mathbb{K}' = S^{-1}\mathbb{K}$. Se $x \in \mathbb{K}'$, então $x = (r_1/s_1)/(r_2/s_2) = \frac{r_1 s_2}{s_1 r_2} = \frac{1}{s_1}\frac{r_1 s_2}{r_2} \in S^{-1}\mathbb{K}$, com $r_i \in R$ e $s_i \in S$, para $i = 1, 2$.

Agora, se $x \in S^{-1}\mathbb{K}$, então existem $a/b \in \mathbb{K}$ e $s \in S$ tal que $x = (a/b)/s = (a/s)/b \in \mathbb{K}'$. Logo $\mathbb{K}' = S^{-1}\mathbb{K}$ e, portanto, $\mathcal{O}_{\mathbb{K}'}(R') = R'$, ou seja, R' é integralmente fechado. ∎

Proposição 2.1.3 *Se R é um anel de Dedekind, então todo anel de frações $R' = S^{-1}R$ é um anel de Dedekind.*

Demonstração: Seja $R' = S^{-1}R$ um anel de frações de R. Primeiramente, R' é um domínio pois R o é. Pelos Corolários 2.1.1 e 2.1.2 garantimos, respectivamente, que R' é noetheriano e integralmente fechado. Resta provar que todo ideal primo não-nulo de R' é maximal. Seja $\mathcal{P}' \subset R'$ um ideal primo não-nulo. Pela injetividade de $\mathcal{P}' \mapsto \mathcal{P}' \cap R$, vista no ítem (ii) da Proposição 2.1.1, segue que $\mathcal{P}' \cap R$ é um ideal primo não-nulo de R. Logo, como R é Dedekind, segue que $\mathcal{P}' \cap R$ é maximal. Seja $\mathcal{I}$ um ideal de R' tal que $\mathcal{P}' \subseteq \mathcal{I} \subseteq R'$. Assim $\mathcal{P}' \cap R \subseteq \mathcal{I} \cap R \subseteq R' \cap R = R$. Desse modo, $\mathcal{I} \cap R = \mathcal{P}' \cap R$ ou $\mathcal{I} \cap R = R$. Mas, pela injetividade da aplicação $\mathcal{I} \mapsto \mathcal{I} \cap R$, tem-se que $\mathcal{I} = \mathcal{P}'$ ou $\mathcal{I} = R'$, ou seja, $\mathcal{P}'$ é um ideal maximal em R'. Portanto, R' é um anel de Dedekind. ∎

Proposição 2.1.4 *Se R é um anel de Dedekind, $\mathcal{P} \subset R$ um ideal primo não-nulo e $S = R - \mathcal{P}$, então $R' = S^{-1}R$ é um anel principal. Mais precisamente, os ideais de R' são da forma $\langle p^n \rangle$, com $p \in R'$ e n um inteiro positivo.*

Demonstração: Seja $\mathcal{P}$ um ideal primo não-nulo de R. Tem-se que $\mathcal{P}$ é único tal que $\mathcal{P} \cap S = \emptyset$, pois se $\mathcal{Q}$ é um ideal primo não-nulo de R tal que $\mathcal{Q} \cap S = \emptyset$, então $\mathcal{Q} \subset \mathcal{P}$, com $\mathcal{Q}$ maximal, e assim $\mathcal{Q} = \mathcal{P}$. Note que o fato de $\mathcal{P}$ ser primo garante que $R' = S^{-1}R$ está bem definido e o isomorfismo $\mathcal{P} \mapsto \mathcal{P}R'$ do ítem (ii) da Proposição 2.1.1 garante que $B := \mathcal{P}R'$ é o único ideal primo não-nulo de R', pela unicidade de $\mathcal{P}$. Pela Proposição 2.1.3, tem-se que R' é Dedekind, assim do Teorema 1.8.1, todo ideal não-nulo de R' se fatora de maneira única como um produto de ideais primos de R'. Desse modo, pela unicidade do ideal primo $B \subset R'$, segue que todo ideal de R' é da forma B^n, sendo n um inteiro positivo. Considere a sequência de ideais

$$\ldots \subseteq B^n \subseteq \ldots \subseteq B^2 \subseteq B \subseteq R'.$$

Seja $p \in B - B^2$. Tem-se que existe $n_o \in \mathbb{N}^*$ tal que $\langle p \rangle = B^{n_o}$, com $\langle p \rangle \subset B$ e $\langle p \rangle \not\subset B^2$. Logo $\langle p \rangle = B$. Mas como $\langle p^n \rangle = \langle p \rangle^n$, segue que $\langle p^n \rangle = B^n$. Portanto, todo ideal de R' é da forma $\langle p^n \rangle$, com $p \in R'$ e n um inteiro positivo. Dessa forma, R' é principal. ∎

Proposição 2.1.5 *Sejam R um domínio e $R' = S^{-1}R$ um anel de frações de R. Se $\mathcal{M}$ é um ideal maximal de R tal que $\mathcal{M} \cap S = \emptyset$, então*

$$\frac{R'}{\mathcal{M}R'} \simeq \frac{R}{\mathcal{M}}.$$

Demonstração: Se $\mathcal{M}$ é um ideal maximal de R, então $R/\mathcal{M}$ é um corpo, que por sua vez é um domínio. Logo $\mathcal{M}$ é um ideal primo de R. Assim, como $\mathcal{M} \cap S = \emptyset$, segue da Proposição 2.1.1, que $\mathcal{M}R'$ é um ideal primo de R'. Considere a aplicação

$$\varphi : R \xrightarrow{\ i\ } R' \xrightarrow{\ \pi\ } R'/(\mathcal{M}R') \ ,$$

onde i é a inclusão e π a projeção. Afirmamos que $Ker(\varphi) = \mathcal{M}$. De fato, $x \in Ker(\varphi)$ se, e somente se, $x \in R$ e $\varphi(x) = \overline{x} = \overline{0}$, que por sua vez é condição necessária e suficiente para que $x \in \mathcal{M}R' \cap R$. Assim, $Ker(\varphi) = \mathcal{M}R' \cap R$. Porém, pelo ítem (ii) da Proposição 2.1.1, tem-se que $\mathcal{M}R' \cap R = \mathcal{M}$, e desse modo $Ker(\varphi) = \mathcal{M}$. Mostremos que φ é sobrejetiva. Seja $\overline{x} \in R'/(\mathcal{M}R')$, em que $x = r/s$, com $r \in R$ e $s \in S$. Como $\mathcal{M} \cap S = \emptyset$, segue que $s \notin \mathcal{M}$. Logo $\overline{s} \neq \overline{0}$ é inversível no corpo $R/\mathcal{M}$, isto é, existe $\overline{b} \in R/\mathcal{M}$ tal que $\overline{s}\overline{b} = \overline{1}$, e deste modo $1 - sb \in \mathcal{M}$. Dessa forma, $\frac{r}{s} - rb = \frac{r}{s}(1 - sb) \in \mathcal{M}R'$, ou seja, $r/s + \mathcal{M}R' = rb + \mathcal{M}R'$. Assim, $\varphi(rb) = rb + \mathcal{M}R' = \overline{x}$, pois $r/s = x$. Portanto φ é sobrejetiva e, desse modo, concluímos que

$$\frac{R}{\mathcal{M}} = \frac{R}{Ker(\varphi)} \simeq Im(\varphi) = \frac{R'}{\mathcal{M}R'},$$

o que prova a proposição. ∎

2.2 Fatoração de um ideal primo

Nesta seção, consideramos R um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$ e $\mathcal{B} = \mathcal{O}_{\mathbb{L}}(R)$. Pelo Teorema 1.7.1, tem-se que $\mathcal{B}$ é um anel de Dedekind. Sendo assim, se $\mathcal{P}$ é um ideal primo não-nulo de R, segue do Teorema 1.8.1 que o ideal $\mathcal{B}\mathcal{P}$ de $\mathcal{B}$ pode ser unicamente expresso na forma

$$\mathcal{B}\mathcal{P} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i},$$

onde os $\mathcal{P}_i$'s são ideais primos de $\mathcal{B}$, com q e e_i inteiros positivos, para $i = 1, \ldots, q$.

Proposição 2.2.1 *Sejam $\mathcal{P}$ um ideal primo não-nulo de R e $\mathcal{B}\mathcal{P} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{B}\mathcal{P}$. Os ideais $\mathcal{P}_i$'s de $\mathcal{B}$ são os únicos tal que $\mathcal{P}_i \cap R = \mathcal{P}$. Além disso, $\mathcal{B}\mathcal{P} \cap R = \mathcal{P}$.*

Demonstração: Como $\mathcal{P}_i$ é um ideal primo de $\mathcal{B}$ e $R \subset \mathcal{B}$, segue que $\mathcal{P}_i \cap R$ é um ideal primo de R. Como $\mathcal{P} \subset \mathcal{B}\mathcal{P} \subset \mathcal{P}_i$, para todo i, segue que $\mathcal{P} \subset \mathcal{P}_i \cap R$. Porém, $\mathcal{P}$ é maximal, pois R é Dedekind, e assim $\mathcal{P} = \mathcal{P}_i \cap R$. Seja, agora, $\mathcal{Q}$ um ideal primo de $\mathcal{B}$ tal que $\mathcal{Q} \cap R = \mathcal{P}$. Logo $\mathcal{P} \subset \mathcal{Q}$ e assim $\mathcal{B}\mathcal{P} \subset \mathcal{B}\mathcal{Q} = \mathcal{Q}$, ou seja, $\prod_{i=1}^{q} \mathcal{P}_i^{e_i} \subset \mathcal{Q}$. Desse modo, existe $j \in \{1, \ldots, q\}$ tal que $\mathcal{P}_j \subset \mathcal{Q}$. Mas, como $\mathcal{B}$ é Dedekind, segue que $\mathcal{P}_j$ é maximal, e assim $\mathcal{P}_j = \mathcal{Q}$. Portanto, $\mathcal{Q}$

é fator na fatoração de $\mathcal{BP}$. Por outro lado, tem-se que $\mathcal{P} \subset \mathcal{BP} \cap R$ e, como $\mathcal{BP} \subset \mathcal{P}_i$, segue que $\mathcal{BP} \cap R \subset \mathcal{P}_i \cap R = \mathcal{P}$. Portanto $\mathcal{BP} \cap R = \mathcal{P}$. ■

Observação 2.2.1 *Sejam $\mathcal{P}$ ideal primo não-nulo de R e $\mathcal{BP} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{BP}$ de $\mathcal{B}$. Como R e $\mathcal{B}$ são anéis de Dedekind, segue que $\mathcal{P}$ e $\mathcal{P}_i$ são ideais maximais de R e $\mathcal{B}$, respectivamente. Dessa forma, $R/\mathcal{P}$ e $\mathcal{B}/\mathcal{P}_i$ são corpos, para todo $i = 1, \ldots, q$.*

Para os próximos resultados, consideramos $\mathcal{P}$ um ideal primo não-nulo de R e $\mathcal{BP} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{BP}$ de $\mathcal{B}$.

Lema 2.2.1 *O corpo $R/\mathcal{P}$ pode ser identificado com um subcorpo de $\mathcal{B}/\mathcal{P}_i$ e, além disso, $\mathcal{B}/\mathcal{P}_i$ é um espaço vetorial de dimensão finita sobre $R/\mathcal{P}$, para todo $i = 1, \ldots, q$.*

Demonstração: Considere a aplicação $\varphi : R \xrightarrow{id} \mathcal{B} \xrightarrow{\pi} \mathcal{B}/\mathcal{P}_i$, em que id é a inclusão e π a projeção. Tem-se que

$$Ker(\varphi) = \{x \in R;\ \varphi(x) = \overline{x} = \overline{0}\} = \{x \in R;\ x \in \mathcal{P}_i\} = R \cap \mathcal{P}_i = \mathcal{P}.$$

Assim $R/\mathcal{P} \simeq Im(\varphi)$, que é subcorpo de $\mathcal{B}/\mathcal{P}_i$. Dados $x + \mathcal{P}_i,\ y + \mathcal{P}_i \in \mathcal{B}/\mathcal{P}_i$ e $a + \mathcal{P} \in R/\mathcal{P}$, mostremos que o espaço vetorial $\mathcal{B}/\mathcal{P}_i$, com as operações $(x + \mathcal{P}_i) + (y + \mathcal{P}_i) = (x + y) + \mathcal{P}_i$ e $(a + \mathcal{P})(x + \mathcal{P}_i) = ax + \mathcal{P}_i$, tem dimensão finita sobre $R/\mathcal{P}$. Pelo Teorema 1.4.1, tem-se que $\mathcal{B}$ é um R-módulo livre de posto n. Seja $\{x_1, \ldots, x_n\}$ uma base de $\mathcal{B}$ sobre R. Se $\overline{b} \in \mathcal{B}/\mathcal{P}_i$, então existem $a_1, \ldots, a_n \in R$ tal que $b = a_1x_1 + \ldots + a_nx_n$. Assim,

$$\overline{b} = b + \mathcal{P}_i = (a_1x_1 + \mathcal{P}_i) + \ldots + (a_nx_n + \mathcal{P}_i) = (a_1 + \mathcal{P})(x_1 + \mathcal{P}_i) + \ldots + (a_n + \mathcal{P})(x_n + \mathcal{P}_i),$$

isto é, $\{\overline{x}_1, \ldots, \overline{x}_n\}$ é um conjunto de geradores de $\mathcal{B}/\mathcal{P}_i$ sobre $R/\mathcal{P}$, portanto $\mathcal{B}/\mathcal{P}_i$ tem dimensão finita sobre $R/\mathcal{P}$. ■

Definição 2.2.1 *O grau $f_i = f(\mathcal{P}_i/R)$ da extensão $\mathcal{B}/\mathcal{P}_i$ sobre $R/\mathcal{P}$ é chamado grau residual de $\mathcal{P}_i$ sobre R. O expoente $e_i = e(\mathcal{P}_i/R)$ é chamado índice de ramificação de $\mathcal{P}_i$ sobre R.*

Lema 2.2.2 *A sequência decrescente*

$$\mathcal{B} \supset \mathcal{P}_1 \supset \mathcal{P}_1^2 \supset \ldots \supset \mathcal{P}_1^{e_1} \supset \mathcal{P}_1^{e_1}\mathcal{P}_2 \supset \ldots \supset \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \supset \ldots \supset \mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q} = \mathcal{BP}$$

de ideais de $\mathcal{B}$ é maximal.

Demonstração: Tem-se que dois elementos consecutivos desta sequência são da forma $\mathcal{Q}$ e $\mathcal{QP}_i$, onde $\mathcal{Q}$ é um produto de alguns ideais $\mathcal{P}_j$, com $j = 1, \ldots, q$. Seja $\mathcal{A}$ um ideal de $\mathcal{B}$ tal que $\mathcal{Q} \supseteq \mathcal{A} \supseteq \mathcal{QP}_i$. Como $\mathcal{B}$ é um domínio, segue que $\mathcal{A}$ e $\mathcal{QP}_i$ são fracionários. Logo, pela

Proposição 1.8.1, segue que $\mathcal{A}$ divide $\mathcal{QP}_i$, isto é, existe um ideal $\mathcal{I}$ de $\mathcal{B}$ tal que $\mathcal{QP}_i = \mathcal{IA}$. Analogamente existe um ideal $\mathcal{J}$ de $\mathcal{B}$ tal que $\mathcal{A} = \mathcal{JQ}$. Assim $\mathcal{QP}_i = \mathcal{IJQ}$, e deste modo $\mathcal{P}_i = \mathcal{IJ}$. Dessa forma, $\mathcal{P}_i = \mathcal{IJ} \subseteq \mathcal{I} \subseteq \mathcal{B}$. Como $\mathcal{B}$ é Dedekind, segue que $\mathcal{P}_i$ é maximal. Logo $\mathcal{I} = \mathcal{P}_i$ ou $\mathcal{I} = \mathcal{B}$. Assim, $\mathcal{P}_i = \mathcal{IJ} = \mathcal{BJ} = \mathcal{J}$, ou seja, $\mathcal{P}_i = \mathcal{I}$ ou $\mathcal{P}_i = \mathcal{J}$. Desse modo, $\mathcal{A} = \mathcal{Q}$ se $\mathcal{P}_i = \mathcal{I}$ ou $\mathcal{A} = \mathcal{QP}_i$ se $\mathcal{P}_i = \mathcal{J}$. Portanto, a sequência é maximal. ∎

Lema 2.2.3 *Considere a sequência decrescente de ideais de $\mathcal{B}$ dada por:*

$$\mathcal{B} \supset \mathcal{P}_1 \supset \mathcal{P}_1^2 \supset \ldots \supset \mathcal{P}_1^{e_1} \supset \mathcal{P}_1^{e_1}\mathcal{P}_2 \supset \ldots \supset \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \supset \ldots \supset \mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q} = \mathcal{BP}.$$

Se $\mathcal{Q}$ é um ideal diferente de $\mathcal{BP}$ desta cadeia, então $\mathcal{Q}/\mathcal{QP}_i$, $\mathcal{B}/\mathcal{Q}$ e $\mathcal{B}/\mathcal{QP}_i$ são espaços vetoriais sobre $R/\mathcal{P}$ e, além disso,

$$[\mathcal{B}/\mathcal{QP}_i : R/\mathcal{P}] = [\mathcal{B}/\mathcal{Q} : R/\mathcal{P}] + [\mathcal{Q}/\mathcal{QP}_i : R/\mathcal{P}].$$

Demonstração: Analogamente ao Lema 2.2.1, mostra-se que $\mathcal{B}/\mathcal{Q}$ e $\mathcal{B}/\mathcal{QP}_i$ são $R/\mathcal{P}$-espaços vetoriais. Seja a aplicação $\varphi : \mathcal{B}/\mathcal{QP}_i \to \mathcal{B}/\mathcal{Q}$ dada por $\varphi(x + \mathcal{QP}_i) = x + \mathcal{Q}$. Tem-se que φ é uma transformação linear sobrejetora. Além disso,

$$Ker(\varphi) = \{x + \mathcal{QP}_i \in \mathcal{B}/\mathcal{QP}_i;\ x + \mathcal{Q} = \varphi(x + \mathcal{QP}_i) = \mathcal{Q}\} = \{\overline{x} \in \mathcal{B}/\mathcal{QP}_i;\ x \in \mathcal{Q}\} = \mathcal{Q}/\mathcal{QP}_i.$$

Assim, $\mathcal{Q}/\mathcal{QP}_i = Ker(\varphi)$ é um espaço vetorial sobre $R/\mathcal{P}$ e, pelo Teorema do Núcleo e da Imagem, segue que

$$[\mathcal{B}/\mathcal{QP}_i : R/\mathcal{P}] = [\mathcal{B}/\mathcal{Q} : R/\mathcal{P}] + [\mathcal{Q}/\mathcal{QP}_i : R/\mathcal{P}],$$

o que prova o lema. ∎

Lema 2.2.4 *Considere a sequência de ideais de $\mathcal{B}$ dada por:*

$$\mathcal{B} \supset \mathcal{P}_1 \supset \mathcal{P}_1^2 \supset \ldots \supset \mathcal{P}_1^{e_1} \supset \mathcal{P}_1^{e_1}\mathcal{P}_2 \supset \ldots \supset \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \supset \ldots \supset \mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q} = \mathcal{BP}.$$

Se $\mathcal{Q}$ é um ideal diferente de $\mathcal{BP}$ desta cadeia, então $\mathcal{Q}/\mathcal{QP}_i$ é um espaço vetorial sobre $\mathcal{B}/\mathcal{P}_i$ e $[\mathcal{Q}/\mathcal{QP}_i : \mathcal{B}/\mathcal{P}_i] = 1$, para todo $i = 1, \ldots, q$.

Demonstração: Dados $x + \mathcal{QP}_i,\ y + \mathcal{QP}_i \in \mathcal{Q}/\mathcal{QP}_i$ e $a + \mathcal{P}_i \in \mathcal{B}/\mathcal{P}_i$, tem-se que $\mathcal{Q}/\mathcal{QP}_i$, com as operações $(x + \mathcal{QP}_i) + (y + \mathcal{QP}_i) = (x + y) + \mathcal{QP}_i$ e $(a + \mathcal{P}_i)(x + \mathcal{QP}_i) = ax + \mathcal{QP}_i$, é um espaço vetorial sobre $\mathcal{B}/\mathcal{P}_i$. Podemos identificar $\mathcal{B}/\mathcal{P}_i$ com um subanel de $\mathcal{Q}/\mathcal{QP}_i$, e dessa forma $\mathcal{B}/\mathcal{P}_i$ pode ser visto como um subespaço de $\mathcal{Q}/\mathcal{QP}_i$. Porém, os únicos subespaços de $\mathcal{Q}/\mathcal{QP}_i$ são os triviais, pois se existir um subespaço não trivial, deve ser da forma $\mathcal{A}/\mathcal{QP}_i$, onde $\mathcal{QP}_i \subsetneq \mathcal{A} \subsetneq \mathcal{Q}$, o que contradiz o Lema 2.2.2. Desse modo, como $\mathcal{B}/\mathcal{P}_i \neq \{0\}$, segue que $\mathcal{B}/\mathcal{P}_i \simeq \mathcal{Q}/\mathcal{QP}_i$, e portanto $[\mathcal{Q}/\mathcal{QP}_i : \mathcal{B}/\mathcal{P}_i] = 1$. ∎

Observação 2.2.2 *Note que $\mathcal{B}/\mathcal{BP}$ é um espaço vetorial de dimensão finita sobre $R/\mathcal{P}$. A verificação é análoga ao Lema 2.2.1, substituindo $\mathcal{P}_i$ por $\mathcal{BP}$.*

Teorema 2.2.1 *Se $f_i = [\mathcal{B}/\mathcal{P}_i : R/\mathcal{P}]$, para $i = 1, \ldots, q$, então*

$$\sum_{i=1}^{q} e_i f_i = [\mathcal{B}/\mathcal{BP} : R/\mathcal{P}].$$

Demonstração: Seja $\mathcal{Q}$ um ideal diferente de $\mathcal{BP}$ da cadeia do Lema 2.2.4. Utilizando os Lemas 2.2.1 e 2.2.4 podemos dizer, a menos de isomorfismo, que $R/\mathcal{P} \subset \mathcal{B}/\mathcal{P}_i \subset \mathcal{Q}/\mathcal{QP}_i$, em que os dois primeiros são corpos e o terceiro é um anel. Ainda, pelos mesmos lemas e pela multiplicidade dos graus, tem-se que

$$[\mathcal{Q}/\mathcal{QP}_i : R/\mathcal{P}] = [\mathcal{Q}/\mathcal{QP}_i : \mathcal{B}/\mathcal{P}_i][\mathcal{B}/\mathcal{P}_i : R/\mathcal{P}] = 1 f_i = f_i,$$

para $i = 1, \ldots, q$. Fixando o índice i e variando as possibilidades para o ideal $\mathcal{Q}$, tem-se exatamente e_i quocientes da forma $\mathcal{Q}/\mathcal{QP}_i$, isto é, pode-se obter de tal cadeia exatamente e_i espaços vetoriais de dimensão f_i sobre $R/\mathcal{P}$. Assim, do Lema 2.2.3, tem-se que

$$\begin{aligned}
[\mathcal{B}/\mathcal{BP} : R/\mathcal{P}] &= [\mathcal{B}/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-1}) : R/\mathcal{P}] + [(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-1})/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q}) : R/\mathcal{P}] \\
&= [\mathcal{B}/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-1}) : R/\mathcal{P}] + f_q \\
&= [\mathcal{B}/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-2}) : R/\mathcal{P}] + [(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-2})/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-1}) : R/\mathcal{P}] + f_q \\
&= [\mathcal{B}/(\mathcal{P}_1^{e_1} \ldots \mathcal{P}_q^{e_q-2}) : R/\mathcal{P}] + f_q + f_q \\
&= [\mathcal{B}/\mathcal{P}_1 : R/\mathcal{P}] + (e_1 - 1)f_1 + e_2 f_2 + \ldots + e_q f_q \\
&= e_1 f_1 + \ldots + e_q f_q \\
&= \sum_{i=1}^{q} e_i f_i,
\end{aligned}$$

o que conclui a demonstração. ∎

Lema 2.2.5 *Se R é um anel principal então $[\mathcal{B}/\mathcal{BP} : R/\mathcal{P}] = n$.*

Demonstração: Como R é principal, pelo Teorema 1.4.1, segue que $\mathcal{B}$ é um R-módulo livre de posto n. Seja $\{x_1, \ldots, x_n\}$ uma base de $\mathcal{B}$ sobre R. Mostremos que $\mathcal{C} = \{x_1 + \mathcal{BP}, \ldots, x_n + \mathcal{BP}\}$ é uma base de $\mathcal{B}/\mathcal{BP}$ sobre $R/\mathcal{P}$. Se $\overline{b} = b + \mathcal{BP} \in \mathcal{B}/\mathcal{BP}$, então existem $a_1, \ldots, a_n \in R$ tal que $\overline{b} = \sum_{i=1}^{n} a_i x_i + \mathcal{BP}$. Logo

$$\overline{b} = (a_1 x_1 + \mathcal{BP}) + \ldots + (a_n x_n + \mathcal{BP}) = (a_1 + \mathcal{P})(x_1 + \mathcal{BP}) + \ldots + (a_n + \mathcal{P})(x_n + \mathcal{BP}),$$

isto é, $\mathcal{C}$ é um gerador de $\mathcal{B}/\mathcal{BP}$ sobre $R/\mathcal{P}$. Agora, suponhamos que $(a_1 + \mathcal{P})(x_1 + \mathcal{BP}) + \ldots + (a_n + \mathcal{P})(x_n + \mathcal{BP}) = 0 + \mathcal{BP} = \overline{0}$. Desse modo $\sum_{i=1}^{n} a_i x_i + \mathcal{BP} = \mathcal{BP}$, isto é, $\sum_{i=1}^{n} a_i x_i \in \mathcal{BP}$.

Assim existem $b_j \in \mathcal{B}$ e $p_j \in \mathcal{P}$, com $j = 1, \ldots, s$, tal que $\sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{s} b_j p_j$. Porém, para cada j, existem $c_{ij}, \ldots, c_{nj} \in R$ tal que $b_j = \sum_{i=1}^{n} c_{ij} x_i$. Logo

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

Dessa forma,

$$\sum_{i=1}^{n} (a_i - \sum_{j=1}^{s} c_{ij} p_j) x_i = 0.$$

Como $\{x_i\}_{i=1}^{n}$ é linearmente independente sobre R, segue que $a_i = \sum_{j=1}^{s} c_{ij} p_j$, o que implica que $a_i \in \mathcal{P}$ para todo $i = 1, \ldots, n$. Assim, $a_i + \mathcal{P} = \overline{0}$ para todo $i = 1, \ldots, n$, e portanto $\mathcal{C} = \{x_1 + \mathcal{BP}, \ldots, x_n + \mathcal{BP}\}$ é linearmente independente sobre $R/\mathcal{P}$ e consequentemente é uma base de $\mathcal{B}/\mathcal{BP}$ sobre $R/\mathcal{P}$. ∎

Observação 2.2.3 *O Lema 2.2.5 é válido para o caso particular em que R é principal. Na seguinte proposição consideramos o caso em que R é apenas Dedekind, de modo a obter o Teorema da Igualdade Fundamental, que é o principal resultado desta seção.*

Proposição 2.2.2 *Se R é um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$, $\mathcal{B} = \mathcal{O}_{\mathbb{L}}(R)$, $\mathcal{P}$ um ideal primo não-nulo de R, $\mathcal{BP} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{BP}$ de $\mathcal{B}$ e $f_i = [\mathcal{B}/\mathcal{P}_i : R/\mathcal{P}]$, para $i = 1, \ldots, q$, então*

$$[\mathcal{B}/\mathcal{BP} : R/\mathcal{P}] = n.$$

Demonstração: Pela Proposição 2.1.4, tem-se que $R' = S^{-1}R$ é um anel principal, onde $S = R - \mathcal{P}$. Além disso, como $\mathbb{L}$ é um domínio, R é um subanel de $\mathbb{L}$ e $S \subset R - \{0\}$ é fechado na multiplicação (pois $\mathcal{P}$ é primo) com $1 \in S$, segue da Proposição 2.1.2 que $\mathcal{O}_{S^{-1}\mathbb{L}}(R') = S^{-1}\mathcal{B}$. Porém, como $\mathbb{L}$ é um corpo com $S \subset \mathbb{L}$, segue que $S^{-1}\mathbb{L} = \mathbb{L}$, e então $\mathcal{O}_{\mathbb{L}}(R') = S^{-1}\mathcal{B}$. Assim, pelo Teorema 1.4.1, tem-se que $\mathcal{B}' := S^{-1}\mathcal{B}$ é um R'-módulo livre de posto n, e do Lema 2.2.5 tem-se $[\mathcal{B}'/\mathcal{B}'\mathcal{P} : R'/R'\mathcal{P}] = n$. Da fatoração $\mathcal{BP} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ em $\mathcal{B}$, obtemos a fatoração $\mathcal{B}'\mathcal{P} = \prod_{i=1}^{q} (\mathcal{B}'\mathcal{P}_i)^{e_i}$ em $\mathcal{B}'$, e como $\mathcal{P}_i \cap R = \mathcal{P}$ (veja Proposição 2.2.1), com $\mathcal{P} \cap S = \emptyset$, e os $\mathcal{B}'\mathcal{P}_i$'s são ideais primos não-nulos de $\mathcal{B}'$, segue do Teorema 2.2.1 que

$$[\mathcal{B}'/\mathcal{B}'\mathcal{P} : R'/R'\mathcal{P}] = \sum_{i=1}^{q} e_i [\mathcal{B}'/\mathcal{B}'\mathcal{P}_i : R'/R'\mathcal{P}].$$

Desse modo, como $R'/R'\mathcal{P} \simeq R/\mathcal{P}$ e $\mathcal{B}'/\mathcal{B}'\mathcal{P}_i \simeq \mathcal{B}/\mathcal{P}_i$ (veja Proposição 2.1.5), concluímos que

$$[\mathcal{B}/\mathcal{BP} : R/\mathcal{P}] = \sum_{i=1}^{q} e_i f_i = \sum_{i=1}^{q} e_i [\mathcal{B}'/\mathcal{B}'\mathcal{P}_i : R'/R'\mathcal{P}] = [\mathcal{B}'/\mathcal{B}'\mathcal{P} : R'/R'\mathcal{P}] = n,$$

o que prova a proposição. ∎

Teorema 2.2.2 *(Igualdade Fundamental) Se R é um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$, $\mathcal{B} = \mathcal{O}_{\mathbb{L}}(R)$, $\mathcal{P}$ um ideal primo não-nulo de R, $\mathcal{B}\mathcal{P} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{B}\mathcal{P}$ de $\mathcal{B}$ e $f_i = [\mathcal{B}/\mathcal{P}_i : R/\mathcal{P}]$, para $i = 1, \ldots, q$, então*

$$\sum_{i=1}^{q} e_i f_i = [\mathcal{B}/\mathcal{B}\mathcal{P} : R/\mathcal{P}] = n.$$

Demonstração: Decorre diretamente do Teorema 2.2.1 e da Proposição 2.2.2.

Proposição 2.2.3 *Com as mesmas hipóteses do Teorema 2.2.2, tem-se que*

$$\frac{B}{B\mathcal{P}} \simeq \frac{B}{\mathcal{P}_1^{e_1}} \times \ldots \times \frac{B}{\mathcal{P}_q^{e_q}}.$$

Demonstração: Afirmamos que, para cada $i = 1, \ldots, q$, $\mathcal{P}_i$ é o único ideal maximal de $\mathcal{B}$ que contém $\mathcal{P}_i^{e_i}$. De fato, $\mathcal{P}_i \supset \mathcal{P}_i^{e_i}$ e como $\mathcal{B}$ é Dedekind e $\mathcal{P}_i$ é um ideal primo não-nulo de $\mathcal{B}$ segue que $\mathcal{P}_i$ é maximal. Suponha, agora, que $\mathcal{M}$ seja um ideal maximal de $\mathcal{B}$ com $\mathcal{M} \supset \mathcal{P}_i^{e_i}$. Assim, $\mathcal{M}$ é primo e $\mathcal{M} \supseteq \mathcal{P}_i$. Desse modo, $\mathcal{P}_i$ é maximal com $\mathcal{P}_i \subseteq \mathcal{M} \subsetneq \mathcal{B}$ ($\mathcal{M} \neq \mathcal{B}$, pois é primo). Logo, $\mathcal{M} = \mathcal{P}_i$. Mostremos agora que $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} = \mathcal{B}$, para $i \neq j$. Se $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} \subsetneq \mathcal{B}$ com $i \neq j$, então existe um ideal maximal $\mathcal{M}$ de $\mathcal{B}$ tal que $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} \subset \mathcal{M} \subset \mathcal{B}$. De $\mathcal{P}_i^{e_i} \subset \mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j}$ segue que $\mathcal{P}_i^{e_i} \subset \mathcal{M}$, e assim $\mathcal{M} = \mathcal{P}_i$. Analogamente, como $\mathcal{P}_j^{e_j} \subset \mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j}$, segue que $\mathcal{P}_j^{e_j} \subset \mathcal{M}$, e assim $\mathcal{M} = \mathcal{P}_j$. Dessa forma $\mathcal{P}_i = \mathcal{P}_j$, o que é uma contradição. Sendo assim, tem-se que $\mathcal{P}_i^{e_i} + \mathcal{P}_j^{e_j} = \mathcal{B}$ para $i \neq j$. Portanto, pelo Lema 1.1.2 de [11], concluímos que

$$\frac{B}{B\mathcal{P}} = \frac{B}{\prod_{i=1}^{q} \mathcal{P}_i^{e_i}} \simeq \frac{B}{\mathcal{P}_1^{e_1}} \times \ldots \times \frac{B}{\mathcal{P}_q^{e_q}},$$

o que demonstra o teorema. ∎

Exemplo 2.2.1 *Seja p um número primo e denotemos $\zeta = \zeta_{p^r}$. Mostraremos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p^{r-1}(p-1)$, utilizando a fatoração de ideais. Considere o p^r-ésimo polinômio ciclotômico*

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

Denotemos $s := p^{r-1}(p-1)$ e $z_1, \ldots, z_s$ as raízes p^r-ésimas primitivas da unidade. O termo constante do polinômio $\phi_{p^r}(x+1)$ é p e suas raízes são $z_j - 1$, com $j = 1, \ldots, s$. Desse modo $\prod_{j=1}^{s}(z_j - 1) = \pm p$. Consideremos o anel $\mathbb{Z}$ de Dedekind, $\mathbb{Q}$ seu corpo de frações, $\mathbb{Q}(\zeta)$ extensão finita de $\mathbb{Q}$, $\mathcal{B} = \mathcal{O}_{\mathbb{Q}(\zeta)}$ o anel de inteiros de $\mathbb{Q}(\zeta)$, o ideal $\langle p \rangle$ primo não-nulo de $\mathbb{Z}$,

$\mathcal{B}p = \mathcal{B}\langle p\rangle = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{B}p$ de $\mathcal{B}$ e $f_i = [\mathcal{B}/\mathcal{P}_i : \mathbb{Z}/\langle p\rangle]$, para $i = 1, \ldots, s$. Tem-se que $z_j \in \mathcal{B}$ e além disso $z_j - 1 \in \mathcal{B}(z_k - 1)$, para todo $j, k = 1, \ldots, s$, pois z_j é uma potência $(z_k)^t$ de z_k e $(z_k)^t - 1 = (z_k - 1)(z_k^{t-1} + \ldots + z_k + 1)$. Assim os ideais $\mathcal{B}(z_j - 1)$ são iguais, para $i = 1, \ldots, s$. Logo,

$$\mathcal{B}p = \prod_{j=1}^{s} \mathcal{B}(z_j - 1) = \mathcal{B}(z_1 - 1)^s.$$

Como $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ coincide com o grau do polinômio minimal de ζ, segue que $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq s$. Assim, pelo Teorema da Igualdade Fundamental, segue que $\sum_{i=1}^{q} e_i f_i \leq s$. Porém, como $f_i \geq 1$ e os e_i's são múltiplos de s, segue que $q = 1$, $f_1 = 1$ e $s = e_1$, e portanto $[\mathbb{Q}(\zeta) : \mathbb{Q}] = e_1 = s$.

2.3 Ramificação via discriminante

Nesta seção, apresentamos resultados que relacionam a fatoração de ideais com o discriminante.

Definição 2.3.1 *Sejam R um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subset \mathbb{L}$ uma extensão finita, $\mathcal{P}$ um ideal primo não-nulo de R e $\mathcal{P}\mathcal{O}_{\mathbb{L}}(R) = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ a fatoração do ideal $\mathcal{P}\mathcal{O}_{\mathbb{L}}(R)$ de $\mathcal{O}_{\mathbb{L}}(R)$. Dizemos que $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}(R)$ se um dos índices de ramificação e_i é maior do que 1.*

Em toda seção, consideramos $\mathbb{K} \subset \mathbb{L}$ corpos de números e $\mathcal{P}$ um ideal primo não-nulo do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Dessa maneira, tem-se que $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind (veja Corolário 1.7.1) e $\mathbb{L}$ é uma extensão finita do corpo de frações $\mathbb{K}'$ de $\mathcal{O}_{\mathbb{K}}$, pois $\mathbb{Q} \subset \mathbb{K}' \subset \mathbb{K} \subset \mathbb{L}$. Além disso, $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{L}}(\mathcal{O}_{\mathbb{K}})$. Sendo assim, podemos definir a ramificação do ideal $\mathcal{P}$ em $\mathcal{O}_{\mathbb{L}}$.

Teorema 2.3.1 *O ideal $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ não é reduzido.*

Demonstração: Suponhamos que $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$, isto é, se $\mathcal{O}_{\mathbb{L}}\mathcal{P} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$ é a fatoração do ideal $\mathcal{O}_{\mathbb{L}}\mathcal{P}$ de $\mathcal{O}_{\mathbb{L}}$, então existe $k \in \{1, \ldots, q\}$ tal que $e_k > 1$. Tem-se que $\mathcal{O}_{\mathbb{L}}\mathcal{P} \subsetneq \mathcal{P}_i$, para todo $i = 1, \ldots, q$, pois se $\mathcal{O}_{\mathbb{L}}\mathcal{P} = \mathcal{P}_j$ para algum j, segue pela unicidade da fatoração de $\mathcal{O}_{\mathbb{L}}\mathcal{P}$, que $e_j = 1$ é o único índice de ramificação, contrariando a hipótese. Seja $a_i \in \mathcal{P}_i - \mathcal{O}_{\mathbb{L}}\mathcal{P}$, para $i = 1, \ldots, q$. Assim, $x = a_1 a_2 \ldots a_q \in \mathcal{O}_{\mathbb{L}} - \mathcal{O}_{\mathbb{L}}\mathcal{P}$, pois $\mathcal{O}_{\mathbb{L}}\mathcal{P}$ é um primo. Logo $\overline{x} = x + \mathcal{O}_{\mathbb{L}}\mathcal{P} \neq \overline{0}$. Pondo $r = e_1 e_2 \ldots e_q$, segue que

$$\overline{x}^r = \overline{x^r} = \overline{(a_1 a_2 \ldots a_q)^r} = a_1^r a_2^r \ldots a_q^r + \mathcal{O}_{\mathbb{L}}\mathcal{P} = \overline{0},$$

pois $a_i^r = (a_i^{e_i})^{e_1 \ldots e_{i-1} e_{i+1} \ldots e_q} \in \mathcal{P}_i^{e_i}$, o que implica que $a_1^r a_2^r \ldots a_q^r \in \prod_{i=1}^{q} \mathcal{P}_i^{e_i} = \mathcal{O}_{\mathbb{L}}\mathcal{P}$. Desse modo, $\overline{x} \neq \overline{0}$ é um elemento nilpotente de $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$, ou seja, $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ não é reduzido. Reciprocamente, suponha que $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ não é reduzido. Pela Proposição 2.2.3, segue que

$$\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}} \simeq \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}_1^{e_1}} \times \ldots \times \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}_q^{e_q}},$$

e assim, existe $\overline{x} \in \mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ não-nulo nilpotente com $\overline{x} = (x_1 + \mathcal{P}_1^{e_1}, \ldots, x_q + \mathcal{P}_q^{e_q}) \neq \overline{0}$. Dessa forma, existe $j \in \{1, \ldots, q\}$ tal que $x_j + \mathcal{P}_j^{e_j} \neq \overline{0}$, isto é, $x_j \notin \mathcal{P}_j^{e_j}$. Além disso, existe um inteiro positivo s tal que $x_j^s \in \mathcal{P}_j^{e_j}$. Logo $e_j > 1$, pois caso contrário teríamos $x_j^s \in \mathcal{P}_j$ com $\mathcal{P}_j$ primo, o que implica que $x_j \in \mathcal{P}_j$, o que é uma contradição. Portanto, $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$. ∎

Corolário 2.3.1 *O ideal $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{D}(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}}/\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}) = \{0\}$.*

Demonstração: Pelo Teorema 2.3.1, tem-se que $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ não é reduzido. Pela Proposição 1.6.3 esta é uma condição necessária e suficiente para que $\mathcal{D}(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}}/\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}) = \{0\}$, o que conclui a demonstração. ∎

Teorema 2.3.2 *O ideal $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{D}(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}) \subset \mathcal{P}$.*

Demonstração: Suponhamos que $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$. Sejam $S = \mathcal{O}_{\mathbb{K}} - \mathcal{P}$, $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $\mathcal{P}' = \mathcal{P}\mathcal{O}'_{\mathbb{K}}$. Pela Proposição 2.1.4, segue que $\mathcal{O}'_{\mathbb{K}}$ é principal e, assim, pelo Teorema 1.4.1 segue que $\mathcal{O}'_{\mathbb{L}} = \mathcal{O}_{\mathbb{L}}(\mathcal{O}'_{\mathbb{K}})$ é um $\mathcal{O}'_{\mathbb{K}}$-módulo livre de posto finito e da Proposição 2.1.5, tem-se que

$$\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}} \simeq \frac{\mathcal{O}'_{\mathbb{K}}}{\mathcal{P}'} \quad \text{e} \quad \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}} \simeq \frac{\mathcal{O}'_{\mathbb{L}}}{\mathcal{O}'_{\mathbb{L}}\mathcal{P}'}.$$

Seja $\{e_1, \ldots, e_n\}$ uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre $\mathcal{O}'_{\mathbb{K}}$. Logo $\{\overline{e}_1, \ldots, \overline{e}_n\} = \{e_1 + \mathcal{O}'_{\mathbb{L}}\mathcal{P}', \ldots, e_n + \mathcal{O}'_{\mathbb{L}}\mathcal{P}'\}$ é uma base de $\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{P}'$ sobre $\mathcal{O}'_{\mathbb{K}}/\mathcal{P}'$, e também uma base de $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{L}}\mathcal{P}$ sobre $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$. Pelo Corolário 2.3.1 tem-se que $\mathcal{D}(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}}/\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}) = \{0\}$. Assim, $\overline{0} = \mathcal{D}(\overline{e}_1, \ldots, \overline{e}_n) = \overline{\mathcal{D}(e_1, \ldots, e_n)} \in \mathcal{O}'_{\mathbb{K}}/\mathcal{P}'$ e deste modo, $\mathcal{D}(e_1, \ldots, e_n) \in \mathcal{P}'$. Agora, se $\{x_1, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}'_{\mathbb{L}}$, então existem $a_{ij} \in \mathcal{O}'_{\mathbb{K}}$ com $1 \leq i, j \leq n$ tal que $x_i = \sum_{j=1}^n a_{ij}e_j$, com $i = 1, \ldots, n$. Assim, pela Proposição 1.6.2 segue que $\mathcal{D}(x_1, \ldots, x_n) = (det(a_{ij}))^2\mathcal{D}(e_1, \ldots, e_n) \in \mathcal{O}'_{\mathbb{K}}\mathcal{P}' \subset \mathcal{P}'$ e como $\mathcal{D}(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}}$, obtemos $\mathcal{D}(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}} \cap \mathcal{P}' = \mathcal{P}$ (veja a Proposição 2.1.1). Portanto, pondo $d := \mathcal{D}(x_1, \ldots, x_n)$, teremos $\mathcal{D}(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}) = d\mathcal{O}_{\mathbb{K}} \subset \mathcal{P}$. Reciprocamente, suponha que $\mathcal{D}(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}) \subset \mathcal{P}$. Tem-se que $e_i = y_i/s_i$, com $y_i \in \mathcal{O}_{\mathbb{L}}$ e $s_i \in S$, $i = 1, \ldots, n$. Pondo $s = s_1 s_2 \ldots s_n$, segue que $e_i = z_i/s$, com $z_i = (s_1 \ldots s_{i-1} s_{i+1} \ldots s_n)y_i \in \mathcal{O}_{\mathbb{L}}$ e $s \in S$. Dessa forma, $\{z_1, \ldots, z_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathcal{O}_{\mathbb{K}}$, pois é linearmente independente sobre $\mathcal{O}'_{\mathbb{K}}$ e consequentemente sobre $\mathcal{O}_{\mathbb{K}}$. Logo,

$$\begin{aligned}
\mathcal{D}(e_1, \ldots, e_n) &= det(Tr_{\mathbb{L}/\mathbb{K}}(e_i e_j)) \\
&= det(Tr_{\mathbb{L}/\mathbb{K}}(\frac{z_i z_j}{s^2})) \\
&= \frac{1}{s^{2n}} det(Tr_{\mathbb{L}/\mathbb{K}}(z_i z_j)) \\
&= \frac{1}{s^{2n}} \mathcal{D}(z_1, \ldots, z_n) \in \mathcal{O}'_{\mathbb{K}}\mathcal{D}(\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{K}}) \subset \mathcal{O}'_{\mathbb{K}}\mathcal{P} = \mathcal{P}'.
\end{aligned}$$

Assim, $\overline{0} = \overline{\mathcal{D}(e_1, \ldots, e_n)} = \mathcal{D}(\overline{e}_1, \ldots, \overline{e}_n) \in \mathcal{O}'_{\mathbb{K}}/\mathcal{P}' \simeq \mathcal{O}_{\mathbb{K}}/\mathcal{P}$, e deste modo $\mathcal{D}(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathcal{P}}/\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}) = \{0\}$. Portanto, pelo Corolário 2.3.1, segue que $\mathcal{P}$ ramifica em $\mathcal{O}_{\mathbb{L}}$. ∎

Exemplo 2.3.1 *Sejam $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\zeta_p)$, com p primo ímpar. Os ideais primos não-nulos de $\mathcal{O}_\mathbb{K} = \mathbb{Z}$ são exatamente os ideais da forma $\langle q \rangle$, com q primo. Pelo Teorema 1.6.1, segue que $|\mathcal{D}_\mathbb{L}| = p^{p-2}$. Dessa forma, pelo Teorema 2.3.2, tem-se que um ideal primo $\langle q \rangle$ de $\mathbb{Z}$ ramifica em $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ se, e somente se, $\langle \pm p^{p-2} \rangle \subset \langle q \rangle$. Assim, se $q = p$, então $\langle \pm p^{p-2} \rangle \subset \langle p \rangle = \langle q \rangle$, e deste modo $\langle q \rangle$ ramifica. Reciprocamente, se o ideal $\langle q \rangle$ ramifica, então $\langle \pm p^{p-2} \rangle \subset \langle q \rangle$, o que implica que $q = p$, pois caso contrário $p^{p-2} \in \langle \pm p^{p-2} \rangle$, com $p^{p-2} \notin \langle q \rangle$, o que acarreta $\langle \pm p^{p-2} \rangle \nsubseteq \langle q \rangle$, que é uma contradição. Portanto, o único ideal primo de $\mathbb{Z}$ que ramifica em $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ é $\langle p \rangle$.*

Corolário 2.3.2 *Existe somente um número finito de ideais primos de $\mathcal{O}_\mathbb{K}$ que ramificam em $\mathcal{O}_\mathbb{L}$.*

Demonstração: Considere a fatoração do ideal

$$\mathcal{D}(\mathcal{O}_\mathbb{L}/\mathcal{O}_\mathbb{K}) = \mathcal{D}_\mathbb{L}\mathcal{O}_\mathbb{K} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$$

de $\mathcal{O}_\mathbb{K}$, em ideais primos não-nulos de $\mathcal{O}_\mathbb{K}$. Pelo Teorema 2.3.2, tem-se que um ideal primo $\mathcal{P}$ de $\mathcal{O}_\mathbb{K}$ ramifica em $\mathcal{O}_\mathbb{L}$ se, e somente se, $\mathcal{D}(\mathcal{O}_\mathbb{L}/\mathcal{O}_\mathbb{K}) \subset \mathcal{P}$. Afirmamos que os ideais $\mathcal{P}_1, \ldots, \mathcal{P}_q$ são os únicos primos que contém $\mathcal{D}(\mathcal{O}_\mathbb{L}/\mathcal{O}_\mathbb{K})$. De fato, seja $\mathcal{M}$ um ideal primo de $\mathcal{O}_\mathbb{K}$ que contém $\mathcal{D}(\mathcal{O}_\mathbb{L}/\mathcal{O}_\mathbb{K}) = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$. Desse modo, tem-se que $\mathcal{M} \supset \mathcal{P}_i$ para algum $i = 1, \ldots, q$, e como $\mathcal{O}_\mathbb{K}$ é Dedekind (veja Corolário 1.7.1), segue que $\mathcal{P}_i$ é maximal, e assim $\mathcal{M} = \mathcal{P}_i$. Portanto, os ideais primos $\mathcal{P}_1, \ldots, \mathcal{P}_q$ de $\mathcal{O}_\mathbb{K}$ são os únicos que ramificam em $\mathcal{O}_\mathbb{L}$. ∎

Considere o caso em que $\mathbb{K} = \mathbb{Q}$.

Definição 2.3.2 *Dizemos que um número primo p ramifica em $\mathcal{O}_\mathbb{L}$ quando o ideal primo $\langle p \rangle$ ramifica em $\mathcal{O}_\mathbb{L}$.*

Teorema 2.3.3 *Os números primos que ramificam em $\mathcal{O}_\mathbb{L}$ são exatamente os primos na fatoração do discriminante $\mathcal{D}_\mathbb{L}$.*

Demonstração: Considere a fatoração do ideal

$$\mathcal{D}(\mathcal{O}_\mathbb{L}/\mathbb{Z}) = \mathcal{D}_\mathbb{L}\mathbb{Z} = \prod_{i=1}^{q} \mathcal{P}_i^{e_i}$$

em ideais primos não-nulos de $\mathbb{Z}$ (veja Teorema 1.8.1). Pelo Corolário 2.3.2, segue que os ideais primos $\mathcal{P}_1, \ldots, \mathcal{P}_q$ de $\mathbb{Z}$ são os únicos que ramificam em $\mathcal{O}_\mathbb{L}$. Por outro lado, considere a fatoração em primos do discriminante $\mathcal{D}_\mathbb{L} = p_1^{e'_1} \ldots p_r^{e'_r}$. Desse modo,

$$\mathcal{D}_\mathbb{L}\mathbb{Z} = (p_1^{e'_1} \ldots p_r^{e'_r})\mathbb{Z} = (p_1^{e'_1}\mathbb{Z}) \ldots (p_r^{e'_r}\mathbb{Z}) = (p_1\mathbb{Z})^{e'_1} \ldots (p_r\mathbb{Z})^{e'_r} = \prod_{i=1}^{r} (p_i\mathbb{Z})^{e'_i}.$$

Assim, pela unicidade de representação, segue que $r = q$ e $\mathcal{P}_i = p_i\mathbb{Z}$, para todo $i = 1, \ldots, r$. Portanto, os ideais primos $p_1\mathbb{Z}, \ldots, p_r\mathbb{Z}$ de $\mathbb{Z}$ são os únicos que ramificam em $\mathcal{O}_\mathbb{L}$, isto é, os números primos $p_1, \ldots, p_r$ são os únicos que ramificam em $\mathcal{O}_\mathbb{L}$. ■

Exemplo 2.3.2 *Seja $\mathbb{L}$ um corpo de números abeliano de grau n primo, cujo condutor é $m = p_1^{e_1} \ldots p_r^{e_r}$. Pelo Teorema 1.6.2, segue que $|\mathcal{D}_\mathbb{L}| = m^{n-1}$. Desse modo, $p_1, \ldots, p_r$ são os únicos primos que ramificam em $\mathcal{O}_\mathbb{L}$.*

Capítulo 3

Reticulados

Neste capítulo, são apresentadas três abordagens sobre reticulados: a Teoria dos Reticulados Clássica, Reticulados Algébricos e Reticulados Ideais. Na primeira, introduzimos o conceito de reticulado no $\mathbb{R}^n$, algumas propriedades e parâmetros que utilizamos no decorrer do texto. Nas duas outras abordagens descrevemos maneiras de se obter reticulados no $\mathbb{R}^n$ via Teoria Algébrica dos Números, fornecendo propriedades e fórmulas explícitas para alguns parâmetros desses reticulados.

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

Apresentamos o conceito de reticulado no $\mathbb{R}^n$, algumas propriedades e parâmetros de importante aplicação, como matriz Gram, volume, diversidade e distância produto mínima.

Definição 3.1.1 *Seja $\{v_1, \ldots, v_m\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. Definimos o reticulado Λ de dimensão m e base $\{v_i\}_{i=1}^m$ como sendo o conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} a_i v_i;\ a_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n.$$

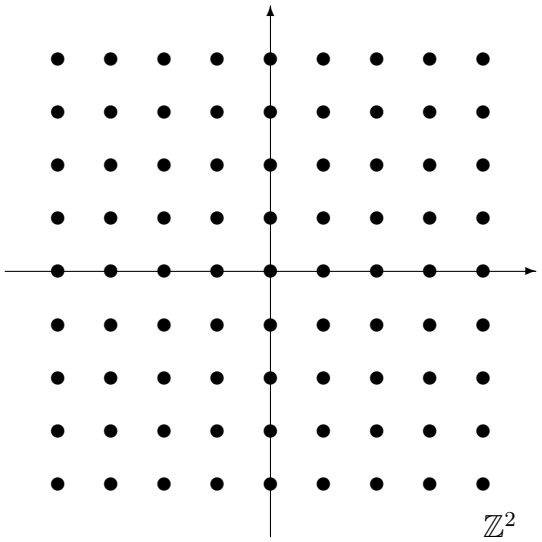
Observação 3.1.1 *De outro modo, o reticulado Λ pode ser expresso como*

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

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

Exemplo 3.1.1 *O espaço $\mathbb{Z}^n$ é um reticulado n-dimensional, gerado pela base canônica*

$$\{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1)\} \subset \mathbb{R}^n.$$



Observação 3.1.2 *Um reticulado Λ é um conjunto discreto do $\mathbb{R}^n$, pois para qualquer subconjunto compacto $\mathbb{K} \subset \mathbb{R}^n$, temos que $\mathbb{K} \cap \Lambda$ é finito.*

Consideramos a partir de agora somente os reticulados no $\mathbb{R}^n$ cuja base apresenta n vetores, ou seja, os reticulados n-dimensionais no $\mathbb{R}^n$.

Proposição 3.1.1 *Sejam $\{v_1, \ldots, v_n\} \subset \mathbb{R}^n$ uma base de um reticulado Λ e $\{w_1, \ldots, w_n\}$ um conjunto de vetores de Λ linearmente independentes sobre $\mathbb{R}$, tal que $w_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Tem-se que $\{w_i\}_{i=1}^n$ é uma base de Λ se, e somente se, $det(a_{ij}) = \pm 1$.*

Demonstração: Como

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

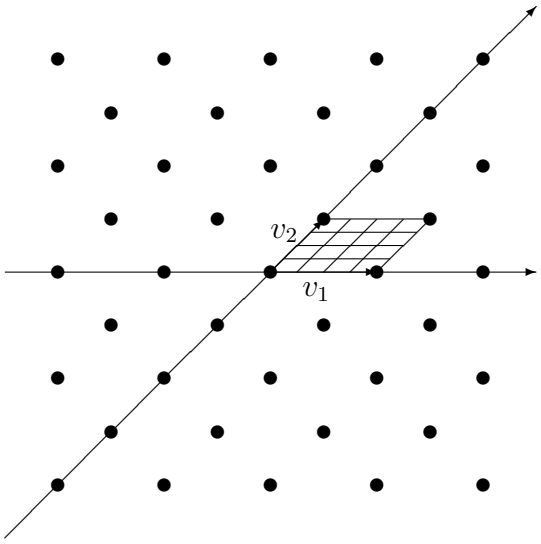
segue que, $\{w_i\}_{i=1}^n$ é uma base de Λ quando (a_{ij}) é a matriz mudança de base, ou seja, quando $det(a_{ij}) = \pm 1$. ∎

Definição 3.1.2 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\beta = \{v_1, \ldots, v_n\}$ uma base de Λ. O conjunto*

$$\mathcal{P}_\beta = \left\{ \sum_{i=1}^{n} \lambda_i v_i;\ \ 0 \leq \lambda_i < 1 \right\},$$

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

Exemplo 3.1.2 *Tem-se que $\Lambda = \{(a, b) \in \mathbb{Z}^2;\ a + b \equiv 0 (mod\ 2)\}$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$, cuja região fundamental está representada na figura abaixo:*



Definição 3.1.3 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\{v_1, \ldots, v_n\}$ uma base de Λ. Dizemos que a matriz*

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

é uma matriz geradora do reticulado Λ, onde $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \ldots, n$.

Observação 3.1.3 *Se M é uma matriz geradora de um reticulado $\Lambda \subset \mathbb{R}^n$, podemos representar o reticulado na forma*

$$\Lambda = \{\lambda M;\ \lambda \in \mathbb{Z}^n\}.$$

Definição 3.1.4 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \ldots, v_n\}$ uma base de Λ, $\mathcal{P}_\beta$ sua região fundamental e $M = (v_{ij})$ a matriz geradora de Λ com respeito à β. Definimos o volume da região fundamental $\mathcal{P}_\beta$ como sendo*

$$\mathcal{V}ol(\mathcal{P}_\beta) = |det(M)|.$$

Se $\{v_1, \ldots, v_n\}, \{w_1, \ldots, w_n\} \subset \mathbb{R}^n$ são duas bases de um reticulado Λ, segue da Proposição 3.1.1 que $|det(v_{ij})| = |det(w_{ij})|$, isto é, o módulo do determinante da matriz geradora de um reticulado independe da base escolhida. Isto nos permite a seguinte definição:

Definição 3.1.5 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\beta = \{v_1, \ldots, v_n\}$ uma base de Λ. Definimos o volume do reticulado Λ por*

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

Definição 3.1.6 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e M uma matriz geradora de Λ. Definimos a matriz Gram de Λ associada à matriz geradora M, como sendo a matriz $G = MM^t$.*

Na seguinte proposição, vemos que o determinante da matriz Gram de um reticulado independe da base escolhida.

Proposição 3.1.2 *Sejam $\{v_1, \ldots, v_n\}, \{w_1, \ldots, w_n\} \subset \mathbb{R}^n$ duas bases de um reticulado Λ. Se $G = MM^t$ e $G' = M'M'^t$, onde $M = (v_{ij})$ e $M' = (w_{ij})$, então $det(G) = det(G')$.*

Demostração: A verificação decorre do fato de que $|det(M)| = |det(M')|$, pois,

$$\begin{aligned} det(G) &= det(M)det(M^t) \\ &= det(M)^2 \\ &= det(M')^2 \\ &= det(M')det(M'^t) \\ &= det(G'), \end{aligned}$$

o que demonstra a proposição. ■

Definição 3.1.7 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e G uma matriz Gram de Λ. Definimos o determinante de Λ por $det(\Lambda) = det(G)$.*

Observação 3.1.4 *Dado um reticulado $\Lambda \subset \mathbb{R}^n$, tem-se que $det(\Lambda) = \mathcal{V}ol(\Lambda)^2$.*

Exemplo 3.1.3 *A matriz identidade Id_n é geradora do reticulado $\mathbb{Z}^n$, isto é,*

$$\mathbb{Z}^n = \{\lambda Id_n;\ \lambda \in \mathbb{Z}^n\}.$$

Assim, a matriz Gram associada é $G = Id_n$ e $\mathcal{V}ol(\mathbb{Z}^n) = det(\mathbb{Z}^n) = 1$. Porém, a matriz M' dada por

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

também é geradora de $\mathbb{Z}^n$, cuja matriz Gram associada é

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

Desse modo, $\mathcal{V}ol(\mathbb{Z}^n) = |det(M')| = 1 = det(G') = det(\mathbb{Z}^n)$. Este fato ilustra a independência do volume e do determinante de um reticulado quanto à base escolhida.

Definição 3.1.8 *Sejam $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ dois vetores no $\mathbb{R}^n$. Definimos a diversidade, ou distância de Hamming, entre x e y por*

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

Definição 3.1.9 *Definimos a diversidade, ou distância mínima de Hamming, de um subconjunto $S \subseteq \mathbb{R}^n$, por*

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

Como um reticulado $\Lambda \subset \mathbb{R}^n$ possui estrutura de grupo aditivo e contém o vetor nulo do $\mathbb{R}^n$, podemos definir a diversidade de um elemento $x \in \Lambda$ como sendo a diversidade entre x e o vetor nulo, como segue:

Definição 3.1.10 *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $x = (x_1, \ldots, x_n) \in \Lambda$.*

(i) A diversidade de x é definida como

$$div(x) = \#\{i;\ x_i \neq 0,\ i = 1, \ldots, n\}.$$

(ii) A diversidade de Λ é definida como

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

Definição 3.1.11 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $x = (x_1, \ldots, x_n) \in \Lambda - \{0\}$.*

(i) A distância produto de x é definida por $d_p(x) = \prod_{x_i \neq 0} |x_i|$.

(ii) A distância produto mínima de Λ é definida por

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

Observação 3.1.5 *Se um reticulado $\Lambda \subset \mathbb{R}^n$ tem diversidade máxima n, então a distância produto de qualquer elemento não-nulo $x = (x_1, \ldots, x_n) \in \Lambda$ poderá ser expressa como*

$$d_p(x) = \prod_{i=1}^{n} |x_i|.$$

Exemplo 3.1.4 *Considere o reticulado $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3$, onde $v_1 = (-1, 1, 0)$, $v_2 = (-1, -1, 1)$ e $v_3 = (0, 0, -1)$. Temos que $div(\Lambda) = 1$, pois v_3 apresenta a diversidade mínima, isto é, $div(v_3) = 1$. Dado o elemento $x = (-1, -1, 2) \in \Lambda$, temos que $d_p(x) = 2$.*

3.2 Reticulados algébricos

Nesta seção, identificamos um $\mathbb{Z}$-módulo livre de posto finito contido num corpo de números $\mathbb{K}$ com um reticulado no $\mathbb{R}^n$, o qual chamamos de reticulado algébrico. Essa identificação permite apresentar algumas características do reticulado obtido através das propriedades do corpo $\mathbb{K}$, de modo que, fornecemos a matriz geradora, matriz Gram e exibimos fórmulas explícitas para o volume do reticulado. Apresentamos duas formas de identificação, via homomorfismo canônico e via perturbação do homomorfismo canônico.

3.2.1 Homomorfismo canônico

Seja $\mathbb{K}$ um corpo de números de grau n. Tem-se que existem exatamente n $\mathbb{Q}$-monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$, com $i = 1, \ldots, n$ (veja o Corolário 1.1.1). Se σ_j é um monomorfismo imaginário, o seu conjugado $\overline{\sigma}_j$ também pertence ao conjunto dos n monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$. Desse modo, caso exista, temos um número par de monomorfismos imaginários. Assim, denotando por r_1 o número de monomorfismos reais e por $2r_2$ o número de monomorfismos imaginários, teremos $n = r_1 + 2r_2$, e podemos reordenar os monomorfismos σ_i's de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam reais e $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ sejam imaginários, com $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$. Isto nos permite a seguinte definição:

Definição 3.2.1 *O homomorfismo injetivo de anéis $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por*

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

é chamado de homomorfismo canônico, ou homomorfismo de Minkowski, onde $\Re$ e $\Im$ representam, respectivamente, as partes real e imaginária de um número complexo.

Exemplo 3.2.1 *Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_3)$, onde $\zeta_3 = e^{\frac{2\pi i}{3}}$. Tem-se que os $\mathbb{Q}$-monomorfismos σ_1 e σ_2 de $\mathbb{K}$ em $\mathbb{C}$, são dados por $\sigma_i(\zeta_3) = \zeta_3^i$, com $i = 1, 2$. Desse modo, $\mathbb{K}$ é totalmente imaginário, com $r_1 = 0$ e $r_2 = 1$. Se $x = a + b\zeta_3 \in \mathbb{K}$, então $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ é dado por*

$$\sigma_{\mathbb{K}}(x) = (\Re(\sigma_1(x)), \Im(\sigma_1(x))) = (\Re(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i), \Im(a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i)) = (a - \frac{b}{2}, \frac{b\sqrt{3}}{2}).$$

Teorema 3.2.1 *Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, cujo volume é dado por*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} |\det(\sigma_i(x_j))_{i,j=1}^n|.$$

Demonstração: Para cada $x_j \in M$, com $j = 1, \ldots, n$, o vetor $\sigma_{\mathbb{K}}(x_j)$ é dado por

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

Considere a matriz quadrada A de ordem n, cuja j-ésima coluna é dada pelo vetor $\sigma_{\mathbb{K}}(x_j)$. Utilizando a relação $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, com $j = 1, \ldots, r_2$, e adicionando e subtraindo as linhas da matriz A convenientemente, de modo a utilizar as igualdades

$$\Re(z) = \tfrac{1}{2}(z + \overline{z}) \;\; e \;\; \Im(z) = \tfrac{1}{2}(z - \overline{z}),$$

para $z \in \mathbb{C}$, obtem-se que

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

$$= \begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n) \\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n) \\ \frac{1}{2}[\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)}] & \ldots & \frac{1}{2}[\sigma_{r_1+1}(x_j) + \overline{\sigma_{r_1+1}(x_j)}] & \ldots & \frac{1}{2}[\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)}] \\ \frac{1}{2i}[\sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)}] & \ldots & \frac{1}{2i}[\sigma_{r_1+1}(x_j) - \overline{\sigma_{r_1+1}(x_j)}] & \ldots & \frac{1}{2i}[\sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)}] \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \frac{1}{2}[\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)}] & \ldots & \frac{1}{2}[\sigma_{r_1+r_2}(x_j) + \overline{\sigma_{r_1+r_2}(x_j)}] & \ldots & \frac{1}{2}[\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)}] \\ \frac{1}{2i}[\sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)}] & \ldots & \frac{1}{2i}[\sigma_{r_1+r_2}(x_j) - \overline{\sigma_{r_1+r_2}(x_j)}] & \ldots & \frac{1}{2i}[\sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)}] \end{vmatrix}$$

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

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

$$= (2i)^{-r_2} \det(\sigma_i(x_j))_{i,j=1}^n.$$

Pela Proposição 1.3.1, temos que $det(\sigma_i(x_j)) \neq 0$, e assim $det(A) \neq 0$. Desse modo, os vetores $\sigma_{\mathbb{K}}(x_j) \in \mathbb{R}^n$ são linearmente independentes sobre $\mathbb{R}$, e como

$$\begin{aligned} \sigma_{\mathbb{K}}(M) &= \mathbb{Z}\sigma_{\mathbb{K}}(x_1) + \ldots + \mathbb{Z}\sigma_{\mathbb{K}}(x_n) \\ &= \left\{ \sum_{j=1}^{n} a_j \sigma_{\mathbb{K}}(x_j);\ a_j \in \mathbb{Z} \right\}, \end{aligned}$$

segue que $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, do qual A^t é uma matriz geradora. Portanto,

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(M)) = |det(A)| = 2^{-r_2}|det(\sigma_i(x_j))_{i,j=1}^n|,$$

o que conclui a demonstração. ∎

Corolário 3.2.1 *Se $\mathcal{I}$ é um ideal não-nulo do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{I})$ são reticulados no $\mathbb{R}^n$, cujos volumes são dados respectivamente por*

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

Demonstração: Temos que $\mathcal{I}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$-módulos livres de posto n (veja Teorema 1.4.1). Assim, pelo Teorema 3.2.1, segue que $\sigma_{\mathbb{K}}(\mathcal{I})$ e $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ são reticulados no $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}_{\mathbb{K}}$, tem-se que

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

pois o discriminante $\mathcal{D}_{\mathbb{K}} = det(\sigma_i(x_j))^2$. Pelo Teorema 1.3.1, tem-se que existem uma $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros não-nulos $a_1, \ldots, a_n$, tal que $\{a_1w_1, \ldots, a_nw_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$. Assim,

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-r_2}|det(\sigma_i(a_jw_j))| = 2^{-r_2}|a_1 \ldots a_n|\,|det(\sigma_i(w_j))|.$$

Porém, pela Proposição 1.5.3, tem-se que $\mathcal{N}(\mathcal{I}) = |a_1 \ldots a_n|$, portanto

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

o que conclui a demonstração. ∎

Exemplo 3.2.2 *Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, onde $i^2 = -1$. Tem-se que seu anel de inteiros é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ (anel dos inteiros de Gauss), com $\mathbb{Z}$-base $\{1, i\}$. Dado $x = a + bi \in \mathbb{K}$, o homomorfismo canônico $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ é definido por*

$$\sigma_{\mathbb{K}}(x) = (\Re(\sigma_1(x)), \Im(\sigma_1(x))) = (a, b),$$

onde $\sigma_1(x) = a + bi$ e $\sigma_2(x) = a - bi$ são os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Seja $\mathcal{I} = \langle 2 - i\rangle$ um ideal principal de $\mathbb{Z}[i]$. Assim, dado $x \in \mathcal{I}$, temos que $x = (2 - i)(a + bi) = (2a + b) + (2b - a)i$, onde $a, b \in \mathbb{Z}$. Logo, a imagem $\sigma_{\mathbb{K}}(\mathcal{I}) \subseteq \mathbb{R}^2$ é dada por

$$\sigma_{\mathbb{K}}(\mathcal{I}) = \{(2a + b, 2b - a) \in \mathbb{R}^2;\ a, b \in \mathbb{Z}\}.$$

Desse modo, $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado no $\mathbb{R}^2$, do qual $\{(2, -1), (1, 2)\}$ é uma base. O volume de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dado por

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-1}\left|det\begin{pmatrix}\sigma_1(1) & \sigma_1(i)\\ \sigma_2(1) & \sigma_2(i)\end{pmatrix}\right| = \frac{1}{2}\left|det\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}\right| = \frac{1}{2}.2 = 1.$$

Além disso, pela Proposição 1.5.1, tem-se que $\mathcal{N}(\mathcal{I}) = |\mathcal{N}(2 - i)| = 5$, e portanto

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{I})) = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))\mathcal{N}(\mathcal{I}) = 5.$$

3.2.2 Perturbação do homomorfismo canônico

Nesta subseção, é apresentada a perturbação σ_α do homomorfismo canônico. Veremos que, além de propriedades semelhantes às obtidas pela identificação $\sigma_{\mathbb{K}}$, os reticulados obtidos pela perturbação σ_α apresentam matriz Gram igual a matriz da forma traço associada. Considere $\mathbb{K}$ um corpo de números de grau n.

Definição 3.2.2 *Sejam $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Um elemento $\alpha \in \mathbb{K}$ tal que $\sigma_i(\alpha) \in \mathbb{R}$, com $\sigma_i(\alpha) > 0$, para todo $i = 1, \ldots, n$, é chamado totalmente positivo.*

Definição 3.2.3 *Seja $\alpha \in \mathbb{K}$ um elemento totalmente positivo. O homomorfismo injetivo $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ dado por*

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))),$$

onde $\alpha_i = \sigma_i(\alpha)$, para $i = 1, \ldots, r_1 + r_2$, é chamado de perturbação do homomorfismo canônico, em que $\Re$ e $\Im$ representam, respectivamente, a parte real e imaginária de um número complexo.

Teorema 3.2.2 *Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, cujo volume é dado por*

$$\mathcal{V}ol(\sigma_\alpha(M)) = (\mathcal{N}(\alpha))^{\frac{1}{2}} |\det(\sigma_i(x_j))_{i,j=1}^n|.$$

Demonstração: Para cada $x_j \in M$, com $j = 1, \ldots, n$, o vetor $\sigma_\alpha(x_j)$ é dado por

$$\sigma_\alpha(x_j) = (\sqrt{\alpha_1}\sigma_1(x_j), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_j), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x_j)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x_j))).$$

Considere a matriz quadrada A de ordem n, cuja j-ésima coluna é dada pelo vetor $\sigma_\alpha(x_j)$. Utilizando a relação $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, com $j = 1, \ldots, r_2$, e adicionando e subtraindo as linhas da matriz A convenientemente, de modo a utilizar as igualdades

$$\Re(z) = \tfrac{1}{2}(z + \overline{z}) \;\; e \;\; \Im(z) = \tfrac{1}{2}(z - \overline{z}),$$

para $z \in \mathbb{C}$, obtem-se que

$$det(A) = \begin{vmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \dots & \sqrt{\alpha_1}\sigma_1(x_j) & \dots & \sqrt{\alpha_1}\sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_j) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) \\ \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x_1)) & \dots & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x_j)) & \dots & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x_n)) \\ \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x_1)) & \dots & \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x_j)) & \dots & \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x_1)) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x_j)) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x_n)) \\ \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x_1)) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x_j)) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix}$$

$$= \begin{vmatrix} \sqrt{\alpha_1}\sigma_1(x_1) & \dots & \sqrt{\alpha_1}\sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_1) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(x_n) \\ \frac{1}{2}\sqrt{2\alpha_{r_1+1}}[\sigma_{r_1+1}(x_1) + \overline{\sigma_{r_1+1}(x_1)}] & \dots & \frac{1}{2}\sqrt{\alpha_{r_1+1}}[\sigma_{r_1+1}(x_n) + \overline{\sigma_{r_1+1}(x_n)}] \\ \frac{1}{2i}\sqrt{2\alpha_{r_1+1}}[\sigma_{r_1+1}(x_1) - \overline{\sigma_{r_1+1}(x_1)}] & \dots & \frac{1}{2i}\sqrt{2\alpha_{r_1+1}}[\sigma_{r_1+1}(x_n) - \overline{\sigma_{r_1+1}(x_n)}] \\ \vdots & \ddots & \vdots \\ \frac{1}{2}\sqrt{2\alpha_{r_1+r_2}}[\sigma_{r_1+r_2}(x_1) + \overline{\sigma_{r_1+r_2}(x_1)}] & \dots & \frac{1}{2}\sqrt{2\alpha_{r_1+r_2}}[\sigma_{r_1+r_2}(x_n) + \overline{\sigma_{r_1+r_2}(x_n)}] \\ \frac{1}{2i}\sqrt{2\alpha_{r_1+r_2}}[\sigma_{r_1+r_2}(x_1) - \overline{\sigma_{r_1+r_2}(x_1)}] & \dots & \frac{1}{2i}\sqrt{2\alpha_{r_1+r_2}}[\sigma_{r_1+r_2}(x_n) - \overline{\sigma_{r_1+r_2}(x_n)}] \end{vmatrix}$$

$$= \left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\cdots\alpha_{r_1}}2\alpha_{r_1+1}\cdots 2\alpha_{r_1+r_2}D,$$

onde,

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

Utilizando propriedades elementares de determinantes, a saber, a adição da (r_1+2l)-ésima linha à sua anterior e pela subtração da (r_1+2l-1)-ésima linha à sua posterior, com $l=1,\ldots,r_2$, tem-se que

$$det(A)=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\ldots\alpha_{r_1}}2\alpha_{r_1+1}\ldots 2\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n)\\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n)\\ \sigma_{r_1+1}(x_1) & \ldots & \sigma_{r_1+1}(x_j) & \ldots & \sigma_{r_1+1}(x_n)\\ \overline{\sigma_{r_1+1}(x_1)} & \ldots & \overline{\sigma_{r_1+1}(x_j)} & \ldots & \overline{\sigma_{r_1+1}(x_n)}\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1+r_2}(x_1) & \ldots & \sigma_{r_1+r_2}(x_j) & \ldots & \sigma_{r_1+r_2}(x_n)\\ \overline{\sigma_{r_1+r_2}(x_1)} & \ldots & \overline{\sigma_{r_1+r_2}(x_j)} & \ldots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

$$=\left(\frac{1}{2i}\right)^{r_2}\sqrt{\alpha_1\ldots\alpha_{r_1}}2\alpha_{r_1+1}\ldots 2\alpha_{r_1+r_2}\begin{vmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_j) & \ldots & \sigma_1(x_n)\\ \sigma_2(x_1) & \ldots & \sigma_2(x_j) & \ldots & \sigma_2(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1}(x_1) & \ldots & \sigma_{r_1}(x_j) & \ldots & \sigma_{r_1}(x_n)\\ \sigma_{r_1+1}(x_1) & \ldots & \sigma_{r_1+1}(x_j) & \ldots & \sigma_{r_1+1}(x_n)\\ \sigma_{r_1+2}(x_1) & \ldots & \sigma_{r_1+2}(x_j) & \ldots & \sigma_{r_1+2}(x_n)\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ \sigma_{r_1+2r_2}(x_1) & \ldots & \sigma_{r_1+2r_2}(x_j) & \ldots & \sigma_{r_1+2r_2}(x_n) \end{vmatrix}$$

$$=(2i)^{-r_2}\sqrt{\alpha_1\ldots\alpha_{r_1}}2\alpha_{r_1+1}\ldots 2\alpha_{r_1+r_2}\det(\sigma_i(x_j))_{i,j=1}^{n}.$$

Pela Proposição 1.3.1, tem-se que $det(\sigma_i(x_j))\neq 0$, e assim $det(A)\neq 0$. Desse modo, os vetores $\sigma_\alpha(x_j)\in\mathbb{R}^n$ são linearmente independentes sobre $\mathbb{R}$, e como

$$\begin{aligned}\sigma_\alpha(M) &= \mathbb{Z}\sigma_\alpha(x_1)+\ldots+\mathbb{Z}\sigma_\alpha(x_n)\\ &= \left\{\sum_{j=1}^{n}a_j\sigma_\alpha(x_j);\ a_j\in\mathbb{Z}\right\},\end{aligned}$$

segue que $\sigma_\alpha(M)$ é um reticulado no $\mathbb{R}^n$, do qual A^t é uma matriz geradora. Dessa forma,

$$\mathcal{V}ol(\sigma_\alpha(M))=|det(A)|=2^{-r_2}\sqrt{\alpha_1\ldots\alpha_{r_1}}2\alpha_{r_1+1}\ldots 2\alpha_{r_1+r_2}|\det(\sigma_i(x_j))_{i,j=1}^{n}|.$$

Agora, temos dois casos a considerar:

(i) Se $r_2 = 0$, então

$$\begin{aligned}\mathcal{V}ol(\sigma_\alpha(M)) &= \sqrt{\alpha_1 \dots \alpha_{r_1}}\, |\det(\sigma_i(x_j))_{i,j=1}^n| \\ &= \left(\prod_{i=1}^n \sigma_i(\alpha)\right)^{\frac{1}{2}} |\det(\sigma_i(x_j))_{i,j=1}^n| \\ &= (\mathcal{N}(\alpha))^{\frac{1}{2}}\, |\det(\sigma_i(x_j))_{i,j=1}^n|.\end{aligned}$$

(ii) Se $r_1 = 0$, então

$$\mathcal{V}ol(\sigma_\alpha(M)) = 2^{-r_2} \prod_{i=1}^{r_2} 2^{r_2} \sigma_i(\alpha) |\det(\sigma_i(x_j))_{i,j=1}^n|.$$

Como $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \dots, r_2$, segue que $\sigma_{r_2+j}(\alpha) = \overline{\sigma_j(\alpha)} = \sigma_j(\alpha)$, pois $\sigma_j(\alpha) \in \mathbb{R}$. Assim,

$$\prod_{i=1}^{r_2} \sigma_i(\alpha) = (\mathcal{N}(\alpha))^{\frac{1}{2}},$$

e portanto,

$$\mathcal{V}ol(\sigma_\alpha(M)) = (\mathcal{N}(\alpha))^{\frac{1}{2}}\, |\det(\sigma_i(x_j))_{i,j=1}^n|,$$

o que prova o teorema. ∎

Corolário 3.2.2 *Se $\mathcal{I}$ é um ideal não-nulo do anel de inteiros $\mathcal{O}_\mathbb{K}$, então $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ e $\sigma_\alpha(\mathcal{I})$ são reticulados no $\mathbb{R}^n$, cujos volumes são dados por:*

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = (|\mathcal{D}_\mathbb{K}|\mathcal{N}(\alpha))^{\frac{1}{2}} \quad e \quad \mathcal{V}ol(\sigma_\alpha(\mathcal{I})) = (|\mathcal{D}_\mathbb{K}|\mathcal{N}(\alpha))^{\frac{1}{2}}\mathcal{N}(\mathcal{I}).$$

Demonstração: Temos que $\mathcal{I}$ e $\mathcal{O}_\mathbb{K}$ são $\mathbb{Z}$-módulos livres de posto n. Assim, pelo Teorema 3.2.2, segue que $\sigma_\alpha(\mathcal{I})$ e $\sigma_\alpha(\mathcal{O}_\mathbb{K})$ são reticulados no $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \dots, x_n\}$ de $\mathcal{O}_\mathbb{K}$, tem-se que

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = (|\mathcal{D}_\mathbb{K}|\mathcal{N}(\alpha))^{\frac{1}{2}},$$

pois o discriminante $\mathcal{D}_\mathbb{K} = \det(\sigma_i(x_j))^2$. Pelo Teorema 1.3.1, tem-se que existem uma $\mathbb{Z}$-base $\{w_1, \dots, w_n\}$ de $\mathcal{O}_\mathbb{K}$ e inteiros não-nulos $a_1, \dots, a_n$, tal que $\{a_1 w_1, \dots, a_n w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$. Assim,

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{I})) = (\mathcal{N}(\alpha))^{\frac{1}{2}}\, |\det(\sigma_i(a_j w_j))| = (\mathcal{N}(\alpha))^{\frac{1}{2}}\, |a_1 \dots a_n|\, |\det(\sigma_i(w_j))|.$$

Porém, pela Proposição 1.5.3, temos que $\mathcal{N}(\mathcal{I}) = |a_1 \dots a_n|$, e portanto

$$\mathcal{V}ol(\sigma_\alpha(\mathcal{I})) = (\mathcal{N}(\alpha))^{\frac{1}{2}} |\mathcal{D}_\mathbb{K}|^{\frac{1}{2}} \mathcal{N}(\mathcal{I}) = (|\mathcal{D}_\mathbb{K}| \mathcal{N}(\alpha))^{\frac{1}{2}} \mathcal{N}(\mathcal{I}),$$

o que conclui a demonstração. ∎

Proposição 3.2.1 *Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{w_1, \dots, w_n\}$ é uma $\mathbb{Z}$-base de M, então a matriz Gram do reticulado $\sigma_\alpha(M)$, com respeito a essa base, é dada por*

$$G = (Tr_{\mathbb{K}/\mathbb{Q}}(\alpha w_i \overline{w_j}))_{i,j=1}^n.$$

Demonstração: Como vimos no Teorema 3.2.2, tem-se que

$$A = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_1)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_1)) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_2)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_2)) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_n)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_n)) \end{pmatrix}$$

é uma matriz geradora do reticulado $\sigma_\alpha(M)$. Desse modo, denotando por $G = (g_{ij})_{i,j=1}^n$ a matriz Gram de $\sigma_\alpha(M)$ com respeito a A, temos que cada termo de $G = AA^t$ é dado por

$$\begin{aligned}
g_{ij} &= \sum_{k=1}^{r_1} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) + \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_i))\sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_j)) \\
&\quad + \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}}\Im(\sigma_{r_1+k}(w_i))\sqrt{2\alpha_{r_1+k}}\Im(\sigma_{r_1+k}(w_j)) \\
&= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}[\Re(\sigma_{r_1+k}(w_i))\Re(\sigma_{r_1+k}(w_j)) + \Im(\sigma_{r_1+k}(w_i))\Im(\sigma_{r_1+k}(w_j))] \\
&= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(w_i)\overline{\sigma_{r_1+k}(w_j)}) \\
&= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k}2\Re(\sigma_{r_1+k}(w_i\overline{w_j})) \\
&= \sum_{k=1}^{r_1} \alpha_k\sigma_k(w_iw_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\sigma_{r_1+k}(w_i\overline{w_j}) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\overline{\sigma_{r_1+k}(w_i\overline{w_j})} \\
&= \sum_{k=1}^{r_1} \sigma_k(\alpha w_i\overline{w_j}) + \sum_{k=1}^{r_2} \sigma_{r_1+k}(\alpha w_i\overline{w_j}) + \sum_{k=1}^{r_2} \overline{\sigma_{r_1+k}(\alpha w_i\overline{w_j})} \\
&= \sum_{k=1}^{r_1+2r_2} \sigma_k(\alpha w_i\overline{w_j}) \\
&= Tr_{\mathbb{K}/\mathbb{Q}}(\alpha w_i\overline{w_j}),
\end{aligned}$$

o que conclui a demonstração. ∎

Definição 3.2.4 *Seja $M \subseteq \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. Os reticulados $\sigma_{\mathbb{K}}(M)$ e $\sigma_{\alpha}(M)$ são chamados de reticulados algébricos.*

Observação 3.2.1 *Note que, quando $\mathbb{K}$ é totalmente real e $\alpha = 1$, tem-se que $\sigma_{\alpha}(M) = \sigma_{\mathbb{K}}(M)$.*

Determinados ideais fracionários do anel de inteiros de um corpo de números apresentam uma estrutura de $\mathbb{Z}$-módulo livre de posto finito, com imagem da forma traço contida em $\mathbb{Z}$ (veja, por exemplo, a referência [20]). Além disso, a Proposição 3.2.1 fornece a matriz Gram de um reticulado algébrico através da forma traço associada, o que motiva a definição de uma classe de reticulados algébricos sobre ideais fracionários, cuja imagem da forma traço está contida em $\mathbb{Z}$, chamados reticulados ideais.

3.3 Reticulados ideais

Introduzimos o conceito de reticulado ideal e apresentamos propriedades sobre alguns parâmetros, como diversidade e distância produto mínima. Considere $\mathbb{K}$ um corpo de números de grau n.

Proposição 3.3.1 *Se $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$.*

Demonstração: Pelo Teorema 1.1.4, tem-se que existe $\beta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\beta)$ e $\{1, \beta, \ldots, \beta^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Seja $\{\gamma_1, \ldots, \gamma_n\}$ uma $\mathbb{Z}$-base de $\mathcal{I}$. Para cada $i = 1, \ldots, n$, temos que $\gamma_i = \sum_{j=0}^{n-1} a_{ij}\beta^j$, com $a_{ij} \in \mathbb{Q}$. Assim, $a_{ij} = b_{ij}/c_{ij}$, com $b_{ij}, c_{ij} \in \mathbb{Z}$ e $c_{ij} \neq 0$. Se $d = mmc\{c_{ij};\ i = 1, \ldots, n,\ j = 0, 1, \ldots, n-1\}$, então $d\gamma_i \in \mathbb{Z}[\beta]$, para todo $i = 1, \cdots, n$. Portanto, $d\mathcal{I} = d\sum_{i=1}^{n} \mathbb{Z}\gamma_i = \sum_{i=1}^{n} \mathbb{Z}d\gamma_i \subset \mathbb{Z}[\beta] \subset \mathcal{O}_{\mathbb{K}}$. ∎

Definição 3.3.1 *Sejam $\alpha \in \mathbb{K}$ um elemento totalmente positivo e $\mathcal{I}$ um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$. Considere a forma traço:*

$$\begin{array}{rccl} Tr_{\alpha} & : & \mathbb{K} \times \mathbb{K} & \longrightarrow & \mathbb{Q} \\ & & (x, y) & \longmapsto & Tr_{\alpha}(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha x \overline{y}). \end{array}$$

Dada uma $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$ de $\mathcal{I}$, a matriz $(Tr_{\alpha}(w_i, w_j))_{i,j=1}^{n}$ é chamada matriz da forma traço associada à $\mathcal{I}$ com respeito à base $\{w_1, \ldots, w_n\}$, e denotada por (Tr_{α}).

Teorema 3.3.1 *Se $\alpha \in \mathbb{K}$ é um elemento totalmente positivo e $\mathcal{I}$ é um ideal fracionário do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, então*

$$det(Tr_{\alpha}) = \mathcal{N}(\mathcal{I})^2 \mathcal{N}(\alpha) |\mathcal{D}_{\mathbb{K}}|.$$

Demonstração: Pela Proposição 3.3.1, temos que existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$. Denotemos $\mathcal{J} = d\mathcal{I}$. Como $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n e $\mathcal{J}$ é um $\mathbb{Z}$-submódulo de $\mathcal{O}_{\mathbb{K}}$, segue, pelo Teorema 1.3.1, que existe uma $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros $a_1, \ldots, a_n$ tal que $\{a_1 w_1, \ldots, a_n w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{J}$. Porém, $\mathcal{I} = d^{-1}\mathcal{J}$, e assim $\{a_1 d^{-1} w_1, \ldots, a_n d^{-1} w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$. Assim, a matriz da forma traço é dada por

$$(Tr_\alpha) = \begin{pmatrix} Tr(\alpha a_1 d^{-1} w_1 \overline{a_1 d^{-1} w_1}) & \cdots & Tr(\alpha a_1 d^{-1} w_1 \overline{a_n d^{-1} w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha a_n d^{-1} w_n \overline{a_1 d^{-1} w_1}) & \cdots & Tr(\alpha a_n d^{-1} w_n \overline{a_n d^{-1} w_n}) \end{pmatrix}$$

$$= \begin{pmatrix} a_1^2 Tr(\alpha (d^{-1})^2 w_1 \overline{w_1}) & \cdots & a_1 a_n Tr(\alpha (d^{-1})^2 w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ a_1 a_n Tr(\alpha (d^{-1})^2 w_n \overline{w_1}) & \cdots & a_n^2 Tr(\alpha (d^{-1})^2 w_n \overline{w_n}) \end{pmatrix}.$$

Dessa forma,

$$det(Tr_\alpha) = (a_1 \cdots a_n)^2 det \begin{pmatrix} Tr(\alpha (d^{-1})^2 w_1 \overline{w_1}) & \cdots & Tr(\alpha (d^{-1})^2 w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha (d^{-1})^2 w_n \overline{w_1}) & \cdots & Tr(\alpha (d^{-1})^2 w_n \overline{w_n}) \end{pmatrix}$$

$$= (a_1 \cdots a_n)^2 ((d^{-1})^2)^n det \begin{pmatrix} Tr(\alpha w_1 \overline{w_1}) & \cdots & Tr(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha w_n \overline{w_1}) & \cdots & Tr(\alpha w_n \overline{w_n}) \end{pmatrix}.$$

Pela Proposição 1.5.3, tem-se que $\mathcal{N}(\mathcal{J}) = |a_1 \ldots a_n|$. Assim,

$$det(Tr_\alpha) = \mathcal{N}(\mathcal{J})^2 ((d^{-1})^2)^n det(G), \tag{3.3.1}$$

onde

$$G = \begin{pmatrix} Tr(\alpha w_1 \overline{w_1}) & \cdots & Tr(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ Tr(\alpha w_n \overline{w_1}) & \cdots & Tr(\alpha w_n \overline{w_n}) \end{pmatrix}.$$

Porém, podemos escrever $G = MM^{\perp}$, onde

$$M = ST = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix} \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix},$$

$M^{\perp}$ é a transposta conjugada de M e $\sigma_1, \ldots, \sigma_n$ são os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Assim,

$$\begin{aligned} det(G) &= det(M)det(M^{\perp}) \\ &= det(S)det(T)det(S^{\perp})det(T^{\perp}) \\ &= (det(S))^2(det(T))^2. \end{aligned}$$

Mas, temos que

$$(det(T))^2 = \sigma_1(\alpha)\ldots\sigma_n(\alpha) = \mathcal{N}(\alpha) \tag{3.3.2}$$

e, além disso,

$$det(S) = det(\sigma_i(w_j))_{i,j=1}^{n} = \sqrt{\mathcal{D}_{\mathbb{K}}}. \tag{3.3.3}$$

Logo, substituindo as Equações (3.3.2) e (3.3.3) na Equação (3.3.1), obtem-se

$$det(Tr_{\alpha}) = \mathcal{N}(\mathcal{J})^2((d^{-1})^2)^n\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|.$$

Porém, como $d \in \mathbb{Z}$, segue que $\mathcal{N}(\mathcal{I}) = \mathcal{N}(\mathcal{J})\mathcal{N}(d^{-1}) = \mathcal{N}(\mathcal{J})(d^{-1})^n$. Portanto,

$$det(Tr_{\alpha}) = \mathcal{N}(\mathcal{I})^2\mathcal{N}(\alpha)|\mathcal{D}_{\mathbb{K}}|,$$

o que conclui a demonstração. ∎

Definição 3.3.2 *Sejam $\alpha \in \mathbb{K}$ um elemento totalmente positivo e $\mathcal{I}$ um ideal fracionário do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, tal que $Tr_{\alpha}(x, y) \in \mathbb{Z}$, para todo $x, y \in \mathcal{I}$. Nesse caso, o reticulado $\sigma_{\alpha}(\mathcal{I})$ é chamado de reticulado ideal, e denotado por $(\mathcal{I}, Tr_{\alpha})$.*

Definição 3.3.3 *O conjunto*

$$\Delta_{\mathbb{K}/\mathbb{Q}}^{-1} = \{x \in \mathbb{K};\ Tr_{\mathbb{K}/\mathbb{Q}}(xy) \in \mathbb{Z},\ \forall\ y \in \mathcal{O}_{\mathbb{K}}\},$$

é chamado de codiferente de $\mathbb{K}$ sobre $\mathbb{Q}$.

Observação 3.3.1 *Note que, se $\alpha \in \mathbb{K}$ é um elemento totalmente positivo e $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então $\alpha\mathcal{I}\phi(\mathcal{I}) \subset \Delta_{\mathbb{K}/\mathbb{Q}}^{-1}$ (onde $\phi : \mathbb{K} \to \mathbb{K}$ é a conjugação complexa) é uma condição suficiente para que o reticulado ideal $(\mathcal{I}, Tr_{\alpha})$ esteja bem definido.*

Proposição 3.3.2 *Se $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então o reticulado ideal $\Lambda = (\mathcal{I}, Tr_{\alpha})$ tem diversidade $div(\Lambda) = r_1 + r_2$.*

Demonstração: Dado $y \in \Lambda$ não-nulo, tem-se que existe $x \in \mathcal{I} - \{0\}$ tal que

$$y = \sigma_{\alpha}(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))).$$

Como $x \neq 0$, segue que $\sigma_i(x) \neq 0$, para todo $i = 1, \ldots, n$. Logo, as primeiras r_1 coordenadas de y são não-nulas. Além disso, nas $2r_2$ coordenadas restantes, temos no mínimo r_2 não-nulas, pois as partes real e imaginária de $\sigma_i(x) \neq 0$ não se anulam simultaneamente, para cada $i = r_1+1, \ldots, n$. Assim, $div(\Lambda) = min\{div(y);\ y \in \Lambda,\ y \neq 0\} \geq r_1 + r_2$. Seja, agora, $\beta \in \mathcal{I} - \{0\}$. Pela Proposição 3.3.1, tem-se que existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathcal{I} \subset \mathcal{O}_{\mathbb{K}}$, e deste modo $d\beta \in \mathcal{O}_{\mathbb{K}}$. Assim, existem $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}$ tal que $(d\beta)^m + a_{m-1}(d\beta)^{m-1} + \ldots + a_1(d\beta) + a_0 = 0$, com $a_0 \neq 0$. Porém, como $\mathcal{I}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo e $d \in \mathcal{O}_{\mathbb{K}}$, segue que $d\beta \in \mathcal{I}$, e assim

$$-a_0 = (d\beta)^m + a_{m-1}(d\beta)^{m-1} + \ldots + a_1(d\beta) \in \mathcal{I}.$$

Como $-a_0 \in \mathbb{Z}$, segue que $\sigma_i(-a_0) = -a_0$, para todo $i = 1, \ldots, n$. Dessa forma, $\sigma_\alpha(-a_0)$ é um elemento de Λ, com $div(\sigma_\alpha(-a_0)) = r_1 + r_2$. Portanto, $div(\Lambda) = r_1 + r_2$. ■

Corolário 3.3.1 *Se $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ e $\Lambda = (\mathcal{I}, Tr_\alpha)$ é um reticulado ideal, então:*

(i) $div(\Lambda) = n$, se $\mathbb{K}$ é totalmente real.

(ii) $div(\Lambda) = \dfrac{n}{2}$, se $\mathbb{K}$ é totalmente imaginário.

Demonstração: Se $\mathbb{K}$ é totalmente real, tem-se que $r_2 = 0$, e assim $div(\Lambda) = r_1 = n$. Agora, se $\mathbb{K}$ é totalmente imaginário, então $div(\Lambda) = r_2 = \dfrac{n}{2}$. ■

Teorema 3.3.2 *Se $\mathbb{K}$ é totalmente real e $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, Tr_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \min(\mathcal{I})\sqrt{\frac{det(Tr_\alpha)}{|\mathcal{D}_{\mathbb{K}}|}},$$

onde $\min(\mathcal{I}) = \min\limits_{0 \neq x \in \mathcal{I}} \dfrac{|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{I})}$.

Demonstração: Dado $y \in \Lambda$, tem-se que existe $x \in \mathcal{I}$ tal que

$$y = \sigma_\alpha(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_n(\alpha)}\sigma_n(x)),$$

pois $\mathbb{K}$ é totalmente real. Pelo Corolário 3.3.1, temos que $div(\Lambda) = n$. Assim, ao denotar $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$, segue que

$$d_{p,min}(\Lambda) \ = \ \min\{d_p(y);\ y \in \Lambda,\ y \neq 0\} = \min_{0 \neq y \in \Lambda} \prod_{i=1}^{n} |y_i|$$

$$
\begin{aligned}
&= \min_{0\neq x\in\mathcal{I}} \prod_{i=1}^{n} \left|\sqrt{\sigma_i(\alpha)}\sigma_i(x)\right| = \prod_{i=1}^{n}\sqrt{\sigma_i(\alpha)}\min_{0\neq x\in\mathcal{I}}\prod_{i=1}^{n}|\sigma_i(x)| \\
&= \sqrt{\mathcal{N}(\alpha)}\min_{0\neq x\in\mathcal{I}}|\mathcal{N}(x)|\,.
\end{aligned}
$$

Pelo Teorema 3.3.1, tem-se que $det(Tr_\alpha) = \mathcal{N}(\mathcal{I})^2\mathcal{N}(\alpha)|\mathcal{D}_\mathbb{K}|$ e, assim, $\sqrt{\mathcal{N}(\alpha)} = \frac{\sqrt{det(Tr_\alpha)}}{\mathcal{N}(\mathcal{I})\sqrt{|\mathcal{D}_\mathbb{K}|}}$. Portanto,

$$
\begin{aligned}
d_{p,min}(\Lambda) &= \frac{\sqrt{det(Tr_\alpha)}}{\mathcal{N}(\mathcal{I})\sqrt{|\mathcal{D}_\mathbb{K}|}}\min_{0\neq x\in\mathcal{I}}|\mathcal{N}(x)| \\
&= \frac{\sqrt{det(Tr_\alpha)}}{\sqrt{|\mathcal{D}_\mathbb{K}|}}\frac{\min_{0\neq x\in\mathcal{I}}|\mathcal{N}(x)|}{\mathcal{N}(\mathcal{I})} \\
&= \min(\mathcal{I})\frac{\sqrt{det(Tr_\alpha)}}{\sqrt{|\mathcal{D}_\mathbb{K}|}},
\end{aligned}
$$

como queríamos demonstrar. ∎

Lema 3.3.1 *Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então*

$$\min_{0\neq x\in\mathcal{I}}|\mathcal{N}(x)| = \mathcal{N}(\mathcal{I}).$$

Demonstração: Como $\mathcal{I}\subset\mathcal{O}_\mathbb{K}$ é um ideal principal, segue que existe $a\in\mathcal{O}_\mathbb{K}$ tal que $\mathcal{I} = \langle a\rangle$. Desse modo, $\mathcal{N}(\mathcal{I}) = |\mathcal{N}(a)|$. Dado $x\in\mathcal{I}-\{0\}$, temos que $x = ay$, para algum $y\in\mathcal{O}_\mathbb{K}$. Assim,

$$|\mathcal{N}(x)| = |\mathcal{N}(a)||\mathcal{N}(y)| \geq \mathcal{N}(\mathcal{I}).$$

Além disso, $|\mathcal{N}(x)| = \mathcal{N}(\mathcal{I})$ para $x = a\in\mathcal{I}$. Portanto, $\min_{0\neq x\in\mathcal{I}}|\mathcal{N}(x)| = \mathcal{N}(\mathcal{I})$. ∎

Corolário 3.3.2 *Se $\mathbb{K}$ é totalmente real e $\mathcal{I}$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então a distância produto mínima de um reticulado ideal $\Lambda = (\mathcal{I}, Tr_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(Tr_\alpha)}{|\mathcal{D}_\mathbb{K}|}}.$$

Demonstração: Decorre diretamente do Teorema 3.3.2 e do Lema 3.3.1. ∎

Observação 3.3.2 *Seja $\Lambda = (\mathcal{I}, Tr_\alpha)$ um reticulado ideal, onde $\mathcal{I}$ é um ideal principal do anel de inteiros $\mathcal{O}_\mathbb{K}$, com $\mathbb{K}$ totalmente real. Se G é uma matriz Gram de Λ, então, pela Proposição 3.2.1, tem-se que $G = (Tr_\alpha)$. Desse modo,*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(G)}{|\mathcal{D}_\mathbb{K}|}}.$$

Capítulo 4

Reticulados de dimensão ímpar via Extensões Cíclicas

Neste capítulo, apresentamos construções de famílias de reticulados algébricos de dimensão ímpar via extensões cíclicas, ou mais precisamente, via subcorpos de extensões ciclotômicas do tipo $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^2})$, $\mathbb{Q}(\zeta_{pq})$ e $\mathbb{Q}(\zeta_{pq^2})$, com p e q primos ímpares. Na Seção 4.1, expomos uma descrição inicial de construção cíclica utilizando o anel de inteiros de subcorpos de $\mathbb{Q}(\zeta_p)$. Visando preparar condições para as construções seguintes, na Seção 4.2 é introduzida uma terminologia dos reticulados $\mathbb{Z}^n$-rotacionados e na Seção 4.3 é apresentado o conceito de anel de grupo, como um modo de intermediar as abordagens feitas em [18] e [20], referências suporte para a Seção 4.4, na qual é feita a obtenção de reticulados $\mathbb{Z}^n$-rotacionados.

4.1 Reticulados de dimensão ímpar sobre $\mathcal{O}_{\mathbb{K}}$

Considerando um corpo de números de grau ímpar $\mathbb{K}$ contido numa extensão ciclotômica $\mathbb{Q}(\zeta_p)$, em que p é um primo ímpar, fazemos a imersão do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ no $\mathbb{R}^n$, via o homomorfismo canônico, obtendo um reticulado algébrico, do qual fornecemos a matriz geradora, matriz Gram e parâmetros como volume, diversidade e distância produto mínima.

Proposição 4.1.1 *Dados um inteiro positivo n e um primo ímpar p tal que $p \equiv 1 (mod\ n)$, temos que existe um único subcorpo $\mathbb{K}$ de $\mathbb{Q}(\zeta_p)$ que satisfaz $[\mathbb{K} : \mathbb{Q}] = n$. Além disso, $\mathbb{Q} \subseteq \mathbb{K}$ é cíclica e p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Seja $\mathcal{G} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Temos que $\circ(\mathcal{G}) = p - 1$ e $\mathcal{G} \simeq \mathbb{Z}_p^*$ é cíclico (veja Teorema 1.1.2). Assim, sendo σ um gerador de $\mathcal{G}$, o grupo cíclico $\mathcal{H} := \langle \sigma^n \rangle \leqslant \mathcal{G}$ tem ordem $(p-1)/n$ e, como $\mathcal{H} \leqslant \mathcal{G} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ e $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ é galoisiana, segue pelo ítem (i) do Teorema 1.1.1, que $\mathcal{H} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$ para algum corpo intermediário $\mathbb{K}$ de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$. Além disso, pelo ítem (ii) do Teorema 1.1.1, tem-se que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ é galoisiana e $\mathcal{H} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$

é o único subgrupo de $\mathcal{G}$ tal que $[\mathbb{K}:\mathbb{Q}]=n$. Desse modo, $\mathbb{K}$ é o único corpo intermediário de $\mathbb{Q}\subset\mathbb{Q}(\zeta_p)$, de grau n sobre $\mathbb{Q}$.

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_p) & & \{Id\} \\
\Big| \frac{p-1}{n} & & \Big| \\
\mathbb{K} & \longleftrightarrow & \mathcal{H}=Gal(\mathbb{Q}(\zeta_p):\mathbb{K}) \\
\Big| n & & \Big| \\
\mathbb{Q} & & \mathcal{G}=Gal(\mathbb{Q}(\zeta_p):\mathbb{Q})
\end{array}$$

Afirmamos que $\mathbb{Q}\subseteq\mathbb{K}$ é cíclica. De fato, como $\mathcal{G}$ é abeliano (pois é cíclico), segue que todo subgrupo de $\mathcal{G}$ é normal e, em particular, $\mathcal{H}=Gal(\mathbb{Q}(\zeta_p):\mathbb{K})\lhd\mathcal{G}$. Assim, pelo ítem (iii) do Teorema 1.1.1, tem-se $\mathbb{Q}\subseteq\mathbb{K}$ é galoisiana e, além disso,

$$Gal(\mathbb{K}:\mathbb{Q})\simeq\frac{Gal(\mathbb{Q}(\zeta_p):\mathbb{Q})}{Gal(\mathbb{Q}(\zeta_p):\mathbb{K})}=\frac{\mathcal{G}}{\mathcal{H}}.$$

Dessa forma, como $\mathcal{G}$ é cíclico, segue que $Gal(\mathbb{K}:\mathbb{Q})$ também o é. Portanto, $\mathbb{Q}\subseteq\mathbb{K}$ é cíclica. Por fim, como $\mathbb{K}\subseteq\mathbb{Q}(\zeta_p)$, segue do Teorema 1.6.1 que $|\mathcal{D}_{\mathbb{K}}|=p^{n-1}$. Portanto, pelo Teorema 2.3.3, temos que p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$. ∎

Nas duas observações seguintes, considere as mesmas notações da Proposição 4.1.1.

Observação 4.1.1 *Como $\mathcal{G}$ é cíclico com gerador σ, segue que $\mathcal{G}/\mathcal{H}$ também é cíclico, cujo gerador é $\overline{\sigma}$. Assim, do isomorfismo natural $\mathcal{G}/\mathcal{H}\simeq Gal(\mathbb{K}:\mathbb{Q})$, segue que $\sigma|_{\mathbb{K}}$ é um gerador de $Gal(\mathbb{K}:\mathbb{Q})$, isto é,*

$$Gal(\mathbb{K}:\mathbb{Q})=\langle\sigma|_{\mathbb{K}}\rangle=\{Id_{\mathbb{K}},\sigma|_{\mathbb{K}},\ldots,\sigma^{n-1}|_{\mathbb{K}}\}.$$

Observação 4.1.2 *Note que, do fato de $\mathcal{G}=\langle\sigma\rangle=Gal(\mathbb{Q}(\zeta_p):\mathbb{Q})=\{\sigma_1,\ldots,\sigma_{p-1}\}$ com $\sigma_i:\zeta_p\mapsto\zeta_p^i$, segue que $\sigma=\sigma_r$ para algum $r\in\{1,\ldots,p-1\}$ e, além disso, como $\mathcal{G}\simeq\mathbb{Z}_p^*$ via o isomorfismo natural $\sigma_i\longmapsto\overline{i}$, segue que $\overline{r}$ é um gerador de $\mathbb{Z}_p^*$, isto é, r é um elemento primitivo módulo p.*

Exemplo 4.1.1 *Dados $n=5$ e $p=11$, pela Proposição 4.1.1, existe uma única extensão cíclica $\mathbb{K}$ de $\mathbb{Q}$ com $\mathbb{K}\subseteq\mathbb{Q}(\zeta_{11})$, tal que $[\mathbb{K}:\mathbb{Q}]=5$. Como $\overline{2}$ é um gerador de $\mathbb{Z}_{11}^*$, segue da Observação 4.1.2, que σ_2 é um gerador de $\mathcal{G}=Gal(\mathbb{Q}(\zeta_{11}):\mathbb{Q})$. Assim, tem-se que $\mathbb{K}$ é o corpo fixo do subgrupo $\langle\sigma_2^5\rangle$ de $\mathcal{G}=\langle\sigma_2\rangle$, isto é, $\langle\sigma_2^5\rangle=Gal(\mathbb{Q}(\zeta_{11}):\mathbb{K})$. Porém, como $\sigma_2^5=\sigma_{2^5}=\sigma_{32}$ e $32\equiv 10(mod\ 11)$, segue que $\sigma_2^5=\sigma_{10}$. Portanto, do fato de $[\mathbb{Q}(\zeta_{11}):\mathbb{K}]=2$, concluímos que $Gal(\mathbb{Q}(\zeta_{11}):\mathbb{K})=\{Id,\sigma_{10}\}$.*

Definição 4.1.1 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão galoisiana de grau n, com $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$ e $M \subset \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. Se existe $c \in M$ tal que $\{\sigma_1(c), \ldots, \sigma_n(c)\}$ é uma $\mathbb{Z}$-base de M, dizemos que tal base é uma base normal de M.*

Note que, temos bem definido o conceito de base normal do anel de inteiros de um corpo de números, bem como de qualquer um de seus ideais (veja Teorema 1.4.1).

Apresentamos agora, três resultados a fim de exibir uma base normal para $\mathcal{O}_{\mathbb{K}}$, no caso em que $\mathbb{K}$ é um corpo intermediário de $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$, com p primo. Para isso, fornecemos também uma base do corpo $\mathbb{K}$ sobre $\mathbb{Q}$.

Lema 4.1.1 *Se $\mathbb{K}$ é um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$, $[\mathbb{K} : \mathbb{Q}] = n$ e σ_r é um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, então o conjunto*

$$\{\zeta_p^{r^{n+1}}, \ldots, \zeta_p^{r^{mn+1}}, \zeta_p^{r^{n+2}}, \ldots, \zeta_p^{r^{mn+2}}, \ldots, \zeta_p^{r^{n+n}}, \ldots, \zeta_p^{r^{mn+n}}\}$$

é linearmente independente sobre $\mathbb{Q}$.

Demonstração: Denotemos $\mathcal{G} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Pela Observação 4.1.2, tem-se que $\mathcal{G} = \langle \sigma_r \rangle$ para algum $r \in \{1, \ldots, p-1\}$ e, do isomorfismo natural $\mathcal{G} \simeq \mathbb{Z}_p^*$, temos que $\mathbb{Z}_p^* = \langle \overline{r} \rangle = \{\overline{r}, \overline{r}^2, \ldots, \overline{r}^{p-1}\}$. Sejam $a_{ij} \in \mathbb{Q}$ tal que

$$\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} \zeta_p^{r^{in+j}} = 0. \tag{4.1.1}$$

Afirmamos que, para $1 \leq i_1, i_2 \leq m$ e $1 \leq j_1, j_2 \leq n$, se $\zeta_p^{r^{i_1 n + j_1}} = \zeta_p^{r^{i_2 n + j_2}}$ então $i_1 = i_2$ e $j_1 = j_2$. De fato, suponhamos que $\zeta_p^{r^{i_1 n + j_1}} = \zeta_p^{r^{i_2 n + j_2}}$ e não valha $i_1 = i_2$ e $j_1 = j_2$. Temos duas possibilidades a analisar; quando uma das duas últimas igualdades não é válida ou quando ambas não são. Suponhamos primeiramente, sem perda de generalidade, que $i_1 = i_2$ e $j_1 \neq j_2$. Como $\zeta_p^{r^{i_1 n + j_1}} = \zeta_p^{r^{i_2 n + j_2}}$, segue que $r^{i_1 n + j_1} \equiv r^{i_2 n + j_2} (mod\ p)$, o que implica que $p \mid r^{i_1 n}(r^{j_1} - r^{j_2})$, pois $i_1 = i_2$. Como p é primo, segue que $p \mid r^{i_1 n}$ ou $p \mid r^{j_1} - r^{j_2}$. Mas a primeira condição não é possível, pois acarretaria que $p \mid r$, o que é uma contradição pelo fato de $r \leq p - 1$. Suponhamos que $j_1 > j_2$. Logo existe $t \in \mathbb{Z}^+$ tal que $j_1 = j_2 + t$. Assim, $p \mid r^{j_2}(r^t - 1)$ e, dessa forma, $r^t \equiv 1 (mod\ p)$ implicando que $\overline{r}^t = \overline{1}$ com $t = j_1 - j_2 \leq n - 1 < n < p - 1$, o que é uma contradição, pois a ordem de $\overline{r}$ é $p - 1$. Consideremos, agora, o caso em que $i_1 \neq i_2$ e $j_1 \neq j_2$ e suponhamos que $i_1 > i_2$ e $j_1 > j_2$. Assim, existem $t_1, t_2 \in \mathbb{Z}^+$ tal que $i_1 = i_2 + t_1$ e $j_1 = j_2 + t_2$ e, então, $t_1 = i_1 - i_2 \leq m - 1$ e $t_2 = j_1 - j_2 \leq n - 1$. Logo, como $p \mid r^{i_1 n + j_1} - r^{i_2 n + j_2}$, segue que $p \mid r^{(i_2 + t_1)n + (j_2 + t_2)} - r^{i_2 n + j_2}$, isto é, $p \mid r^{i_2 n + j_2}(r^{t_1 n + t_2} - 1)$. Dessa forma, $r^{t_1 n + t_2} \equiv 1 (mod\ p)$, ou seja, $\overline{r}^{t_1 n + t_2} = \overline{1}$. Porém, como $t_1 \leq m - 1$ e $t_2 \leq n - 1$, segue que $t_1 n \leq (m-1)n$ e, assim,

$t_1n+t_2 \leq mn-1 = p-2 < p-1$, contradição. Dessa forma, os valores $\zeta_p^{r^{in+j}}$, com $1 \leq i \leq m$ e $1 \leq j \leq n$, são todos distintos, num total de $mn = p-1$ elementos. Podemos, então, reescrever a Equação (4.1.1) na forma

$$\sum_{k=1}^{p-1} b_k \zeta_p^k = 0,$$

com $b_k \in \mathbb{Q}$, para todo $k = 1, \ldots, p-1$ e, como $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ é uma $\mathbb{Q}$-base de $\mathbb{Q}(\zeta_p)$, segue que $b_k = 0$, para todo $k = 1, \ldots, p-1$. Portanto, $a_{ij} = 0$ para todo $i = 1, \ldots, m$ e $j = 1, \ldots, n$ e, dessa forma, o conjunto $\{\zeta_p^{r^{n+1}}, \ldots, \zeta_p^{r^{mn+1}}, \zeta_p^{r^{n+2}}, \ldots, \zeta_p^{r^{mn+2}}, \ldots, \zeta_p^{r^{n+n}}, \ldots, \zeta_p^{r^{mn+n}}\}$ é linearmente independente sobre $\mathbb{Q}$. ■

Teorema 4.1.1 *Se $\mathbb{K}$ é um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo, então $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$.*

Demonstração: Temos que $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) \in \mathbb{K}$, e assim $\mathbb{Q}(\theta) \subset \mathbb{K}$. Denotemos $[\mathbb{K} : \mathbb{Q}] = n$, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$ e seja $\sigma = \sigma_r$ um gerador de $\mathcal{G} = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Pela unicidade de $\mathbb{K}$, segue da Proposição 4.1.1, que

$$Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) = \langle \sigma^n \rangle = \{\sigma^n, \sigma^{2n}, \ldots, \sigma^{mn}\} = \{\sigma_{r^n}, \sigma_{r^{2n}}, \ldots, \sigma_{r^{mn}}\}.$$

Dessa forma,

$$\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p) = \sigma_{r^n}(\zeta_p) + \sigma_{r^{2n}}(\zeta_p) + \ldots + \sigma_{r^{mn}}(\zeta_p) = \zeta_p^{r^n} + \zeta_p^{r^{2n}} + \ldots + \zeta_p^{r^{mn}}.$$

Como $\mathcal{G}$ é abeliano, segue que $\mathbb{Q} \subset \mathbb{Q}(\theta)$ é galoisiana. Seja $f(x) = x^s + a_{s-1}x^{s-1} + \ldots + a_1x + a_0$ o polinômio minimal de θ sobre $\mathbb{Q}$. Assim

$$\theta^s + a_{s-1}\theta^{s-1} + \ldots + a_1\theta + a_0 = 0. \tag{4.1.2}$$

Aplicando σ_{r^i}, com $i = 1, 2, \ldots, n$, na Equação (4.1.2) obtemos

$$0 = \sigma_{r^i}(\theta^s + a_{s-1}\theta^{s-1} + \ldots + a_1\theta + a_0) = [\sigma_{r^i}(\theta)]^s + a_{s-1}[\sigma_{r^i}(\theta)]^{s-1} + \ldots + a_1\sigma_{r^i}(\theta) + a_0,$$

isto é, $\sigma_{r^i}(\theta)$ é uma raíz de $f(x)$, para todo $i = 1, 2, \ldots, n$. Mas, como $\mathbb{Q} \subset \mathbb{Q}(\theta)$ é galoisiana, segue que $\sigma_{r^i}(\theta) \in \mathbb{Q}(\theta)$, para todo $i = 1, 2, \ldots, n$. Sejam $b_1, b_2, \ldots, b_n \in \mathbb{Q}$ tal que

$$b_1\sigma_r(\theta) + b_2\sigma_{r^2}(\theta) + \cdots + b_n\sigma_{r^n}(\theta) = 0.$$

Logo,

$$0 = b_1(\zeta_p^{r^{n+1}} + \ldots + \zeta_p^{r^{mn+1}}) + b_2(\zeta_p^{r^{n+2}} + \ldots + \zeta_p^{r^{mn+2}}) + \ldots + b_n(\zeta_p^{r^{n+n}} + \ldots + \zeta_p^{r^{mn+n}})$$

$$= b_1\zeta_p^{r^{n+1}} + \ldots + b_1\zeta_p^{r^{mn+1}} + b_2\zeta_p^{r^{n+2}} + \ldots + b_2\zeta_p^{r^{mn+2}} + \ldots + b_n\zeta_p^{r^{n+n}} + \ldots + b_n\zeta_p^{r^{mn+n}}.$$

Desse modo, pelo Lema 4.1.1, temos que $b_i = 0$, para todo $i = 1, 2, \ldots, n$, ou seja, o conjunto $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\} \subset \mathbb{Q}(\theta)$ é linearmente independente sobre $\mathbb{Q}$. Dessa forma, $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq n$ com $\mathbb{Q}(\theta) \subseteq \mathbb{K}$. Portanto, $\mathbb{K} = \mathbb{Q}(\theta)$. ∎

Exemplo 4.1.2 *Denotando $n = 5$ e $p = 11$, considere o corpo intermediário $\mathbb{K}$ de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{11})$ com $[\mathbb{K} : \mathbb{Q}] = 5$, obtido no Exemplo 4.1.1. Pelo Teorema 4.1.1, temos que $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{K}}(\zeta_{11})$. Porém, como $Gal(\mathbb{Q}(\zeta_{11}) : \mathbb{K}) = \{Id, \sigma_{10}\}$, segue que*

$$\theta = Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{K}}(\zeta_{11}) = \zeta_{11} + \sigma_{10}(\zeta_{11}) = \zeta_{11} + \zeta_{11}^{10} = \zeta_{11} + \zeta_{11}^{-1}.$$

Portanto, $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ é o subcorpo maximal real de $\mathbb{Q}(\zeta_{11})$.

Corolário 4.1.1 *Se $\mathbb{K}$ é um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo, $[\mathbb{K} : \mathbb{Q}] = n$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e σ_r é um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, então*

$$\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$$

é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, isto é, uma base normal de $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Pelo Teorema 4.1.1, temos que $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$ é uma base de $\mathbb{K} = \mathbb{Q}(\theta)$ sobre $\mathbb{Q}$. Logo, este conjunto é também linearmente independente sobre $\mathbb{Z}$, restando apenas verificar que é um gerador do anel de inteiros $\mathcal{O}_{\mathbb{K}}$, visto como $\mathbb{Z}$-módulo. Para isso, dado $\sigma_{r^i}(\theta) \in \mathbb{K}$ com $i \in \{1, \ldots, n\}$ e denotando $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = m$, tem-se que $\sigma_{r^i}(\theta) = \sigma_{r^i}(\zeta_p^{r^n} + \ldots + \zeta_p^{r^{mn}}) = \zeta_p^{r^{n+i}} + \ldots + \zeta_p^{r^{mn+i}}$ e, como ζ_p é um inteiro sobre $\mathbb{Z}$, segue que $\sigma_{r^i}(\theta)$ também o é, como uma soma de produtos de ζ_p. Dessa forma, $\sigma_{r^i}(\theta) \in \mathcal{O}_{\mathbb{K}}$, para todo $i = 1, \ldots, n$, ou seja,

$$\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\} \subset \mathcal{O}_{\mathbb{K}}.$$

Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathbb{K}$, segue que existem $a_i \in \mathbb{Q}$, com $i = 1, \ldots, n$, tal que

$$\alpha = a_1\sigma_r(\theta) + a_2\sigma_{r^2}(\theta) + \cdots + a_n\sigma_{r^n}(\theta).$$

Assim,

$$\alpha = a_1\zeta_p^{r^{n+1}} + \ldots + a_1\zeta_p^{r^{mn+1}} + a_2\zeta_p^{r^{n+2}} + \ldots + a_2\zeta_p^{r^{mn+2}} + \ldots + a_n\zeta_p^{r^{n+n}} + \ldots + a_n\zeta_p^{r^{mn+n}}.$$

Utilizando o mesmo argumento que fizemos para a Equação (4.1.1) no Lema 4.1.1, podemos escrever

$$\alpha = b_1\zeta_p + b_2\zeta_p^2 + \ldots + b_{p-1}\zeta_p^{p-1}, \text{ com } b_j \in \mathbb{Q}, \text{ para } j = 1, \ldots, p-1.$$

Como $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$, segue que $\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ (veja o Teorema 2.6 de [7]). Logo, $\alpha \in \mathbb{Z}[\zeta_p]$. Assim, pela unicidade de representação de um elemento de $\mathbb{Q}(\zeta_p)$ na $\mathbb{Q}$-base $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$, sendo esta também uma $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_p]$, podemos concluir que $b_j \in \mathbb{Z}$, para todo $j = 1, \ldots, p-1$. Logo, $a_i \in \mathbb{Z}$, para todo $i = 1, \ldots, n$. Dessa forma, $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$ é um gerador de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e, portanto, é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. ∎

No Corolário 4.1.1 podemos dizer que $\{\sigma_r(\theta), \sigma_{r^2}(\theta), \ldots, \sigma_{r^n}(\theta)\}$ é base normal de $\mathcal{O}_{\mathbb{K}}$, pois $\theta \in \mathcal{O}_{\mathbb{K}}$ e, pela Observação 4.1.1, segue que $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_r|_{\mathbb{K}}, \ldots, \sigma_{r^n}|_{\mathbb{K}}\}$. Além disso, podemos caracterizar esta base de outro modo, como na seguinte observação:

Observação 4.1.3 *Com as mesmas notações do Corolário 4.1.1 e denotando $\sigma = \sigma_r$, tem-se que $\sigma^s = \sigma_{r^s}$, pois $\sigma^s(\zeta_p) = \sigma_{r^s}(\zeta_p)$, para todo $s = 1, \ldots, n$. Dessa forma, no Corolário 4.1.1, podemos dizer que*

$$\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$$

é uma base normal de $\mathcal{O}_{\mathbb{K}}$, sendo σ um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.

Exemplo 4.1.3 *Considere o subcorpo maximal real $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ de $\mathbb{Q}(\zeta_{11})$ obtido no Exemplo 4.1.2. Denotando por $\sigma = \sigma_2$ o gerador de $Gal(\mathbb{Q}(\zeta_{11}) : \mathbb{Q})$, segue do Corolário 4.1.1 (veja Observação 4.1.3), que*

$$\{\theta, \sigma(\theta), \sigma^2(\theta), \sigma^3(\theta), \sigma^4(\theta)\}$$

é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, onde $\theta = Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{K}}(\zeta_{11})$. Porém, pelo Exemplo 4.1.2, temos que $\theta = \zeta_{11} + \zeta_{11}^{-1}$. Desse modo,

$$\begin{aligned}
\sigma(\theta) &= \sigma_2(\zeta_{11} + \zeta_{11}^{-1}) = \zeta_{11}^2 + \zeta_{11}^9 \\
\sigma^2(\theta) &= \sigma_4(\zeta_{11} + \zeta_{11}^{-1}) = \zeta_{11}^4 + \zeta_{11}^7 \\
\sigma^3(\theta) &= \sigma_8(\zeta_{11} + \zeta_{11}^{-1}) = \zeta_{11}^8 + \zeta_{11}^3 \\
\sigma^4(\theta) &= \sigma_{16}(\zeta_{11} + \zeta_{11}^{-1}) = \zeta_{11}^5 + \zeta_{11}^6.
\end{aligned}$$

Portanto,

$$\{\zeta_{11} + \zeta_{11}^{-1},\ \zeta_{11}^2 + \zeta_{11}^9,\ \zeta_{11}^4 + \zeta_{11}^7,\ \zeta_{11}^8 + \zeta_{11}^3,\ \zeta_{11}^5 + \zeta_{11}^6\}$$

é uma base normal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Proposição 4.1.2 *Se $\mathbb{Q} \subseteq \mathbb{K}$ é uma extensão galoisiana de grau ímpar, então $\mathbb{K}$ é totalmente real.*

Demonstração: Seja $[\mathbb{K} : \mathbb{Q}] = n$ ímpar. Pelo Teorema 1.1.4, existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$. Sejam $p(x)$ o polinômio minimal de α sobre $\mathbb{Q}$ e $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Como $gr(p(x)) = n$ é ímpar, segue que $p(x)$ possui uma raiz real β. Mostremos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Como $\mathbb{Q} \subseteq \mathbb{K}$ é galoisiana, segue que existe $\sigma_i \in Gal(\mathbb{K} : \mathbb{Q})$ tal que $\sigma_i(\alpha) = \beta$. Assim, $\beta \in \mathbb{Q}(\alpha)$ e, desse modo, $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. Porém, como o polinômio minimal de β sobre $\mathbb{Q}$ é o próprio $p(x)$, segue que $[\mathbb{Q}(\beta) : \mathbb{Q}] = n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Dessa forma, $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Como

$$\mathbb{K} = \mathbb{Q}(\beta) = \{a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1};\ a_i \in \mathbb{Q}\} \subset \mathbb{R},$$

segue que $\sigma_i(\mathbb{K}) = \mathbb{K} \subset \mathbb{R}$, para todo $i = 1, \ldots, n$. Portanto, $\mathbb{K}$ é totalmente real. ■

Observação 4.1.4 *Se $\mathbb{K}$ é um corpo de números totalmente real de grau n e $\mathcal{I}$ é um ideal fracionário do anel de inteiros $\mathcal{O}_\mathbb{K}$, segue pelo Corolário 3.3.1 que um reticulado ideal $(\mathcal{I}, Tr_\alpha)$ tem diversidade máxima n. Portanto, reticulados ideais definidos sobre extensões galoisianas de grau ímpar apresentam diversidade máxima.*

4.1.1 Obtenção do reticulado $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$

Seja $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo ímpar e $[\mathbb{K} : \mathbb{Q}] = n$ ímpar. Pelo Teorema 3.2.1, temos que $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ é um reticulado no $\mathbb{R}^n$, com diversidade máxima (veja Observação 4.1.4), cujo volume é dado por

$$\mathcal{V}ol(\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})) = 2^{-r_2}|\mathcal{D}_\mathbb{K}|^{\frac{1}{2}} = \sqrt{p^{n-1}},$$

pois $r_2 = 0$ e $|\mathcal{D}_\mathbb{K}| = p^{n-1}$ (veja Teorema 1.6.1).

Considerando a $\mathbb{Z}$-base $\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$ de $\mathcal{O}_\mathbb{K}$ obtida no Corolário 4.1.1, temos que

$$\{\sigma_\mathbb{K}(\theta), \sigma_\mathbb{K}(\sigma(\theta)), \ldots, \sigma_\mathbb{K}(\sigma^{n-1}(\theta))\} \subset \mathbb{R}^n$$

é uma base do reticulado $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$, cuja matriz geradora associada é

$$M = \begin{pmatrix} \theta & \sigma(\theta) & \cdots & \sigma^{n-1}(\theta) \\ \sigma(\theta) & \sigma^2(\theta) & \cdots & \theta \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(\theta) & \theta & \cdots & \sigma^{n-2}(\theta) \end{pmatrix},$$

pois, $\sigma_\mathbb{K}$ é definido por

$$\begin{array}{rccl} \sigma_\mathbb{K} & : & \mathbb{K} & \longrightarrow \quad \mathbb{R}^n \\ & & x & \longmapsto \ \sigma_\mathbb{K}(x) = (x, \sigma(x), \ldots, \sigma^{n-1}(x)), \end{array}$$

pelo fato de que $Gal(\mathbb{K} : \mathbb{Q}) = \{Id_{\mathbb{K}}, \sigma|_{\mathbb{K}}, \ldots, \sigma^{n-1}|_{\mathbb{K}}\}$ (veja Observação 4.1.1), com $\mathbb{K}$ totalmente real. Note que $M = M^t$, da qual a i-ésima linha é dada por

$$\sigma_{\mathbb{K}}(\sigma^i(\theta)) = (\sigma^i(\theta), \sigma^{i+1}(\theta), \ldots, \sigma^{i+n-1}(\theta)),$$

para $i = 0, 1, \ldots, n-1$. Dessa forma, denotando por $G = (g_{ij})_{i,j=0}^{n-1}$ a matriz Gram de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ com respeito à M, tem-se que cada termo de $G = MM^t$ pode ser escrito como

$$\begin{aligned}
g_{ij} &= \langle \sigma_{\mathbb{K}}(\sigma^i(\theta)), \sigma_{\mathbb{K}}(\sigma^j(\theta)) \rangle \\
&= \sigma^i(\theta)\sigma^j(\theta) + \sigma^{i+1}(\theta)\sigma^{j+1}(\theta) + \ldots + \sigma^{i+n-1}(\theta)\sigma^{j+n-1}(\theta) \\
&= \sum_{a=0}^{n-1} \sigma^{i+a}(\theta)\sigma^{j+a}(\theta) \\
&\overset{(*)}{=} \sum_{a=0}^{n-1} \sigma^{a}(\theta)\sigma^{j+a-i}(\theta) \\
&= \sum_{a=0}^{n-1} \sigma^{a}(\theta\ \sigma^{j-i}(\theta)) \\
&= Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta)),\ i, j = 0, 1, \ldots, n-1.
\end{aligned}$$

A igualdade $(*)$ segue do fato de que $\sigma^n|_{\mathbb{K}} = Id_{\mathbb{K}}$ e $\sigma^{n-s}|_{\mathbb{K}} = \sigma^{-s}|_{\mathbb{K}}$, para todo $s \in \mathbb{Z}^+$. Dessa forma,

$$G = \left(Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta))\right)_{i,j=0}^{n-1}.$$

Observação 4.1.5 *De maneira análoga, também podemos escrever* $G = (Tr_{\mathbb{K}/\mathbb{Q}}(\sigma^i(\theta)\sigma^j(\theta)))_{i,j=0}^{n-1}$. *Ou seja, a matriz Gram coincide com a matriz da forma traço, com respeito à base* $\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$ *de* $\mathcal{O}_{\mathbb{K}}$.

Teorema 4.1.2 *Se* $\mathbb{K}$ *é um corpo intermediário de* $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, *com* p *primo ímpar,* $[\mathbb{K} : \mathbb{Q}] = n$ *ímpar,* σ *um gerador de* $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ *e* $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$, *então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \begin{cases} p - (\frac{p-1}{n}) , & \text{se } t = 0 \\ -(\frac{p-1}{n}) , & \text{se } t \neq 0 , \end{cases}$$

onde $t = 0, 1, \ldots, n-1$.

Demonstração: Seja $r \in \{1, \ldots, p-1\}$ tal que $\sigma = \sigma_r$ e denotemos, por simplicidade, $\zeta = \zeta_p$. Como $Gal(\mathbb{K} : \mathbb{Q}) = \{Id_{\mathbb{K}}, \sigma|_{\mathbb{K}}, \ldots, \sigma^{n-1}|_{\mathbb{K}}\}$ e $\theta \in \mathbb{K}$, segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \sum_{a=0}^{n-1} \sigma^a(\theta\ \sigma^t(\theta)),$$

para $t = 0, 1, \ldots, n-1$. Mas,

$$\theta\ \sigma^t(\theta) = \sum_{c=1}^{\frac{p-1}{n}} \sigma^{cn}(\zeta) \sum_{j=1}^{\frac{p-1}{n}} \sigma^{t+jn}(\zeta) = \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{cn}(\zeta)\sigma^{t+jn}(\zeta),$$

pois $Gal(\mathbb{Q}(\zeta_p) : \mathbb{K}) = \langle \sigma^n \rangle$, cuja ordem é $(p-1)/n$. Assim,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) &= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(\zeta)\sigma^{a+t+jn}(\zeta) \\ &= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \zeta^{r^{a+cn}} \zeta^{r^{a+t+jn}} = \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p-1}{n}} \zeta^{r^{a+cn}+r^{a+t+jn}}. \end{aligned}$$

Denotemos $l = (p-1)/n$. Como $\overline{r}$ é um gerador de $\mathbb{Z}_p^*$ (veja Observação 4.1.2), segue que $r^{p-1} \equiv 1(mod\ p)$, e assim $r^{(p-1)q} = (r^{p-1})^q \equiv 1^q = 1(mod\ p)$, para todo $q \in \mathbb{Z}$. Logo,

$$r^{a+(lq+c)n} = r^{a+(\frac{p-1}{n}q+c)n} = r^{a+(p-1)q+cn} = r^{a+cn} r^{(p-1)q} \equiv r^{a+cn}(mod\ p).$$

Desse modo, $\zeta^{r^{a+cn}} = \zeta^{r^{a+(lq+c)n}}$, para todo $q \in \mathbb{Z}$. Note, porém, que se $s \equiv c(mod\ l)$ então $s = lq + c$, para algum $q \in \mathbb{Z}$, o que implica que $\zeta^{r^{a+sn}} = \zeta^{r^{a+cn}}$. Assim, a menos da congruência módulo l, podemos pôr o parâmetro c variando em $\mathbb{Z}_l$. O mesmo argumento se aplica ao parâmetro j. Dessa forma, podemos escrever

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \sum_{a=0}^{n-1} \sum_{c,j \in \mathbb{Z}_l} \zeta^{r^{a+cn}+r^{a+t+jn}} = \sum_{c \in \mathbb{Z}_l} \sum_{a=0}^{n-1} \sum_{j \in \mathbb{Z}_l} \zeta^{r^{a+cn}+r^{a+t+jn}}.$$

Além disso, fazendo a mudança de variáveis $d \equiv c - j(mod\ l)$, isto é, $c \equiv d + j(mod\ l)$, teremos que $\zeta^{r^{a+cn}} = \zeta^{r^{a+(d+j)n}}$ e, como c varia em $\mathbb{Z}_l$, segue que d também varia em $\mathbb{Z}_l$. Logo,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) &= \sum_{d \in \mathbb{Z}_l} \sum_{a=0}^{n-1} \sum_{j \in \mathbb{Z}_l} \zeta^{r^{a+(d+j)n}+r^{a+t+jn}} \\ &= \sum_{d \in \mathbb{Z}_l} \sum_{a=0}^{n-1} \sum_{j \in \mathbb{Z}_l} \zeta^{(r^{dn}+r^t)r^{a+jn}} = \sum_{d=1}^{\frac{p-1}{n}} \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta^{(r^{dn}+r^t)r^{a+jn}}. \end{aligned}$$

Note que r^{a+jn}, para $a \in \{0, 1, \ldots, n-1\}$ e $j \in \{1, \ldots, \frac{p-1}{n}\}$, toma valores congruentes a $s = 1, \ldots, p-1$ módulo p, pois $\langle \overline{r} \rangle = \mathbb{Z}_p^* = \{\overline{1}, \ldots, \overline{p-1}\}$, e assim $\overline{r}^{a+jn} = \overline{s}$ para algum $s = 1, \ldots, p-1$, isto é, $r^{a+jn} \equiv s(mod\ p)$. Logo, $\zeta^{r^{a+jn}} = \zeta^s$, para algum $s = 1, \ldots, p-1$.

Dessa forma, como $n(\frac{p-1}{n}) = p-1$, segue que

$$\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}} \zeta^{(r^{dn}+r^t)r^{a+jn}} = \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}} (\zeta^{r^{a+jn}})^{r^{dn}+r^t} = \sum_{s=1}^{p-1}(\zeta^s)^{r^{dn}+r^t} = \sum_{s=1}^{p-1}(\zeta^{r^{dn}+r^t})^s.$$

Sendo assim, denotando $\omega_{d,t} = \zeta^{r^{dn}+r^t}$, teremos

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \sum_{d=1}^{\frac{p-1}{n}}\sum_{s=1}^{p-1}(\omega_{d,t})^s,$$

onde

$$\sum_{s=1}^{p-1}(\omega_{d,t})^s = \begin{cases} p-1\ , & \text{se } \omega_{d,t} = 1 \\ -1\ , & \text{se } \omega_{d,t} \neq 1\ ; \quad t = 0, 1, \ldots, n-1\ . \end{cases}$$

O primeiro caso desta igualdade é trivial. Para $\omega_{d,t} \neq 1$, basta notar que $\omega_{d,t} = \zeta^{r^{dn}+r^t}$ é uma raíz do polinômio

$$\frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1$$

e, desse modo,

$$\sum_{s=1}^{p-1}(\omega_{d,t})^s = (\omega_{d,t})^{p-1} + \ldots + (\omega_{d,t})^2 + \omega_{d,t} = -1.$$

Agora, para avaliar $Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta))$ devemos considerar dois casos, quando $t = 0$ e $t \neq 0$. Mas, para isso, mostremos antes que

$$\omega_{d,t} = 1 \iff t = 0 \text{ e } d = \frac{p-1}{2n}. \tag{4.1.3}$$

De fato, suponhamos que $t = 0$ e $d = (p-1)/2n$. Temos que $r^{p-1} \equiv 1(mod\ p)$. Como $p-1$ é par, segue que existe $m \in \mathbb{Z}$ tal que $p - 1 = 2m$. Logo, $(r^m)^2 = r^{2m} \equiv 1(mod\ p)$. Assim, $p \mid (r^m)^2 - 1 = (r^m + 1)(r^m - 1)$, o que implica que $r^m \equiv 1(mod\ p)$ ou $r^m \equiv -1(mod\ p)$. Porém, como a primeira congruência não é possível, pois $p-1$ é o menor inteiro positivo com tal propriedade, segue que $r^m \equiv -1(mod\ p)$. Dessa forma, $r^{\frac{p-1}{2}} + 1 \equiv 0(mod\ p)$ e, portanto,

$$\omega_{d,t} = \zeta^{r^{dn}+1} = \zeta^{r^{(\frac{p-1}{2n})n}+1} = \zeta^{r^{\frac{p-1}{2}}+1} = 1.$$

Reciprocamente, se $\omega_{d,t} = 1$, isto é, $\zeta^{r^{dn}+r^t} = 1$, então

$$\begin{aligned} r^{dn} + r^t \equiv 0(mod\ p) &\Leftrightarrow r^{dn} \equiv -r^t(mod\ p) \\ &\overset{(1)}{\Leftrightarrow} r^{dn} \equiv r^{m+t}(mod\ p) \\ &\overset{(2)}{\Leftrightarrow} m + t \equiv dn(mod\ p-1) \end{aligned}$$

$$\Leftrightarrow p-1 \mid m+t-dn$$
$$\Leftrightarrow \exists\ k_1 \in \mathbb{Z} \text{ tal que } t = dn - m + k_1(p-1).$$

A equivalência (1) é válida devido ao fato de $r^{m+t} \equiv -r^t (mod\ p)$ e a equivalência (2) segue do Teorema 6.2 de [3]. Por outro lado, temos que $n \mid dn$, $n \mid k_1(p-1)$ (pois $n \mid p-1$) e $n \mid m$ (pois $n(\frac{p-1}{2n}) = m$), e assim $n \mid t$. Porém, como $t = 0, 1, \ldots, n-1$, podemos concluir que $t = 0$. Desse modo, $dn = m - k_1(p-1)$. Logo,

$$d = \frac{p-1}{2n} - k_1(\frac{p-1}{n}) = \frac{p-1}{2n}(1-2k_1) = k_2(\frac{p-1}{2n}), \quad \text{com } k_2 = 1-2k_1 \text{ ímpar.}$$

Note que k_2 deve ser positivo, pois caso contrário teríamos $d \leq 0$. Porém, só se pode ter $k_2 = 1$ ou 2, pois se $k_2 \geq 3$ teríamos $d > (p-1)/n$. Mas, como k_2 é ímpar, resta somente $k_2 = 1$. Portanto $d = (p-1)/2n$, o que conclui a demonstração da Equivalência (4.1.3). Observe que o número inteiro $\frac{p-1}{2n}$ está bem definido devido ao fato de n ser ímpar e $(\frac{p-1}{n})n = p-1$ ser par, o que garante que $\frac{p-1}{n}$ é par. Voltando a avaliar $Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta))$, suponhamos que $t \neq 0$. Pela Equivalência (4.1.3) temos $\omega_{d,t} \neq 1$, o que implica $\sum_{s=1}^{p-1}(\omega_{d,t})^s = -1$. Logo,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \sum_{d=1}^{\frac{p-1}{n}}\sum_{s=1}^{p-1}(\omega_{d,t})^s = \sum_{d=1}^{\frac{p-1}{n}} -1 = -\left(\frac{p-1}{n}\right).$$

Suponha, agora, que $t = 0$. Pela Equivalência (4.1.3), se $d = (p-1)/2n$ então $\omega_{d,t} = 1$, e se $d \neq (p-1)/2n$ então $\omega_{d,t} \neq 1$. Portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^t(\theta)) = \sum_{d=1}^{\frac{p-1}{n}}\sum_{s=1}^{p-1}(\omega_{d,t})^s = (p-1) + \sum_{\substack{d=1 \\ d\neq\frac{p-1}{2n}}}^{\frac{p-1}{n}} -1 = (p-1) - \left(\frac{p-1}{n} - 1\right) = p - \left(\frac{p-1}{n}\right),$$

o que conclui a demonstração. ∎

Observação 4.1.6 *No Capítulo IV de [10], foi citado o resultado acima para n primo ímpar. Aqui, obtemos o resultado exigindo que a dimensão n, de $\mathbb{K}$ sobre $\mathbb{Q}$, seja apenas ímpar.*

Temos que σ^{j-i} percorre σ^t, com $t = 0, 1, \ldots, n-1$, quando $i, j = 0, 1, \ldots, n-1$. Dessa forma, pelo Teorema 4.1.2, tem-se

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta)) = \begin{cases} p - (\frac{p-1}{n})\ , & \text{se } i = j \\ -(\frac{p-1}{n})\ , & \text{se } i \neq j\ ; \quad i, j = 0, 1, \ldots, n-1\ . \end{cases}$$

Portanto, a matriz Gram do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ com respeito à matriz geradora M, é dada por

$$G = \begin{pmatrix} p-(\frac{p-1}{n}) & -(\frac{p-1}{n}) & \cdots & -(\frac{p-1}{n}) \\ -(\frac{p-1}{n}) & p-(\frac{p-1}{n}) & \cdots & -(\frac{p-1}{n}) \\ \vdots & \vdots & \ddots & \vdots \\ -(\frac{p-1}{n}) & -(\frac{p-1}{n}) & \cdots & p-(\frac{p-1}{n}) \end{pmatrix}.$$

Pelo Corolário 3.3.2, a distância produto mínima de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \sqrt{\frac{det(G)}{|\mathcal{D}_{\mathbb{K}}|}}.$$

Mas, como $\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, segue que

$$|\mathcal{D}_{\mathbb{K}}| = \mathcal{D}(\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)) = det(Tr_{\mathbb{K}/\mathbb{Q}}(\theta\ \sigma^{j-i}(\theta)))_{i,j=0}^{n-1} = det(G).$$

Portanto, tem-se que

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 1.$$

Ou seja, a distância produto mínima do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é sempre unitária, sendo este o reticulado algébrico canônico com relação a tal parâmetro.

Observação 4.1.7 *Como $\mathbb{K}$ é totalmente real, segue que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = \sigma_{\alpha}(\mathcal{O}_{\mathbb{K}})$, para $\alpha = 1$. Assim, podemos denotar $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ como sendo o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, Tr_1)$.*

4.1.2 Algoritmo de construção

Nesta subseção, apresentamos um algoritmo que descreve a família de reticulados algébricos obtidos na Subseção 4.1.1

Teorema 4.1.3 *([6],pág.523)(Teorema de Dirichlet) Se a, m são inteiros tal que $1 \leq a \leq m$ e $mdc(a, m) = 1$, então a progressão aritmética $\{a, a+m, a+2m, \ldots, a+km, \ldots\}$ contém infinitos primos.*

Dados uma dimensão ímpar n e p um primo ímpar satisfazendo $p \equiv 1(mod\ n)$, existe uma única extensão cíclica $\mathbb{K}$ de grau n sobre $\mathbb{Q}$, com $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ (veja Proposição 4.1.1) e, consequentemente, temos definido o reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$. Porém, pelo Teorema de Dirichlet, a progressão $\{1, 1+n, 1+2n, \ldots, 1+kn, \ldots\}$ possui infinitos primos, isto é, existem infinitos primos ímpares p tal que $p \equiv 1(mod\ n)$. Desse modo, para cada dimensão ímpar n, obtemos

uma família de reticulados $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, variando segundo o parâmetro p primo ímpar satisfazendo $p \equiv 1(mod\ n)$. Podemos assim, fornecer um algoritmo de construção do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$.

Algoritmo

1. *Escolha uma dimensão ímpar n.*

2. *Escolha um primo ímpar p, satisfazendo $p \equiv 1(mod\ n)$.*

3. *Encontre um elemento r primitivo módulo p ($\overline{r}$ gerador de $\mathbb{Z}_p^*$).*

4. *Calcule $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e seus conjugados $\sigma^i(\theta)$, para $i = 1, \ldots, n-1$, com $\langle\sigma\rangle = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.*

5. *Calcule a matriz geradora M, utilizando $\zeta_p = e^{\frac{2\pi i}{p}}$.*

Descrevemos, assim, uma família de reticulados n-dimensionais $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, com diversidade máxima n, da qual

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \sqrt{p^{n-1}} \quad \text{e} \quad d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 1.$$

A Tabela 4.1[1] apresenta algumas dimensões e parâmetros correspondentes aos reticulados que podem ser obtidos através desta construção.

n	p	r	div	vol	$d_{p,min}$
3	7	3	3	7	1
3	13	2	3	13	1
5	11	2	5	121	1
5	31	3	5	961	1
7	29	2	7	29^3	1
11	23	5	11	23^5	1
11	67	2	11	67^5	1
13	53	2	13	53^6	1
17	103	5	17	103^8	1
19	191	19	19	191^9	1
23	47	5	23	47^{11}	1
29	59	2	29	59^{14}	1

Tabela 4.1:

[1]Alguns cálculos foram feitos com auxílio do software Wolfram Mathematica.

Exemplo 4.1.4 *Considere o seguinte exemplo de construção do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ através do algoritmo descrito acima.*

1. *Escolhemos a dimensão $n = 5$.*

2. *Escolhemos $p = 11$ satisfazendo $p \equiv 1 (mod\ 5)$. Estes parâmetros definem $\mathbb{K} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ (veja os Exemplos 4.1.1 e 4.1.2) e, consequentemente, pelo Corolário 4.1.1 tem-se que o anel de inteiros $\mathcal{O}_{\mathbb{K}} = \theta\mathbb{Z} + \sigma(\theta)\mathbb{Z} + \ldots + \sigma^4(\theta)\mathbb{Z}$. Assim, temos definido o reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, cuja base é $\{\sigma_{\mathbb{K}}(\theta), \sigma_{\mathbb{K}}(\sigma(\theta)), \ldots, \sigma_{\mathbb{K}}(\sigma^4(\theta))\}$.*

3. *Consideremos $r = 2$, pois $\overline{2}$ é um gerador do grupo multiplicativo $\mathbb{Z}_{11}^* = \{\overline{1}, \overline{2}, \ldots, \overline{10}\}$.*

4. *Desse modo, $\sigma = \sigma_2$ é um gerador de $Gal(\mathbb{Q}(\zeta_{11}) : \mathbb{Q})$. Pelos Exemplos 4.1.2 e 4.1.3, segue que $\theta = Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{K}}(\zeta_{11}) = \zeta_{11} + \zeta_{11}^{-1}$ e seus conjugados $\sigma^i(\theta)$, para $i = 1, 2, 3, 4$, são dados por*

$$\begin{aligned}
\sigma(\theta) &= \zeta_{11}^2 + \zeta_{11}^9 \\
\sigma^2(\theta) &= \zeta_{11}^4 + \zeta_{11}^7 \\
\sigma^3(\theta) &= \zeta_{11}^8 + \zeta_{11}^3 \\
\sigma^4(\theta) &= \zeta_{11}^5 + \zeta_{11}^6.
\end{aligned}$$

5. *A matriz geradora M do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$M = \begin{pmatrix} \theta & \sigma(\theta) & \cdots & \sigma^4(\theta) \\ \sigma(\theta) & \sigma^2(\theta) & \cdots & \theta \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^4(\theta) & \theta & \cdots & \sigma^3(\theta) \end{pmatrix}.$$

Buscando valores numéricos[2] para as entradas de M, utilizamos $\zeta_{11} = e^{\frac{2\pi i}{11}}$, assim

$$\theta = \zeta_{11} + \zeta_{11}^{-1} = e^{\frac{2\pi i}{11}} + e^{\frac{20\pi i}{11}} = 2\ \cos(2\pi/11) = 1,682507066$$

$$\sigma(\theta) = \zeta_{11}^2 + \zeta_{11}^9 = e^{\frac{4\pi i}{11}} + e^{\frac{18\pi i}{11}} = 2\ sen(3\pi/22) = 0,830830026$$

$$\sigma^2(\theta) = \zeta_{11}^4 + \zeta_{11}^7 = e^{\frac{8\pi i}{11}} + e^{\frac{14\pi i}{11}} = -2\ sen(5\pi/22) = -1,309721468$$

$$\sigma^3(\theta) = \zeta_{11}^8 + \zeta_{11}^3 = e^{\frac{16\pi i}{11}} + e^{\frac{6\pi i}{11}} = -2\ sen(\pi/22) = -0,284629676$$

$$\sigma^4(\theta) = \zeta_{11}^5 + \zeta_{11}^6 = e^{\frac{10\pi i}{11}} + e^{\frac{12\pi i}{11}} = -2\ \cos(\pi/11) = -1,918985947.$$

[2]Parte da obtenção dos valores numéricos da matriz M foi feita com auxílio do software Wolfram Mathematica.

Portanto, temos que

$$M = \begin{pmatrix} 1,6825 & 0,8308 & -1,3097 & -0,2846 & -1,9189 \\ 0,8308 & -1,3097 & -0,2846 & -1,9189 & 1,6825 \\ -1,3097 & -0,2846 & -1,9189 & 1,6825 & 0,8308 \\ -0,2846 & -1,9189 & 1,6825 & 0,8308 & -1,3097 \\ -1,9189 & 1,6825 & 0,8308 & -1,3097 & -0,2846 \end{pmatrix}$$

é uma matriz geradora de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$*, para* $n = 5$ *e* $p = 11$*. Além disso,* $\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 121$*,* $div(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 5$ *e* $d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 1$*. Por fim, note que o Teorema 4.1.2 fornece uma matriz Gram do reticulado* $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$*, a qual nesse caso é dada pela seguinte matriz de ordem cinco:*

$$G = \begin{pmatrix} 9 & -2 & \cdots & -2 \\ -2 & 9 & \cdots & -2 \\ \vdots & \vdots & \ddots & \vdots \\ -2 & -2 & \cdots & 9 \end{pmatrix}.$$

Observação 4.1.8 *Utilizando ainda as mesmas notações da construção feita nesta seção, de um modo geral temos*

$$Tr_{\mathbb{K}/\mathbb{Q}}(\theta) = Tr_{\mathbb{K}/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1.$$

Logo,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\sigma^t(\theta)) = \sum_{a=0}^{n-1} \sigma^a(\sigma^t(\theta)) = \sum_{a=0}^{n-1} \sigma^t(\sigma^a(\theta)) = \sigma^t(\sum_{a=0}^{n-1} \sigma^a(\theta)) = \sigma^t(Tr_{\mathbb{K}/\mathbb{Q}}(\theta)) = \sigma^t(-1) = -1,$$

para todo $t = 0, 1, \ldots, n-1$*. O resultado fornecido pelo Teorema 4.1.2 juntamente com esta condição, faz com que a base normal de* $\mathcal{O}_{\mathbb{K}}$ *encontrada no Corolário 4.1.1 seja dita uma base de Lagrange e, além disso, ela é única a menos de reordenação no caso n primo ímpar (veja Definição IV.8.1 e Lema IV.8.2 de [10]).*

Observação 4.1.9 *O reticulado que construimos nesta seção não necessariamente é um reticulado* $\mathbb{Z}^n$*-rotacionado. Nas próximas construções, trabalhamos com subreticulados do reticulado aqui obtido, os quais fornecem reticulados* $\mathbb{Z}^n$*-rotacionados.*

4.2 Terminologia dos reticulados $\mathbb{Z}^n$-rotacionados

Nesta seção, introduzimos o conceito e a aplicabilidade dos reticulados $\mathbb{Z}^n$-rotacionados, onde apresentamos uma condição suficiente para obtê-los.

Um reticulado no $\mathbb{R}^n$ é chamado de $\mathbb{Z}^n$-reticulado, quando é isomorfo à $\mathbb{Z}^n$, visto como um $\mathbb{Z}$-módulo. Se $\mathbb{K}$ é um corpo de números e $\mathcal{I} \subset \mathbb{K}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, um reticulado ideal $(\mathcal{I}, Tr_\alpha)$ é dito um reticulado $\mathbb{Z}^n$-rotacionado quando for um $\mathbb{Z}^n$-reticulado. Do mesmo modo, quando $M \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto finito, o reticulado algébrico $\sigma_{\mathbb{K}}(M)$ é chamado de $\mathbb{Z}^n$-rotacionado, quando for um $\mathbb{Z}^n$-reticulado. O termo "rotacionado" sugere o fato de que, dependendo da escolha de α, ou da base que define um reticulado, o que fazemos é rotacioná-lo sobre o reticulado $\mathbb{Z}^n$, quando eles forem isomorfos.

Há na atualidade um interesse pela busca de $\mathbb{Z}^n$-reticulados devido à sua aplicabilidade. Eles são utilizados na transmissão de sinais sobre o canal Rayleigh Fading, que é um meio de transmissão para comunicações sem fio. Como detalhado em [15], para um reticulado n-dimensional Λ sobre o canal Rayleigh Fading, temos o seguinte limitante para a probabilidade de erros $\mathcal{P}_e(\Lambda)$ na transmissão:

$$\mathcal{P}_e(\Lambda) \leq \frac{1}{2} \sum_{l=L}^{n} \frac{K_l}{(\frac{\eta E_b}{8N_o})^l},$$

onde $K_l = \sum_{d_p} A_{d_p}/(d_p)^2 \Lambda_{d_p}$, L é a diversidade e $d_p = d_p(x)$, para $x \in \Lambda - \{0\}$. Os demais parâmetros são relacionados à aplicação computacional.

Dessa maneira, maximizando L e $d_{p,min}(\Lambda)$, diminuimos a probabilidade de erros na transmissão. Sendo de interesse, portanto, a busca por reticulados $\mathbb{Z}^n$-rotacionados que apresentem diversidade e distância produto mínima relativamente altas.

Nas próximas construções, trabalharemos com reticulados cuja diversidade é máxima. Mas para que isso seja proveitoso, tais reticulados devem ser $\mathbb{Z}^n$-rotacionados. Vejamos agora uma condição suficiente para que isto ocorra.

Seja $\Lambda = \{\lambda M;\ \lambda \in \mathbb{Z}^n\}$ um reticulado no $\mathbb{R}^n$, em que M é uma matriz geradora. Considere o seguinte epimorfismo de $\mathbb{Z}$-módulos

$$\begin{array}{rccc} \phi & : & \mathbb{Z}^n & \longrightarrow & \Lambda \\ & & \lambda & \longmapsto & \phi(\lambda) = \lambda M\ . \end{array}$$

Se a matriz Gram $G = MM^t$ coincide com a matriz identidade, então ϕ é injetivo e, dessa forma, temos que Λ é isomorfo à $\mathbb{Z}^n$, isto é, Λ é um $\mathbb{Z}^n$-reticulado. Mas, além disso, se $G = cId_n$, para algum $c \in \mathbb{Z}$, também podemos obter um $\mathbb{Z}^n$-reticulado. Para isso, basta considerar um reticulado Λ', cuja matriz geradora é dada por $M' = \frac{1}{\sqrt{c}} M$. Nesse caso, a matriz Gram

associada é dada por

$$G' := M'M'^t = \frac{1}{c}G = Id_n.$$

Portanto, uma condição suficiente para que um reticulado no $\mathbb{R}^n$ possa fornecer um reticulado $\mathbb{Z}^n$-rotacionado, é que sua matriz Gram seja a identidade a menos de uma constante. É justamente com esta condição que trabalhamos para obter reticulados $\mathbb{Z}^n$-rotacionados nas próximas seções. Mas, como a matriz Gram de um reticulado ideal coincide com a matriz da forma traço associada, o problema se resume a um estudo do comportamento da forma traço.

Por outro lado, se $(\mathcal{I}, Tr_\alpha)$ é um reticulado ideal, o qual apresenta uma matriz Gram que satisfaz $G = cId_n$, para algum $c \in \mathbb{Z}$, teremos que $det(G) = c^n$. Logo, pelo Teorema 3.3.1, segue que

$$\mathcal{N}(\alpha)\mathcal{N}(\mathcal{I})^2|\mathcal{D}_\mathbb{K}| = c^n. \tag{4.2.4}$$

Desse modo, a equação (4.2.4) fornece uma condição necessária, mas não suficiente, sobre α de modo que $(\mathcal{I}, Tr_\alpha)$ possa fornecer um reticulado $\mathbb{Z}^n$-rotacionado. Sendo assim, o parâmetro α serve de ajuste na tentativa de rotacionar um reticulado ideal sobre o $\mathbb{Z}^n$.

Faremos, agora, o estudo de algumas propriedades do conceito de anel de grupo, visando fornecer ferramentas que são utilizadas nas construções das próximas seções.

4.3 Anéis de grupos

A partir de um anel e de um grupo, definimos uma nova estrutura de anel, a qual também pode ser vista como módulo. O intuito, como veremos, é estabelecer uma interação entre as abordagens feitas em [18] e [20], das quais extraímos material que compõe a próxima seção.

Sejam G um grupo e R um anel. Denotemos por RG o conjunto de todas combinações lineares formais do tipo

$$\alpha = \sum_{g \in G} \alpha_g g, \quad \text{com } \alpha_g \in R,$$

tal que $\alpha_g = 0$ para quase todo $g \in G$, isto é, $\alpha_g \neq 0$ somente para um número finito de índices $g \in G$. Podemos olhar para um elemento α de RG como uma aplicação quase-nula dada por

$$\begin{array}{rccc} \alpha & : & G & \longrightarrow & R \\ & & g & \longmapsto & \alpha(g) = \alpha_g \ . \end{array}$$

O que permite interpretar a combinação linear formal que define $\alpha \in RG$, como um modo de exprimir os valores $\alpha(g) = \alpha_g$ da aplicação α.

Dados dois elementos $\alpha, \beta \in RG$, dizemos que $\alpha = \beta$ quando $\alpha_g = \beta_g$, para todo $g \in G$.

A soma e o produto em RG são definidas por:

(1) $\alpha + \beta = \sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$

(2) $\alpha\beta = \sum_{g\in G} \alpha_g g \sum_{h\in G} \beta_h h = \sum_{g,h\in G} (\alpha_g \beta_h) gh$.

Dado $\lambda \in R$, o produto escalar sobre RG é definido por:

(3) $\lambda\alpha = \lambda(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} (\lambda\alpha_g) g$.

As operações (1) e (3) estão bem definidas mediante as aplicações $(\alpha+\beta)(g) = \alpha(g)+\beta(g) = \alpha_g+\beta_g$ e $(\lambda\alpha)(g) = \lambda\alpha(g) = \lambda\alpha_g$, respectivamente. Já para justificar a boa definição do produto, pondo $u = gh$ e definindo

$$\begin{array}{rccl} \gamma \ : & G & \longrightarrow & R \\ & u = gh & \longmapsto & \gamma(gh) = \sum\limits_{gh=u\in G} \alpha_g \beta_h = \sum\limits_{h=g^{-1}u} \alpha_g \beta_h \ , \end{array}$$

teremos

$$\sum_{u=gh} \gamma_u u = \sum_{g=h^{-1}u} \sum_{h=g^{-1}u} \alpha_g \beta_h gh = \alpha\beta \ ,$$

isto é, o produto $\alpha\beta$ está bem definido mediante a aplicação γ.

Veremos agora que, munido das operações (1) e (2), o conjunto RG possui uma estrutura de anel, denominado anel de grupo de G sobre R.

Proposição 4.3.1 *Se G é um grupo e R é um anel, então $(RG, +, \cdot)$ é um anel. Além disso, se R possui elemento unidade, então RG é um anel com unidade.*

Demonstração: Com respeito à adição em RG, a associatividade e a comutatividade decorrem imediatamente das propriedades correspondentes em R. O elemento neutro, denotado por θ, é definido como $\theta(g) = \theta_g = 0_R$, para todo $g \in G$, uma vez que

$$\alpha + \theta = \sum_{g\in G} (\alpha_g + \theta_g) g = \sum_{g\in G} \alpha_g g = \alpha = \theta + \alpha, \quad \text{para todo } \alpha \in RG \ .$$

O elemento simétrico $-\alpha$ de $\alpha \in RG$ é definido por $(-\alpha)(g) = -\alpha_g$, e assim

$$\alpha + (-\alpha) = \sum_{g\in G} (\alpha_g - \alpha_g) g = \sum_{g\in G} \theta_g g = \theta = -\alpha + \alpha \ .$$

Dessa forma, $(RG, +)$ é um grupo abeliano. Com respeito à multiplicação em RG, a associatividade decorre das propriedades corresponentes em R e em G, e a distributividade decorre da distributiva em R. Com essas propriedades, RG apresenta uma estrutura de anel. Além disso, se R possui elemento unidade 1_R, definindo $I(1_G) = 1_R$ e $I(g) = 0_R$, para todo $g \in G - \{1_G\}$, teremos que

$$I = \sum_{g \in G} I_g g = 1_R 1_G + \sum_{\substack{g \in G \\ g \neq 1_G}} I_g g = 1_R 1_G + \sum_{g \in G} \theta_g g = 1_R 1_G + \theta = 1_R 1_G \ .$$

Logo,

$$\alpha I = \left(\sum_{g \in G} \alpha_g g \right) 1_R 1_G = \sum_{g \in G} (\alpha_g 1_R) g 1_G = \sum_{g \in G} \alpha_g g = \alpha = I\alpha, \quad \text{para todo } \alpha \in RG \ .$$

Portanto, I é unidade em RG. ∎

Observação 4.3.1 *Se R é comutativo e G abeliano, então o anel de grupo RG é comutativo, o que decorre diretamente da definição do produto em RG. Nesse caso, dizemos que RG é uma álgebra de grupo de G sobre R.*

Proposição 4.3.2 *Se G é um grupo e R um anel com unidade então, munido com a adição e o produto escalar, RG é um R-módulo. Além disso, G é uma base de RG sobre R.*

Demonstração: Como visto na Proposição 4.3.1, temos que $(RG, +)$ é um grupo abeliano. Com respeito ao produto escalar, as propriedades decorrem diretamente das propriedades associativa e distributiva em R, e do fato de R possuir unidade. Portanto, RG é um R-módulo. Definindo

$$\begin{array}{rccl} i & : & G & \longrightarrow & RG \\ & & h & \longmapsto & i(h) = \displaystyle\sum_{g \in G} x_g g \ , \end{array}$$

tal que $x(h) = 1_R$ e $x(g) = 0_R$, para todo $g \in G - \{h\}$, teremos que $i(h) = 1_R h$ para todo $h \in G$. Assim, identificamos G com o subconjunto $i(G) \subset RG$ via o monomorfismo i e, desse modo, podemos olhar para G como um subconjunto de RG. Temos que, todo elemento de RG é escrito como combinação linear de elementos de G, ou seja, G é um gerador de RG sobre R. Sejam $g_1, \ldots, g_n \in G$ tal que $r_1 g_1 + \ldots + r_n g_n = \theta$, com $r_i \in R$, para $i = 1, \ldots, n$. Podemos expressar essa igualdade da seguinte maneira

$$\sum_{g \in G} r_g g = r_1 g_1 + \ldots + r_n g_n = \theta = \sum_{g \in G} \theta_g g \ ,$$

com $r_g = r_i$, para $g = g_i$, e $r_g = 0$ quando tivermos $g \neq g_i$, para todo $i = 1, \ldots, n$. Assim, $r_g = \theta_g = 0$ para todo $g \in G$, isto é, $r_i = 0$ para todo $i = 1, \ldots, n$. Portanto, G é um conjunto linearmente independente sobre R. Desse modo, tem-se que G é uma base de RG sobre R e, portanto, RG é um R-módulo livre, cujo posto coincide com a ordem do grupo G. ■

Exemplo 4.3.1 *Sejam $\mathbb{K}$ um corpo de números e $G = Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Com isso temos bem definido o anel de grupo $\mathbb{Z}G$ que, do fato de G ser finito, pode ser representado como*

$$\mathbb{Z}G = \left\{ \sum_{i=1}^{n} \alpha_i \sigma_i ;\ \alpha_i \in \mathbb{Z} \right\}.$$

Temos que, $\mathbb{Z}G$ é um anel com unidade e se $G = Gal(\mathbb{K} : \mathbb{Q})$ for abeliano, $\mathbb{Z}G$ será comutativo, isto é, uma álgebra de grupo de G sobre $\mathbb{Z}$. Além disso, $\mathbb{Z}G$ é um $\mathbb{Z}$-módulo livre de posto n, cuja base é $G = Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$.

Se G é um grupo e R um anel com unidade, segue pela Proposição 4.3.1, que RG é um anel com unidade e, desse modo, podemos definir módulos sobre RG, como no seguinte exemplo:

Exemplo 4.3.2 *Considerando as mesmas hipóteses do Exemplo 4.3.1, definamos o seguinte produto escalar*

$$\begin{array}{rccl} \cdot\ : & \mathbb{Z}G \times \mathbb{K} & \longrightarrow & \mathbb{K} \\ & (\alpha, x) & \longmapsto & \alpha x = (\sum_{i=1}^{n} \alpha_i \sigma_i)x = \sum_{i=1}^{n} \alpha_i \sigma_i(x)\ . \end{array}$$

Temos que $1.Id_{\mathbb{K}}$ é unidade em $\mathbb{Z}G$ e $(1Id_{\mathbb{K}})x = 1Id_{\mathbb{K}}(x) = x$, para todo $x \in \mathbb{K}$. Dados $\alpha, \beta \in \mathbb{Z}G$ e $x, y \in \mathbb{K}$, temos satisfeitas as propriedades $(\alpha\beta)x = \alpha(\beta x)$, $(\alpha + \beta)x = \alpha x + \beta x$ e $\alpha(x + y) = \alpha x + \alpha y$, das quais a justificativa decorre da linearidade dos elementos de $G = Gal(\mathbb{K} : \mathbb{Q})$, e da propriedade distributiva no corpo $\mathbb{K}$. Assim, como $(\mathbb{K}, +)$ é um grupo abeliano teremos que $\mathbb{K}$, juntamente com o produto escalar sobre $\mathbb{Z}G$, é um $\mathbb{Z}G$-módulo. Note que, dados $c_1, c_2, \ldots, c_r \in \mathbb{K}$, o conjunto $\mathbb{Z}Gc_1 + \mathbb{Z}Gc_2 + \ldots + \mathbb{Z}Gc_r$ é um $\mathbb{Z}G$-submódulo de $\mathbb{K}$, gerado por $c_1, c_2, \ldots, c_r$.

Proposição 4.3.3 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão galoisiana de grau n, $G = Gal(\mathbb{K} : \mathbb{Q})$ e $M \subset \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. Temos que, M possui uma base normal se, e somente se, M é um $\mathbb{Z}G$-módulo livre de posto um.*

Demonstração: Seja $G = Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Suponhamos que M possui uma base normal, isto é, que existe $c \in M$ tal que $\{\sigma_1(c), \ldots, \sigma_n(c)\}$ é uma $\mathbb{Z}$-base de M. Logo,

$$\begin{aligned} M &= \mathbb{Z}\sigma_1(c) + \ldots + \mathbb{Z}\sigma_n(c) \\ &= \left\{ \sum_{i=1}^{n} \alpha_i \sigma_i(c);\ \alpha_i \in \mathbb{Z} \right\} = \left\{ (\sum_{i=1}^{n} \alpha_i \sigma_i)c;\ \alpha_i \in \mathbb{Z} \right\}, \end{aligned}$$

e assim $M = \{\alpha c;\ \alpha \in \mathbb{Z}G\} = \mathbb{Z}Gc$, ou seja, M é um $\mathbb{Z}G$-módulo gerado por c. Seja $\alpha = \sum_{i=1}^{n} \alpha_i \sigma_i \in \mathbb{Z}G$ tal que $0 = \alpha c = (\sum_{i=1}^{n} \alpha_i \sigma_i)c = \sum_{i=1}^{n} \alpha_i \sigma_i(c)$. Como $\{\sigma_i(c)\}_{i=1}^{n}$ é linearmente independente sobre $\mathbb{Z}$, segue que $\alpha_i = 0$, para todo $i = 1, \ldots, n$ e, assim, $\alpha = 0$. Portanto, $\{c\}$ é linearmente independente sobre $\mathbb{Z}G$ e, dessa forma, é uma base de M sobre $\mathbb{Z}G$. Logo, M é $\mathbb{Z}G$-módulo livre de posto 1. Reciprocamente, suponhamos que existe $c \in M$ tal que $M = \mathbb{Z}Gc$, com $\{c\}$ linearmente independente sobre $\mathbb{Z}G$. Logo, $M = \mathbb{Z}Gc = \mathbb{Z}\sigma_1(c) + \ldots + \mathbb{Z}\sigma_n(c)$. Sejam $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tal que $\alpha_1\sigma_1(c) + \ldots + \alpha_n\sigma_n(c) = 0$, ou seja,

$$\alpha c = (\sum_{i=1}^{n} \alpha_i \sigma_i)c = \sum_{i=1}^{n} \alpha_i \sigma_i(c) = 0, \quad \text{com } \alpha \in \mathbb{Z}G\ .$$

Assim, $\alpha = 0$, o que implica que $\alpha_i = 0$, para todo $i = 1, \ldots, n$. Portanto $\{\sigma_1(c), \ldots, \sigma_n(c)\}$ é uma $\mathbb{Z}$-base de M, ou seja, uma base normal de M. ∎

Exemplo 4.3.3 *Sejam $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo, $[\mathbb{K} : \mathbb{Q}] = n$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e σ um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Pela Observação 4.1.3, temos que*

$$\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$$

é uma base normal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Denotando $G = Gal(\mathbb{K} : \mathbb{Q})$, segue da Proposição 4.3.3, que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}G$-módulo livre de posto 1, ou mais precisamente, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}G\theta$, sendo $\{\theta\}$ linearmente independente sobre $\mathbb{Z}G$.

A importância do resultado apresentado pela Proposição 4.3.3 é justamente devida à busca de bases normais para anéis de inteiros de corpos de números, bem como para ideais de anéis de inteiros. Essa busca consiste em identificar ideais de anéis de inteiros com módulos livres de posto unitário sobre anéis de grupos . Nas referências [10], [20] e [21] foram feitas algumas construções com tal característica, utilizando ferramentas provindas dos anéis de grupos de modo a obter bases normais que forneçam propriedades proveitosas em reticulados, como a identificação da forma traço com a matriz identidade.

Na próxima seção faremos construções de reticulados $\mathbb{Z}^n$-rotacionados utilizando como base a referência [18], a qual originou-se das construções algébricas obtidas via anéis de grupos desenvolvidas por Erez - [20] e Ullom - [21]. Nosso foco não é permear diretamente essas duas últimas, mas citaremos alguns de seus resultados quando necessário.

4.4 Reticulados $\mathbb{Z}^n$-rotacionados de dimensão (prima) ímpar n

Dada uma extensão galoisiana $\mathbb{Q} \subset \mathbb{K}$ de grau ímpar n, P. E. Conner e R. Perlis provaram, no Lema (V.4.1) de [10], a existência de um único ideal fracionário $\mathcal{A}$ de $\mathcal{O}_{\mathbb{K}}$ tal que

$$\mathcal{A}^2 = \Delta_{\mathbb{K}/\mathbb{Q}}^{-1} ,$$

onde $\Delta_{\mathbb{K}/\mathbb{Q}}^{-1}$ é o codiferente de $\mathbb{K}$ sobre $\mathbb{Q}$. Foi então questionada a existência de uma base normal $\{e_1, \ldots, e_n\}$ para $\mathcal{A}$ sobre $\mathbb{Z}$, tal que

$$Tr_{\mathbb{K}/\mathbb{Q}}(e_i e_j) = \delta_{ij} , \quad \text{com } i, j = 1, \ldots, n ,$$

em que δ_{ij} é o delta de Kronecker.

Quatro anos mais tarde, em 1988, B. Erez resolveu tal problema, em [20], adicionando as condições de que $\mathbb{Q} \subset \mathbb{K}$ seja cíclica de grau primo ímpar, encontrando um elemento $x \in \mathcal{A}$ tal que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\sigma_i(x)\sigma_j(x)) = c\delta_{ij} , \quad \text{com } i, j = 1, \ldots, n ,$$

onde c é um inteiro positivo e $G := Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. O elemento $x \in \mathcal{A}$ descrito por Erez originou-se de construções algébricas desenvolvidas por S. Ullom, em [21], e a base normal $\{\sigma_1(x), \ldots, \sigma_n(x)\}$ é obtida ao demonstrar que $\mathcal{A}$ possui uma estrutura de $\mathbb{Z}G$-módulo livre de posto unitário gerado por x (veja Proposição 4.3.3). Note que, ao exibir tal base trazemos uma descrição explícita para o ideal fracionário $\mathcal{A}$, como um $\mathbb{Z}$-módulo livre de posto finito n.

Nesta seção, descrevemos a estrutura do $\mathbb{Z}$-módulo livre $\mathcal{A}$ e apresentamos uma construção de reticulados $\mathbb{Z}^n$-rotacionados obtidos do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{A})$, tomando como principal referência o parágrafo V de [18], desenvolvido por E. Bayer-Fluckiger, F. Oggier e E. Viterbo. A construção e a apresentação do elemento $x \in \mathcal{A}$ são divididas em três casos de ramificação, devido ao fato da extensão cíclica $\mathbb{K}$ ser subcorpo de extensões ciclotômicas, que são caracterizadas justamente pela ramificação de primos em $\mathcal{O}_{\mathbb{K}}$.

Proposição 4.4.1 *Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão abeliana de grau primo n, então pelo menos um primo p ramifica em $\mathcal{O}_{\mathbb{K}}$. Além disso, se p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$, então $p = n$ ou $p \equiv 1 (mod\ n)$.*

Demonstração: Pelo Teorema 1.1.3, tem-se que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$, para algum inteiro positivo m. Suponhamos que m seja o condutor de $\mathbb{K}$. Logo, do Teorema 1.6.2, obtemos que $|\mathcal{D}_{\mathbb{K}}| = m^{n-1}$. Como $m > 1$ (pois caso contrário teríamos $\mathbb{K} = \mathbb{Q}$), segue que $|\mathcal{D}_{\mathbb{K}}| > 1$, assim, existe pelo menos um primo na fatoração do discriminante $\mathcal{D}_{\mathbb{K}}$ e, dessa forma, existe pelo menos um primo

que ramifica em $\mathcal{O}_{\mathbb{K}}$ (veja Teorema 2.3.3). Se um único primo p ramifica em $\mathcal{O}_{\mathbb{K}}$, então p é o único primo na fatoração de $\mathcal{D}_{\mathbb{K}}$, o que acarreta que p também é único primo em m, isto é, existe um inteiro positivo r, tal que $m = p^r$ e, desse modo, tem-se que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p^r})$. Como $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r) = p^{r-1}(p-1)$, segue que $[\mathbb{K} : \mathbb{Q}] = n$ divide $p^{r-1}(p-1)$. Logo, $n \mid p$ ou $n \mid p-1$ e, assim, $n = p$ ou $p \equiv 1(mod\ n)$. ■

Desse modo, dada uma extensão cíclica $\mathbb{Q} \subset \mathbb{K}$ de grau primo ímpar n, segue pela Proposição 4.4.1, que pelo menos um primo ramifica em $\mathcal{O}_{\mathbb{K}}$. Porém, o caso em que um único primo ramifica se bifurca, de modo que, devemos considerar as três seguintes possibilidades:

Caso I: $p \neq n$ é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$, com $p \equiv 1(mod\ n)$;
Caso II: $p = n$ é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$;
Caso III: pelo menos dois primos ramificam em $\mathcal{O}_{\mathbb{K}}$.

Excepcionalmente no Caso I, a construção é feita exigindo que a dimensão n, de $\mathbb{K}$ sobre $\mathbb{Q}$, seja apenas ímpar, não necessariamente prima.

4.4.1 Caso I: um único primo $p \neq n$ ramifica em $\mathcal{O}_{\mathbb{K}}$, com n ímpar

Dados n ímpar e um primo ímpar p satisfazendo $p \equiv 1(mod\ n)$, segue pela Proposição 4.1.1, que existe uma única extensão cíclica $\mathbb{Q} \subseteq \mathbb{K}$ de grau n, com $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$, tal que p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$.

Lema 4.4.1 *Sejam p um primo ímpar, $\sigma = \sigma_r$ um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ e $m = \frac{p-1}{2}$. Denotando $\zeta = \zeta_p$, definindo*

$$\alpha = \prod_{k=0}^{m-1} (1 - \zeta^{r^k})$$

e tomando um inteiro λ tal que $\lambda(r-1) \equiv 1(mod\ p)$, temos válidas as seguintes igualdades:

(a) $\sigma(\alpha) = -\zeta^{p-1}\alpha$,

(b) $\sigma(\zeta^{\lambda}\alpha) = -\zeta^{\lambda}\alpha$,

(c) $(\zeta^{\lambda}\alpha)^2 = (-1)^m p$.

Demonstração: Antes de demonstrar cada ítem, iremos justificar a existência do inteiro λ satisfazendo $\lambda(r-1) \equiv 1(mod\ p)$. Temos que p não divide $r-1$, pois caso contrário teríamos $r \equiv 1(mod\ p)$, o que é uma contradição, pois $p-1$ é o menor inteiro tal que $r^{p-1} \equiv 1(mod\ p)$, pelo fato de $\overline{r}$ ser um gerador de $\mathbb{Z}_p^*$ (veja Observação 4.1.2). Assim, $mdc(p, r-1) = 1$, e pelo Teorema 2.8 de [3], segue que a congruência $y(r-1) \equiv 1(mod\ p)$ possui uma única solução

$y = \lambda$ incongruente módulo p, isto é, todas as outras soluções são congruentes a λ módulo p.

(a) Temos que

$$\sigma(\alpha) = \prod_{k=0}^{m-1} \sigma(1 - \zeta^{r^k}) = \prod_{k=0}^{m-1} (1 - \sigma(\zeta^{r^k})) \ .$$

Como $\sigma(\zeta^{r^k}) = \sigma(\zeta)^{r^k} = (\zeta^r)^{r^k} = \zeta^{r^{k+1}}$, segue que

$$\begin{aligned} \sigma(\alpha) &= \prod_{k=0}^{m-1} (1 - \zeta^{r^{k+1}}) \\ &= (1-\zeta)^{-1}(1-\zeta) \prod_{k=0}^{m-2} (1 - \zeta^{r^{k+1}})(1 - \zeta^{r^m}) \ . \end{aligned}$$

Porém,

$$\alpha = (1-\zeta) \prod_{k=1}^{m-1} (1 - \zeta^{r^k}) = (1-\zeta) \prod_{k=0}^{m-2} (1 - \zeta^{r^{k+1}})$$

e assim,

$$\sigma(\alpha) = (1-\zeta)^{-1}(1 - \zeta^{r^m})\alpha \ .$$

Mas, como $r^m \equiv -1 (mod\ p)$, segue que $\zeta^{r^m} = \zeta^{-1}$. Dessa forma, $\sigma(\alpha) = (1-\zeta)^{-1}(1-\zeta^{-1})\alpha$ e, como $\zeta^{p-1} = \zeta^{-1}$, segue que

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

Porém, $\zeta = \zeta_p$ é uma raíz do polinômio

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

Assim, $-\zeta^{p-1} = \zeta^{p-2} + \ldots + \zeta + 1$ e, portanto, $\sigma(\alpha) = -\zeta^{p-1}\alpha$.

(b) Utilizando o ítem (a), temos que

$$\sigma(\zeta^\lambda \alpha) = \sigma(\zeta^\lambda)\sigma(\alpha) = \zeta^{r\lambda}(-\zeta^{p-1}\alpha) \ .$$

Mas, como $\lambda(r-1) \equiv 1 (mod\ p)$, segue que $\lambda r \equiv \lambda + 1 (mod\ p)$ e assim, $\zeta^{r\lambda} = \zeta^{\lambda+1}$. Portanto,

$$\sigma(\zeta^\lambda \alpha) = \zeta^{\lambda+1}(-\zeta^{p-1}\alpha) = -\zeta^{\lambda+p}\alpha = -\zeta^\lambda \alpha \ .$$

(c) Considere o p-ésimo polinômio ciclotômico

$$\phi_p(x) = \prod_{j=1}^{p-1}(x - \zeta^j) = x^{p-1} + x^{p-2} + \ldots + x + 1 \ .$$

Como ζ é uma raíz de $\phi_p(x)$, segue que cada elemento de

$$Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \langle\sigma\rangle = \{Id, \sigma, \sigma^2, \ldots, \sigma^{p-2}\}$$

aplicado em ζ é uma raíz de $\phi_p(x)$, pois $\phi_p(\sigma^k(\zeta)) = \sigma^k(\phi_p(\zeta)) = 0$, isto é, os elementos $\sigma^k(\zeta)$, com $k = 0, 1, \ldots, p-2$, são exatamente as raízes distintas de $\phi_p(x)$. Dessa forma,

$$\phi_p(x) = \prod_{k=0}^{p-2}(x - \sigma^k(\zeta)) = \prod_{k=0}^{p-2}(x - \zeta^{r^k}) \ .$$

Assim, avaliando $\phi_p(x)$ para $x = 1$, temos que

$$p = \phi_p(1) = \prod_{k=0}^{p-2}(1 - \zeta^{r^k}) \ .$$

Por outro lado, como $r^m \equiv -1(mod\ p,)$, segue que $r^{m+i} = r^m r^i \equiv -r^i(mod\ p)$, para todo inteiro i. Assim, $\zeta^{r^{m+i}} = \zeta^{-r^i}$, para todo $i = 0, 1, \ldots, m-1$. Desse modo,

$$\prod_{k=m}^{p-2}(1 - \zeta^{r^k}) = \prod_{i=0}^{m-1}(1 - \zeta^{r^{m+i}}) = \prod_{i=0}^{m-1}(1 - \zeta^{-r^i})$$

e portanto,

$$p = \prod_{k=0}^{p-2}(1 - \zeta^{r^k}) = \prod_{k=0}^{m-1}(1 - \zeta^{r^k}) \prod_{k=m}^{p-2}(1 - \zeta^{r^k}) = \alpha \prod_{i=0}^{m-1}(1 - \zeta^{-r^i}) \ .$$

Porém,

$$\alpha \prod_{i=0}^{m-1} \zeta^{-r^i} = \prod_{i=0}^{m-1}(\zeta^{-r^i} - 1) = \begin{cases} \prod_{i=0}^{m-1}(1 - \zeta^{-r^i}) \ , & \text{se } m \text{ é par} \\ -\prod_{i=0}^{m-1}(1 - \zeta^{-r^i}) \ , & \text{se } m \text{ é ímpar} \end{cases}$$

ou seja,

$$(-1)^m \alpha \prod_{i=0}^{m-1} \zeta^{-r^i} = \prod_{i=0}^{m-1}(1 - \zeta^{-r^i}) \ .$$

Dessa forma, temos

$$p = (-1)^m \alpha^2 \prod_{i=0}^{m-1} \zeta^{-r^i} \ .$$

Note que, $\dfrac{1-r^m}{r-1} = -r^{m-1} - \ldots - r - 1$. Logo,

$$\prod_{i=0}^{m-1} \zeta^{-r^i} = \zeta^{-r^{m-1}-\ldots-r-1} = \zeta^{\frac{1-r^m}{r-1}} \ .$$

Porém, $r^m \equiv -1 (mod\, p)$ implica $1-r^m \equiv 2 (mod\, p)$ e a hipótese $\lambda(r-1) \equiv 1 (mod\, p)$ garante que $2\lambda(r-1) \equiv 2 (mod\, p)$. Assim, $1-r^m \equiv 2\lambda(r-1) (mod\, p)$, isto é, $\frac{1-r^m}{r-1}(r-1) \equiv 2\lambda(r-1) (mod\, p)$. Como $mdc(p, r-1) = 1$, segue que $\frac{1-r^m}{r-1} \equiv 2\lambda (mod\, p)$. Logo, $\zeta^{\frac{1-r^m}{r-1}} = \zeta^{2\lambda}$. Desse modo, teremos $p = (-1)^m \alpha^2 \zeta^{2\lambda}$ e, portanto,

$$(-1)^m p = (-1)^{2m} \alpha^2 \zeta^{2\lambda} = (\alpha \zeta^{\lambda})^2 \ ,$$

o que prova o lema. ∎

Teorema 4.4.1 *Sejam p um primo ímpar, $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com $[\mathbb{K} : \mathbb{Q}] = n$ ímpar e σ um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Considere α e λ definidos como no Lema 4.4.1 e $\zeta = \zeta_p$. Se*

$$z = \zeta^{\lambda} \alpha (1 - \zeta) \quad e \quad x = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(z)$$

então

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = \begin{cases} p^2 \ , & se\ t = 0 \\ 0 \ , & se\ t \neq 0 \ ; \end{cases}$$

com $t = 0, 1, \ldots, n-1$.

Demonstração: Como no Lema 4.4.1, considere $\sigma = \sigma_r$ e $m = \frac{p-1}{2}$. Note que x e $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x))$ estão bem definidos, pois $z \in \mathbb{Q}(\zeta_p)$ e $x, \sigma^t(x) \in \mathbb{K}$. Desse modo, como $Gal(\mathbb{K} : \mathbb{Q}) = \{Id_{\mathbb{K}}, \sigma|_{\mathbb{K}}, \ldots, \sigma^{n-1}|_{\mathbb{K}}\}$, segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = \sum_{a=0}^{n-1} \sigma^a(x\ \sigma^t(x)), \quad t = 0, 1, \ldots, n-1 \ .$$

Como

$$x\ \sigma^t(x) = \sum_{c=1}^{\frac{p-1}{n}} \sigma^{cn}(z) \sum_{j=1}^{\frac{p-1}{n}} \sigma^{t+jn}(z) = \sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{cn}(z)\sigma^{t+jn}(z) \ ,$$

segue que,

$$\begin{aligned}
Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) &= \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\
&= \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(\zeta^\lambda\alpha(1-\zeta))\sigma^{a+t+jn}(\zeta^\lambda\alpha(1-\zeta)) \\
&\overset{(1)}{=} \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}} (-1)^{a+cn}\zeta^\lambda\alpha(1-\zeta^{r^{a+cn}})(-1)^{a+t+jn}\zeta^\lambda\alpha(1-\zeta^{r^{a+t+jn}}) \\
&\overset{(2)}{=} \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}} (-1)^{t+c+j}(\zeta^\lambda\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\
&= (-1)^t\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j(\zeta^\lambda\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\
&\overset{(3)}{=} (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}})\ .
\end{aligned}$$

As igualdades (1) e (3) decorrem dos ítens (b) e (c) do Lema 4.4.1, respectivamente. Já a igualdade (2) segue do fato de que $(-1)^{a+cn}(-1)^{a+t+jn} = (-1)^{2a}(-1)^t(-1)^{cn}(-1)^{jn} = (-1)^{t+c+j}$, pois n é ímpar e, assim, $(-1)^{cn} = (-1)^c$ e $(-1)^{jn} = (-1)^j$. Como

$$\begin{aligned}
&\sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\
&= \sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}}-\zeta^{r^{a+t+jn}}+\zeta^{r^{a+cn}}\zeta^{r^{a+t+jn}}) \\
&= \sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}}) - \sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+t+jn}} + \sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}\ ,
\end{aligned}$$

segue que, $Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) =$

$$(-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\left(\sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}}) - \sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+t+jn}} + \sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}\right).$$

Temos que $\frac{p-1}{n}$ é par, pois $(\frac{p-1}{n})n = p-1$ é par e n é ímpar. Assim,

$$\sum_{j=1}^{\frac{p-1}{n}}(-1)^j(1-\zeta^{r^{a+cn}}) = 0\ ,$$

pois o termo $(1-\zeta^{r^{a+cn}})$ não depende de j. Logo, $Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) =$

$$(-1)^{t+m}p\left(-\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+t+jn}}+\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}\right).$$

Dessa forma, como $\frac{p-1}{n}$ é par e o termo

$$\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+t+jn}}$$

não depende de c, segue que

$$\begin{aligned}
Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) &= (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}\\
&\overset{(*)}{=} (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{\frac{p-1}{n}}\zeta^{r^{a+dn+kn}+r^{a+t+kn}}\\
&= (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{\frac{p-1}{n}}\zeta^{(r^{dn}+r^t)r^{a+kn}}\ .
\end{aligned}$$

Para os detalhes da mudança de variáveis feita na igualdade $(*)$, veja o Teorema 4.1.2. Ainda, pelo mesmo Teorema, pondo $s=1,\ldots,p-1$, teremos que

$$\sum_{a=0}^{n-1}\sum_{k=1}^{\frac{p-1}{n}}\zeta^{(r^{dn}+r^t)r^{a+kn}}=\sum_{s=1}^{p-1}(\zeta^{r^{dn}+r^t})^s\ .$$

Assim, denotando $\omega_{d,t}=\zeta^{r^{dn}+r^t}$, obtemos que

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x))=(-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{s=1}^{p-1}(\omega_{d,t})^s\ ,$$

onde

$$\sum_{s=1}^{p-1}(\omega_{d,t})^s=\begin{cases}p-1\ , & \text{se } \omega_{d,t}=1\\ -1\ , & \text{se } \omega_{d,t}\neq 1\ ;\end{cases}\qquad t=0,1,\ldots,n-1\ .$$

Como verificado no Teorema 4.1.2, temos a seguinte equivalência

$$\omega_{d,t}=1\iff t=0\ \text{ e }\ d=\frac{p-1}{2n}\ .$$

Suponhamos que $t \neq 0$. Nesse caso, teremos $\omega_{d,t} \neq 1$, e assim

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{s=1}^{p-1}(\omega_{d,t})^s = (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d(-1) = 0\ ,$$

pois $(p-1)/n$ é par. Suponha, agora, que $t = 0$. Se $d = (p-1)/2n$, então $\omega_{d,t} = 1$ e se $d \neq (p-1)/2n$, então $\omega_{d,t} \neq 1$. Assim,

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) &= (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{s=1}^{p-1}(\omega_{d,t})^s \\ &= (-1)^m p(-1)^{\frac{p-1}{2n}}(p-1) + (-1)^m p\sum_{\substack{d=1 \\ d\neq\frac{p-1}{2n}}}^{\frac{p-1}{n}}(-1)^d(-1)\ . \end{aligned}$$

Porém, $m = \frac{p-1}{2}$ e $\frac{p-1}{2n}$ têm a mesma paridade, e portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = p(p-1) + p = p^2\ ,$$

o que conclui a demonstração. ∎

Proposição 4.4.2 *Nas mesmas hipóteses do Teorema 4.4.1, temos que o conjunto*

$$\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$$

é um $\mathbb{Z}$-módulo livre de posto n, contido no anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Considere o homomorfismo canônico $\sigma_{\mathbb{K}}$. Pela Proposição 4.1.2, temos que $\mathbb{K}$ é totalmente real. Logo,

$$\sigma_{\mathbb{K}}(\sigma^i(x)) = (\sigma^i(x), \sigma^{i+1}(x), \ldots, \sigma^{i+n-1}(x))\ ,$$

para $i = 0, 1, \ldots, n-1$. Assim, como verificado na Seção 4.1.1, segue do Teorema 4.4.1, que

$$\langle\sigma_{\mathbb{K}}(\sigma^i(x)), \sigma_{\mathbb{K}}(\sigma^j(x))\rangle = Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^{j-i}(x)) = p^2\delta_{ij}\ ,$$

com $i, j = 0, 1, \ldots, n-1$. Ou seja, o conjunto $\{\sigma_{\mathbb{K}}(x), \sigma_{\mathbb{K}}(\sigma(x)), \ldots, \sigma_{\mathbb{K}}(\sigma^{n-1}(x))\} \subset \mathbb{R}^n$ é ortogonal, isto é, seus vetores são linearmente independente sobre $\mathbb{R}$ e, consequentemente, sobre $\mathbb{Z}$. Desse modo, supondo $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ tal que $a_0x + a_1\sigma(x) + \ldots + a_{n-1}\sigma^{n-1}(x) = 0$, temos que $a_0\sigma_{\mathbb{K}}(x) + a_1\sigma_{\mathbb{K}}(\sigma(x)) + \ldots + a_{n-1}\sigma_{\mathbb{K}}(\sigma^{n-1}(x)) = \sigma_{\mathbb{K}}(a_0x + a_1\sigma(x) + \ldots + a_{n-1}\sigma^{n-1}(x)) = 0$.

Logo, $a_0 = a_1 = \ldots = a_{n-1} = 0$, ou seja, $\{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$ é linearmente independente sobre $\mathbb{Z}$. Portanto, $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}$-módulo livre de posto finito n. Além disso, pela definição de x, temos que $\sigma^i(x) \in \mathbb{K}$ é um inteiro sobre $\mathbb{Z}$ (pois ζ_p o é). Dessa forma, $\sigma^i(x) \in \mathcal{O}_{\mathbb{K}}$, para todo $i = 0, 1, \ldots, n-1$, e portanto $\mathcal{A} \subset \mathcal{O}_{\mathbb{K}}$. ■

Observação 4.4.1 *Seja $\mathcal{G} = Gal(\mathbb{K} : \mathbb{Q})$. Pela Proposição 4.3.3, temos que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}\mathcal{G}$-módulo livre de posto unitário cuja base é $\{x\}$, isto é, $\mathcal{A} = \mathbb{Z}\mathcal{G}x$. Boas Erez demonstrou, em [20], que $\mathcal{A} = \mathbb{Z}\mathcal{G}x$ é justamente o ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ que satisfaz $\mathcal{A}^2 = \Delta_{\mathbb{K}/\mathbb{Q}}^{-1}$, para o caso n primo ímpar.*

Obtenção do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$

Sejam $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo ímpar, $[\mathbb{K} : \mathbb{Q}] = n$ ímpar e σ um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Temos que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}$-módulo livre de posto finito n, contido em $\mathcal{O}_{\mathbb{K}}$, onde $x \in \mathcal{O}_{\mathbb{K}}$ é o elemento definido no Teorema 4.4.1. Desse modo, temos definido o reticulado algébrico n-dimensional $\sigma_{\mathbb{K}}(\mathcal{A})$, do qual o conjunto

$$\{\sigma_{\mathbb{K}}(x), \sigma_{\mathbb{K}}(\sigma(x)), \ldots, \sigma_{\mathbb{K}}(\sigma^{n-1}(x))\} \subset \mathbb{R}^n$$

é uma base e, como $\sigma_{\mathbb{K}}$ é dado por

$$\begin{array}{rccl} \sigma_{\mathbb{K}} & : & \mathbb{K} & \longrightarrow & \mathbb{R}^n \\ & & y & \longmapsto & \sigma_{\mathbb{K}}(y) = (y, \sigma(y), \ldots, \sigma^{n-1}(y)) \ , \end{array}$$

segue que a matriz geradora de $\sigma_{\mathbb{K}}(\mathcal{A})$ associada a tal base, é descrita como

$$M = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{n-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(x) & x & \cdots & \sigma^{n-2}(x) \end{pmatrix}.$$

Assim, denotando por $G = (g_{ij})_{i,j=0}^{n-1}$ a matriz Gram de $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M, temos que cada termo de $G = MM^t$ é dado por

$$g_{ij} = \langle \sigma_{\mathbb{K}}(\sigma^i(x)), \sigma_{\mathbb{K}}(\sigma^j(x)) \rangle = Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^{j-i}(x)) \overset{(*)}{=} p^2\delta_{ij} \ ,$$

com $i, j = 0, 1, \ldots, n-1$, onde a igualdade $(*)$ segue do Teorema 4.4.1. Dessa forma, a matriz Gram do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M tem a seguinte característica:

$$G = \begin{pmatrix} p^2 & 0 & \cdots & 0 \\ 0 & p^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p^2 \end{pmatrix} = p^2 Id \ .$$

Como descrito na Seção 4.2, podemos rotacionar o reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ sobre o $\mathbb{Z}^n$. Ao definir a matriz $M' = \frac{1}{p}M$, temos que M' é uma matriz geradora do reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$, onde

$$\mathcal{A}' = \mathbb{Z}\frac{x}{p} + \mathbb{Z}\frac{\sigma(x)}{p} + \ldots + \mathbb{Z}\frac{\sigma^{n-1}(x)}{p} \subset \mathbb{K}$$

é um $\mathbb{Z}$-módulo livre de posto n. Desse modo, a matriz Gram G' de $\sigma_{\mathbb{K}}(\mathcal{A}')$ com respeito à M' é dada por

$$G' = M'M'^t = \frac{1}{p}M\frac{1}{p}M^t = \frac{1}{p^2}G = Id \ .$$

Assim, $\sigma_{\mathbb{K}}(\mathcal{A}')$ é isomorfo à $\mathbb{Z}^n$, ou seja, é um reticulado $\mathbb{Z}^n$-rotacionado. Como $n = [\mathbb{K} : \mathbb{Q}]$ é ímpar, segue pela Proposição 4.1.2, que $\mathbb{K}$ é totalmente real. Logo, $\sigma_{\mathbb{K}}(\mathcal{A}')$ tem diversidade máxima n. Para avaliar a distância produto mínima, utilizamos o seguinte resultado:

Proposição 4.4.3 *Com as mesmas notações, ao denotar $\mathcal{G} = Gal(\mathbb{K} : \mathbb{Q})$, temos que o anel de grupo $\mathbb{Z}\mathcal{G}$ é isomorfo ao anel de inteiros $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Seja $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$. Pelo Exemplo 4.3.3 temos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\mathcal{G}\theta$ e, assim, como $\mathcal{G} = Gal(\mathbb{K} : \mathbb{Q}) = \{Id_{\mathbb{K}}, \sigma|_{\mathbb{K}}, \ldots, \sigma^{n-1}|_{\mathbb{K}}\}$, definimos de modo natural o seguinte homomorfismo de anéis:

$$\begin{array}{rccc} \psi \ : & \mathbb{Z}\mathcal{G} & \longrightarrow & \mathcal{O}_{\mathbb{K}} \\ & \displaystyle\sum_{i=0}^{n-1} a_i\sigma^i & \longmapsto & (\displaystyle\sum_{i=0}^{n-1} a_i\sigma^i)\theta = \displaystyle\sum_{i=0}^{n-1} a_i\sigma^i(\theta) \ , \end{array}$$

onde por simplicidade denotamos $\sigma^i = \sigma^i|_{\mathbb{K}}$. Temos que ψ está bem definida e a sobrejetividade segue de modo natural. Para a injetividade, sejam $\sum_{i=0}^{n-1} a_i\sigma^i(\theta) = \sum_{i=0}^{n-1} b_i\sigma^i(\theta) \in \mathcal{O}_{\mathbb{K}}$. Assim,

$$\sum_{i=0}^{n-1}(a_i - b_i)\sigma^i(\theta) = 0 \ .$$

Como $\{\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, segue que $a_i = b_i$, para todo $i = 0, \ldots, n-1$ e, então, $\sum_{i=0}^{n-1} a_i\sigma^i = \sum_{i=0}^{n-1} b_i\sigma^i$. Portanto, ψ é um isomorfismo de anéis. Além disso, do produto escalar em anéis de grupos temos que ψ preserva o produto escalar e, desse modo, $\mathbb{Z}\mathcal{G}$

e $\mathcal{O}_{\mathbb{K}}$ também são isomorfos como $\mathbb{Z}$-módulos. ■

Sendo assim, como $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x) = \mathbb{Z}\mathcal{G}x$ e $\mathbb{Z}\mathcal{G} \simeq \mathcal{O}_{\mathbb{K}}$, podemos considerar $\mathcal{A} = \mathcal{O}_{\mathbb{K}}x$, isto é, $\mathcal{A}$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$. Do mesmo modo, podemos dizer que $\mathcal{A}' = \mathbb{Z}\mathcal{G}(\frac{x}{p})$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$. Dessa forma, pelo Corolário 3.3.2, segue que a distância produto mínima é dada por

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \sqrt{\frac{det(G')}{|\mathcal{D}_{\mathbb{K}}|}} \ .$$

Porém, temos que $G' = Id$ e $|\mathcal{D}_{\mathbb{K}}| = p^{n-1}$ (veja Teorema 1.6.1). Logo,

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{\sqrt{p^{n-1}}} \ .$$

Sendo assim, dado n ímpar, o menor primo ímpar p satisfazendo $p \equiv 1(mod\ n)$, fornece o reticulado de menor probabilidade de erros na dimensão n (veja Seção 4.2).

Observação 4.4.2 *Como $\mathbb{K}$ é totalmente real, segue que $\sigma_{\mathbb{K}}(\mathcal{A}') = \sigma_{\gamma}(\mathcal{A}')$, para $\gamma = 1$. Assim, podemos denotar $\sigma_{\mathbb{K}}(\mathcal{A}')$ como sendo o reticulado ideal $(\mathcal{A}', Tr_1)$.*

Algoritmo de Construção

Dados n um inteiro positivo ímpar e p um primo ímpar satisfazendo $p \equiv 1(mod\ n)$, existe uma única extensão cíclica $\mathbb{K}$ de grau n sobre $\mathbb{Q}$, com $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$, tal que p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$ (veja Proposição 4.1.1). Podemos então, definir o $\mathbb{Z}$-módulo $\mathcal{A}'$ e, consequentemente, descrever o reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$. Desse modo, para cada dimensão ímpar n, obtemos uma família de reticulados $\sigma_{\mathbb{K}}(\mathcal{A}')$, variando segundo o parâmetro p primo ímpar satisfazendo $p \equiv 1(mod\ n)$. Note que, para definir a matriz geradora M', devemos obter o elemento $x \in \mathcal{O}_{\mathbb{K}}$, o qual obtemos por recorrência através dos elementos α e z apresentados nesta seção.

Fornecemos então, o seguinte algoritmo de construção:

1. *Escolha uma dimensão ímpar n.*

2. *Escolha um primo ímpar p, satisfazendo $p \equiv 1(mod\ n)$.*

3. *Encontre um elemento r primitivo módulo p ($\overline{r}$ gerador de $\mathbb{Z}_p^*$) e um inteiro λ tal que $\lambda(r-1) \equiv 1(mod\ p)$.*

4. *Calcule $\alpha = \prod_{k=0}^{m-1}(1-\zeta^{r^k})$ e $z = \zeta^{\lambda}\alpha(1-\zeta)$, ambos na base $\{1, \zeta, \ldots, \zeta^{p-2}\}$ de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$, onde $m = (p-1)/2$ e $\zeta = \zeta_p$.*

5. *Calcule* $x = Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(z)$ *e seus conjugados* $\sigma^i(x)$, *para* $i = 1, \ldots, n-1$, *na base* $\{1, \zeta, \ldots, \zeta^{p-2}\}$, *com* $\langle\sigma\rangle = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.

6. *Calcule a matriz geradora* M *de* $\sigma_{\mathbb{K}}(\mathcal{A})$, *utilizando* $\zeta_p = e^{\frac{2\pi i}{p}}$.

7. *Obtenha a matriz geradora* $M' = \frac{1}{p}M$ *de* $\sigma_{\mathbb{K}}(\mathcal{A}')$.

Descrevemos, assim, uma família de reticulados n-dimensionais $\sigma_{\mathbb{K}}(\mathcal{A}')$, com

$$div(\sigma_{\mathbb{K}}(\mathcal{A}')) = n \quad e \quad d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{\sqrt{p^{n-1}}} .$$

Note que, os reticulados obtidos não dependem da escolha dos parâmetros r e λ. Esses elementos definem o elemento x e, consequentemente, a base do reticulado, o qual já está determinado a partir dos parâmetros n e p.

A Tabela 4.2[3] apresenta algumas dimensões e parâmetros correspondentes aos reticulados que podem ser obtidos através do algoritmo.

n	p	r	λ	div	$d_{p,min}$
3	7	3	4	3	$1/7$
3	13	2	1	3	$1/13$
5	11	2	1	5	$1/121$
5	31	3	16	5	$1/961$
7	29	2	1	7	$1/29^3$
11	23	5	6	11	$1/23^5$
11	67	2	1	11	$1/67^5$
13	53	2	1	13	$1/53^6$
17	103	5	26	17	$1/103^8$
19	191	19	138	19	$1/191^9$
23	47	5	12	23	$1/47^{11}$
29	59	2	1	29	$1/59^{14}$

Tabela 4.2:

Exemplo 4.4.1 *Utilizando o algoritmo que descrevemos acima, faremos um exemplo de construção de um reticulado* $\sigma_{\mathbb{K}}(\mathcal{A}')$.

1. *Escolhemos a dimensão* $n = 3$.

2. *Escolhemos* $p = 13$ *satisfazendo* $p \equiv 1 (mod\ 3)$. *Estes dois parâmetros determinam o corpo* $\mathbb{K}$, *o qual não precisamos conhecer explicitamente para obter o reticulado, mas, o faremos aqui. Como vimos,* $\mathbb{K}$ *é corpo intermediário de* $\mathbb{Q} \subset \mathbb{Q}(\zeta_{13})$. *Logo, do Teorema 4.1.1, segue que*

[3]Alguns cálculos foram feitos com auxílio do software Wolfram Mathematica.

$\mathbb{K} = \mathbb{Q}(\theta)$, *com* $\theta = Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{K}}(\zeta_{13})$. *Devemos então determinar* $Gal(\mathbb{Q}(\zeta) : \mathbb{K})$, *onde* $\zeta = \zeta_{13}$. *Como* $\overline{2}$ *é um gerador de* $\mathbb{Z}_{13}^*$, *segue que* $\sigma_2 : \zeta \to \zeta^2$ *é um gerador de* $Gal(\mathbb{Q}(\zeta) : \mathbb{Q})$ *(veja Observação 4.1.2). Desse modo, temos que* $Gal(\mathbb{Q}(\zeta) : \mathbb{K}) = \langle \sigma_2^3 \rangle = \langle \sigma_8 \rangle$, *cuja ordem é* 4 *(veja Proposição 4.1.1).*

$$\begin{array}{c} \mathbb{Q}(\zeta_{13}) \\ {\scriptstyle \langle \sigma_8 \rangle} \Big| {\scriptstyle 4} \\ \mathbb{K} \\ {\scriptstyle \langle \sigma_2|_{\mathbb{K}} \rangle} \Big| {\scriptstyle 3} \\ \mathbb{Q} \end{array}$$

Assim,

$$\begin{aligned} \theta = Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(\zeta) &= \zeta + \sigma_8(\zeta) + \sigma_8^2(\zeta) + \sigma_8^3(\zeta) \\ &= \zeta + \zeta^8 + \zeta^{8^2} + \zeta^{8^3} \\ &= \zeta + \zeta^8 + \zeta^{64} + \zeta^{512} \\ &= \zeta + \zeta^5 + \zeta^8 + \zeta^{12} \ , \end{aligned}$$

pois $64 \equiv 12 (mod\ 13)$ *e* $512 \equiv 5 (mod\ 13)$. *Portanto,* $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^5 + \zeta^8 + \zeta^{12})$ *e, além disso, temos que* $|\mathcal{D}_{\mathbb{K}}| = 13^2$ *(veja Teorema 1.6.1), isto é,* 13 *é o único primo que ramifica em* $\mathcal{O}_{\mathbb{K}}$.

3. *Consideremos o elemento* $r = 2$, *primitivo módulo* 13, *e* $\lambda = 1$ *satisfazendo* $\lambda \equiv 1 (mod\ 13)$.

4. *Temos que,*

$$\begin{aligned} \alpha &= \prod_{k=0}^{5} (1 - \zeta^{2^k}) \\ &= (1-\zeta)(1-\zeta^2)(1-\zeta^4)(1-\zeta^8)(1-\zeta^3)(1-\zeta^6) \\ &= -1 + \zeta - \zeta^2 - \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 - \zeta^8 - \zeta^9 + \zeta^{10} - \zeta^{11} \ . \end{aligned}$$

Logo, $z = \alpha\zeta(1-\zeta) = 1 - \zeta + 2\zeta^2 - 2\zeta^3 + 2\zeta^5 - 2\zeta^9 + 2\zeta^{11} - 2\zeta^{12}$. *Como* $-\zeta^{12} = \zeta^{11} + \ldots + \zeta + 1$, *segue que*

$$z = 3 + \zeta + 4\zeta^2 + 2\zeta^4 + 4\zeta^5 + 2\zeta^6 + 2\zeta^7 + 2\zeta^8 + 2\zeta^{10} + 4\zeta^{11} \ .$$

5. *Dessa forma, utilizando a congruência módulo* 13 *e a igualdade* $\zeta^{12} = -\zeta^{11} - \ldots - \zeta - 1$, *obtemos*

$$\begin{aligned} x = Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(z) &= z + \sigma_8(z) + \sigma_8^2(z) + \sigma_8^3(z) \\ &= 5 + 3\zeta^2 + 3\zeta^3 - \zeta^4 - \zeta^6 - \zeta^7 - \zeta^9 + 3\zeta^{10} + 3\zeta^{11} \ . \end{aligned}$$

Assim, denotando $\sigma = \sigma_2$, temos que

$$\begin{aligned}\sigma(x) &= 5 + 3\sigma(\zeta)^2 + 3\sigma(\zeta)^3 - \sigma(\zeta)^4 - \sigma(\zeta)^6 - \sigma(\zeta)^7 - \sigma(\zeta)^9 + 3\sigma(\zeta)^{10} + 3\sigma(\zeta)^{11} \\ &= 6 + \zeta^2 + \zeta^3 + 4\zeta^4 + 4\zeta^6 + 4\zeta^7 + 4\zeta^9 + \zeta^{10} + \zeta^{11} \ ,\end{aligned}$$

$$\begin{aligned}\sigma^2(x) &= 6 + \sigma(\zeta)^2 + \sigma(\zeta)^3 + 4\sigma(\zeta)^4 + 4\sigma(\zeta)^6 + 4\sigma(\zeta)^7 + 4\sigma(\zeta)^9 + \sigma(\zeta)^{10} + \sigma(\zeta)^{11} \\ &= 2 - 4\zeta^2 - 4\zeta^3 - 3\zeta^4 - 3\zeta^6 - 3\zeta^7 - 3\zeta^9 - 4\zeta^{10} - 4\zeta^{11} \ .\end{aligned}$$

6. *A matriz geradora M de $\sigma_{\mathbb{K}}(\mathcal{A})$ é dada por*

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) \\ \sigma(x) & \sigma^2(x) & x \\ \sigma^2(x) & x & \sigma(x) \end{pmatrix}.$$

Buscando valores numéricos[4] *para as entradas de M e utilizando $\zeta = e^{\frac{2\pi i}{13}}$, obtemos*

$$x = 5 + 3e^{\frac{4\pi i}{13}} + 3e^{\frac{6\pi i}{13}} - e^{\frac{8\pi i}{13}} - e^{\frac{12\pi i}{13}} - e^{\frac{14\pi i}{13}} - e^{\frac{18\pi i}{13}} + 3e^{\frac{20\pi i}{13}} + 3e^{\frac{22\pi i}{13}} = 11,78268 \ ,$$

$$\sigma(x) = 6 + e^{\frac{4\pi i}{13}} + e^{\frac{6\pi i}{13}} + 4e^{\frac{8\pi i}{13}} + 4e^{\frac{12\pi i}{13}} + 4e^{\frac{14\pi i}{13}} + 4e^{\frac{18\pi i}{13}} + e^{\frac{20\pi i}{13}} + e^{\frac{22\pi i}{13}} = -3,22712 \ ,$$

$$\sigma^2(x) = 2 - 4e^{\frac{4\pi i}{13}} - 4e^{\frac{6\pi i}{13}} - 3e^{\frac{8\pi i}{13}} - 3e^{\frac{12\pi i}{13}} - 3e^{\frac{14\pi i}{13}} - 3e^{\frac{18\pi i}{13}} - 4e^{\frac{20\pi i}{13}} - 4e^{\frac{22\pi i}{13}} = 4,44444 \ .$$

Desse modo,

$$M = \begin{pmatrix} 11,78268 & -3,22712 & 4,44444 \\ -3,22712 & 4,44444 & 11,78268 \\ 4,44444 & 11,78268 & -3,22712 \end{pmatrix}.$$

7. *Portanto, temos que*

$$M' = \frac{1}{13}M = \begin{pmatrix} 0,90636 & -0,24824 & 0,34188 \\ -0,24824 & 0,34188 & 0,90636 \\ 0,34188 & 0,90636 & -0,24824 \end{pmatrix}$$

é uma matriz geradora do reticulado $\mathbb{Z}^n$-rotacionado $\sigma_{\mathbb{K}}(\mathcal{A}')$, para $n = 3$ e $p = 13$, do qual $div(\sigma_{\mathbb{K}}(\mathcal{A}')) = 3$ e $d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = 1/13$.

Observação 4.4.3 *Em [18] e [20], o estudo nesse caso de ramificação é feito exigindo que a dimensão n seja um primo ímpar. Aqui, como sugerido em [19], exigimos que n seja apenas ímpar, não necessariamente primo.*

[4]Parte da obtenção dos valores numéricos da matriz M foi feita com auxílio de Wolfram Mathematica.

4.4.2 Caso II: n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$

Dada uma extensão cíclica $\mathbb{Q} \subset \mathbb{K}$ de grau primo ímpar n, tal que n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$, segue pelo Teorema 2.3.3, que n é o único primo na fatoração do discriminante $\mathcal{D}_{\mathbb{K}}$ e, desse modo, o condutor do corpo $\mathbb{K}$ é n^r, para algum inteiro positivo r (veja Teorema 1.6.2). Nesse caso, pelo Lema 2a de [20], segue que $r = 2$, isto é, temos necessariamente $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{n^2})$.

Na seguinte proposição vemos que uma extensão cíclica satisfazendo as condições acima é única e pode ser determinada pela dimensão n.

Proposição 4.4.4 *Dado n primo ímpar, existe um único corpo intermediário $\mathbb{K}$ de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$ que satisfaz $[\mathbb{K} : \mathbb{Q}] = n$. Além disso, $\mathbb{Q} \subset \mathbb{K}$ é cíclica e n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Seja $\mathcal{G} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})$. Temos que $\circ(\mathcal{G}) = n(n-1)$ e $\mathcal{G} \simeq \mathbb{Z}_{n^2}^*$ é cíclico (veja Teorema 1.1.2). Assim, sendo σ um gerador de $\mathcal{G}$, o grupo cíclico $\mathcal{H} := \langle \sigma^n \rangle \leqslant \mathcal{G}$ tem ordem $n-1$ e, como $\mathcal{H} \leqslant \mathcal{G} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})$ e $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$ é galoisiana, segue pelo ítem (i) do Teorema 1.1.1, que $\mathcal{H} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{K})$ para algum corpo intermediário $\mathbb{K}$ de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$. Além disso, pelo ítem (ii) do Teorema 1.1.1, tem-se que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{n^2})$ é galoisiana e $\mathcal{H} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{K})$ é o único subgrupo de $\mathcal{G}$ tal que $[\mathbb{K} : \mathbb{Q}] = n$. Desse modo, $\mathbb{K}$ é o único corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$, de grau n sobre $\mathbb{Q}$.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_{n^2}) & & \{Id\} \\ \Big| {\scriptstyle n-1} & & \Big| \\ \mathbb{K} & \longleftrightarrow & \mathcal{H} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{K}) \\ \Big| {\scriptstyle n} & & \Big| \\ \mathbb{Q} & & \mathcal{G} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q}) \end{array}$$

Afirmamos que $\mathbb{Q} \subseteq \mathbb{K}$ é cíclica. De fato, como $\mathcal{G}$ é abeliano, segue que todo subgrupo de $\mathcal{G}$ é normal e, em particular, $\mathcal{H} = Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{K}) \lhd \mathcal{G}$. Assim, pelo ítem (iii) do Teorema 1.1.1, tem-se $\mathbb{Q} \subseteq \mathbb{K}$ é galoisiana e além disso

$$Gal(\mathbb{K} : \mathbb{Q}) \simeq \frac{Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})}{Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{K})} = \frac{\mathcal{G}}{\mathcal{H}}.$$

Dessa forma, como $\mathcal{G}$ é cíclico, segue que $Gal(\mathbb{K} : \mathbb{Q})$ também o é. Portanto, $\mathbb{Q} \subseteq \mathbb{K}$ é cíclica. Afirmamos que n^2 é o condutor de $\mathbb{K}$. De fato, suponhamos que $m \neq n^2$ é o condutor de $\mathbb{K}$. Assim $m < n^2$ e $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$. Logo, pelo Teorema 1.6.2, temos que $|\mathcal{D}_{\mathbb{K}}| = m^{n-1}$. Por outro lado, como $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{n^2})$, segue do Teorema 1.6.3 que $|\mathcal{D}_{\mathbb{K}}| = n^s$, para algum inteiro s. Assim, $m = n^r$ para algum inteiro r, o que implica que $r < 2$, o que é uma contradição. Portanto, n^2

é o condutor de $\mathbb{K}$. Desse modo, temos que $|\mathcal{D}_{\mathbb{K}}| = n^{2(n-1)}$, o que nos permite concluir que n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$. ■

Lema 4.4.2 *Se n é um primo, então $Tr_{\mathbb{Q}(\zeta_{n^2})/\mathbb{Q}}(\zeta_{n^2}) = 0$.*

Demonstração: O conjunto dos elementos $j = 1, \ldots, n^2$, tal que $mdc(j, n^2) = 1$, é dado por

$$\mathcal{B} = \{1, \ldots, n-1, n+1, \ldots, 2n-1, 2n+1, \ldots, \ldots, (n-1)n-1, (n-1)n+1, \ldots, n^2-1\} \ ,$$

pois se j é um múltiplo de n então $mdc(j, n^2) \neq 1$ e, além disso, os únicos divisores (positivos) de n^2 são 1, n e n^2. Dessa forma, denotando $\zeta = \zeta_{n^2}$, o polinômio ciclotômico $\phi_{n^2}(x)$ é dado por

$$\phi_{n^2}(x) = \prod_{\substack{j=1 \\ mdc(j,n^2)=1}}^{n^2} (1 - \zeta^j) = \prod_{j \in \mathcal{B}} (1 - \zeta^j) \ .$$

Seja σ um gerador de $Gal(\mathbb{Q}(\zeta) : \mathbb{Q})$. Como os conjugados $\sigma^i(\zeta)$ de ζ são exatamente as raízes do seu polinômio minimal, que é o próprio $\phi_{n^2}(x)$, segue que

$$Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = \sum_{i=0}^{n(n-1)-1} \sigma^i(\zeta) = \sum_{j \in \mathcal{B}} \zeta^j \ .$$

Por outro lado,

$$\begin{aligned} \frac{x^{n^2}-1}{x-1} &= x^{n^2-1} + \ldots + x^{(n-1)n+1} + x^{(n-1)n} + x^{(n-1)n-1} + \ldots + x^{n+1} + x^n + x^{n-1} + \ldots + x + 1 \\ &= (x^{n^2-1} + \ldots + x^{(n-1)n+1} + x^{(n-1)n-1} + \ldots + x + 1) + (x^{(n-1)n} + \ldots + x^{2n} + x^n) \\ &= \sum_{j \in \mathcal{B}} x^j + \sum_{k=1}^{n-1} x^{kn} + 1 \ . \end{aligned}$$

Assim, como $\zeta^n = (\zeta_{n^2})^n = \zeta_n$, segue que

$$0 = \frac{\zeta^{n^2}-1}{\zeta - 1} = \sum_{j \in \mathcal{B}} \zeta^j + \sum_{k=1}^{n-1} (\zeta^n)^k + 1 = Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) + Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) + 1 \ .$$

Desse modo, como

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = \sum_{k=1}^{n-1} (\zeta_n)^k = -1 \ ,$$

concluímos que

$$Tr_{\mathbb{Q}(\zeta_{n^2})/\mathbb{Q}}(\zeta_{n^2}) = 0 \ ,$$

o que prova o lema. ■

Teorema 4.4.2 *Sejam n um primo ímpar, $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$, com $[\mathbb{K} : \mathbb{Q}] = n$ e σ um gerador de $Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})$. Se*

$$T = Tr_{\mathbb{Q}(\zeta_{n^2})/\mathbb{K}}(\zeta_{n^2}) \quad e \quad x = 1 + T$$

então

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = \begin{cases} n^2\ , & se\ t = 0 \\ 0\ , & se\ t \neq 0\ , \end{cases}$$

com $t = 0, 1, \ldots, n-1$.

Demonstração: Seja $r \in \{1, \ldots, p-1\}$ tal que $\sigma = \sigma_r$ e denotemos $\zeta = \zeta_{n^2}$. Temos que $Gal(\mathbb{Q}(\zeta) : \mathbb{K}) = \langle \sigma^n \rangle$, e assim

$$T = Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(\zeta) = \sum_{j=1}^{n-1} \sigma^{nj}(\zeta)\ .$$

Desse modo, como $Gal(\mathbb{K} : \mathbb{Q}) = \langle \sigma|_{\mathbb{K}} \rangle$, segue que

$$\begin{aligned}
Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) &= \sum_{a=0}^{n-1} \sigma^a((1+T)\ \sigma^t(1+T)) \\
&= \sum_{a=0}^{n-1} (1 + \sigma^{a+t}(T) + \sigma^a(T) + \sigma^a(T)\sigma^{a+t}(T)) \\
&= n + \sum_{a=0}^{n-1} \sigma^{a+t}(T) + \sum_{a=0}^{n-1} \sigma^a(T) + \sum_{a=0}^{n-1} \sigma^a(T)\sigma^{a+t}(T)) \\
&= n + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \sigma^{a+t+nj}(\zeta) + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \sigma^{a+nj}(\zeta) + \sum_{a=0}^{n-1}\sum_{j,k=1}^{n-1} \sigma^{a+nj}(\zeta)\sigma^{a+t+nk}(\zeta) \\
&= n + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \zeta^{r^{a+t+nj}} + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \zeta^{r^{a+nj}} + \sum_{a=0}^{n-1}\sum_{j,k=1}^{n-1} \zeta^{r^{a+nj}+r^{a+t+nk}} \\
&= n + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \zeta^{r^{a+t+nj}} + \sum_{a=0}^{n-1}\sum_{j=1}^{n-1} \zeta^{r^{a+nj}} + \sum_{a=0}^{n-1}\sum_{d,c=1}^{n-1} \zeta^{(r^{nd}+r^t)r^{a+nc}}\ .
\end{aligned}$$

Para os detalhes sobre a mudança de variáveis feita na última igualdade, veja o Teorema 4.1.2. Note que $(a + nc)$, para $a = 0, \ldots, n-1$ e $c = 1, \ldots, n-1$, percorre os mesmos valores que $s = 0, \ldots, n(n-1) - 1$. O mesmo argumento se aplica para $(a + nj)$. Assim, podemos pôr

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = n + \sum_{s=0}^{n(n-1)-1} \zeta^{r^{t+s}} + \sum_{s=0}^{n(n-1)-1} \zeta^{r^s} + \sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1} \zeta^{(r^{nd}+r^t)r^s}\ .$$

Temos, $Gal(\mathbb{Q}(\zeta):\mathbb{Q}) = \langle\sigma\rangle$ cíclico. Assim podemos escrever

$$\begin{aligned}\langle\sigma\rangle &= \{Id, \sigma, \ldots, \sigma^{n(n-1)-1}\} \\ &= \{\sigma^t \circ Id, \sigma^t \circ \sigma, \ldots, \sigma^t \circ \sigma^{n(n-1)-1}\} \\ &= \{\sigma^t, \sigma^{t+1}, \ldots, \sigma^{t+n(n-1)-1}\}\end{aligned}$$

como uma translação dos elementos de $\langle\sigma\rangle$, resultando apenas numa reordenação de seus elementos. Desse modo,

$$\sum_{s=0}^{n(n-1)-1} \zeta^{r^s} = \sum_{s=0}^{n(n-1)-1} \sigma^s(\zeta) = Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = \sum_{s=0}^{n(n-1)-1} \sigma^{t+s}(\zeta) = \sum_{s=0}^{n(n-1)-1} \zeta^{r^{t+s}} \ .$$

Porém, pelo Lema 4.4.2, temos que $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = 0$. Assim, denotando $\omega_{d,t} = \zeta^{r^{nd}+r^t}$, segue que

$$\begin{aligned}Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) &= n + \sum_{d=1}^{n-1} \sum_{s=0}^{n(n-1)-1} \zeta^{(r^{nd}+r^t)r^s} \\ &= n + \sum_{d=1}^{n-1} \sum_{s=0}^{n(n-1)-1} (\omega_{d,t})^{r^s} \\ &= n + \sum_{d=1}^{n-1} Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) \ .\end{aligned}$$

Note que, $\omega_{d,t}$ é uma raíz do polinômio $x^{n^2} - 1$ e, desse modo, pode satisfazer uma das três seguintes possibilidades:

(a) $\omega_{d,t} = 1$. Nesse caso teremos

$$Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = \sum_{s=1}^{n(n-1)} \sigma^s(1) = \sum_{s=1}^{n(n-1)} 1 = n(n-1) \ .$$

(b) $\omega_{d,t}$ é uma raíz n^2-ésima primitiva da unidade, ou seja, é raíz do polinômio ciclotômico $\phi_{n^2}(x)$. Nesse caso, segue do Lema 4.4.2, que $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = 0$.

(c) $\omega_{d,t}$ é uma raíz n^2-ésima da unidade não primitiva, isto é, é raíz de $x^{n^2} - 1$, mas não é raíz de $\phi_{n^2}(x)$. Nesse caso, como visto no Lema 4.4.2, temos que $\omega_{d,t} = \zeta^{kn}$ com $k \in \{1, \ldots, n-1\}$. Como todo grupo cíclico de ordem $n-1$ é isomorfo a $\mathbb{Z}_{n-1}$, segue que

$$Gal(\mathbb{Q}(\zeta):\mathbb{K}) \simeq \mathbb{Z}_{n-1} \simeq Gal(\mathbb{Q}(\zeta_n):\mathbb{Q}) \ ,$$

e assim $Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(\omega_{d,t}) = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\omega_{d,t}) = -1$, pois $\omega_{d,t} = (\zeta_{n^2})^{kn} = (\zeta_n)^k$ é uma raíz n-ésima primitiva da unidade. Portanto,

$$Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = Tr_{\mathbb{K}/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(\omega_{d,t})) = Tr_{\mathbb{K}/\mathbb{Q}}(-1) = \sum_{j=0}^{n-1} -1 = -n \ .$$

Afirmamos que

$$\omega_{d,t} = 1 \iff t = 0 \text{ e } d = \frac{n-1}{2} \ .$$

De fato, suponhamos que $t = 0$ e $d = (n-1)/2$. Temos que $\overline{r}$ é gerador de $\mathbb{Z}_{n^2}^*$. Logo $r^{n(n-1)} \equiv 1(mod\ n^2)$. Como $n(n-1) = n^2 - n$ é par, segue que existe $m \in \mathbb{Z}$ tal que $n(n-1) = 2m$. Logo, $(r^m)^2 = r^{2m} \equiv 1(mod\ n^2)$. Assim, $n^2 \mid (r^m)^2 - 1 = (r^m + 1)(r^m - 1)$ e como $mdc(n^2, r^m - 1) = 1$, segue que $n^2 \mid (r^m + 1)$. Dessa forma, $r^{\frac{n(n-1)}{2}} + 1 \equiv 0(mod\ n^2)$ e, portanto,

$$\omega_{d,t} = \zeta^{r^{nd}+1} = \zeta^{r^{n(\frac{n-1}{2})}+1} = 1 \ .$$

Reciprocamente, suponhamos que $\omega_{d,t} = 1$, isto é, $\zeta^{r^{nd}+r^t} = 1$. Assim

$$\begin{aligned} r^{nd} + r^t \equiv 0(mod\ p) &\Leftrightarrow r^{nd} \equiv -r^t(mod\ n^2) \\ &\Leftrightarrow r^{nd} \equiv r^{m+t}(mod\ n^2) \\ &\Leftrightarrow m + t \equiv nd(mod\ n(n-1)) \\ &\Leftrightarrow \exists\ k_1 \in \mathbb{Z} \text{ tal que } t = nd - m + k_1 n(n-1) \ . \end{aligned}$$

Desse modo, como $n \mid nd$, $n \mid m$ e $n \mid k_1 n(n-1)$, segue que $n \mid t$, com $t = 0, 1, \ldots, n-1$. Logo $t = 0$. Neste caso, $nd = m - k_1 n(n-1)$ e, assim,

$$d = \frac{n-1}{2} - k_1(n-1) = \frac{n-1}{2}(1 - 2k_1) = k_2(\frac{n-1}{2}), \text{ com } k_2 = 1 - 2k_1 \text{ ímpar} \ .$$

Note que k_2 deve ser positivo, pois caso contrário teríamos $d \leq 0$. Porém, só se pode ter $k_2 = 1$ ou 2, pois se $k_2 \geq 3$ teríamos $d > n - 1$. Mas, como k_2 é ímpar, resta somente $k_2 = 1$. Portanto $d = (n-1)/2$, o que conclui a demonstração da equivalência. Façamos, então, o cálculo de $Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x))$, distinguindo os casos $t = 0$ e $t \neq 0$. Suponhamos que $t = 0$. No caso $d = (n-1)/2$ temos $\omega_{d,t} = 1$ e, assim, $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = n(n-1)$. Consideremos o caso $d \neq (n-1)/2$. Temos que $\omega_{d,t} \neq 1$, restando somente duas possibilidades: $\omega_{d,t}$ ser raíz primitiva ou não. Suponhamos que $\omega_{d,t}$ não é uma raíz primitiva, isto é, $\omega_{d,t} = \zeta^{kn}$ para algum $k = 1, \ldots, n-1$. Assim,

$$\zeta^{r^{nd}+1} = \zeta^{kn} \Rightarrow r^{nd} + 1 \equiv kn(mod\ n^2) \Rightarrow r^{nd} + 1 \equiv kn(mod\ n) \Rightarrow r^{nd} + 1 \equiv 0(mod\ n) \ .$$

Porém, $r^m \equiv -1(mod\ n^2)$, o que implica que $r^m \equiv -1(mod\ n)$. Logo

$$r^{nd} \equiv r^m(mod\ n) \Rightarrow nd \equiv m(mod\ n-1) \Rightarrow \exists\ k_3 \in \mathbb{Z} \text{ tal que } k_3(n-1) = nd - \frac{n(n-1)}{2}\ .$$

Note que $n \mid k_3(n-1)$, e assim $n \mid k_3$. Dessa forma,

$$d = \frac{n-1}{2} + \frac{k_3}{n}(n-1) = \frac{n-1}{2}\left(1 + 2\frac{k_3}{n}\right) = \left(\frac{n-1}{2}\right)k_4, \quad \text{com } k_4 = 1 + 2\frac{k_3}{n} \text{ ímpar}\ .$$

Assim, temos $k_4 = 1$, o que implica que $d = (n-1)/2$, o que é uma contradição. Portanto, para $d \neq (n-1)/2$ temos que $\omega_{d,t}$ é uma raíz n^2-ésima primitiva da unidade e, dessa forma, $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = 0$. Podemos então concluir que, para $t = 0$,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = n + \sum_{d=1}^{n-1} Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = n + n(n-1) = n^2\ .$$

Suponhamos agora que $t \neq 0$. Temos $\omega_{d,t} \neq 1$, restando as possibilidades de $\omega_{d,t}$ ser primitiva ou não. Analizemos o caso em que $\omega_{d,t}$ é raíz n^2-ésima não primitiva. Esse caso acontece se, e somente se, $\omega_{d,t} = \zeta^{kn}$, para algum $k = 1, \ldots, n-1$. Assim, temos que

$$r^{nd} + r^t \equiv kn(mod\ n^2) \Rightarrow r^{nd} \equiv -r^t(mod\ n) \Rightarrow r^{nd} \equiv r^{m+t}(mod\ n) \Rightarrow nd \equiv m + t(mod\ n-1)\ .$$

Logo, existe $k_5 \in \mathbb{Z}$ tal que $k_5(n-1) = nd - m - t$, e portanto $d = \frac{t-k_5}{n} + \frac{n-1}{2} + k_5$. Além disso, temos que $n \mid (t + k_5 n - k_5)$ e como $n \mid k_5 n$ segue que existe $k' \in \mathbb{Z}$ tal que $k_5 = t + k'n$. Desse modo, podemos escrever $d = k'(n-1) + \frac{n-1}{2} + t$. Note que não se pode ter $k' < 0$ pois teríamos valores negativos para d em alguns casos de t. Afirmamos que $k' = 0$. De fato, se $k' = 1$ então $d > n-1$, o que é uma contradição. E se $k' > 1$ então $k'(n-1) > n-1$, o que implica que $d = k'(n-1) + \frac{n-1}{2} + t > k'(n-1) > n-1$, uma contradição. Portanto, $k' = 0$ e assim $d = \frac{n-1}{2} + t$, para cada $t = 1, \ldots, n-1$. Dessa forma, temos, para cada $t = 1, \ldots, n-1$, um único valor de d tal que $\omega_{d,t}$ não é primitiva. E como $\omega_{d,t} \neq 1$, segue que todas as demais são primitivas. Assim, podemos concluir que, para $t \neq 0$,

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^t(x)) = n + \sum_{d=1}^{n-1} Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega_{d,t}) = n - n = 0\ ,$$

o que conclui a demonstração. ∎

Proposição 4.4.5 *Nas mesmas hipóteses do Teorema 4.4.2, temos que o conjunto*

$$\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$$

é um $\mathbb{Z}$-módulo livre de posto n, contido no anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Demonstração: A demonstração é análoga à da Proposição 4.4.2.

Observação 4.4.4 *Seja $\mathcal{G} = Gal(\mathbb{K} : \mathbb{Q})$. Pela Proposição 4.3.3, temos que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}\mathcal{G}$-módulo livre de posto unitário cuja base é $\{x\}$, isto é, $\mathcal{A} = \mathbb{Z}\mathcal{G}x$, o qual pode ser visto como um ideal principal cujo gerador é x.*

Obtenção do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$

Sejam $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$, com n primo ímpar, $[\mathbb{K} : \mathbb{Q}] = n$ e σ um gerador de $Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})$. Temos que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}$-módulo livre de posto finito n, contido em $\mathcal{O}_{\mathbb{K}}$, onde $x \in \mathcal{O}_{\mathbb{K}}$ é o elemento definido no Teorema 4.4.2. Consideremos o reticulado algébrico n-dimensional $\sigma_{\mathbb{K}}(\mathcal{A})$, do qual o conjunto

$$\{\sigma_{\mathbb{K}}(x), \sigma_{\mathbb{K}}(\sigma(x)), \ldots, \sigma_{\mathbb{K}}(\sigma^{n-1}(x))\}$$

é uma base e

$$M = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{n-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-1}(x) & x & \cdots & \sigma^{n-2}(x) \end{pmatrix}$$

é uma matriz geradora. Assim, denotando por $G = (g_{ij})_{i,j=0}^{n-1}$ a matriz Gram de $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M, temos que cada termo de $G = MM^t$ é dado por

$$g_{ij} = \langle \sigma_{\mathbb{K}}(\sigma^i(x)), \sigma_{\mathbb{K}}(\sigma^j(x)) \rangle = Tr_{\mathbb{K}/\mathbb{Q}}(x\ \sigma^{j-i}(x)) \overset{(*)}{=} n^2\delta_{ij}\ ,$$

com $i, j = 0, 1, \ldots, n-1$, onde a igualdade $(*)$ segue do Teorema 4.4.2. Dessa forma, a matriz Gram do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M tem a seguinte característica

$$G = \begin{pmatrix} n^2 & 0 & \cdots & 0 \\ 0 & n^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n^2 \end{pmatrix} = n^2 Id.$$

Sendo assim, podemos rotacionar o reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ sobre o $\mathbb{Z}^n$. Definindo $M' = \frac{1}{n}M$, temos que M' é uma matriz geradora do reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$, onde

$$\mathcal{A}' = \mathbb{Z}\frac{x}{n} + \mathbb{Z}\frac{\sigma(x)}{n} + \ldots + \mathbb{Z}\frac{\sigma^{n-1}(x)}{n} \subset \mathbb{K}$$

é um $\mathbb{Z}$-módulo livre de posto n. Desse modo, a matriz Gram G' de $\sigma_{\mathbb{K}}(\mathcal{A}')$ com respeito à M' é dada por

$$G' = M'M'^t = \frac{1}{n}M\frac{1}{n}M^t = \frac{1}{n^2}G = Id \ .$$

Logo, $\sigma_{\mathbb{K}}(\mathcal{A}')$ é isomorfo à $\mathbb{Z}^n$, ou seja, é um reticulado $\mathbb{Z}^n$-rotacionado. Como $n = [\mathbb{K} : \mathbb{Q}]$ é ímpar, segue da Proposição 4.1.2 que $\mathbb{K}$ é totalmente real. Logo, $\sigma_{\mathbb{K}}(\mathcal{A}')$ tem diversidade máxima n. Além disso, como o ideal $\mathcal{A}' = \mathbb{Z}\mathcal{G}(\frac{x}{n})$ é principal, segue pelo Corolário 3.3.2 que a distância produto mínima é dada por

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \sqrt{\frac{det(G')}{|\mathcal{D}_{\mathbb{K}}|}} \ .$$

Porém, temos que $G' = Id$ e $|\mathcal{D}_{\mathbb{K}}| = n^{2(n-1)}$ (veja Proposição 4.4.4). Logo,

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{n^{n-1}} \ .$$

Desse modo, a distância produto do reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$ depende somente do parâmetro n.

Observação 4.4.5 *Podemos denotar $\sigma_{\mathbb{K}}(\mathcal{A}')$ como sendo o reticulado ideal $(\mathcal{A}', Tr_1)$, pois $\mathbb{K}$ é totalmente real.*

Algoritmo de Construção

Dado um primo ímpar n, existe uma única extensão cíclica $\mathbb{K}$ de grau n sobre $\mathbb{Q}$, com $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{n^2})$, tal que n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}}$ (veja Proposição 4.4.4). Podemos assim, definir o $\mathbb{Z}$-módulo $\mathcal{A}'$ e, consequentemente, descrever o reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$. Desse modo, para cada dimensão prima ímpar n obtemos um reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$. Note que, para definir o reticulado basta apresentar sua matriz geradora M', e para isso devemos calcular o elemento $x \in \mathcal{O}_{\mathbb{K}}$ e seus conjugados $\sigma^i(x),\ i = 1, \ldots, n-1$. Sendo assim, fornecemos o seguinte algoritmo de construção:

1. *Escolha uma dimensão prima ímpar n.*

2. *Encontre um elemento r primitivo módulo n^2 ($\overline{r}$ gerador de $\mathbb{Z}_{n^2}^*$).*

3. *Calcule $x = 1 + Tr_{\mathbb{Q}(\zeta_{n^2})/\mathbb{K}}(\zeta_{n^2})$ e seus conjugados $\sigma^i(x)$, para $i = 1, \ldots, n-1$, onde σ é um gerador de $Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q})$.*

4. *Calcule a matriz geradora M de $\sigma_{\mathbb{K}}(\mathcal{A})$, utilizando $\zeta_{n^2} = e^{\frac{2\pi i}{n^2}}$.*

5. *Obtenha a matriz geradora $M' = \frac{1}{n}M$ de $\sigma_{\mathbb{K}}(\mathcal{A}')$.*

Descrevemos, assim, uma família de reticulados n-dimensionais $\sigma_{\mathbb{K}}(\mathcal{A}')$, com

$$div(\sigma_{\mathbb{K}}(\mathcal{A}')) = n \quad e \quad d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{n^{n-1}} .$$

A Tabela 4.3[5] apresenta algumas dimensões e parâmetros correspondentes aos reticulados que podem ser obtidos através do algoritmo.

n	r	div	$d_{p,min}$
3	2	3	$1/9$
5	2	5	$1/625$
7	3	7	$1/117649$
11	2	11	$1/11^{10}$
13	2	13	$1/13^{12}$
17	3	17	$1/17^{16}$
19	2	19	$1/19^{18}$
23	5	23	$1/23^{22}$
29	2	29	$1/29^{28}$

Tabela 4.3:

Exemplo 4.4.2 *Faremos agora um exemplo de construção de um reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$ utilizando o algoritmo descrito acima.*

1. *Escolhemos a dimensão $n = 3$.*

2. *Consideremos o elemento $r = 2$, primitivo módulo 9 ($\overline{2}$ é gerador do grupo multiplicativo $\mathbb{Z}_9^*$).*

3. *Calculemos $x = 1 + Tr_{\mathbb{Q}(\zeta_9)/\mathbb{K}}(\zeta_9)$. Para isso devemos conhecer um gerador de $Gal(\mathbb{Q}(\zeta_9) : \mathbb{K})$; denotemos $\zeta = \zeta_9$. Como $\overline{2}$ é um gerador de $\mathbb{Z}_9^*$, segue que $\sigma_2 : \zeta \to \zeta^2$ é um gerador de $Gal(\mathbb{Q}(\zeta) : \mathbb{Q})$. Assim, $Gal(\mathbb{Q}(\zeta) : \mathbb{K}) = \langle \sigma_2^3 \rangle = \langle \sigma_8 \rangle$, cuja ordem é 2. Logo $Gal(\mathbb{Q}(\zeta) : \mathbb{K}) = \{Id, \sigma_8\}$.*

$$\begin{array}{c} \mathbb{Q}(\zeta_9) \\ {\scriptstyle \langle \sigma_8 \rangle} \,\big|\, 2 \\ \mathbb{K} \\ {\scriptstyle \langle \sigma_2|_{\mathbb{K}} \rangle} \,\big|\, 3 \\ \mathbb{Q} \end{array}$$

Dessa forma,

$$x = 1 + Tr_{\mathbb{Q}(\zeta)/\mathbb{K}}(\zeta) = 1 + \zeta + \sigma_8(\zeta) = 1 + \zeta + \zeta^8,$$

e denotando $\sigma = \sigma_2$, temos que

[5] Alguns cálculos foram feitos com auxílio do software Wolfram Mathematica.

$$\sigma(x) = \sigma(1+\zeta+\zeta^8) = 1+\zeta^2+\zeta^7,$$
$$\sigma^2(x) = \sigma^2(1+\zeta+\zeta^8) = 1+\zeta^4+\zeta^5.$$

4. *A matriz M geradora de $\sigma_{\mathbb{K}}(\mathcal{A})$ é dada por*

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) \\ \sigma(x) & \sigma^2(x) & x \\ \sigma^2(x) & x & \sigma(x) \end{pmatrix}.$$

Buscando valores numéricos para as entradas de M e utilizando $\zeta = e^{\frac{2\pi i}{9}}$, obtemos

$$x = 1 + e^{\frac{2\pi i}{9}} + e^{\frac{16\pi i}{9}} = 2,53209\ ,$$
$$\sigma(x) = 1 + e^{\frac{4\pi i}{9}} + e^{\frac{14\pi i}{9}} = 1,3473\ ,$$
$$\sigma^2(x) = 1 + e^{\frac{8\pi i}{9}} + e^{\frac{10\pi i}{9}} = -0,879385\ .$$

Desse modo,

$$M = \begin{pmatrix} 2,53209 & 1,3473 & -0,879385 \\ 1,3473 & -0,879385 & 2,53209 \\ -0,879385 & 2,53209 & 1,3473 \end{pmatrix}.$$

5. *Portanto, temos que*

$$M' = \frac{1}{3}M = \begin{pmatrix} 0,84403 & 0,4491 & -0,29313 \\ 0,4491 & -0,29313 & 0,84403 \\ -0,29313 & 0,84403 & 0,4491 \end{pmatrix}$$

é uma matriz geradora do reticulado $\mathbb{Z}^n$-rotacionado $\sigma_{\mathbb{K}}(\mathcal{A}')$ para $n = 3$, com $div(\sigma_{\mathbb{K}}(\mathcal{A}')) = 3$ e $d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = 1/9$.

4.4.3 Caso III: pelo menos dois primos ramificam em $\mathcal{O}_{\mathbb{K}}$, com n primo ímpar

Dada uma extensão cíclica $\mathbb{Q} \subset \mathbb{K}$ de grau primo ímpar, consideramos durante a construção o caso em que exatamente dois primos ramificam em $\mathcal{O}_{\mathbb{K}}$, de modo que o caso onde mais que dois primos ramificam pode ser trabalhado por recorrência.

Proposição 4.4.6 *Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão cíclica de grau n primo ímpar e p_1 e p_2 são os únicos primos (distintos) que ramificam em $\mathcal{O}_{\mathbb{K}}$, então:*

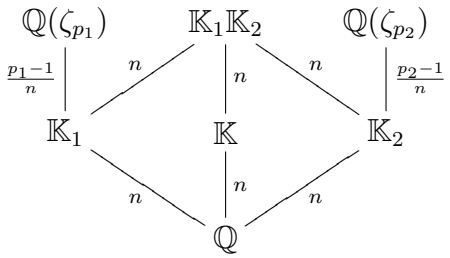
(i) p_1p_2 é condutor de $\mathbb{K}$, se $n \neq p_1$ e $n \neq p_2$;

(ii) p_1n^2 é condutor de $\mathbb{K}$, se $n \neq p_1$ e $n = p_2$.

Demonstração: Pelo Teorema 1.1.3, temos que $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$, para algum inteiro positivo m. Suponhamos que m seja o condutor de $\mathbb{K}$. Pelo Teorema 1.6.2, segue que $|\mathcal{D}_{\mathbb{K}}| = m^{n-1}$. Como p_1 e p_2 são os únicos primos que ramificam em $\mathcal{O}_{\mathbb{K}}$, então são os únicos primos na fatoração de $\mathcal{D}_{\mathbb{K}}$ e, assim, são os únicos primos na fatoração de m, isto é, existem r_1 e r_2 inteiros positivos tal que $m = p_1^{r_1}p_2^{r_2}$. Desse modo, pelo Lema $2a$ de [20], segue que $r_1 = r_2 = 1$ no caso em que $n \neq p_1$ e $n \neq p_2$, e no caso $n \neq p_1$ e $n = p_2$ tem-se que $r_1 = 1$ e $r_2 = 2$. ∎

Proposição 4.4.7 *Se n é um primo ímpar e p_1 e p_2 são primos distintos tal que $p_i \equiv 1(mod\ n)$, com $i = 1, 2$, então existe uma extensão cíclica $\mathbb{Q} \subset \mathbb{K}$ de grau n, tal que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_i$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p_i})$ com $[\mathbb{K}_i : \mathbb{Q}] = n$, em que p_i é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_i}$, com $i = 1, 2$.*

Demonstração: Como $p_i \equiv 1(mod\ n)$, segue pela Proposição 4.1.1 que existe uma única extensão cíclica $\mathbb{Q} \subset \mathbb{K}_i$ de grau n, com $\mathbb{K}_i \subset \mathbb{Q}(\zeta_{p_i})$, para $i = 1, 2$. Como $\mathbb{Q} \subset \mathbb{K}_i$ é galoisiana, segue que $\mathbb{Q} \subset \mathbb{K}_1\mathbb{K}_2$ e, consequentemente, $\mathbb{K}_i \subset \mathbb{K}_1\mathbb{K}_2$ são galoisianas, para $i = 1, 2$. Além disso, $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_i) \simeq Gal(\mathbb{K}_j : \mathbb{K}_1 \cap \mathbb{K}_2)$, com $i \neq j$. Mas como $mdc(p_1, p_2) = 1$, temos que $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$, e assim $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_i) \simeq Gal(\mathbb{K}_j : \mathbb{Q})$. Logo, $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_i] = \circ(Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_i)) = n$, com $i = 1, 2$. Desse modo, temos que $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}] = n^2$. Assim, como n é primo e divide $\circ(Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}))$, segue que existe um subgrupo $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$ de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q})$, de ordem n, onde $\mathbb{K}$ é um corpo intermediário de $\mathbb{Q} \subset \mathbb{K}_1\mathbb{K}_2$.

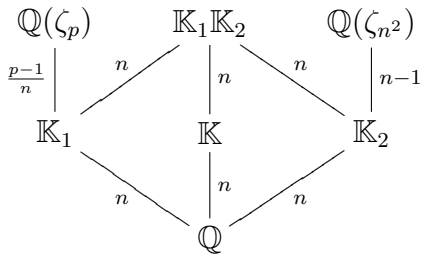


Como $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$, segue que $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}) \simeq Gal(\mathbb{K}_1 : \mathbb{Q}) \times Gal(\mathbb{K}_2 : \mathbb{Q})$ é abeliano. Logo, $\mathbb{Q} \subset \mathbb{K}$ é galoisiana e, assim, $\circ(Gal(\mathbb{K} : \mathbb{Q})) = [\mathbb{K} : \mathbb{Q}] = n$, sendo n primo. Portanto $\mathbb{Q} \subset \mathbb{K}$ é cíclica de grau n, com $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. ∎

A seguinte proposição é um resultado análogo à Proposição 4.4.7, pondo $p_1 = p$ e $p_2 = n$.

Proposição 4.4.8 *Se n e p são primos ímpares tal que $p \equiv 1(mod\ n)$, então existe uma extensão cíclica $\mathbb{Q} \subset \mathbb{K}$ de grau n, tal que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_1$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ com $[\mathbb{K}_1 : \mathbb{Q}] = n$, e $\mathbb{K}_2$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$ com $[\mathbb{K}_2 : \mathbb{Q}] = n$.*

Demonstração: A prova é análoga à da Proposição 4.4.7.



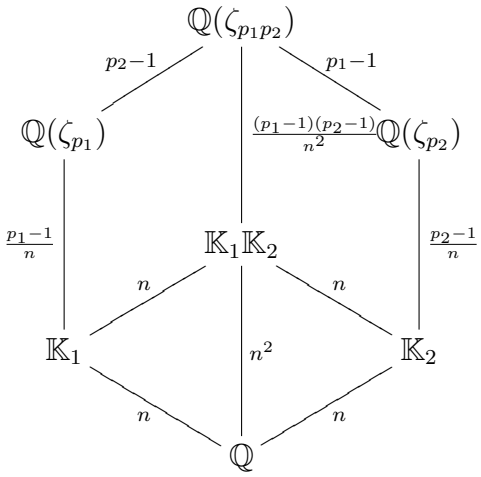
Observação 4.4.6 *A Proposição 4.4.7 (respectivamente 4.4.8) não garante a unicidade de $\mathbb{K}$, e que p_1 e p_2 (respectivamente n e p) ramificam em $\mathcal{O}_{\mathbb{K}}$. Sendo assim, nos próximos resultados supomos, como hipótese, a asserção de que exatamente dois primos ramificam.*

Proposição 4.4.9 *Sejam n um primo ímpar e p_1 e p_2 primos distintos tal que $p_i \equiv 1(mod\ n)$ e $p_i \not\equiv 1(mod\ n^2)$, com $i = 1, 2$. Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão cíclica de grau n tal que p_1 e p_2 são os únicos primos que ramificam em $\mathcal{O}_{\mathbb{K}}$, então $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_i$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p_i})$ com $[\mathbb{K}_i : \mathbb{Q}] = n$, em que p_i é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_i}$, para $i = 1, 2$.*

Demonstração: Temos que $\zeta_{p_2} = e^{\frac{2\pi i}{p_2}} = (e^{\frac{2\pi i}{p_1 p_2}})^{p_1} = (\zeta_{p_1p_2})^{p_1} \in \mathbb{Q}(\zeta_{p_1p_2})$, o que implica que $\mathbb{Q}(\zeta_{p_2}) \subset \mathbb{Q}(\zeta_{p_1p_2})$. Analogamente, $\mathbb{Q}(\zeta_{p_1}) \subset \mathbb{Q}(\zeta_{p_1p_2})$. Assim $\mathbb{K}_1\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{p_1})\mathbb{Q}(\zeta_{p_2}) \subset \mathbb{Q}(\zeta_{p_1p_2})$, onde $\mathbb{K}_i$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p_i})$, para $i = 1, 2$, obtido na Proposição 4.1.1. Porém,

$$[\mathbb{Q}(\zeta_{p_1})\mathbb{Q}(\zeta_{p_2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p_1}) : \mathbb{Q}][\mathbb{Q}(\zeta_{p_2}) : \mathbb{Q}] = \varphi(p_1)\varphi(p_2) = \varphi(p_1p_2) = [\mathbb{Q}(\zeta_{p_1p_2}) : \mathbb{Q}] \ ,$$

onde φ é a função de Euller. Assim $\mathbb{Q}(\zeta_{p_1})\mathbb{Q}(\zeta_{p_2}) = \mathbb{Q}(\zeta_{p_1p_2})$. Desse modo, usando a mesma argumentação feita na Proposição 4.4.7, podemos apresentar a seguinte torre de extensões:



Pela Proposição 4.4.6, temos que $\mathbb{K} \subset \mathbb{Q}(\zeta_{p_1p_2})$. Mostremos que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. Seja $\mathcal{G} = Gal(\mathbb{Q}(\zeta_{p_1p_2}) : \mathbb{Q})$. Como $mdc(p_1, p_2) = 1$, segue que $\mathbb{Q}(\zeta_{p_1}) \cap \mathbb{Q}(\zeta_{p_2}) = \mathbb{Q}$. Logo,

$$\begin{aligned} \mathcal{G} \simeq Gal(\mathbb{Q}(\zeta_{p_1}) : \mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_{p_2}) : \mathbb{Q}) &\simeq \mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \\ &\simeq \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_{\frac{p_1-1}{n}} \times \mathbb{Z}_{\frac{p_2-1}{n}} \ . \end{aligned}$$

Desse modo, como $p_i \not\equiv 1(mod\ n^2)$, segue que o produto acima pode ser visto como o produto (unicamente representado) dos n-subgrupos de Sylow com os q_i-subgrupos de Sylow de $\mathcal{G}$, onde $q_i \neq n$, ou seja, $mdc(q_i, n) = 1$. Seja $\mathcal{H} = Gal(\mathbb{Q}(\zeta_{p_1p_2}) : \mathbb{K}_1\mathbb{K}_2)$. Assim $\mathcal{H} \leqslant \mathcal{G}$, com $\circ(\mathcal{H}) = \frac{p_1-1}{n}\frac{p_2-1}{n}$. Dessa forma, $\mathcal{H}$ corresponde ao produto dos q_i-subgrupos de Sylow de $\mathcal{G}$, pois $mdc(\circ(\mathcal{H}), n) = 1$. Seja agora, $\mathcal{I} = Gal(\mathbb{Q}(\zeta_{p_1p_2}) : \mathbb{K})$. Temos que $\mathcal{I} \leqslant \mathcal{G}$ é abeliano com $\circ(\mathcal{I}) = \frac{(p_1-1)(p_2-1)}{n} = n\frac{p_1-1}{n}\frac{p_2-1}{n}$. Logo, $\mathcal{I}$ possui um subgrupo $\mathcal{J}$ de ordem $\frac{p_1-1}{n}\frac{p_2-1}{n}$. Sendo assim, $\mathcal{J}$ também corresponde ao produto dos q_i-subgrupos de Sylow de $\mathcal{G}$ em que $mdc(q_i, n) = 1$ e, pela unicidade de representação, segue que $\mathcal{J} = \mathcal{H}$. Dessa forma, $\mathcal{H} \leqslant \mathcal{I}$ e, portanto, $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. ∎

A seguinte proposição é um resultado análogo à Proposição 4.4.9, considerando agora o caso em que n ramifica em $\mathcal{O}_{\mathbb{K}}$.

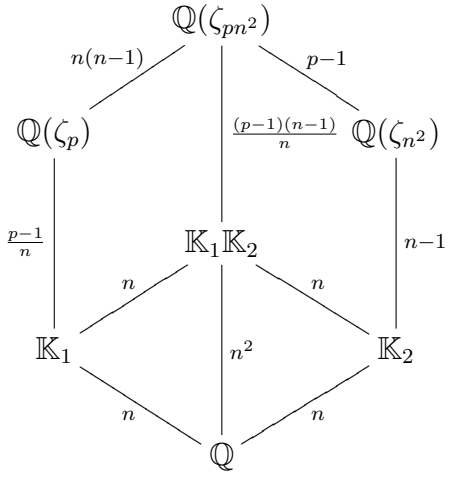
Proposição 4.4.10 *Sejam n e p primos ímpares tal que $p \equiv 1(mod\ n)$ e $p \not\equiv 1(mod\ n^2)$. Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão cíclica de grau n, tal que p e n são os únicos primos que ramificam em $\mathcal{O}_{\mathbb{K}}$, então $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_1$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ com $[\mathbb{K}_1 : \mathbb{Q}] = n$, em que p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_1}$; e $\mathbb{K}_2$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$ com $[\mathbb{K}_2 : \mathbb{Q}] = n$, em que n é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_2}$.*

Demonstração: Temos que $\mathbb{K}_1\mathbb{K}_2 \subset \mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_{n^2}) \subset \mathbb{Q}(\zeta_{pn^2})$, onde $\mathbb{K}_1$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ obtido na Proposição 4.1.1 e $\mathbb{K}_2$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$ obtido

na Proposição 4.4.4. Porém,

$$[\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}][\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q}] = \varphi(p)\varphi(n^2) = \varphi(pn^2) = [\mathbb{Q}(\zeta_{pn^2}) : \mathbb{Q}] \ ,$$

onde φ é a função de Euller. Assim $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_{n^2}) = \mathbb{Q}(\zeta_{pn^2})$. Desse modo, podemos apresentar a seguinte torre de extensões:



Pela Proposição 4.4.6, temos que pn^2 é o condutor de $\mathbb{K}$. Mostremos que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. Seja $\mathcal{G} = Gal(\mathbb{Q}(\zeta_{pn^2}) : \mathbb{Q})$. Como $mdc(p, n^2) = 1$, segue que $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_{n^2}) = \mathbb{Q}$. Logo,

$$\begin{aligned} \mathcal{G} \simeq Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q}) &\simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{n(n-1)} \\ &\simeq \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_{\frac{p-1}{n}} \times \mathbb{Z}_{n-1} \ . \end{aligned}$$

Seja $\mathcal{H} = Gal(\mathbb{Q}(\zeta_{pn^2}) : \mathbb{K}_1\mathbb{K}_2)$ e $\mathcal{I} = Gal(\mathbb{Q}(\zeta_{pn^2}) : \mathbb{K})$. Temos que $\mathcal{H} \leqslant \mathcal{G}$ com $\circ(\mathcal{H}) = \frac{(p-1)(n-1)}{n}$ e $\mathcal{I} \leqslant \mathcal{G}$ com $\circ(\mathcal{I}) = (p-1)(n-1) = n\frac{(p-1)(n-1)}{n}$. Desse modo, como $\circ(\mathcal{H})$ divide $\circ(\mathcal{I})$, segue que $\mathcal{H} \leqslant \mathcal{I}$ e, portanto, $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. ∎

Proposição 4.4.11 *Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ extensões cíclicas disjuntas (isto é, $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$) com $Gal(\mathbb{K}_1 : \mathbb{Q}) = \langle\sigma\rangle$, $Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle\tau\rangle$ e $\mathbb{Q} \subset \mathbb{K}$ uma extensão cíclica de grau n, com $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$. Se existem $x_1 \in \mathbb{K}_1$ e $x_2 \in \mathbb{K}_2$ tal que*

(i) $Tr_{\mathbb{K}_1/\mathbb{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p_1^2$,

(ii) $Tr_{\mathbb{K}_2/\mathbb{Q}}(x_2\tau^t(x_2)) = \delta_{0,t}p_2^2$, $\quad t = 0, 1, \ldots, n-1$;

então existe $x \in \mathbb{K}$, dado por $x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2)$, tal que

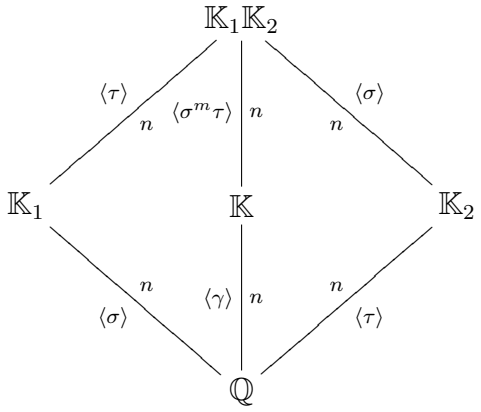
$$Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) = \delta_{0,t}p_1^2p_2^2 \ ,$$

para $t = 0, 1, \ldots, n-1$, onde γ é um gerador de $Gal(\mathbb{K} : \mathbb{Q})$.

Demonstração: Temos que $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}) \simeq Gal(\mathbb{K}_1 : \mathbb{Q}) \times Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle$, pois $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$, o que também garante $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_2) \simeq Gal(\mathbb{K}_1 : \mathbb{Q}) = \langle\sigma\rangle$ e $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}_1) \simeq Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle\tau\rangle$. Desse modo, se $y_i \in \mathbb{K}_i$, com $i = 1, 2$, então

$$\begin{aligned} Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{Q}}(y_1y_2) &= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}(\sigma^k\tau^j)(y_1y_2) \\ &= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}(\sigma^k\tau^j)(y_1)(\sigma^k\tau^j)(y_2) \\ &= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\sigma^k(y_1)\tau^j(y_2) \\ &= \sum_{k=0}^{n-1}\sigma^k(y_1)\sum_{j=0}^{n-1}\tau^j(y_2) \\ &= Tr_{\mathbb{K}_1/\mathbb{Q}}(y_1)Tr_{\mathbb{K}_2/\mathbb{Q}}(y_2)\ . \end{aligned}$$

Por outro lado, como $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$ é cíclico (pois tem ordem prima n) e é um subgrupo de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}) = \{\sigma^k\tau^j;\ j, k = 0, \ldots, n-1\}$, segue que existem $r, s \in \{0, \ldots, n-1\}$ tal que $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}) = \langle\sigma^r\tau^s\rangle$. Porém, todo elemento não unitário de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K}) \simeq \mathbb{Z}_n$ é um gerador. Assim, tomando s' tal que $\tau^{ss'} = \tau$, temos que $\sigma^{rs'}\tau = (\sigma^r\tau^s)^{s'}$ também é seu gerador. Logo, pondo $m = rs'$, podemos escrever $\langle\sigma^m\tau\rangle = Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$. Além disso, como $Gal(\mathbb{K} : \mathbb{Q}) \simeq \mathbb{Z}_n$, segue que podemos escolher $\gamma = \sigma^{-m}\tau|_{\mathbb{K}}$ como seu gerador.



Assim,

$$x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2) = \sum_{b=0}^{n-1}(\sigma^m\tau)^b(x_1x_2) = \sum_{b=0}^{n-1}\sigma^{mb}(x_1)\tau^b(x_2)\ ,$$

o que implica

$$x\gamma^t(x) = \sum_{b=0}^{n-1}\sigma^{mb}(x_1)\tau^b(x_2)\sum_{c=0}^{n-1}\sigma^{-mt}\tau^t\sigma^{mc}(x_1)\sigma^{-mt}\tau^t\tau^c(x_2)$$

$$
\begin{aligned}
&= \sum_{b,c=0}^{n-1} \sigma^{mb}(x_1)\tau^b(x_2)\sigma^{-mt}\sigma^{mc}(x_1)\tau^t\tau^c(x_2) \\
&= \sum_{b,c=0}^{n-1} \sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\tau^b(x_2\tau^{t+c-b}(x_2)) \ .
\end{aligned}
$$

Dessa forma,

$$
\begin{aligned}
n\ Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) &= Tr_{\mathbb{K}/\mathbb{Q}}(n\ x\gamma^t(x)) \\
&= Tr_{\mathbb{K}/\mathbb{Q}}\left(Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x\gamma^t(x))\right) \\
&= Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{Q}}(x\gamma^t(x)) \\
&= \sum_{b,c=0}^{n-1} Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{Q}}\left(\sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\tau^b(x_2\tau^{t+c-b}(x_2))\right) \\
&= \sum_{b,c=0}^{n-1} Tr_{\mathbb{K}_1/\mathbb{Q}}\left(\sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\right) Tr_{\mathbb{K}_2/\mathbb{Q}}\left(\tau^b(x_2\tau^{t+c-b}(x_2))\right) \\
&= \sum_{b,c=0}^{n-1} Tr_{\mathbb{K}_1/\mathbb{Q}}\left(x_1\sigma^{m(c-t-b)}(x_1)\right) Tr_{\mathbb{K}_2/\mathbb{Q}}\left(x_2\tau^{t+c-b}(x_2)\right) \ .
\end{aligned}
$$

Se $t = 0$, então

$$
n\ Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) = \sum_{b,c=0}^{n-1} Tr_{\mathbb{K}_1/\mathbb{Q}}\left(x_1\sigma^{m(c-b)}(x_1)\right) Tr_{\mathbb{K}_2/\mathbb{Q}}\left(x_2\tau^{c-b}(x_2)\right) \ .
$$

Por hipótese, se $b = c$ temos que $Tr_{\mathbb{K}_1/\mathbb{Q}}\left(x_1\sigma^{m(c-b)}(x_1)\right) = p_1^2$ e $Tr_{\mathbb{K}_2/\mathbb{Q}}\left(x_2\tau^{c-b}(x_2)\right) = p_2^2$. Já se $b \neq c$ temos ambos nulos e, assim, $n\ Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) = n\ p_1^2p_2^2$. Portanto,

$$
Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) = p_1^2p_2^2 \ .
$$

Agora se $t \neq 0$, então $Tr_{\mathbb{K}_2/\mathbb{Q}}\left(x_2\tau^{t+c-b}(x_2)\right) \neq 0$ somente quando $t + c - b = 0$. Mas nesse caso, temos que $m(c-t-b) \neq 0$, o que implica que $Tr_{\mathbb{K}_1/\mathbb{Q}}\left(x_1\sigma^{m(c-t-b)}(x_1)\right) = 0$. De modo análogo, temos que $Tr_{\mathbb{K}_1/\mathbb{Q}}\left(x_1\sigma^{m(c-t-b)}(x_1)\right) \neq 0$ somente quando $Tr_{\mathbb{K}_2/\mathbb{Q}}\left(x_2\tau^{t+c-b}(x_2)\right) = 0$. Portanto,

$$
Tr_{\mathbb{K}/\mathbb{Q}}(x\gamma^t(x)) = 0 \ ,
$$

o que conclui a demonstração. ∎

Proposição 4.4.12 *Com as mesmas hipóteses da Proposição 4.4.11, temos que o conjunto*

$$
\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\gamma(x) + \ldots + \mathbb{Z}\gamma^{n-1}(x)
$$

é um $\mathbb{Z}$-módulo livre de posto n, contido no anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Demonstração: A demonstração é análoga à da Proposição 4.4.2.

Observação 4.4.7 *Seja $\mathcal{G} = Gal(\mathbb{K} : \mathbb{Q})$. Pela Proposição 4.3.3, temos que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\sigma(x) + \ldots + \mathbb{Z}\sigma^{n-1}(x)$ é um $\mathbb{Z}\mathcal{G}$-módulo livre de posto unitário cuja base é $\{x\}$, isto é, $\mathcal{A} = \mathbb{Z}\mathcal{G}x$, o qual pode ser visto como um ideal principal cujo gerador é x.*

Nas Proposições 4.4.9 e 4.4.10 obtemos necessariamente a condição $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, distinguindo, respectivamente, o caso em que a dimensão n não ramifica e o caso em que n ramifica em $\mathcal{O}_\mathbb{K}$. Se n não ramifica em $\mathcal{O}_\mathbb{K}$, temos que $\mathbb{K}_i \subset \mathbb{Q}(\zeta_{p_i})$, onde os corpos $\mathbb{K}_i$, para $i = 1, 2$, são obtidos através da construção feita na Seção 4.4.1. E, se n ramifica temos que $\mathbb{K}_1 \subset \mathbb{Q}(\zeta_p)$ e $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{n^2})$, onde o corpo $\mathbb{K}_1$ é obtido na Seção 4.4.1 e $\mathbb{K}_2$ na Seção 4.4.2. Sendo assim, dividimos a construção em dois casos, quando n não ramifica e quando n ramifica em $\mathcal{O}_\mathbb{K}$.

Caso III-a: n não ramifica em $\mathcal{O}_\mathbb{K}$

Seja $\mathbb{Q} \subset \mathbb{K}$ uma extensão cíclica de grau primo ímpar n, tal que p_1 e p_2 são os únicos primos (distintos) que ramificam em $\mathcal{O}_\mathbb{K}$, com $p_i \equiv 1(mod\ n)$ e $p_i \not\equiv 1(mod\ n^2)$, para $i = 1, 2$.

Pela Proposição 4.4.9, temos que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_i$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{p_i})$, com $[\mathbb{K}_i : \mathbb{Q}] = n$, em que p_i é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_i}$, para $i = 1, 2$. Desse modo, denotando $Gal(\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}) = \langle\sigma_i\rangle$, segue do Teorema 4.4.1, que existe $x_i \in \mathbb{K}_i$ tal que $Tr_{\mathbb{K}_i/\mathbb{Q}}(x_i\sigma_i^t(x_i)) = \delta_{0,t}p_i^2$, com $t = 0, 1, \ldots, n-1$ e $i = 1, 2$. Temos, assim, satisfeitas as hipóteses da Proposição 4.4.11.

Dessa forma, pela Proposição 4.4.12, tem-se que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\gamma(x) + \ldots + \mathbb{Z}\gamma^{n-1}(x)$ é um $\mathbb{Z}$-módulo livre de posto n, contido em $\mathcal{O}_\mathbb{K}$, onde γ é um gerador de $Gal(\mathbb{K} : \mathbb{Q})$ e

$$x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2).$$

Considere o reticulado algébrico n-dimensional $\sigma_\mathbb{K}(\mathcal{A})$, do qual o conjunto

$$\{\sigma_\mathbb{K}(x), \sigma_\mathbb{K}(\gamma(x)), \ldots, \sigma_\mathbb{K}(\gamma^{n-1}(x))\}$$

é uma base e

$$M = \begin{pmatrix} x & \gamma(x) & \cdots & \gamma^{n-1}(x) \\ \gamma(x) & \gamma^2(x) & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{n-1}(x) & x & \cdots & \gamma^{n-2}(x) \end{pmatrix}$$

é uma matriz geradora. Assim, denotando por $G = (g_{ij})_{i,j=0}^{n-1}$ a matriz Gram de $\sigma_\mathbb{K}(\mathcal{A})$ com respeito à M, temos que cada termo de $G = MM^t$ é dado por

$$g_{ij} = \langle\sigma_\mathbb{K}(\gamma^i(x)), \sigma_\mathbb{K}(\gamma^j(x))\rangle = Tr_{\mathbb{K}/\mathbb{Q}}(x\ \gamma^{j-i}(x)) \overset{(*)}{=} \delta_{ij}p_1^2p_2^2\ ,$$

com $i, j = 0, 1, \ldots, n-1$, onde a igualdade $(*)$ segue da Proposição 4.4.11. Dessa forma, a matriz Gram do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M é dada por

$$G = \begin{pmatrix} p_1^2p_2^2 & 0 & \cdots & 0 \\ 0 & p_1^2p_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_1^2p_2^2 \end{pmatrix} = p_1^2p_2^2Id.$$

Assim, podemos rotacionar o reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ sobre o $\mathbb{Z}^n$. Definindo $M' = \frac{1}{p_1p_2}M$, temos que M' é uma matriz geradora do reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$, onde

$$\mathcal{A}' = \mathbb{Z}\frac{x}{p_1p_2} + \mathbb{Z}\frac{\gamma(x)}{p_1p_2} + \ldots + \mathbb{Z}\frac{\gamma^{n-1}(x)}{p_1p_2} \subset \mathbb{K}$$

é um $\mathbb{Z}$-módulo livre de posto n. Desse modo, a matriz Gram G' de $\sigma_{\mathbb{K}}(\mathcal{A}')$ com respeito à M' é dada por

$$G' = M'M'^t = \frac{1}{p_1p_2}M\frac{1}{p_1p_2}M^t = \frac{1}{p_1^2p_2^2}G = Id\ .$$

Logo, $\sigma_{\mathbb{K}}(\mathcal{A}')$ é isomorfo à $\mathbb{Z}^n$, ou seja, é um reticulado $\mathbb{Z}^n$-rotacionado. Como $n = [\mathbb{K} : \mathbb{Q}]$ é ímpar, segue que $\sigma_{\mathbb{K}}(\mathcal{A}')$ tem diversidade máxima n. Além disso, como o ideal $\mathcal{A}' = \mathbb{Z}\mathcal{G}(\frac{x}{p_1p_2})$ é principal, temos que

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \sqrt{\frac{det(G')}{|\mathcal{D}_{\mathbb{K}}|}}\ .$$

Porém, pela Proposição 4.4.6, tem-se que p_1p_2 é o condutor de $\mathbb{K}$. Assim, pelo Teorema 1.6.2, segue que $|\mathcal{D}_{\mathbb{K}}| = (p_1p_2)^{n-1}$. Logo,

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{\sqrt{(p_1p_2)^{n-1}}}\ .$$

Sendo assim, dada uma dimensão prima ímpar n, os dois menores primos p_1 e p_2 distintos satisfazendo $p_i \equiv 1(mod\ n)$, com $i = 1, 2$, fornecem o reticulado de menor probabilidade de erros em tal dimensão.

Observação 4.4.8 *Note que, podemos denotar $\sigma_{\mathbb{K}}(\mathcal{A}')$ como sendo o reticulado ideal $(\mathcal{A}', Tr_\alpha)$, para $\alpha = 1$, pois $\mathbb{K}$ é totalmente real.*

Algoritmo de Construção

Dados n um primo ímpar e p_1 e p_2 primos distintos tal que $p_i \equiv 1(mod\ n)$ e $p_i \not\equiv 1(mod\ n^2)$, com $i = 1, 2$, temos que existe uma única extensão cíclica $\mathbb{K}_i$ de grau n sobre $\mathbb{Q}$, com

$\mathbb{K}_i \subset \mathbb{Q}(\zeta_{p_i})$. Suponhamos que $\mathbb{K}$ é uma extensão cíclica de grau n, tal que p_1 e p_2 são os únicos primos que ramificam em $\mathcal{O}_\mathbb{K}$. Como visto na Proposição 4.4.11, ao denotar $Gal(\mathbb{K}_1 : \mathbb{Q}) = \langle\sigma\rangle$ e $Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle\tau\rangle$, temos que $(\sigma \circ \tau)$ é um gerador de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$. Assim, encontrando um gerador γ para $Gal(\mathbb{K} : \mathbb{Q})$, podemos calcular $x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2)$ e seus conjugados $\gamma^t(x)$, para $t = 1, \ldots, n-1$, os quais fornecem a matriz geradora M do reticulado $\sigma_\mathbb{K}(\mathcal{A})$. Considere, então, o seguinte algoritmo de construção:

1. *Escolha uma dimensão prima ímpar n.*

2. *Escolha dois primos p_1 e p_2 distintos tal que $p_i \equiv 1(mod\ n)$ e $p_i \not\equiv 1(mod\ n^2)$, com $i = 1, 2$.*

3. *Calcule $x_1 \in \mathbb{K}_1$ e $x_2 \in \mathbb{K}_2$, obtidos pelo Teorema 4.4.1, e seus conjugados $\sigma^t(x_1)$ e $\tau^t(x_2)$, com $t = 1, \ldots, n-1$.*

4. *Calcule $x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2)$, utilizando o gerador $(\sigma \circ \tau)$ de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$.*

5. *Encontre um gerador γ para $Gal(\mathbb{K} : \mathbb{Q})$ e calcule os conjugados $\gamma^t(x)$, onde $t = 1, \ldots, n-1$.*

6. *Calcule a matriz geradora M de $\sigma_\mathbb{K}(\mathcal{A})$, utilizando $\zeta_{p_1p_2} = e^{\frac{2\pi i}{p_1p_2}}$.*

7. *Obtenha a matriz geradora $M' = \frac{1}{p_1p_2}M$ de $\sigma_\mathbb{K}(\mathcal{A}')$.*

Descrevemos, assim, uma família de reticulados n-dimensionais $\sigma_\mathbb{K}(\mathcal{A}')$, com

$$div(\sigma_\mathbb{K}(\mathcal{A}')) = n \quad e \quad d_{p,min}(\sigma_\mathbb{K}(\mathcal{A}')) = \frac{1}{\sqrt{(p_1p_2)^{n-1}}}\ .$$

A Tabela 4.4 apresenta algumas dimensões e parâmetros correspondentes aos reticulados que podem ser obtidos através do algoritmo.

n	p_1	p_2	div	$d_{p,min}$
3	7	13	3	$1/91$
5	11	31	5	$1/341^2$
7	22	29	7	$1/638^3$
11	23	67	11	$1/1541^5$
13	14	53	13	$1/742^6$
17	35	103	17	$1/3605^8$
19	20	39	19	$1/780^9$
23	47	70	23	$1/3290^{11}$
29	30	59	29	$1/1770^{14}$

Tabela 4.4:

Caso III-b: n ramifica em $\mathcal{O}_{\mathbb{K}}$

Seja $\mathbb{Q} \subset \mathbb{K}$ uma extensão cíclica de grau primo ímpar n, tal que p e n são os únicos primos que ramificam em $\mathcal{O}_{\mathbb{K}}$, com $p \equiv 1(mod\ n)$ e $p \not\equiv 1(mod\ n^2)$.

Pela Proposição 4.4.10, temos que $\mathbb{K} \subset \mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_1$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ com $[\mathbb{K}_1 : \mathbb{Q}] = n$, em que p é o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_1}$, e $\mathbb{K}_2$ é o corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n^2})$, sendo $n = [\mathbb{K}_2 : \mathbb{Q}]$ o único primo que ramifica em $\mathcal{O}_{\mathbb{K}_2}$. Desse modo, denotando $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = \langle\sigma\rangle$ e $Gal(\mathbb{Q}(\zeta_{n^2}) : \mathbb{Q}) = \langle\tau\rangle$, segue dos Teoremas 4.4.1 e 4.4.2, que existem, respectivamente, $x_1 \in \mathbb{K}_1$ tal que $Tr_{\mathbb{K}_1/\mathbb{Q}}(x_1\sigma^t(x_1)) = \delta_{0,t}p^2$ e $x_2 \in \mathbb{K}_2$ tal que $Tr_{\mathbb{K}_2/\mathbb{Q}}(x_2\tau^t(x_2)) = \delta_{0,t}n^2$, com $t = 0, 1, \ldots, n-1$.

Dessa forma, pela Proposição 4.4.12, segue que $\mathcal{A} = \mathbb{Z}x + \mathbb{Z}\gamma(x) + \ldots + \mathbb{Z}\gamma^{n-1}(x)$ é um $\mathbb{Z}$-módulo livre de posto n, onde γ é um gerador de $Gal(\mathbb{K} : \mathbb{Q})$ e

$$x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2).$$

Considere o reticulado algébrico n-dimensional $\sigma_{\mathbb{K}}(\mathcal{A})$, do qual

$$M = \begin{pmatrix} x & \gamma(x) & \cdots & \gamma^{n-1}(x) \\ \gamma(x) & \gamma^2(x) & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{n-1}(x) & x & \cdots & \gamma^{n-2}(x) \end{pmatrix}$$

é uma matriz geradora. Assim, denotando por $G = (g_{ij})_{i,j=0}^{n-1}$ a matriz Gram de $\sigma_{\mathbb{K}}(\mathcal{A})$ com respeito à M, temos que cada termo de $G = MM^t$ é dado por

$$g_{ij} = \langle\sigma_{\mathbb{K}}(\gamma^i(x)), \sigma_{\mathbb{K}}(\gamma^j(x))\rangle = Tr_{\mathbb{K}/\mathbb{Q}}(x\ \gamma^{j-i}(x)) = \delta_{ij}p^2n^2\ ,$$

com $i, j = 0, 1, \ldots, n-1$. Dessa forma, a matriz Gram G do reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ tem a seguinte característica:

$$G = \begin{pmatrix} p^2n^2 & 0 & \cdots & 0 \\ 0 & p^2n^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p^2n^2 \end{pmatrix} = p^2n^2Id\ .$$

Podemos, então, rotacionar o reticulado $\sigma_{\mathbb{K}}(\mathcal{A})$ sobre o $\mathbb{Z}^n$. Definindo $M' = \frac{1}{pn}M$, segue que M' é uma matriz geradora do reticulado $\sigma_{\mathbb{K}}(\mathcal{A}')$, onde

$$\mathcal{A}' = \mathbb{Z}\frac{x}{pn} + \mathbb{Z}\frac{\gamma(x)}{pn} + \ldots + \mathbb{Z}\frac{\gamma^{n-1}(x)}{pn} \subset \mathbb{K}\ .$$

Desse modo, a matriz Gram G' de $\sigma_{\mathbb{K}}(\mathcal{A}')$ com respeito à M' é dada por

$$G' = M'M'^t = \frac{1}{pn}M\frac{1}{pn}M^t = \frac{1}{p^2n^2}G = Id\ .$$

Assim, $\sigma_{\mathbb{K}}(\mathcal{A}')$ é um reticulado $\mathbb{Z}^n$-rotacionado com diversidade máxima n e, como o ideal $\mathcal{A}' = \mathbb{Z}\mathcal{G}(\frac{x}{pn})$ é principal, segue que

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \sqrt{\frac{det(G')}{|\mathcal{D}_{\mathbb{K}}|}}\ .$$

Porém, pela Proposição 4.4.6, tem-se que pn^2 é o condutor de $\mathbb{K}$. Segue então, do Teorema 1.6.2, que $|\mathcal{D}_{\mathbb{K}}| = (pn^2)^{n-1}$. Assim,

$$d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{n^{n-1}\sqrt{p^{n-1}}}\ .$$

Desse modo, dado n um primo ímpar, o menor primo p satisfazendo $p \equiv 1(mod\ n)$ fornece o reticulado de menor probabilidade de erros na dimensão n.

Observação 4.4.9 *Podemos denotar $\sigma_{\mathbb{K}}(\mathcal{A}')$ como sendo o reticulado ideal $(\mathcal{A}', Tr_1)$, pois $\mathbb{K}$ é totalmente real.*

Algoritmo de Construção

Dados n um primo ímpar e p um primo tal que $p \equiv 1(mod\ n)$ e $p \not\equiv 1(mod\ n^2)$, temos que existe uma única extensão cíclica $\mathbb{K}_1$ de grau n sobre $\mathbb{Q}$, com $\mathbb{K}_1 \subset \mathbb{Q}(\zeta_p)$ e uma única extensão cíclica $\mathbb{K}_2$ de grau n sobre $\mathbb{Q}$, com $\mathbb{K}_2 \subset \mathbb{Q}(\zeta_{n^2})$. Suponhamos que $\mathbb{K}$ é uma extensão cíclica de grau n, tal que p e n são os únicos primos que ramificam em $\mathcal{O}_{\mathbb{K}}$. Denotando $Gal(\mathbb{K}_1 : \mathbb{Q}) = \langle\sigma\rangle$ e $Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle\tau\rangle$, temos que $(\sigma \circ \tau)$ é um gerador de $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$. Assim, encontrando um gerador γ para $Gal(\mathbb{K} : \mathbb{Q})$, podemos calcular $x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2)$ e seus conjugados $\gamma^t(x)$, para $t = 1, \ldots, n-1$, o que permite fornecer o seguinte algoritmo de construção:

1. *Escolha uma dimensão prima ímpar n.*

2. *Escolha um primo ímpar p tal que $p \equiv 1(mod\ n)$ e $p \not\equiv 1(mod\ n^2)$.*

3. *Calcule $x_1 \in \mathbb{K}_1$ e $x_2 \in \mathbb{K}_2$ obtidos pelos Teoremas 4.4.1 e 4.4.2, respectivamente, e calcule seus conjugados $\sigma^t(x_1)$ e $\tau^t(x_2)$, para $t = 1, \ldots, n-1$.*

4. *Calcule* $x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2)$*, utilizando o gerador* $(\sigma \circ \tau)$ *de* $Gal(\mathbb{K}_1\mathbb{K}_2 : \mathbb{K})$*.*

5. *Encontre um gerador* γ *para* $Gal(\mathbb{K} : \mathbb{Q})$ *e calcule os conjugados* $\gamma^t(x)$*, onde* $t = 1, \ldots, n-1$*.*

6. *Calcule a matriz geradora* M *de* $\sigma_{\mathbb{K}}(\mathcal{A})$*, utilizando* $\zeta_{pn} = e^{\frac{2\pi i}{pn}}$*.*

7. *Obtenha a matriz geradora* $M' = \frac{1}{pn}M$ *de* $\sigma_{\mathbb{K}}(\mathcal{A}')$*.*

Descrevemos, assim, uma família de reticulados n-dimensionais $\sigma_{\mathbb{K}}(\mathcal{A}')$, com

$$div(\sigma_{\mathbb{K}}(\mathcal{A}')) = n \quad e \quad d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = \frac{1}{n^{n-1}\sqrt{p^{n-1}}} \ .$$

A Tabela 4.5 apresenta algumas dimensões e parâmetros correspondentes aos reticulados que podem ser obtidos através do algoritmo.

n	p	div	$d_{p,min}$
3	7	3	$1/63$
5	11	5	$1/(5^4 \times 11^2)$
7	22	7	$1/(7^6 \times 22^3)$
11	23	11	$1/(11^{10} \times 23^5)$
13	14	13	$1/(13^{12} \times 14^6)$
17	35	17	$1/(17^{16} \times 35^8)$
19	20	19	$1/(19^{18} \times 20^9)$
23	47	23	$1/(23^{22} \times 47^{11})$
29	30	29	$1/(29^{28} \times 30^{14})$

Tabela 4.5:

Exemplo 4.4.3 *Segue um exemplo de construção de um reticulado* $\sigma_{\mathbb{K}}(\mathcal{A}')$*, utilizando o algoritmo que descrevemos acima.*

1. *Escolhemos a dimensão* $n = 3$*.*

2. *Escolhemos* $p = 13$*, satisfazendo* $p \equiv 1(mod\ 3)$ *e* $p \not\equiv 1(mod\ 9)$*.*

3. *Temos que* $Gal(\mathbb{K}_1 : \mathbb{Q}) = \langle \sigma|_{\mathbb{K}_1} \rangle$ *e* $Gal(\mathbb{K}_2 : \mathbb{Q}) = \langle \tau|_{\mathbb{K}_2} \rangle$*, com* $\sigma : \zeta_{13} \mapsto \zeta_{13}^2$ *e* $\tau : \zeta_9 \mapsto \zeta_9^2$*. Nos Exemplos 4.4.1 e 4.4.2 obtemos, respectivamente,*

$$x_1 = 5 + 3\zeta_{13}^2 + 3\zeta_{13}^3 - \zeta_{13}^4 - \zeta_{13}^6 - \zeta_{13}^7 - \zeta_{13}^9 + 3\zeta_{13}^{10} + 3\zeta_{13}^{11}$$

$$\sigma(x_1) = 6 + \zeta_{13}^2 + \zeta_{13}^3 + 4\zeta_{13}^4 + 4\zeta_{13}^6 + 4\zeta_{13}^7 + 4\zeta_{13}^9 + \zeta_{13}^{10} + \zeta_{13}^{11}$$

$$\sigma^2(x_1) = 2 - 4\zeta_{13}^2 - 4\zeta_{13}^3 - 3\zeta_{13}^4 - 3\zeta_{13}^6 - 3\zeta_{13}^7 - 3\zeta_{13}^9 - 4\zeta_{13}^{10} - 4\zeta_{13}^{11} \ ,$$

e

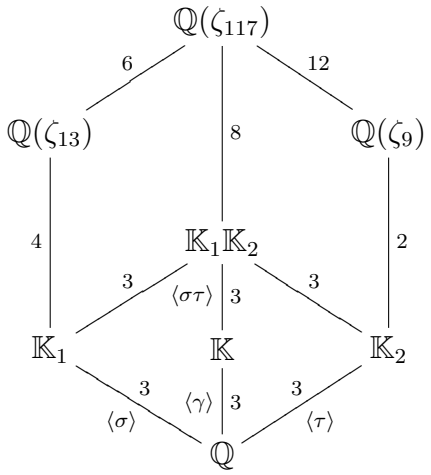
$$x_2 = 1 + \zeta_9 + \zeta_9^8$$
$$\tau(x_2) = 1 + \zeta_9^2 + \zeta_9^7$$
$$\tau^2(x_2) = 1 + \zeta_9^4 + \zeta_9^5 \ .$$

Porém, $\zeta_{13} = \zeta_{117}^9$ *e* $\zeta_9 = \zeta_{117}^{13}$*. Logo, denotando* $\zeta = \zeta_{117}$*, podemos escrever*

$$x_1 = 5 + 3\zeta^{18} + 3\zeta^{27} - \zeta^{36} - \zeta^{54} - \zeta^{63} - \zeta^{81} + 3\zeta^{90} + 3\zeta^{99}$$
$$\sigma(x_1) = 6 + \zeta^{18} + \zeta^{27} + 4\zeta^{36} + 4\zeta^{54} + 4\zeta^{63} + 4\zeta^{81} + \zeta^{90} + \zeta^{99}$$
$$\sigma^2(x_1) = 2 - 4\zeta^{18} - 4\zeta^{27} - 3\zeta^{36} - 3\zeta^{54} - 3\zeta^{63} - 3\zeta^{81} - 4\zeta^{90} - 4\zeta^{99}$$

e

$$x_2 = 1 + \zeta^{13} + \zeta^{104}$$
$$\tau(x_2) = 1 + \zeta^{26} + \zeta^{91}$$
$$\tau^2(x_2) = 1 + \zeta^{52} + \zeta^{65} \ .$$



4. *Temos que*

$$\begin{aligned} x = Tr_{\mathbb{K}_1\mathbb{K}_2/\mathbb{K}}(x_1x_2) &= \sum_{t=0}^{2}(\sigma\tau)^t(x_1x_2) \\ &= \sum_{t=0}^{2}\sigma^t(x_1)\tau^t(x_2) \\ &= x_1x_2 + \sigma(x_1)\tau(x_2) + \sigma^2(x_1)\tau^2(x_2) \ . \end{aligned}$$

Assim, utilizando a congruência módulo 117*, obtemos que*

$$x = 13 + \zeta - 3\zeta^2 + 3\zeta^5 + \zeta^8 + 4\zeta^{10} - 3\zeta^{11} + 5\zeta^{13} + 3\zeta^{14} - 3\zeta^{16} - \zeta^{23} - 4\zeta^{25} + 6\zeta^{26} + 4\zeta^{28} - 3\zeta^{29} + 3\zeta^{31} - 4\zeta^{34} + 4\zeta^{37} - 4\zeta^{38} + 3\zeta^{40} - \zeta^{41} + \zeta^{44} - 4\zeta^{47} - \zeta^{49} - \zeta^{50} + 2\zeta^{52} + \zeta^{53} + 4\zeta^{55} + 4\zeta^{62} +$$

$\zeta^{64} + 2\zeta^{65} - \zeta^{67} - \zeta^{68} - 4\zeta^{70} + \zeta^{73} - \zeta^{76} + 3\zeta^{77} - 4\zeta^{79} + 4\zeta^{80} - 4\zeta^{83} + 3\zeta^{86} - 3\zeta^{88} + 4\zeta^{89} + 6\zeta^{91} - 4\zeta^{92} - \zeta^{94} - 3\zeta^{101} + 3\zeta^{103} + 5\zeta^{104} - 3\zeta^{106} + 4\zeta^{107} + \zeta^{109} + 3\zeta^{112} - 3\zeta^{115} + \zeta^{116}$

5. *Como qualquer elemento não unitário de* $Gal(\mathbb{K} : \mathbb{Q}) \simeq \mathbb{Z}_3$ *é um gerador, considere o gerador* $\gamma|_{\mathbb{K}} : \zeta \mapsto \zeta^{40}$. *Desse modo,*

$\gamma(x) = 13 - 4\zeta - \zeta^2 + \zeta^5 - 4\zeta^8 - 3\zeta^{10} - \zeta^{11} + 6\zeta^{13} + \zeta^{14} - \zeta^{16} + 4\zeta^{23} + 3\zeta^{25} + 2\zeta^{26} - 3\zeta^{28} - \zeta^{29} + \zeta^{31} + 3\zeta^{34} - 3\zeta^{37} + 3\zeta^{38} + \zeta^{40} + 4\zeta^{41} - 4\zeta^{44} + 3\zeta^{47} + 4\zeta^{49} + 4\zeta^{50} + 5\zeta^{52} - 4\zeta^{53} - 3\zeta^{55} - 3\zeta^{62} - 4\zeta^{64} + 5\zeta^{65} + 4\zeta^{67} + 4\zeta^{68} + 3\zeta^{70} - 4\zeta^{73} + 4\zeta^{76} + \zeta^{77} + 3\zeta^{79} - 3\zeta^{80} + 3\zeta^{83} + \zeta^{86} - \zeta^{88} - 3\zeta^{89} + 2\zeta^{91} + 3\zeta^{92} + 4\zeta^{94} - \zeta^{101} + \zeta^{103} + 6\zeta^{104} - \zeta^{106} - 3\zeta^{107} - 4\zeta^{109} + \zeta^{112} - \zeta^{115} - 4\zeta^{116}$

e

$\gamma^2(x) = 13 + 3\zeta + 4\zeta^2 - 4\zeta^5 + 3\zeta^8 - \zeta^{10} + 4\zeta^{11} + 2\zeta^{13} - 4\zeta^{14} + 4\zeta^{16} - 3\zeta^{23} + \zeta^{25} + 5\zeta^{26} - \zeta^{28} + 4\zeta^{29} - 4\zeta^{31} + \zeta^{34} - \zeta^{37} + \zeta^{38} - 4\zeta^{40} - 3\zeta^{41} + 3\zeta^{44} + \zeta^{47} - 3\zeta^{49} - 3\zeta^{50} + 6\zeta^{52} + 3\zeta^{53} - \zeta^{55} - \zeta^{62} + 3\zeta^{64} + 6\zeta^{65} - 3\zeta^{67} - 3\zeta^{68} + \zeta^{70} + 3\zeta^{73} - 3\zeta^{76} - 4\zeta^{77} + \zeta^{79} - \zeta^{80} + \zeta^{83} - 4\zeta^{86} + 4\zeta^{88} - \zeta^{89} + 5\zeta^{91} + \zeta^{92} - 3\zeta^{94} + 4\zeta^{101} - 4\zeta^{103} + 2\zeta^{104} + 4\zeta^{106} - \zeta^{107} + 3\zeta^{109} - 4\zeta^{112} + 4\zeta^{115} + 3\zeta^{116}$.

6. *A matriz geradora* M *de* $\sigma_{\mathbb{K}}(\mathcal{A})$ *é dada por*

$$M = \begin{pmatrix} x & \gamma(x) & \gamma^2(x) \\ \gamma(x) & \gamma^2(x) & x \\ \gamma^2(x) & x & \gamma(x) \end{pmatrix}.$$

Em valores numéricos,

$$M = \begin{pmatrix} 21,5785 & -12,545 & 29,9665 \\ -12,545 & 29,9665 & 21,5785 \\ 29,9665 & 21,5785 & -12,545 \end{pmatrix}.$$

7. *Portanto, temos que*

$$M' = \frac{1}{39}M = \begin{pmatrix} 0,55329 & -0,32166 & 0,76837 \\ -0,32166 & 0,76837 & 0,55329 \\ 0,76837 & 0,55329 & -0,32166 \end{pmatrix}$$

é uma matriz geradora do reticulado $\mathbb{Z}^n$*-rotacionado* $\sigma_{\mathbb{K}}(\mathcal{A}')$, *para* $n = 3$ *e* $p = 13$, *do qual* $div(\sigma_{\mathbb{K}}(\mathcal{A}')) = 3$ *e* $d_{p,min}(\sigma_{\mathbb{K}}(\mathcal{A}')) = 1/117$.

4.5 Conclusões e perspectivas futuras

A utilização de reticulados $\mathbb{Z}^n$-rotacionados no canal Rayleigh Fading é viável quando trabalhamos com diversidade e distância produto mínima relativamente altas, de modo a minimizar a probabilidade de erros na transmissão de sinais (veja Seção 4.2). Os reticulados descritos neste capítulo apresentam diversidade máxima e livre escolha da dimensão ímpar (ou prima ímpar) a ser trabalhada. A partir da Seção 4.4, a distância produto mínima dos reticulados $\mathbb{Z}^n$-rotacionados obtidos depende da dimensão n e de parâmetros que podem ser ajustáveis via congruência módulo n, possibilitando a escolha de parâmetros de modo a maximizar a distância produto mínima numa dada dimensão.

Nas construções deste capítulo, foram utilizadas $\mathbb{Z}$-bases normais contidas em extensões cíclicas, o que favorece a formulação de algoritmos de construção e a avaliação da forma traço associada. Como vimos, a obtenção de bases normais está relacionada com a ramificação de números primos numa extensão. Se $\mathbb{Q} \subset \mathbb{K}$ é uma extensão abeliana cujo grau não ramifica em $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{O}_{\mathbb{K}}$ possui uma base normal (Teorema IV.7.1 - [10]). Desse modo, se $\mathbb{K}$ é um corpo de números de grau primo n contido numa extensão ciclotômica $\mathbb{Q}(\zeta_{p^r})$, com p primo ímpar e $n \neq p$, então existe uma base normal para $\mathcal{O}_{\mathbb{K}}$. Consideramos a possibilidade de encontrar uma tal base, de modo semelhante ao apresentado na Seção 4.1, o que permitiria a construção de uma família de reticulados que contém, como caso particular, a exibida na Seção 4.1.

Sejam $\mathbb{K}$ um corpo intermediário de $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$, com p primo ímpar e $[\mathbb{K} : \mathbb{Q}] = n$ ímpar. Considere o reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = (\mathcal{O}_{\mathbb{K}}, Tr_1)$ obtido na Seção 4.1. Nosso intuito é trabalhar com a possibilidade de rotacioná-lo sobre o $\mathbb{Z}^n$. Como vimos na Seção 4.2, a igualdade

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)|\mathcal{D}_{\mathbb{K}}| = c^n,$$

para algum $c \in \mathbb{Z}$, é uma condição necessária para o parâmetro α, de modo que o reticulado $(\mathcal{O}_{\mathbb{K}}, Tr_\alpha)$ possa ser $\mathbb{Z}^n$-rotacionado. Pondo $c = p$, segue que $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = p$, pois $|\mathcal{D}_{\mathbb{K}}| = p^{n-1}$. Porém,

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

Desse modo,

$$\alpha = \mathcal{N}_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(1-\zeta_p) = \prod_{i=1}^{\frac{p-1}{n}} \sigma^{in}(1-\zeta_p) = \prod_{i=1}^{\frac{p-1}{n}} (1-\zeta_p^{r^{in}}),$$

onde σ é um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Ou seja, o elemento $\alpha \in \mathbb{K}$ descrito acima satisfaz uma condição necessária para que $(\mathcal{O}_{\mathbb{K}}, Tr_\alpha)$ forneça um reticulado $\mathbb{Z}^n$-rotacionado. Porém, a verificação de que este reticulado fornece um $\mathbb{Z}^n$-reticulado depende do cálculo do traço $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\theta\sigma^t(\theta))$, para $t = 0, 1, \ldots, n-1$, onde $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$, o qual está por ser concluido.

Referências Bibliográficas

[1] STEWART, I. N. **Galois Theory**. London: Chapman and Hall, 2003.

[2] MILIES, F. C. P. **Anéis e Módulos**. São Paulo: L.P.M., 1972.

[3] SANTOS, J. P. O. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2006.

[4] STEWART, I. N.; TALL, D. O. **Algebraic Number Theory**. London: Chapman and Hall, 1987.

[5] SAMUEL, P. **Algebraic Theory of Numbers**. Paris: Hermann, 1970.

[6] RIBENBOIM, P. **Classical Theory of Algebraic Numbers**. New York: Springer-Verlag, 2001.

[7] WASHINGTON, L. C. **Introduction to Cyclotomic Fields**. New York: Springer-Verlag, 1982.

[8] MILIES, F. C. P. **Anéis de Grupos**. São Paulo: S.B.M., 1976.

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

[10] CONNER, P. E.; PERLIS, R. **A Survey of Trace Forms of Algebraic Number Fields**. Singapore: World Scientific Publishing, 1984.

[11] JORGE, G. C. **Reticulados Ideais via Corpos Abelianos**. São José do Rio Preto: IBILCE/UNESP, 2008. 176 p. Dissertação (Mestrado) - Programa de Pós-Graduação em Matemática, Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[12] FERRARI, A. J. **Reticulados Algébricos via Corpos Abelianos**. São José do Rio Preto: IBILCE/UNESP, 2008. 105 p. Dissertação (Mestrado) - Programa de Pós-Graduação em Matemática, Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[13] OGGIER, F. **Algebraic Methods for Channel Coding**. Lausanne: École Polytechnique Fédérale de Lausanne, 2005. 125 p. Tese (Doutorado) - Programa de Pós-Graduação em Matemática e Informática, École Polytechnique Fédérale de Lausanne, Lausanne, 2005.

[14] LOPES, J. O. D. **Discriminante dos Corpos Abelianos**. Campinas: UNICAMP, 2003. 56 p. Tese (Doutorado) - Programa de Pós-Graduação em Matemática, Universidade Estadual de Campinas, Campinas, 2003.

[15] BOUTROS, J.; VITERBO, E.; RATELLO, C.; BELFIORE, J. C. *Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels*. **IEEE Transactions on Information Theory**, New-York, v. 42, n. 2, p. 502-517, 1996.

[16] BAYER-FLUCKIGER, E. *Ideal Lattices*. In: CONFERENCE IN HONOR OF ALAN BAKER, 2002, Cambridge. **Proceedings**... Cambridge: Cambridge University Press, 2002.

[17] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. *Algebraic Lattice Constellations: Bounds on Performance*. **IEEE Transactions on Information Theory**, New-York, v. 52, n. 1, p. 319-327, Jan. 2006.

[18] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. *New Algebraic Constructions of Rotated $\mathbb{Z}^n$-lattice Constellations for the Rayleigh Fading Channel*. **IEEE Transactions on Information Theory**, New-York, v. 50, n. 4, p. 702-714, Apr. 2004.

[19] ELIA, P.; KUMAR, P. V.; SETHURAMAN, B. A. *Perfect Space-Time Codes for Any Number of Antenas*. **IEEE Transactions on Information Theory**, New-York, v. 53, n. 11, Nov. 2007.

[20] EREZ, B. *The Galois Struture of the Trace Form in Extensions of Odd Prime Degree*. **Journal of Algebra**, New Jersey, v. 118, p. 438-446, 1988.

[21] ULLOM, S. *Normal Bases in Galois Extensions of Number Fields*. **Nagoya Math. J.**, Nagoya, v. 34, p. 153-167, 1969.

Índice Remissivo