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

Carlos Roberto Lopes Vicente

Construções de reticulados algébricos via extensões galoisianas de grau prima

São José do Rio Preto

2018

Carlos Roberto Lopes Vicente

Construções de reticulados algébricos via extensões galoisianas de grau prima

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

Financiadora: FAPESP - Proc. 2015/20595-4

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto

2018

Vicente, Carlos Roberto Lopes.
Construções de reticulados algébricos via extensões galoisianas de grau prima / Carlos Roberto Lopes Vicente. -- São José do Rio Preto, 2018
137 f. : il., tab.

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

1. Matemática. 2. Teoria dos números algébricos. 3. Teoria dos reticulados. 4. Extensões de corpos (Matemática) 5. Teoria dos sinais (Telecomunicações) I. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. II. Título.

CDU – 512.91

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

Carlos Roberto Lopes Vicente

Construções de reticulados algébricos via extensões galoisianas de grau prima

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

Financiadora: FAPESP - Proc. 2015/20595-4

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Professor Livre-Docente
UNESP - São José do Rio Preto - SP
Orientador

Prof. Dr. Ali Messaoudi
Professor Livre-Docente
UNESP - São José do Rio Preto - SP

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

São José do Rio Preto, 23 de fevereiro de 2018.

Dedico à minha

mãe, irmão e amigos.

Agradecimentos

À minha mãe e meu irmão, Antonia Benedita Lopes e Marcelo Augusto Lopes Malavazi, pelo amor e incentivo.

Aos meus amigos, Aldimir Bruzadin, Amanda Monteiro, Daniel Ferreira, Eduardo Paixão, Gabriel Gomes, Laura Gambera, Luan Medeiros, Lucas Lodi, Maurício Rodrigues e Rafaela Carvalho, pela amizade e por serem o meu alicerce durante esse árduo percurso.

Aos todos meus amigos de PET, graduação, pós graduação e da vida, em especial, à Ana Valente, André Marçal, Bruno de Souza, Caroline Signorini, Danytelle Gregui, Décio Libralão, Denis Vinha, Eliton Moro, Everton Sampaio, Gabriel Fazoli, Lucas Morelli, Lucas Santos, Marcus Roversi, Matheus Andrade, Matheus Roversi, Mauro da Silva, Otávio Perez, Pedro Melo, Plínio Sicuti, Rodrigo Bononi, Rodrigo Contreiras, Ronaldo Felipe, Sara Vinha, Vinícius Vitório e Wesley Tavares, entre outros, pela amizade, conselhos e apoio.

Ao "Cinema (ou não)", por tudo, não consigo por em palavras o quão vocês são especiais e o tanto que me ajudam.

Aos animes e séries que assisti, em especial ao autor de One Piece, Eiichiro Oda, e à criadora e produtora de Grey's Anatomy, Shonda Rhimes, por me ensinarem através destas formas de arte a valorizar mais minha família e amigos, pelas lições de vida e por me motivarem a ser sempre uma pessoa melhor.

À Florence and the Machine, Lana Del Rey, Lorde, Marina and the Diamonds e MØ, por serem a trilha sonora que sempre me deu forças durante os estudos e noites em claro.

A meu orientador, Prof. Dr. Antonio, pela paciência e dedicação para o desenvolvimento deste trabalho.

À Profa. Dra. Maria Gorete Carreira Andrade e Prof. Dr. Adalberto Spezamiglio pelos ensinamentos, conselhos e ajuda nos anos de PET.

Aos professores Andréa, Claudio Buzzi, Clotilzio, Ermínia, João Carlos, Márcio, Michelle e Ricardo, pelos ensinamentos.

Aos professores da Comissão Examinadora.

À FAPESP pelo apoio financeiro, processo 2015/20595-4.

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

"Somos mais do que as partes que nos formam".

O Nome do Vento (Patrick Rothfuss)

Resumo

Na busca por novos sistemas de comunicações muitos trabalhos têm sido realizados com o objetivo de obter constelações de sinais e códigos geometricamente uniformes no espaço euclidiano. Neste contexto, nossa proposta é identificar uma estrutura algébrica e geométrica para reticulados algébricos provenientes do homomorfismo canônico que possuam densidade centro ótima. Nesse sentido, a presente dissertação tem como foco as extensões galoisianas de grau primo ímpar p e encontrar estruturas de $\mathbb{Z}$-módulos via essas extensões que gerem reticulados algébricos com densidade de centro ótima.

Palavras-chave: corpos de números, reticulados algébricos, densidade de centro, empacotamento de esferas.

Abstract

In the search for new communication systems many works have been performed in order to get constellation geometrically uniform signs and codes in Euclidean space. In this context, our proposal is to identify an algebraic and geometric structure for algebraic lattices from the canonical homomorphism possessing great center density. In this sense, this project focuses on the galoisian extensions of p odd prime degree and find $\mathbb{Z}$-module structures via these extensions that create algebraic lattices with great center density.

Keywords: *number fields, algebraic lattices, center density, sphere packing.*

Lista de Símbolos

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{C}$	Conjunto dos números complexos
Σ	Somatório
Π	Produtório
$\#A$	Cardinalidade do conjunto A
$\overline{x}$	Conjugado complexo de x
$M = (a_{ij})$	Matriz de entradas a_{ij}
$det(A)$	Determinante da matriz A
$a\|b$	a divide b
$a \equiv b\ (mod\ m)$	a congruente a b módulo m
$\varphi(n)$	Função de Euler aplicada à n
$Ker(f)$	Núcleo da função f
$Im(f)$	Imagem da função f
$m_\alpha(x)$	Polinômio minimal de α
$f_\alpha(x)$	Polinômio característico de α
$\partial(f(x))$	Grau do polinômio $f(x)$
$\Re(z)$	Parte real do número complexo z
$\Im(z)$	Parte imaginária do número complexo z
H, G	Grupos
$A[x]$	Anel de polinômios com coeficientes em A
$\mathcal{I}, \mathcal{J}, \mathcal{P}, \mathcal{Q}, \mathcal{B}$	Ideais

$A/\mathcal{I}$	Anel quociente
G/H	Grupo quociente
$[G : H]$	Índice do subgrupo H no grupo G
$\mathbb{K}$, $\mathbb{L}$, $\mathbb{M}$	Corpos
$\mathbb{L}\|\mathbb{K}$	O corpo $\mathbb{L}$ é uma extensão do corpo $\mathbb{K}$
$[\mathbb{L} : \mathbb{K}]$	Grau da extensão $\mathbb{L}\|\mathbb{K}$
$Gal(\mathbb{L}\|\mathbb{K})$	O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$Tr_{\mathbb{L}\|\mathbb{K}}(\alpha)$	O traço de α em relação à $\mathbb{L}\|\mathbb{K}$
$N_{\mathbb{L}\|\mathbb{K}}(\alpha)$	A norma de α em relação à $\mathbb{L}\|\mathbb{K}$
$N(\mathcal{I})$	A norma do ideal $\mathcal{I}$
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$\mathcal{D}(\alpha_1, \ldots, \alpha_n)$	Discriminante de $(\alpha_1, \ldots, \alpha_n)$
$\mathcal{D}_{\mathbb{K}}$	Discriminante do corpo $\mathbb{K}$
ζ_n	Raiz n-ésima primitiva da unidade
$\mathbb{Q}(\zeta_n)$	n-ésimo corpo ciclotômico
$cond(\mathbb{K})$	Condutor do corpo $\mathbb{K}$
Λ	Reticulado
$\mathcal{V}ol(\Lambda)$	Volume do reticulado Λ
$\delta(\Lambda)$	Densidade de centro de Λ
$\sigma_{\mathbb{K}}$	Homomorfismo canônico

Sumário

Introdução

O empacotamento de esferas é um tema atual, principalmente pelas suas conexões com diversas áreas do conhecimento, em especial com a Teoria da Informação. Os primeiros resultados que se conhece são anteriores a Gauss, Newton e outros grandes nomes que foram notáveis pensadores da matemática. Em 1900, o problema do empacotamento de esferas foi destacado por Hilbert, numa seleta de grandes problemas que seriam de importante relevância no século seguinte, devido a sua importância e complexidade. Ao longo dos últimos anos, muito tem sido feito e muito mais existe por se fazer. A relação comprovada entre a densidade de um empacotamento de esferas e a eficiência de um código corretor de erros, têm aumentado o interesse no assunto e novas técnicas na geração de reticulados tem sido obtidas.

Assim, no estudo de reticulados algébricos um dos parâmetros importantes é o estudo de sua densidade de empacotamento, e um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo de fácil manipulação. Encontrar um corpo de números de um grau previamente determinado e discriminante mínimo é um problema clássico e as poucas soluções que se conhecem são para corpos de grau baixo, valorizando a sua assinatura. A solução para tal problema tem implicações imediatas em outras áreas do conhecimento, especialmente na Teoria da Informação, quando se constrói codificadores de fonte baseados em reticulados algébricos.

Desta forma, uma vez que a teoria dos números algébricos é muito utilizada na obtenção de novas estruturas de reticulados, o principal objetivo deste trabalho é o estudo das extensões galoisianas de grau primo p ímpar, analisando separadamente em função da fatoração do condutor em produto de primos os casos em que p é ramificado e não ramificado. E, construir exemplos de reticulados no espaço $\mathbb{R}^n$ que possuem densidade de centro ótimas para determinadas dimensões, via essas extensões e via polinômios.

No Capítulo 1, apresentamos os conceitos básicos necessários para o desenvolvimento do trabalho. Começamos com definições e resultados sobre módulos e módulos noetherianos. Em seguida, apresentamos os conceitos sobre anel de inteiros, norma, traço, anel de Dedekind e norma de um ideal. Na seção seguinte, apresentamos o conceito de discriminante de uma extensão de anéis. E por fim, apresentamos a decomposição de ideais. No decorrer deste capítulo fizemos uso das referências [3], [8], [11], [12], [18], [21], [23], [24], [31], [32], [33].

No Capítulo 2, apresentamos resultados sobre uma classe de corpos de números muito importante, os corpos ciclotômicos. Inicialmente apresentamos resultados sobre raízes da unidade, e nas seções seguintes determinamos o anel de inteiros, uma base e o discriminante desses corpos. Para este capítulo utilizamos as referências [1], [8], [14], [18], [23], [33].

No Capítulo 3, apresentamos resultados sobre extensões abelianas de grau primo ímpar p. Apresentamos um elemento primitivo para $\mathbb{K}$, onde $\mathbb{K}$ é um corpo de números abeliano de grau finito p, com p um primo ímpar, uma base integral para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, caracterizamos um elemento de $\mathcal{O}_{\mathbb{K}}$ tal que pertença à um ideal primo especifico de $\mathcal{O}_{\mathbb{K}}$ e encontramos o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$. Na primeira seção, consideramos o caso em que o condutor de $\mathbb{K}$ é da forma $\prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i primo para $i = 1, \ldots, s$. Em seguida, apresentamos o caso em que o condutor de $\mathbb{K}$ é da forma p^2, com p um primo ímpar. E por fim, na seção seguinte, o caso em que o condutor é da forma $p^2 \prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i's primos, para $i = 1, \ldots, s$. Para o desenvolvimento deste capítulo foram utilizados as referências [2], [6], [13], [16], [19], [20], [22], [25], [26], [27], [28].

No Capítulo 4, apresentamos resultados sobre reticulados. Inicialmente, na primeira seção, apresentamos os conceitos básicos sobre reticulados no $\mathbb{R}^n$, onde o principal objetivo é a fórmula para o cálculo da densidade de centro. Na seção seguinte, apresentamos os reticulados com densidade de centro ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12, 16 e 24. E por fim, na seção seguinte, identificamos através do homomorfismo canônico um $\mathbb{Z}$-módulo livre de posto finito contido num corpo de números $\mathbb{K}$ com um reticulado no $\mathbb{R}^n$, que chamamos de reticulado algébrico. Neste capítulo, utilizamos as referências [1], [2], [4], [5], [7], [14], [20], [31].

No Capítulo 5, construímos exemplos de reticulados algébricos via homomorfismo canônico, que possuem densidade de centro ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12 e 24. Para este capítulo foram utilizados as referências [3], [6], [9], [10], [14], [15], [17], [27], [29], [30].

E por fim, apresentamos as conclusões do trabalho.

Capítulo

1

Conceitos preliminares

Neste capítulo, veremos conceitos e resultados da teoria do números que serão úteis no decorrer deste trabalho. Primeiro, na Seção 1.1, apresentamos os conceitos de módulos e módulos noetherianos e algumas propriedades. Em seguida, na Seção 1.2, apresentamos definições e resultados da teoria algébrica dos números, como, anel de inteiros, traço, norma, anel de Dedekind e norma de um ideal. Na Seção 1.3, apresentamos resultados sobre discriminante. E, finalmente na Seção 1.4, apresentamos resultados sobre ramificação de ideais.

A demostração de alguns resultados são omitidos, por se tratarem de resultados clássicos ou pela extensa demonstração. Mas, contudo, adicionamos a referência nos resultados sem demonstração.

1.1 Módulos livres e noetherianos

Neste capítulo, apresentamos os conceitos de módulos, módulos sobre anéis principais e módulos noetherianos. Na Subseção 1.1.1, apresentamos resultados importantes sobre módulos sobre anéis principais. Na Subseção 1.1.2, apresentamos os conceitos de módulos noetherianos e anéis noetherianos.

1.1.1 Módulos

Nesta seção, faremos um estudo de módulos. Para isso, consideramos A um anel comutativo com unidade.

Definição 1.1.1. *Um* A-***módulo*** *é um grupo abeliano* M*, munido com uma aplicação* $\varphi : A \times M \longrightarrow M$*, dada por* $(a, m) \longrightarrow \varphi(a, m) = am$*, tal que*

1. $(a + b)m = am + bm$,
2. $a(m + n) = am + an$,
3. $(ab)m = a(bm)$,
4. $1m = m$,

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

Definição 1.1.2. *Sejam* M *um* A*-módulo e* $N \subset M$*,* $N \neq \emptyset$*. Dizemos que* N *é um* ***submódulo*** *do* A*-módulo* M *se:*

1. N *é um subgrupo de* M*.*
2. $an \in N$*, para todo* $a \in A$ *e* $n \in N$*.*

Definição 1.1.3. *Seja* M *um* A*-módulo.*

1. *Dizemos que um conjunto* $\{x_1, x_2, \ldots, x_n\}$ *de elementos de* M *é* ***linearmente independente*** *se a equação* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$*, com* $a_1, \ldots, a_n \in A$*, possui somente a solução nula, ou seja,* $a_1 = a_2 = \cdots = a_n = 0$*.*
2. *Dizemos que um conjunto* $B = \{x_i\}_{i \in I}$ *de elementos de* M*, onde* I *é um conjunto de índices, é* ***linearmente independente*** *quando todo subconjunto finito de* B *é linearmente independente.*
3. *Dizemos que um elemento* $x \in M$ *é uma* ***combinação linear*** *de um conjunto finito* $B = \{x_1, x_2, \ldots, x_n\}$ *de elementos de* M*, se existem elementos* $a_i, a_2, \ldots, a_n \in A$ *tal que* $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$*.*
4. *Dizemos que um conjunto* $B = \{x_i\}_{i \in I}$*, onde* I *é um conjunto de índices,* ***gera*** M *se todo elemento de* M *é escrito como uma combinação linear de um subconjunto finito de* B*. Neste caso, escrevemos* $M = \langle B \rangle$*. Além disso, se* B *for finito, dizemos que* M *é* ***finitamente gerado*** *ou* ***do tipo finito****.*

Definição 1.1.4. *Seja M um A-módulo. Dizemos que um conjunto $B = \{x_i\}_{i\in I}$, onde I é um conjunto de índices, é uma* ***base*** *de M sobre A se B é linearmente independente e gera M.*

Definição 1.1.5. *Dizemos que um A-módulo M é um A-**módulo livre** quando existe um conjunto B de elementos de M que é uma base de M sobre A. Se B é finito, dizemos que M é um A-**módulo livre de posto finito**.*

Lema 1.1.1. *[31, pág. 20] Se T é um conjunto parcialmente ordenado, então as seguintes afirmações são equivalentes:*

1. *Todo subconjunto não vazio de T tem um elemento maximal.*
2. *Toda sequência crescente $(t_n)_{n\geq 0}$ de elementos de T é estacionária, ou seja, existe n_0 tal que $t_n = t_{n_0},\ \forall n \geq n_0$.* ■

Teorema 1.1.1. *[31, pág. 20] Seja M um A-módulo. As seguintes condições são equivalentes:*

1. *Toda familia não-vazia de submódulos de M contém um elemento maximal, com relação à inclusão.*
2. *Toda sequência crescente $(M_n)_{n\geq 0}$, com relação à inclusão, de submódulos de M é estacionária.*
3. *Todo submódulo de M é do tipo finito.* ■

Lema 1.1.2. *[31, pág. 18] Se $\mathcal{I}$ e $\mathcal{J}$ são ideais de A tal que $\mathcal{I} + \mathcal{J} = A$, então $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$ e o homomorfismo canônico $\varphi : A \longrightarrow A/\mathcal{I} \times A/\mathcal{J}$ induz um isomorfismo $\theta : A/\mathcal{I}\mathcal{J} \longrightarrow A/\mathcal{I} \times A/\mathcal{J}$.* ■

Lema 1.1.3. *[31, pág. 18] Se $\{\mathcal{I}_i\}_{1\leq i\leq r}$ é um conjunto finito de ideais de A tal que $\mathcal{I}_i + \mathcal{I}_j = A$, para $i \neq j$, então existe um isomorfismo canônico de $A/\mathcal{I}_1 \cdots \mathcal{I}_r$ em $\prod_{i=1}^{r} A/\mathcal{I}_i$.* ■

A partir de agora apresentamos resultados sobre módulos sobre anéis principais juntamente com suas principais propriedades.

Proposição 1.1.1. *[31, pág. 20] Se A é um anel principal, então toda familia não vazia de ideais de A possui um elemento maximal.* ■

Teorema 1.1.2. *[31, pág 21] Se A é um anel principal, M um A-módulo livre de posto n e M' um A-submódulo de M, então*

1. *M' é livre de posto q, onde $0 \leq q \leq n$.*

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

Corolário 1.1.1. *[31, pág. 22] Se A é um anel principal, e M um A-módulo do tipo finito, então M é isomorfo a $\prod_{i=1}^{n} A/\mathcal{I}_i$, onde os $\mathcal{I}_i$'s são ideais de A tais que $\mathcal{I}_n \subset \cdots \subset \mathcal{I}_2 \subset \mathcal{I}_1$.* ■

Definição 1.1.6. *Sejam A um anel principal e M um A-módulo. Dizemos que M é **livre de torção** se $ax = 0$, com $a \in A$, $x \in M$, implicar que $a = 0$ ou $x = 0$.*

Corolário 1.1.2. *[31, pág. 22] Se A é um anel principal e M módulo sobre A do tipo finito que é livre de torção, então M é livre.* ■

Corolário 1.1.3. *[31, pág. 22] Se A é um anel principal e M módulo sobre A do tipo finito, então M é isomorfo a um produto finito de módulos M_i, onde cada M_i é igual a A ou ao quociente A/Ap^s, com p primo.* ■

Corolário 1.1.4. *[31, pág. 22] Se G é um grupo comutativo finito, então existe $x \in G$, cuja ordem é o mínimo múltiplo comum das ordens dos elementos de G.* ■

1.1.2 Módulos noetherianos

Nesta seção, apresentamos as definições e algumas propriedades sobre módulos noetherianos e anéis noetherianos, onde um dos principais resultados é que todo ideal não nulo de um anel noetheriano contém um produto de ideais primos.

Definição 1.1.7. *Sejam A um anel e M um A-módulo. Dizemos que M é um A-**módulo noetheriano** se satisfaz uma das seguintes condições:*

1. *Todo conjunto não vazio de submódulos de M contém um elemento maximal.*

2. *Toda sequência crescente de submódulos de M é estacionária.*

3. *Todo submódulo de M é finitamente gerado.*

Definição 1.1.8. *Um anel A é chamado* ***anel noetheriano*** *quando considerado como um A-módulo for noetheriano.*

Observação 1.1.1. *Se A é um anel principal, então A é noetheriano, uma vez que seus ideais são submódulos gerados por um único elemento.*

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

Demonstração: Suponha que M é noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M', que também é uma sequência de submódulos de M. Como M é noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária, ou seja, M' é noetheriano. Para mostrarmos que $\frac{M}{M'}$ é noetheriano, sejam $S = \{$conjunto dos submódulos de M contendo $M'\}$ e $S' = \{$conjunto dos submódulos de $\frac{M}{M'}\}$. Assim, existe uma aplicação bijetora $\varphi : S \longrightarrow S'$ definida por $\varphi(H) = \phi(H)$ onde $\phi : M \longrightarrow \frac{M}{M'}$ é o homomorfismo canônico. A inversa de φ é dada por $\theta : S' \longrightarrow S$, onde $\theta(H') = \phi^{-1}(H')$. Através do isomorfismo ϕ, segue que $\frac{M}{M'}$ também é noetheriano, uma vez que se $(H'_n)_{n\geq 0}$ é uma sequência crescente de submódulos de $\frac{M}{M'}$, então $(\theta(H'_n))_{n\geq 0}$ é uma sequência crescente de submódulos de M e como M é noetheriano, segue que $(\theta(H'_n))_{n\geq 0}$ é estacionária, o que implica que $(H'_n)_{n\geq 0}$ é estacionária, isto é, $\frac{M}{M'}$ é noetheriano. Reciprocamente, suponha que M' e $\frac{M}{M'}$ são noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M. Como M' é noetheriano, segue que a sequência $(M' \cap M_n)_{n\geq 0}$ é estacionária, e como $\frac{M}{M'}$ é noetheriano, segue que a sequência $\left(\frac{M_n + M'}{M'}\right)_{n\geq 0}$ é estacionária. Assim, a sequência $(M_n + M')_{n\geq 0}$ é estacionária, e portanto, $(M_n)_{n\geq 0}$ é estacionária, ou seja, M é noetheriano. ■

Corolário 1.1.5. *Se A é um anel e $M_1, \ldots, M_n$ são A-módulos noetherianos, então $M_1 \times \cdots \times M_n$ é um A-módulo noetheriano.*

Demonstração: Faremos a prova por indução sobre n. Para $n = 2$, identificando $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$ e $M_2 \simeq \{0\} \times M_2 \subseteq M_1 \times M_2$, segue que $\frac{M_1 \times M_2}{M_1 \times \{0\}}$ é isomorfo a M_2. Como M_2 e $M_1 \times \{0\}$ são noetherianos, segue da Proposição 1.1.2, que $M_1 \times M_2$ é noetheriano. Agora, suponha por hipótese de indução, que $M = M_1 \times \cdots \times M_{n-1}$ é noetheriano. Como M_n é noetheriano, segue do caso $n = 2$ que $M = M_1 \times \cdots \times M_n$ é noetheriano. ■

Corolário 1.1.6. *Se A é um anel noetheriano e M um A-módulo finitamente gerado, então M é um A-módulo noetheriano.*

Demonstração: Seja $\{e_1, \ldots, e_n\}$ um conjunto de geradores de M sobre A. A aplicação $\varphi : A^n \longrightarrow M$ definida por $\varphi(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i e_i$ é um homomorfismo sobrejetor e $\frac{A^n}{Ker(\varphi)}$ é isomorfo a M. Pelo Corolário 1.1.5, segue que A^n é noetheriano, e da Proposição 1.1.2, segue que $Ker(\varphi)$ e M são noetherianos. ■

Proposição 1.1.3. *Se um ideal primo $\mathcal{P}$ de um anel A contém um produto $\mathcal{I}_1 \cdots \mathcal{I}_n$ de ideais de A, então $\mathcal{P}$ contém pelo menos um dos ideais $\mathcal{I}_i$.*

Demonstração: Suponha que $\mathcal{I}_i \not\subset \mathcal{P}$, $\forall\, i = 1, \ldots, n$. Assim, para cada $i = 1, \ldots, n$ existe um elemento $\alpha_i \in \mathcal{I}_i - \mathcal{P}$. Assim, $\alpha_1 \cdots \alpha_n \notin \mathcal{P}$, pois $\mathcal{P}$ é um ideal primo, e $\alpha_1 \cdots \alpha_n \in \mathcal{I}_1 \cdots \mathcal{I}_n \subset \mathcal{P}$ o que é um absurdo, uma vez que $\alpha_i \notin \mathcal{P}$, $\forall\, i = 1, \ldots, n$. Portanto, $\mathcal{I}_i \subset \mathcal{P}$, para algum $i = 1, \ldots, n$. ■

Proposição 1.1.4. *Se A é um anel noetheriano, então todo ideal não nulo de A contém um produto de ideais primos não nulos de A.*

Demonstração: Sendo A noetheriano, segue que seus ideais são A-módulos noetherianos. Seja F o conjunto de todos os ideais não nulos de A que não contém um produto de ideais primos não nulos de A e suponha que $F \neq \emptyset$. Como A é noetheriano segue que F possui um elemento maximal M. O ideal M não é primo, pois caso contrário, M não pertenceria a F. Além disso, $M \neq A$. Como M não é um ideal primo, segue que existem elementos $x, y \in A - M$ tais que $xy \in M$, e que os ideais $\langle x \rangle + M$ e $\langle y \rangle + M$ contém M propriamente. Pela maximalidade de M, segue que estes ideais não estão em F, e assim, existem ideais primos não nulos $\mathcal{P}_1, \ldots, \mathcal{P}_r$, $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$ de A, tais que $\langle x \rangle + M \supset \mathcal{P}_1 \cdots \mathcal{P}_r$ e $\langle y \rangle + M \supset \mathcal{Q}_1 \cdots \mathcal{Q}_s$. Assim, $M \supset \langle xy \rangle + M \supset \mathcal{P}_1 \cdots \mathcal{P}_r \mathcal{Q}_1 \cdots \mathcal{Q}_s$, o que é um absurdo. Portanto $F = \emptyset$, isto é, todo ideal não nulo de A contém um produto de ideais primos não nulos de A. ■

1.2 Anel de inteiros e anel de Dedekind

Nesta seção apresentamos conceitos introdutórios da Teoria Algébrica dos Números e conceitos um pouco mais avançados, onde os principais objetivos são os resultados sobre anel de inteiros, provar que o anel de inteiros algébricos de um corpo de números é um domínio de Dedekind e mostrar a unicidade da fatoração de um ideal não nulo como um produto de

ideais primos. Na Subseção 1.2.1, apresentamos o conceito de elementos inteiros sobre um anel e mostramos que o conjunto dos elementos inteiros sobre um anel forma um anel. Na Subseção 1.2.2, apresentamos o conceito de norma e traço em uma extensão de anéis e sobre extensões de corpos. Nas Subseção 1.2.3, apresentamos os anéis de Dedekind, onde provamos que em um anel de Dedekind todo ideal é um produto de ideais primos. Na Subseção 1.2.4, apresentamos a definição e divisibilidade sobre ideais fracionáiros. E por fim, na Subseção 1.2.5, apresentamos a norma de ideais e principais resultados.

1.2.1 Elementos inteiros

Nesta seção, apresentamos o conceito de elementos inteiros sobre um anel e definimos o anel de inteiros.

Definição 1.2.1. *Sejam $A \subseteq B$ anéis. Um elemento $\alpha \in B$ é chamado* ***inteiro sobre*** *A se α é raiz de um polinômio mônico com coeficientes em A, isto é, se existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Em particular, todo elemento de A é inteiro sobre A. Se B é o corpo dos números complexos e A é corpo dos números racionais, o elemento α é chamado* ***número algébrico****. Se o anel A for os números inteiros, o elemento α é chamado* ***inteiro algébrico****.*

Teorema 1.2.1. *[31, pág. 27] Sejam $A \subseteq B$ anéis e α um elemento de B. As seguintes afirmações são equivalentes:*

1. *α é inteiro sobre A.*
2. *O anel $A[\alpha]$ é um A-módulo finitamente gerado.*
3. *Existe um subanel R de B contendo A e α que é um A-módulo finitamente gerado.* ■

Proposição 1.2.1. *[31, pág. 28] Sejam $A \subseteq B$ anéis e $\alpha_1, \alpha_2, \ldots, \alpha_n \in B$. Se α_i é inteiro sobre A e α_i é inteiro sobre $A[\alpha_1, \ldots, \alpha_{i-1}]$, para $i = 1, \ldots, n$, então $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ é um A-módulo finitamente gerado.* ■

Corolário 1.2.1. *Sejam $A \subseteq B$ anéis. Se $\alpha_1, \ldots, \alpha_n$ são elementos de B que são inteiros sobre A, então $A[\alpha_1, \alpha_2, \ldots, \alpha_n]$ é um A-módulo finitamente gerado.*

Demonstração: Como α_i é inteiro sobre A, segue que α_i é inteiro sobre $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$, para $i = 1, 2, \ldots, n$. Pela Proposição 1.2.1, segue o resultado. ■

Corolário 1.2.2. *Sejam $A \subseteq B$ anéis. Se α e β são elementos de B que são inteiros sobre A, então $\alpha+\beta$, $\alpha-\beta$ e $\alpha\beta$ são inteiros sobre A.*

Demonstração: Como $A[\alpha,\beta]$ é um subanel de B e $\alpha,\beta \in A[\alpha,\beta]$, segue que $\alpha+\beta$, $\alpha-\beta$ e $\alpha\beta \in A[\alpha,\beta]$. Pela Proposição 1.2.1, como α e β são inteiros sobre A, segue que $A[\alpha,\beta]$ é um A-módulo finitamente gerado. Logo, existe o subanel $R = A[\alpha,\beta]$ de B contendo A, $\alpha+\beta$, $\alpha-\beta$ e $\alpha\beta \in A[\alpha,\beta]$. Assim, pelo item 3 do Teorema 1.2.1, segue que $\alpha+\beta$, $\alpha-\beta$ e $\alpha\beta$ são inteiros sobre A. ■

Definição 1.2.2. *Sejam A e B anéis tal que $A \subseteq B$. O conjunto dos elementos de B que são inteiros sobre A é chamado* ***fêcho inteiro*** *de A em B ou* ***anel de inteiros*** *de A em B e denotado por $\mathcal{O}_B$. Se A é um domínio e $B = \mathbb{K}$ é o seu corpo de frações, dizemos que $\mathcal{O}_{\mathbb{K}}$ é o* ***anel de inteiros*** *de A em $\mathbb{K}$.*

Corolário 1.2.3. *Sejam A e B anéis tais que $A \subseteq B$.*

1. *O conjunto $\mathcal{O}_B$ é um subanel de B que contém A.*
2. *Se R é um subanel de B que é um A-módulo finitamente gerado, então R está contido em $\mathcal{O}_B$.*

Demonstração: Pelo Corolário 1.2.2, segue que $\mathcal{O}_B$ é um subanel de B. Já que todo elemento de A é inteiro sobre A, segue que $\mathcal{O}_B$ contém A. Para o item 2, sejam R um subanel de B que é um A-módulo finitamente gerado e $\{\alpha_1,\ldots,\alpha_n\}$ um conjunto finito de geradores de R. Se $\alpha \in R$, então $A[\alpha]$ é finitamente gerado como A-módulo, pois $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, com $a_i \in A$. Assim, pelo Teorema 1.2.1, segue que α é inteiro sobre A, ou seja, $\alpha \in \mathcal{O}_B$. Portanto, R está contido em $\mathcal{O}_B$. ■

Definição 1.2.3. *Sejam A e B anéis tais que $A \subseteq B$. Quando $\mathcal{O}_B = B$, dizemos que B* ***é inteiro sobre*** *A.*

Proposição 1.2.2. *[31, pág. 29] Sejam $A \subseteq B \subseteq R$ anéis. Assim, R é inteiro sobre B e B é inteiro sobre A, se, e somente se, R é inteiro sobre A.* ■

Proposição 1.2.3. *[31, pág. 29] Sejam B um domínio e A um anel tal que $A \subseteq B$ e B é inteiro sobre A. Assim, B é um corpo se, e somente se, A é um corpo.* ■

Definição 1.2.4. *Sejam A e B anéis tal que $A \subseteq B$. Dizemos que A é* ***integralmente fechado*** *em B quando $\mathcal{O}_B = A$. Se A é um domínio e $\mathbb{K}$ é o seu corpo de frações, dizemos que A é* ***integralmente fechado*** *se $\mathcal{O}_{\mathbb{K}} = A$.*

Definição 1.2.5. *$\mathbb{K}$ é* ***corpo de números*** *se é uma extensão finita de $\mathbb{Q}$.*

Definição 1.2.6. *Se $\mathbb{K}$ é um corpo de números, então qualquer base de $\mathcal{O}_{\mathbb{K}}$ é chamada de* ***base integral*** *de $\mathbb{K}$.*

Observação 1.2.1. *Sejam A um domínio e $\mathbb{K}$ o seu corpo de frações. O fêcho inteiro $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado. De fato, o corpo $\mathbb{K}$ também é o corpo de frações de $\mathcal{O}_{\mathbb{K}}$ e o fêcho inteiro de $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre $\mathcal{O}_{\mathbb{K}}$. Como $A \subseteq \mathcal{O}_{\mathbb{K}}$, segue que $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre A. Portanto, todo elemento inteiro de $\mathcal{O}_{\mathbb{K}}$ inteiro sobre A pertence a $\mathcal{O}_{\mathbb{K}}$. Assim, $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado.*

Observação 1.2.2. *Todo anel principal é integralmente fechado. De fato, por definição, um anel principal é um domínio. Seja α um elemento de $\mathbb{K}$, onde $\mathbb{K}$ o corpo de frações de A. Suponha que $\alpha \in \mathcal{O}_{\mathbb{K}}$, ou seja, que α é inteiro sobre A. Logo, α é raiz de um polinômio mônico com coeficientes em A, ou seja, $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ com $a_i \in A$, para $i = 1, 2, \ldots, n-1$. Tomando $\alpha = \frac{b}{c}$, onde b e c são elementos de A e primos entre si, e substituindo na equação, segue que $\frac{b^n}{c^n} + a_{n-1}\frac{b^{n-1}}{c^{n-1}} + \cdots + a_1\frac{b}{c} + a_0 = 0$. Agora, multiplicando por c^n ficamos com $b^n + a_{n-1}b^{n-1}c + \cdots + a_1bc^{n-1} + a_0c^n = b^n + c(a_{n-1}b^{n-1} + \cdots + a_1bc^{n-2} + a_0c^{n-1}) = 0$. Assim, $b^n = -c(a_{n-1}b^{n-1} + \cdots + a_1bc^{n-2} + a_0c^{n-1})$, e assim, c divide b^n. Como b e c são primos entre si, aplicando repetidamente o Lema de Euclides, segue que c divide b. Logo, c é um elemento inversível em A, e assim, $\alpha = \frac{b}{c} \in A$. Portanto, A é integralmente fechado.*

1.2.2 Norma e traço

Nesta seção, apresentamos os conceitos de norma e traço de um elemento e suas principais propriedades.

Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto finito n. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de B sobre A e $\varphi : B \longrightarrow B$ um homomorfismo. Assim,

$$\begin{cases} \varphi(\alpha_1) = a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n \\ \varphi(\alpha_2) = a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n \\ \qquad \vdots \\ \varphi(\alpha_n) = a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n, \end{cases}$$

com $a_{ij} \in A$, e $1 \leq i, j \leq n$. Na forma matricial, segue que

$$\begin{pmatrix} \varphi(\alpha_1) \\ \varphi(\alpha_2) \\ \vdots \\ \varphi(\alpha_n) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Definição 1.2.7. *Seja o endomorfismo $\varphi_\alpha : B \longrightarrow B$ dado por $\varphi_\alpha(x) = \alpha x$, com $\alpha \in B$.*

1. *O **traço** de $\alpha \in B$ relativo a A é definido como o traço do endomorfismo φ_α e denotamos por $Tr_{B|A}(\alpha) = Tr_{B|A}(\varphi_\alpha)$.*

2. *A **norma** de $\alpha \in B$ relativo a A é definida como o determinante do endomorfismo φ_α e denotamos por $N_{B|A}(\alpha) = det(\varphi_\alpha)$.*

3. *O **polinômio característico** de $\alpha \in B$ relativo a A é definido como o polinômio característico do endomorfismo φ_α e denotamos por $f_\alpha(x) = det(xI - \varphi_\alpha)$.*

Observação 1.2.3. *Se $\alpha, \beta \in B$ e $a \in A$, então*

1. *$\varphi_\alpha + \varphi_\beta = \varphi_{\alpha+\beta}$,*

2. *$\varphi_\alpha \circ \varphi_\beta = \varphi_{\alpha\beta}$ e*

3. *$\varphi_{a\alpha} = a\varphi_\alpha$.*

Além disso, a matriz de φ_a em relação a uma base de B sobre A é uma matriz diagonal, onde a é a entrada de todas as diagonais.

Para um endomorfismo φ, segue da Álgebra Linear que

1. o **traço** de φ é definido por $Tr_{B|A}(\varphi) = \sum_{i=1}^{n} a_{ii}$,

2. a **norma** de φ é definida por $N_{B|A}(\varphi) = \det(a_{ij})$, e

3. o **polinômio característico** de φ é definido por $det(xI - \varphi) = det(x\delta_{ij} - a_{ij})$.

Para os endomorfismos φ e ρ, segue que

1. $Tr_{B|A}(\varphi + \rho) = Tr_{B|A}(\varphi) + Tr_{B|A}(\rho)$,

2. $det(\varphi \cdot \rho) = det(\varphi)det(\rho)$ e

3. $det(xI - \varphi) = x^n - (Tr_{B|A}(\varphi))x^{n-1} + \cdots + (-1)^n det(\varphi)$.

Agora, sejam $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{M}$ corpos tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{K}] = n$. 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. $N_{\mathbb{L}|\mathbb{K}}(a) = a^n$;

5. $N_{\mathbb{L}|\mathbb{K}}(a\alpha) = a^n N_{\mathbb{L}|\mathbb{K}}(\alpha)$;

6. $N_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\beta)$;

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

8. $T_{\mathbb{L}|\mathbb{K}}(\alpha) = T_{\mathbb{M}|\mathbb{K}}(T_{\mathbb{L}|\mathbb{M}}(\alpha))$.

Proposição 1.2.4. *[31, pág. 36] Sejam $\mathbb{K}$ um corpo finito ou de característica zero, $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$ de grau n e α um elemento de $\mathbb{L}$. Se $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$-vezes, então*

1. $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n$,

2. $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n$ *e*

3. $m_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

Além disso, o polinômio característico é a $[\mathbb{L} : \mathbb{K}(\alpha)]$-ésima potência do polinômio minimal de α sobre $\mathbb{K}$. ■

Observação 1.2.4. *Da Proposição 1.2.4, segue que*

1. $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = mTr_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha)$,

2. $N_{\mathbb{L}|\mathbb{K}}(\alpha) = (N_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha))^m$ *e*

3. $f_\alpha(x) = (m_\alpha(x))^m$.

Proposição 1.2.5. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações, onde $\mathbb{K}$ tem característica zero. Se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e $\alpha \in \mathbb{L}$ é um elemento inteiro sobre A, então os coeficientes do polinômio característico f_α são inteiros sobre A. Em particular, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são inteiros sobre A.*

Demonstração: Pela Proposição 1.2.4, segue que o polinômio característico de α é dado por $f_\alpha(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, onde $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α. Como os coeficientes de $f_\alpha(x)$ são, a menos de isomorfismo, somas e produtos dos α_i, segue que é suficiente mostrar que os α_i são inteiros sobre A, uma vez que, pelo Corolário 1.2.2, segue que a soma, a diferença e o produto são inteiros sobre A. Pela Teoria de Galois, segue que, cada α_i é um conjugado de α sobre $\mathbb{K}$, e assim, existe um $\mathbb{K}$-isomomorfismo $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$ tal que $\sigma_i(\alpha) = \alpha_i$, para todo $i = 1, \ldots, n$. Assim, como α é inteiro sobre A, segue que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, com $a_i \in A$, não todos nulos. Aplicando σ_i, segue que $\sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \cdots + a_0 = 0$, e consequentemente, $\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_1\alpha_i + a_0 = 0$, ou seja, α_i é inteiro sobre A, para cada $i = 1, 2, \ldots, n$. Portanto, os coeficientes de $f_\alpha(x)$ são inteiros sobre A. ■

Corolário 1.2.4. *Se A é um anel integralmente fechado, então os coeficientes do polinômio característico $f_\alpha(x)$ são elementos de A. Em particular, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de A.*

Demonstração: Por definição esses elementos são elementos de $\mathbb{K}$. Como A é integralmente fechado, segue que os coeficientes de $f_\alpha(x)$ pertencem a A. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de A. ■

Proposição 1.2.6. *Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_\mathbb{L}$ o anel de inteiros de A em $\mathbb{L}$. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$, onde $\det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$ e $\alpha \in \mathbb{L}$. Se $Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.*

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

$$0 = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\alpha_j) = a_1 Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_j) + a_2 Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_j) + \cdots + a_n Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_j),$$

para cada $j = 1, \ldots, n$, e na forma matricial,

$$\begin{bmatrix} Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_1) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_1) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_1) \\ Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_2) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_2) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_n) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_n) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$, segue que $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ■

Corolário 1.2.5. *A aplicação $\rho : \mathbb{L} \longrightarrow Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$ dada por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta)$, com $\beta \in \mathbb{L}$ é um isomorfismo.*

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

$$\begin{aligned} \rho(\alpha_1 + \alpha_2)(\beta) = S_{\alpha_1+\alpha_2}(\beta) = Tr_{\mathbb{L}|\mathbb{K}}((\alpha_1 + \alpha_2)\beta) &= Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\beta) + Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\beta) \\ &= S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (\rho(\alpha_1) + \rho(\alpha_2))(\beta), \ e \\ \rho(a\alpha)(\beta) = S_{a\alpha}(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(a\alpha\beta) = aTr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) &= aS_\alpha(\beta) = a\rho(\alpha)(\beta), \end{aligned}$$

para todo $\beta \in \mathbb{L}$. Assim, ρ é um homomorfismo. Agora, se $\alpha \in \mathbb{L}$ é tal que $\rho(\alpha) = 0$, então $\rho(\alpha)(\beta) = S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{L}$. Pela Proposição 1.2.6, segue que $\alpha = 0$. Assim, ρ é injetora. Além disso, como $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K}))$, segue que ρ é sobrejetora. Portanto, ρ é um isomorfismo. ■

Teorema 1.2.2. *Se A é um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_\mathbb{L}$ o anel de inteiros de A em $\mathbb{L}$, então $\mathcal{O}_\mathbb{L}$ é um A-submódulo de um A-módulo livre.*

Demonstração: Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como toda extensão finita é algébrica, segue que os α_i's são algébricos sobre $\mathbb{K}$, ou seja, existem $a_i \in A$, para $i = 0, 1, \ldots, n$, não todos nulos, tal que $a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_0 = 0$. Supondo, sem perda de generalidade, que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1}, segue que

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

ou seja, $a_n\alpha_i$ é inteiro sobre A, para $i = 1, 2, \ldots, n$. Agora, seja $a_n\alpha_i = \beta_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. Provemos que $\{\beta_1, \ldots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Para isso, suponhamos que $b_1\beta_1+b_2\beta_2+\cdots+b_n\beta_n = 0$, onde $b_i \in A$, para $i = 1, \ldots, n$. Logo, $b_1a_n\alpha_1+b_2a_n\alpha_2+\cdots+b_na_n\alpha_n = 0$, e como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_ia_n = 0$, e portanto, $b_i = 0$ para $i = 1, \ldots, n$. Assim, $\{\beta_1, \ldots, \beta_n\}$ é linearmente independente e como possui n elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.2.5, segue que para $i, j = 1, \ldots, n$, existe uma base dual $\{\gamma_1, \ldots, \gamma_n\}$ tal que $\rho(\beta_i)(\gamma_j) = S_{\beta_i}(\gamma_j) = Tr_{\mathbb{L}|\mathbb{K}}(\beta_i\gamma_j) = \delta_{ij}$. Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $\alpha\beta_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \ldots, n$. Pelo Corolário 1.2.4, segue que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta_i) \in A$, para $i = 1, \ldots, n$. Assim, como $\alpha = c_1\gamma_1 + \cdots + c_n\gamma_n$, com $c_i \in \mathbb{K}$, para $i = 1, \ldots, n$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta_i) = c_i \in A$, para $i = 1, \ldots, n$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A-módulo livre gerado por $\{\gamma_1, \ldots, \gamma_n\}$. ■

Corolário 1.2.6. *Se A é um anel principal, então:*

1. *$\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

2. *Se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal, então $\mathcal{I}$ é um A-módulo livre de posto n.*

Demonstração: Provemos o item 1. Se A é um anel principal, então pelo Teorema 1.1.2, segue que um submódulo de um A-módulo livre é livre de posto menor ou igual a n. Logo, pelo Teorema 1.2.2, segue que $\mathcal{O}_{\mathbb{L}}$ contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$ que possui n elementos. Portanto, $\mathcal{O}_{\mathbb{L}}$ tem posto n. Já para a prova do item 2, sejam α um elemento não nulo de $\mathcal{I}$ e $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$. Se $a_1\alpha\alpha_1 + \cdots + a_n\alpha\alpha_n = 0$, com $a_i \in A$, para $i = 1, \ldots, n$, então $a_i\alpha = 0$ para $i = 1, \ldots, n$. Como A é um domínio, segue que $a_i = 0$, para $i = 1, \ldots, n$. Assim, $\{\alpha\alpha_1, \ldots, \alpha\alpha_n\} \subset \mathcal{I}$ é linearmente independente sobre A. Portanto, $\mathcal{I}$ é um A-módulo livre de posto n. ■

Proposição 1.2.7. *Se A é um anel noetheriano e integralmente fechado, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado e um anel noetheriano.*

Demonstração: Pelo Teorema 1.2.2, segue que $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre de posto n, e portanto, $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado. Pelo Corolário 1.1.6, segue que $\mathcal{O}_{\mathbb{L}}$ é um A-módulo noetheriano. Como os ideais de $\mathcal{O}_{\mathbb{L}}$ são A-submódulos de $\mathcal{O}_{\mathbb{L}}$, e sendo $\mathcal{O}_{\mathbb{L}}$ um A-módulo noetheriano, segue que os ideais de $\mathcal{O}_{\mathbb{L}}$ são noetherianos. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano. ■

1.2.3 Anel de Dedekind

Nesta subseção os principais objetivos são provar que o anel de inteiros algébricos de um corpo de números é um domínio de Dedekind e mostrar a unicidade da fatoração de um ideal não nulo como um produto de ideais primos neste domínio.

Definição 1.2.8. *Um domínio A é chamado um **anel de Dedekind**, se A é noetheriano, integralmente fechado e se todo ideal primo não nulo de A é maximal.*

Observação 1.2.5. *Todo domínio principal A é um domínio de Dedekind. De fato, pelo Observação 1.1.1, segue que A é noetheriano. Pela Observação 1.2.2, segue que é A integralmente fechado. Além disso, em um domínio principal todo ideal primo não nulo é maximal. Portanto, A é um domínio de Dedekind.*

Proposição 1.2.8. *Se $A \subset B$ são anéis e $\mathcal{P}$ um ideal primo de B, então $\mathcal{P} \cap A$ é um ideal primo de A.*

Demonstração: Consideremos os seguintes homomorfismos $A \xrightarrow{i} B \xrightarrow{\pi} \dfrac{B}{\mathcal{P}}$, onde i é a inclusão e π a projeção, e seja o homomorfismo $\theta = \pi \circ i : A \longrightarrow B/\mathcal{P}$ definido por $\theta(a) = a+\mathcal{P}$, $\forall a \in A$. Assim, θ é um homomorfismo, pois é composição de homomorfismos, e $Ker(\theta) = A \cap \mathcal{P}$, pois se $x \in Ker(\theta)$ então $x \in A$ e $\theta(x) = \overline{0}$ o que implica que $x \in A$ e $x + \mathcal{P} = \overline{0}$, ou seja, $x \in A \cap \mathcal{P}$. Logo, $Ker(\theta) \subset A \cap \mathcal{P}$. Por outro lado, se $y \in A \cap \mathcal{P}$ então $\theta(y) = (\pi \circ i)(y) = \pi(y) = y + \mathcal{P} = \overline{0}$ e assim, $y \in Ker(\theta)$, ou seja, $A \cap \mathcal{P} \subset Ker(\theta)$. Portanto, $Ker(\theta) = A \cap \mathcal{P}$. Logo, pelo Teorema do Isomorfismo de anéis, segue que $A/A \cap \mathcal{P} \simeq Im(\theta) \subset B/\mathcal{P}$. Mas como $B/\mathcal{P}$ é um domínio, segue que $Im(\theta)$ é um domínio. Portanto, $A/A \cap \mathcal{P}$ é um domínio, ou seja, $A \cap \mathcal{P}$ é um ideal primo. ■

Teorema 1.2.3. *Se A é um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de grau finita de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind.*

Demonstração: Sabemos que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado, noetheriano e é um A-módulo finitamente gerado. Falta mostrar que todo ideal primo $\mathcal{P} \neq \langle 0 \rangle$ de $\mathcal{O}_{\mathbb{L}}$ é maximal. Pela Proposição 1.2.8, segue que $\mathcal{P} \cap A$ é um ideal primo de A. Seja $\alpha \in \mathcal{P} - \langle 0 \rangle$ e consideremos a equação de dependência inteira de α sobre A dada por $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, com $a_i \in A$ para $i = 1, \ldots, n-1$, não todos nulos, de grau mínimo. Assim, $a_0 \neq 0$, pois caso contrário obteríamos uma equação de grau menor. Portanto, $a_0 = -\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) \in$

$\mathcal{O}_{\mathbb{L}}\alpha \cap A \subset \mathcal{P} \cap A$, ou seja, $\mathcal{P} \cap A \neq \langle 0 \rangle$. Como A é Dedekind, segue que $\mathcal{P} \cap A$ é um ideal maximal de A, e portanto, $A/(\mathcal{P} \cap A)$ é um corpo. Além disso, $A/\mathcal{P} \cap A$ pode ser identificado com um subanel de $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$, e como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre A, segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ é inteiro sobre $A/\mathcal{P}\cap A$. Assim, pela Proposição 1.2.3, segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ é corpo, e portanto, $\mathcal{P}$ é maximal. ■

Observação 1.2.6. *Pelo Teorema 1.2.3, segue que o anel do inteiros de um corpo de números é um anel de Dedekind.*

Definição 1.2.9. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Um A-submódulo $\mathcal{I}$ de $\mathbb{K}$ é chamado de* ***ideal fracionário*** *de A se existe um $d \in A - \{0\}$ tal que $d\mathcal{I} \subset A$. Quando $d = 1$ dizemos que $\mathcal{I}$ é um* ***ideal inteiro****.*

Observação 1.2.7. *Segue da Definição 1.2.9 que os elementos de um ideal fracionário $\mathcal{I}$ tem um denominador comum $d \in A$.*

Proposição 1.2.9. *Se A é um domínio noetheriano então todo ideal fracionário $\mathcal{I}$ de A é um A-módulo finitamente gerado.*

Demonstração: Como $\mathcal{I}$ é um ideal fracionário, por definição existe $d \in A - \{0\}$ tal que $d\mathcal{I} \subset A$. Assim, $\mathcal{I} \subset d^{-1}A$. Além disso, $d^{-1}A$ é um A-módulo e a função $\varphi : A \longrightarrow d^{-1}A$ tal que $\varphi(x) = d^{-1}x$ define um isomorfismo entre A e $d^{-1}A$, e como A é noetheriano, segue que $d^{-1}A$ é noetheriano. Portanto, $\mathcal{I}$ é um A-módulo finitamente gerado. ■

Proposição 1.2.10. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Se $\mathcal{I}$ é um A-submódulo finitamente gerado de $\mathbb{K}$, então $\mathcal{I}$ é um ideal fracionário.*

Demonstração: Se $\{x_1, \ldots, x_n\}$ é um conjunto finito de geradores de $\mathcal{I}$, então os x_i's tem um denominador comum d dado pelo produto dos denominadores d_i, onde $x_i = a_i d_i^{-1}$, com a_i, $d_i \in A$. Assim, $d\mathcal{I} \subset A$, e portanto, $\mathcal{I}$ é um ideal fracionário. ■

Observação 1.2.8. *O produto $\mathcal{I}\mathcal{I}'$ de dois ideais fracionários $\mathcal{I}$ e $\mathcal{I}'$ é definido como o conjunto das somas $\sum x_i y_i$ com $x_i \in \mathcal{I}$ e $y_i \in \mathcal{I}$. Se $\mathcal{I}$ e $\mathcal{I}'$ são ideais fracionários com denominadores comuns d e d', então $\mathcal{I} \cap \mathcal{I}'$, $\mathcal{I} + \mathcal{I}'$ e $\mathcal{I}\mathcal{I}'$ são ideais fracionários, os quais são A-submódulos de $\mathbb{K}$ e tem denominadores comuns d ou d', dd' e dd', respectivamente.*

Lema 1.2.1. *Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Se $\mathcal{J}$ é um ideal maximal de A, então $\mathcal{J}' = \{x \in \mathbb{K} : x\mathcal{J} \subset A\}$ é um ideal fracionário de $\mathbb{K}$.*

Demonstração: Como A não é um corpo, segue que $\mathcal{J} \neq \{0\}$ e que $\mathcal{J}' \neq \emptyset$, pois $0 \in \mathcal{J}'$. Sejam x, $y \in \mathcal{J}'$. Pela definição de $\mathcal{J}'$, segue que $x\mathcal{J} \subset A$ e $y\mathcal{J} \subset A$, e portanto, $(x+y)\mathcal{J} = x\mathcal{J} + y\mathcal{J} \subset A$, ou seja, $x+y \in \mathcal{J}'$. Agora, sejam $x \in \mathcal{J}'$ e $a \in A$. Assim, $x\mathcal{J} \subset A$, e portanto, $(xa)\mathcal{J} = a(x\mathcal{J}) \subset A$, isto é, $xa \in \mathcal{J}'$. Por fim, $d\mathcal{J} \subset A$, para todo $d \in A - \{0\}$, ou seja, $\mathcal{J}'$ é um ideal fracionário de $\mathbb{K}$. ■

Teorema 1.2.4. *Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Se $\mathcal{J}$ é um ideal maximal de A, então $\mathcal{J}$ é inversível no conjunto dos ideais fracionários de A.*

Demonstração: Seja $\mathcal{J}$ um ideal maximal de A. Pelo Lema 1.2.1, segue que $\mathcal{J}' = \{x \in \mathbb{K} : \alpha\mathcal{J} \subset A\}$ é um ideal fracionário de $\mathbb{K}$. Pela definição de $\mathcal{J}'$, segue que $\mathcal{J}'\mathcal{J} \subset A$, e como $\mathcal{J}$ é um ideal de A, segue que $\mathcal{J} = \mathcal{J}A \subset \mathcal{J}\mathcal{J}' \subset A$. Como $\mathcal{J}$ é maximal, segue que $\mathcal{J}\mathcal{J}' = \mathcal{J}$ ou $\mathcal{J}\mathcal{J}' = A$. Mostremos que $\mathcal{J}\mathcal{J}' \neq \mathcal{J}$. Para isto, suponhamos por absurdo que $\mathcal{J}\mathcal{J}' = \mathcal{J}$. Seja $\alpha \in \mathcal{J}'$, então $\alpha\mathcal{J} \subset \mathcal{J}, \alpha^2\mathcal{J} \subset \mathcal{J}, \ldots, \alpha^n\mathcal{J} \subset \mathcal{J}$. Se $d \in \mathcal{J}$ é não nulo, então $\alpha^n d \in A$, para todo $n \in \mathcal{J}$. Assim, $A[\alpha]$ é um ideal fracionário de A, e como A é noetheriano, segue da Proposição 1.2.9 que, $A[\alpha]$ é um A-módulo finitamente gerado. Portanto, pelo Teorema 1.2.1, segue que α é inteiro sobre A, e como A é integralmente fechado, segue que $\alpha \in A$, ou seja, $\mathcal{J}' \subset A$. E como $A \subset \mathcal{J}'$, segue que $A = \mathcal{J}'$. Por outro lado, se $a \in \mathcal{J} - \langle 0 \rangle$, então pela Proposição 1.1.4, o ideal aA contém um produto de ideais primos não nulos $\mathcal{P}_1 \cdots \mathcal{P}_n$, de A com n o menor possível. Assim, $\mathcal{J} \supset aA \supset \mathcal{P}_1 \cdots \mathcal{P}_n$. Pela Proposição 1.1.3, segue que $\mathcal{J} \supset \mathcal{P}_i$, para algum $i = 1, \ldots, n$, e sem perda de generalidade, digamos que $\mathcal{J} \supset \mathcal{P}_1$. Como $\mathcal{P}_1$ é maximal pois A é Dedekind, segue que $\mathcal{J} = \mathcal{P}_1$. Tomando $\mathcal{B} = \mathcal{P}_2 \cdots \mathcal{P}_n$, segue que $aA \supset \mathcal{J}\mathcal{B}$ e $aA \not\supset \mathcal{B}$ devido a minimalidade de n. Assim, existe $z \in \mathcal{B}$ tal que $z \notin aA$. Como $\mathcal{J}\mathcal{B} \subset aA$, segue que $\mathcal{J}\frac{z}{a} \subset A$. Assim, $\frac{z}{a} \in \mathcal{J}'$, e como $z \notin aA$, segue que $\frac{z}{a} \notin A$, ou seja, $\mathcal{J}' \neq A$, o que contradiz o fato de $\mathcal{J}' = A$. Portanto, $\mathcal{J}\mathcal{J}' = A$, ou seja, $\mathcal{J}'$ é o inverso de $\mathcal{J}$. ■

Teorema 1.2.5. *Seja A um anel de Dedekind. Se $\mathcal{I} \neq A$ é um ideal não nulo de A, então existem ideais primos não nulos $\mathcal{P}_1, \ldots, \mathcal{P}_t$ de A e inteiros positivos $e_1, \ldots, e_t$ de tal forma que $\mathcal{I}$ pode ser expresso de maneira única como $\mathcal{I} = \prod_{i=1}^{t} \mathcal{P}_i^{e_i}$.*

Demonstração: Pela Proposição 1.1.4, segue que existem ideais primos $\mathcal{P}_1, \ldots, \mathcal{P}_v$ não nulos de A tal que $\mathcal{P}_1 \cdots \mathcal{P}_v \subset \mathcal{I}$. Provemos que $\mathcal{I}$ é um produto de ideais primos por indução sobre v. Se $v = 1$, então $\mathcal{P}_1 \subset \mathcal{I}$, mas como $\mathcal{P}_1$ é maximal, pois A é Dedekind, então segue que $\mathcal{I} = \mathcal{P}_1$, e portanto, $\mathcal{I}$ é primo. Agora, suponhamos que todo ideal que contém um produto

com $v-1$ ideais primos não nulos de A é um produto de ideais primos de A. Temos que $\mathcal{P}_1\cdots\mathcal{P}_v \subset \mathcal{I}$, e como A é Dedekind, segue que $\mathcal{I}$ está contido em um ideal maximal $\mathcal{J}$ de A. Seja $\mathcal{J}^{-1}$ o ideal fracionário inverso de $\mathcal{J}$. Como $\mathcal{J} \supset \mathcal{I} \supset \mathcal{P}_1\cdots\mathcal{P}_v$, segue da Proposição 1.1.3, que $\mathcal{J}$ contém um dos $\mathcal{P}_i's$, para $i = 1,\dots v$. Suponhamos que $\mathcal{J} \supset \mathcal{P}_v$, e assim, $\mathcal{J} = \mathcal{P}_v$, pois $\mathcal{P}_v$ é maximal. Portanto, $\mathcal{P}_1\cdots\mathcal{P}_{v-1} \subset \mathcal{I}\mathcal{J}^{-1} \subset \mathcal{J}\mathcal{J}^{-1} = A$. Da hipótese de indução decorre que $\mathcal{I}\mathcal{J}^{-1} = \mathcal{Q}_1\cdots\mathcal{Q}_s$, com $\mathcal{Q}_j$'s, para $j = 1,\dots,s$, ideais primos não nulos de A, e portanto, $\mathcal{I} = \mathcal{Q}_1\cdots\mathcal{Q}_s\mathcal{P}_v$, como queríamos. Para provar a unicidade, se $\prod_{i=1}^{t}\mathcal{P}^{e_i} = \prod_{j=1}^{h}\mathcal{P}^{e_j}$, então $A = \prod\mathcal{P}^{e_i-e_j}$. Se $e_i - e_j \neq 0$, podemos separar os expoentes positivos e os expoentes negativos e reescrevê-los como $\mathcal{P}_1^{\alpha_1}\mathcal{P}_2^{\alpha_2}\cdots\mathcal{P}_r^{\alpha_r} = \mathcal{Q}_1^{\beta_1}\mathcal{Q}_2^{\beta_2}\cdots\mathcal{Q}_v^{\beta_v}$, com $\mathcal{P}_i$, $\mathcal{Q}_j$ ideais primos não nulos de A e $\alpha_i, \beta_j > 0$ para $\mathcal{P}_i \neq \mathcal{Q}_j$, $\forall i, j$. Portanto, $\mathcal{P}_1$ contém $\mathcal{Q}_1^{\beta_1}\mathcal{Q}_2^{\beta_2}\cdots\mathcal{Q}_v^{\beta_v}$ e pela Proposição 1.1.3, segue que $\mathcal{P}_1 \supset \mathcal{Q}_j$, para algum j. Suponhamos, sem perda de generalidade, que $\mathcal{P}_1 \supset \mathcal{Q}_1$. Como $\mathcal{P}_1$ e $\mathcal{Q}_1$ são ideais maximais, segue que $\mathcal{P}_1 = \mathcal{Q}_1$. Portanto, $e_i - e_j = 0$, isto é, $e_i = e_j$, o que é uma contradição pois $\mathcal{P}_i \neq \mathcal{Q}_j$, $\forall i, j$ e assim, concluímos que a expressão é única. ■

1.2.4 Divisibilidade de ideais fracionários

Definição 1.2.10. *Sejam $\mathcal{I}$ e $\mathcal{J}$ ideais fracionários de um domínio A. Dizemos que $\mathcal{I}$ **divide** $\mathcal{J}$, e denotamos por $\mathcal{I} \mid \mathcal{J}$, quando existe um ideal inteiro $\mathcal{Q}$ de A tal que $\mathcal{J} = \mathcal{I}\mathcal{Q}$.*

Observação 1.2.9. *Note que se $\mathcal{I} \mid \mathcal{J}$, então $\mathcal{J} \subset \mathcal{I}$. De fato, se $\mathcal{I} \mid \mathcal{J}$, então existe um ideal integral $\mathcal{Q}$ de A tal que $\mathcal{J} = \mathcal{I}\mathcal{Q}$. Daí, $\mathcal{J} = \mathcal{I}\mathcal{Q} \subset \mathcal{I}A = \mathcal{I}$.*

Proposição 1.2.11. *Sejam $\mathcal{I}$ e $\mathcal{J}$ ideais fracionários não nulos de um domínio de Dedekind A. Assim, $\mathcal{I} \mid \mathcal{J}$ se, e somente se, $\mathcal{J} \subset \mathcal{I}$.*

Demonstração: Já vimos que $\mathcal{I} \mid \mathcal{J}$ implica $\mathcal{J} \subset \mathcal{I}$. Assim, suponha $\mathcal{J} \subset \mathcal{I}$. Como o conjunto dos ideais fracionários forma um grupo multiplicativo, segue que existe um ideal fracionário $\mathcal{I}^{-1}$ de A. Assim, $\mathcal{J}\mathcal{I}^{-1} \subset \mathcal{I}\mathcal{I}^{-1} = A$, de onde vem que $\mathcal{J}\mathcal{I}^{-1}$ é um ideal inteiro de A que satisfaz $(\mathcal{J}\mathcal{I}^{-1})\mathcal{I} = \mathcal{J}$, o que prova que $\mathcal{I} \mid \mathcal{J}$. ■

Proposição 1.2.12. *Se $\mathcal{I}$ é um ideal não nulo de um domínio de Dedekind A, então existe uma quantidade finita de ideais de A dividindo $\mathcal{I}$.*

Demonstração: Fatorando $\mathcal{I}$ em produto de ideais primos de A, digamos $\mathcal{I} = \prod_{i=1}^{m}\mathcal{P}_i^{e_i}$, segue que os únicos ideais que dividem $\mathcal{I}$ são os da forma $\prod_{i=1}^{m}\mathcal{P}_i^{f_i}$, onde $0 \leq f_i \leq e_i$, para todo

$i = 1, 2, \ldots, m$. ■

1.2.5 Norma de um ideal

Nesta seção, apresentamos o conceito de norma de um ideal do anel de inteiros de um corpo de números e suas principais propriedades, que serão úteis para o cálculo da densidade de centro de reticulados obtidos via corpos de números através do homomorfismo de Minkowski.

Definição 1.2.11. *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_\mathbb{K}$ o anel de inteiros e $\mathcal{I}$ um ideal de $\mathcal{O}_\mathbb{K}$. A **norma do ideal** $\mathcal{I}$ é definida como sendo o número de elementos do anel quociente $\mathcal{O}_\mathbb{K}/\mathcal{I}$, ou seja,*

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

Observação 1.2.10. *Se $0 \neq \alpha \in \mathcal{O}_\mathbb{K}$, então pelo Corolário 1.2.4, segue que $N(\alpha) \in \mathbb{Z}$.*

Proposição 1.2.13. *Se $\alpha \in \mathcal{O}_\mathbb{K}$, então*

$$|N(\alpha)| = \#\frac{\mathcal{O}_\mathbb{K}}{\mathcal{O}_\mathbb{K}\alpha},$$

onde $\mathcal{O}_\mathbb{K}\alpha = \langle\alpha\rangle$ é o ideal de $\mathcal{O}_\mathbb{K}$ gerado por α.

Demonstração: Pelo Corolário 1.2.6, segue que $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\varphi : \mathcal{O}_\mathbb{K} \longrightarrow \mathcal{O}_\mathbb{K}\alpha$ definida por $\varphi(a) = a\alpha$, para $\alpha \in \mathcal{O}_\mathbb{K}$, é um isomorfismo, segue pelo Teorema 1.1.2 que $\mathcal{O}_\mathbb{K}\alpha$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\mathbb{Z}$ é um anel principal e $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre, segue que existe uma base $\{e_1, \ldots, e_n\}$ de $\mathcal{O}_\mathbb{K}$ e $c_1, \ldots, c_n \in \mathbb{Z}$ tal que $\{c_1e_1, \ldots, c_ne_n\}$ é uma base de $\mathcal{O}_\mathbb{K}\alpha$. A aplicação $\psi : \mathcal{O}_\mathbb{K} \longrightarrow \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_n\mathbb{Z}$ definida por $\psi(\sum_{i=1}^{n} a_ie_i) = (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})$ é um homomorfismo sobrejetor, e $\ker(\psi) = \mathcal{O}_\mathbb{K}\alpha$, pois $a = \sum_{i=1}^{n} a_ie_i \in \ker(\psi)$ se, e somente se, $\psi(a) = \bar{0}$ se, e somente se, $\overline{a_i} = \bar{0}$, para $i = 1, \ldots, n$, se, e somente se, $a_i \in c_i\mathbb{Z}$, para $i = 1, \ldots, n$, se, e somente se, c_i divide a_i, para $i = 1, \ldots, n$, se, e somente se, $a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i$. Como $b_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, n$, segue que $a \in \mathcal{O}_\mathbb{K}\alpha$. Portanto, $\ker(\psi) = \langle\alpha\rangle$, e desta forma,

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

Assim, $\#\frac{A}{A\alpha} = c_1c_2\cdots c_n$. Seja a aplicação $\mathbb{Z}$-linear $\mu : \mathcal{O}_\mathbb{K} \longrightarrow \mathcal{O}_\mathbb{K}\alpha$ definida por $\mu(e_i) = c_ie_i$, para $i = 1, \ldots, n$. Logo, $\mu(e_1) = c_1e_1 + 0e_2 + \cdots + 0e_n, \ldots, \mu(e_n) = 0e_1 + \cdots + c_ne_n$ e

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

Proposição 1.2.14. *A norma $N(\mathcal{I})$ é finita.*

Demonstração: Se $\alpha \in \mathcal{I}$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathcal{I}$. Além disso, podemos escrever $\mathcal{O}_{\mathbb{K}}/\mathcal{I}$ como um quociente de $\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$. Assim,

$$\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} = \#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{I}}\#\frac{\mathcal{I}}{\mathcal{O}_{\mathbb{K}}\alpha}.$$

Mas, pela Proposição 1.2.13, segue que $\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}$ é finito. Portanto, $\#\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{I}}$ é finito. ■

Proposição 1.2.15. *[31, pág. 52] Se $\mathcal{I}$ e $\mathcal{J}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$.* ■

Seja $\mathcal{P} \subset \mathcal{O}_{\mathbb{K}}$ um ideal primo. Sejam os homomorfismos de anéis $\mathbb{Z} \xrightarrow{i} A \xrightarrow{\pi} \mathcal{O}_{\mathbb{K}}/\mathcal{P}$, onde i é a inclusão e π a projeção. Assim, $Ker(\pi\circ i) = \mathcal{P}\cap\mathbb{Z}$. Como $\mathbb{Z}/\langle p\rangle \simeq Im(\pi\circ i)$ e $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ é um domínio, segue que $ker(\pi) = \langle p\rangle$, onde p é um número primo. Portanto, $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$, que é um corpo, pode ser visto como um espaço vetorial sobre $\mathbb{Z}/\langle p\rangle$, cuja dimensão é chamada **grau de inércia** de $\mathcal{P}$.

Proposição 1.2.16. *Seja $\mathbb{K}$ um corpo de números.*

1. *Se $\mathcal{P}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{P}) = p^f$, onde f é o grau de inércia de $\mathcal{P}$ e p é o único número primo em $\mathcal{P}$.*

2. *Seja $\mathcal{I}$ um ideal não nulo. Assim, $N(\mathcal{I}) = 1$ se, e somente se, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$.*

3. *Se $N(\mathcal{I})$ é um número primo, então o ideal $\mathcal{I}$ é primo.*

4. *Se $\mathcal{I}$ é um múltiplo do ideal $\mathcal{J}$ e $N(\mathcal{I}) = N(\mathcal{J})$, então $\mathcal{I} = \mathcal{J}$.*

Demonstração: (1) Segue do fato que $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ de dimensão f, ou seja, $N(\mathcal{P}) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{P}}\right) = p^f$. Para (2), se $N(\mathcal{I}) = 1$, então $\#(\mathcal{O}_{\mathbb{K}}/\mathcal{I}) = 1$. Assim,

$\mathcal{O}_{\mathbb{K}} = \mathcal{I}$. Para (3), se $\mathcal{I}$ não é um ideal primo, então, $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$ ou $\mathcal{I} = \mathcal{J}\mathcal{B}$, onde $\mathcal{J}$ e $\mathcal{B}$ são ideais não nulos e distintos de $\mathcal{O}_{\mathbb{K}}$. Assim,

1. Se $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{I}) = 1$, que é contra a hipótese.

2. Se $\mathcal{I} = \mathcal{J}\mathcal{B}$, então $N(\mathcal{I}) = N(\mathcal{J})N(\mathcal{B})$ e como por hipótese $N(\mathcal{I}) = p$, onde p é um número primo, segue que $N(\mathcal{J}) = 1$ e $N(\mathcal{B}) = p$ ou $N(\mathcal{J}) = p$ e $N(\mathcal{B}) = 1$. Porém, se isso ocorrer, por (2), segue que $\mathcal{J} = \mathcal{O}_{\mathbb{K}}$ ou $\mathcal{B} = \mathcal{O}_{\mathbb{K}}$, o que é contra a hipótese. Portanto, $\mathcal{I}$ é um ideal primo.

Para (4), se $\mathcal{I}$ é múltiplo do ideal $\mathcal{J}$, então existe um ideal $\mathcal{B}$ de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{I} = \mathcal{J}\mathcal{B}$. Assim, $N(\mathcal{I}) = N(\mathcal{J})N(\mathcal{B})$. Como $N(\mathcal{I}) = N(\mathcal{J})$, segue que $N(\mathcal{B}) = 1$. Logo, $\mathcal{B} = \mathcal{O}_{\mathbb{K}}$ e $\mathcal{I} = \mathcal{J}$. ■

1.3 Discriminante

Neste seção, apresentamos o cálculo do discriminante de uma extensão de anéis utilizando a teoria algébrica dos números.

1.3.1 Discriminante de uma extensão de anéis

Nesta subseção, apresentamos o conceito de discriminante de uma extensão de anéis. Para isso, sejam A e B anéis tais que $A \subseteq B$ e B é um A-módulo livre de posto finito n. Primeiramente, apresentamos o conceito do discriminante de uma n-upla.

Definição 1.3.1. *Seja $\{\alpha_1, \ldots, \alpha_n\}$ um conjunto de elementos de B. O* ***discriminante da n-upla*** *$(\alpha_1, \ldots, \alpha_n)$ é definido por*

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

onde $i, j = 1, 2, \ldots, n$.

Proposição 1.3.1. *Se $\{\beta_1, \ldots, \beta_n\}$ é um conjunto de elementos de B tal que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in A$, para $i = 1, \ldots, n$, então $\mathcal{D}_{B|A}(\beta_1, \ldots, \beta_n) = (\det(a_{ij}))^2\mathcal{D}_{B|A}(\alpha_1, \ldots, \alpha_n)$.*

Demonstração: Pela definição, segue que

$$\mathcal{D}_{B|A}(\beta_1, \ldots, \beta_n) = \det(Tr_{B|A}(\beta_r\beta_s)),$$

onde $\beta_r = \sum_{i=1}^{n} a_{ri}\alpha_i$, $\beta_s = \sum_{j=1}^{n} a_{sj}\alpha_j$ e $\beta_r\beta_s = \sum_{i=1}^{n} a_{ri}a_{sj}\alpha_i\alpha_j$. Assim,

$$Tr_{B|A}(\beta_r\beta_s) = \sum_{i=1}^{n} a_{ri}a_{sj}Tr_{B|A}(\alpha_i\alpha_j),$$

e na forma matricial

$$(Tr_{B|A}(\beta_r\beta_s)) = (a_{ri})(Tr_{B|A}(\alpha_i\alpha_j))(a_{sj})^t.$$

Logo,

$$\begin{aligned}\mathcal{D}_{B|A}(\beta_1,\ldots,\beta_n) &= \det(Tr_{B|A}(\beta_r\beta_s)) = \det((a_{ri})(Tr_{B|A}(\alpha_i\alpha_j))(a_{sj})^t)\\ &= \det(a_{ri})\det(Tr_{B|A}(\alpha_i\alpha_j))\det((a_{sj})^t) = (\det(a_{i,j}))^2\mathcal{D}_{B|A}(\alpha_1,\ldots,\alpha_n),\end{aligned}$$

o que prova a proposição. ■

Corolário 1.3.1. *Seja A um domínio. Se $\{\alpha_1,\ldots,\alpha_n\}$ e $\{\beta_1,\ldots,\beta_n\}$ são bases de B, então $\mathcal{D}_{B|A}(\alpha_1,\ldots,\alpha_n)$ e $\mathcal{D}_{B|A}(\beta_1,\ldots,\beta_n)$ são associados ou ambos possuem determinantes nulos.*

Demonstração: Como $\{\alpha_1,\ldots,\alpha_n\}$ e $\{\beta_1,\ldots,\beta_n\}$ são bases de B, segue que existem elementos $a_{ij} \in A$ tais que $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, para todo $j = 1,\ldots,n$. Assim, pela Proposição 1.3.1, segue que

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

Como (a_{ij}) é uma matriz inversível, segue que $\det(a_{ij})$ é uma unidade do anel A. Logo, $\mathcal{D}_{B|A}(\alpha_1,\ldots,\alpha_n)$ e $\mathcal{D}_{B|A}(\beta_1,\ldots,\beta_n)$ são elementos associados ou ambos determinantes são nulos. ■

O Corolário 1.3.1 mostra que o discriminante de bases de B sobre A são associados em A, isto é, a matriz (a_{ij}) que expressa uma base em termos da outra tem uma inversa com entradas em A. Assim, $\det(a_{ij})$ e $\det((a_{ij})^{-1})$ são inversíveis em A.

Definição 1.3.2. *O **discriminante de** B **sobre** A é definido como o ideal de A, gerado por $\mathcal{D}_{B|A}(\alpha_1,\ldots,\alpha_n)$, onde $\{\alpha_1,\ldots,\alpha_n\}$ é uma base de B sobre A, e denotado por $\mathcal{D}_{B|A}$ ou $\mathcal{D}(B|A)$.*

Definição 1.3.3. *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ e $\{\alpha_1,\ldots,\alpha_n\}$ uma base de $\mathcal{O}_{\mathbb{K}}$. Definimos o **discriminante** de $\mathbb{K}$ com sendo o discriminante $\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(\alpha_1,\ldots,\alpha_n)$ e denotamos por $\mathcal{D}_{\mathbb{K}}$.*

Proposição 1.3.2. *Seja A um domínio. Se o conjunto $\{\alpha_1, \ldots, \alpha_n\}$ de elementos de B é linearmente dependente sobre A, então $\mathcal{D}_{B|A}(\alpha_1, \ldots, \alpha_n) = 0$.*

Demonstração: Como $\{\alpha_1, \ldots, \alpha_n\}$ é linearmente dependente sobre A, segue que existem $a_1, \ldots, a_n \in A$, não todos nulos, tal que $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$. Reordenando e tomando $a_1 \neq 0$, consideremos o conjunto $\{\alpha'_1, \ldots, \alpha'_n\}$ de elementos de B, onde $\alpha'_1 = 0$ e $\alpha'_i = \alpha_i$, para $i = 2, \ldots, n$. Assim, $\alpha'_i = a_{1i}\alpha_1 + \cdots + a_{ni}\alpha_n$ para $i = 1, 2, \ldots, n$, onde $a_{j1} = a_j$, e se $i > 1$, então $a_{ji} = 1$ para $j = i$ e $a_{ji} = 0$ para $j \neq i$. Assim, $\mathcal{D}_{B|A}(\alpha'_1, \ldots, \alpha'_n) = \mathcal{D}_{B|A}(0, \alpha_2, \ldots, \alpha_n) = 0$, pois a matriz da aplicação traço possui a primeira linha nula. Desta forma, pela Proposição 1.3.1, segue que

$$0 = \mathcal{D}_{B|A}(0, \alpha_2, \ldots, \alpha_n) = \mathcal{D}_{B|A}(\alpha'_1, \ldots, \alpha'_n) = (\det(a_{ij}))^2 \mathcal{D}_{B|A}(\alpha_1, \ldots, \alpha_n).$$

E como

$$(a_{ij}) = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

segue que $\det(a_{ij}) = a_1 \neq 0$. Como A é um domínio, segue que $\mathcal{D}_{B|A}(\alpha_1, \cdots, \alpha_n) = 0$. ■

Lema 1.3.1 (Lema de Dedekind)**.** *Se G é um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \ldots, \sigma_n$ são homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então os σ_i's são linearmente independentes sobre $\mathbb{K}$.*

Demonstração: Suponha por absurdo, que os σ_i's são linearmente dependentes. Assim, existem $a_1, \ldots, a_n \in \mathbb{K}$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i = 0$, com o número r dos a_i's não nulos o menor possível. Assim, $r \geq 2$, pois os σ_i's são não nulos. Se $g \in G$, então

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \cdots + a_r\sigma_r(g) = 0. \tag{1.1}$$

Como os σ_i's são homomorfismos, segue que a Equação (1.1) é válida para todo $g \in G$. Assim, para gh, com $h \in G$, segue que

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_2(h) + \cdots + a_r\sigma_r(g)\sigma_r(h) = 0. \tag{1.2}$$

Multiplicando a Equação (1.1) por $\sigma_1(h)$, segue que

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_1(h) + \cdots + a_r\sigma_r(g)\sigma_1(h) = 0, \tag{1.3}$$

e subtraindo da Equação (1.2), segue que

$$a_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + a_r(\sigma_1(h) - \sigma_r(h))\sigma_r(g) = 0. \tag{1.4}$$

Como isso vale para todo $g \in G$ e como tomamos r o menor possível, segue que $a_2(\sigma_1(h) - \sigma_2(h)) = 0$. Assim, $\sigma_1(h) = \sigma_2(h)$, para todo $h \in G$, pois $a_2 \neq 0$. Mas isto contradiz a hipótese de que os σ_i's são distintos. Portanto, os σ_i's são linearmente independentes. ■

Proposição 1.3.3. *Sejam $\mathbb{L}$ uma extensão finita de grau n de um corpo $\mathbb{K}$, onde $\mathbb{K}$ é finito ou tem característica zero, e $\sigma_1, \ldots, \sigma_n$, os distintos $\mathbb{K}$-isomorfismo de $\mathbb{L}$. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

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

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

$$\begin{aligned} \mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) &= \det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right). \end{aligned}$$

Assim,

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

Logo, $\det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) = \det\left(\sigma_i(\alpha_j)\right)^2$. Portanto, $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$. Agora,

se $\det(\sigma_i(\alpha_j)) = 0$, então existem $a_1, \ldots, a_n \in \mathbb{C}$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$, para $j = 1, \ldots, n$. Pela linearidade, segue que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{L}$, o que é um absurdo, pois pelo Lema 1.3.1 os σ_i são linearmente independentes. Logo, $\det(\sigma_i(\alpha_j))^2 \neq 0$. Portanto, $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0$, como queríamos. ■

Proposição 1.3.4. *Sejam $\mathbb{K}$ um corpo de números de grau n, $\{x_1, \ldots, x_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida no anel $\mathcal{O}_\mathbb{K}$ de inteiros de $\mathbb{K}$. Se o discriminante $\mathcal{D}(x_1, \ldots, x_n)$ é livre de quadrados, então $\{x_1, \ldots, x_n\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$.*

Demonstração: Se $\{e_1, \ldots, e_n\}$ é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$, então $x_j = \sum_{i=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathbb{Z}$. Pela Proposição 1.3.1, segue que $\mathcal{D}(x_1, \ldots, x_n) = (\det(a_{ij}))^2\mathcal{D}(e_1, \ldots, e_n)$. Como $\mathcal{D}(x_1, \ldots, x_n)$ é livre de quadrados, segue que $\det(a_{ij}) = \pm 1$, ou seja, $\{x_1, \ldots, x_n\}$ também é uma base de $\mathcal{O}_\mathbb{K}$ sobre $\mathbb{Z}$. ■

A proposição anterior é muitas vezes útil para determinar o anel de inteiros de um corpo de números.

Proposição 1.3.5. *Sejam $B_1, \ldots, B_r$ anéis comutativos contendo um domínio A. Se cada anel B_i, para $i = 1, 2, \ldots, r$, é um A-módulo livre de posto finito, então*

$$\mathcal{D}(B_1 \times \cdots \times B_r/A) = \prod_{i=1}^{n} \mathcal{D}(B_i/A).$$

Demonstração: Por indução, é suficiente provar a afirmação para $n = 2$. Assim, se $\{\alpha_1, \ldots, \alpha_r\}$ é uma base de B_1 sobre A e se $\{\beta_1, \ldots, \beta_s\}$ é uma base de B_2 sobre A, então $\{(\alpha_1, 0), \ldots, (\alpha_r, 0), (0, \beta_1), \ldots, (0, \beta_s)\}$ é uma base de $B_1 \times B_2$ sobre A. Tomando $\gamma_i = (\alpha_i, 0)$ para $i = 1, \ldots, r$ e $\gamma_{r+i} = (0, \beta_i)$ para $i = 1, \ldots, s$, segue que $\mathcal{D}(B_1 \times B_2/A)$ é o ideal principal de A gerado por $\det(Tr_{B_1\times B_2|A}(\gamma_i\gamma_j)) = \mathcal{D}_{B_1\times B_2|A}(\gamma_1, \ldots, \gamma_{r+s})$. Agora, se $\theta \in B_1$, então $Tr_{B_1\times B_2|A}(\theta, 0) = Tr_{B_1|A}(\theta)$, que podem ser deduzidos considerando as matrizes do endomorfismo $\varphi_{(\theta,0)}$ de $B_1 \times B_2$ e φ_θ de B_1, relativos as bases $\{\beta_1, \ldots, \beta_{r+s}\}$ e $\{\alpha_1, \ldots, \alpha_r\}$, respectivamente. Analogamente, $Tr_{B_1\times B_2|A}(0, \theta) = Tr_{B_2|A}(\theta)$. Assim,

$$\begin{aligned} det(Tr_{B_1\times B_2|A}(\gamma_i\gamma_j)) &= det\begin{pmatrix} Tr_{B_1|A}(\alpha_i\alpha_j) & 0 \\ 0 & Tr_{B_2|A}(\beta_i\beta_j) \end{pmatrix} \\ &= det(Tr_{B_1|A}(\alpha_i\alpha_j)) \det(Tr_{B_2|A}(\beta_i\beta_j)), \end{aligned}$$

e este elemento gera o ideal $\mathcal{D}(B_1/A)\mathcal{D}(B_2/A)$. ■

1.3.2 Discriminante de polinômios

Nesta seção, apresentamos o conceito de discriminante de polinômios.

Definição 1.3.4. *Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$ um polinômio mônico de grau n com raízes $\alpha_1, \ldots, \alpha_n$. O **discriminante de** $f(x)$ é definido por*

$$\mathcal{D}(f) = \prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\alpha_j - \alpha_i) = \prod_{i=1}^{n}\prod_{j=i+1}^{n}(\alpha_j - \alpha_i)^2.$$

Proposição 1.3.6. *Se $\mathbb{K}$ é um corpo finito ou de característica zero, $\mathbb{L} = \mathbb{K}[\alpha]$ uma extensão finita de $\mathbb{K}$ de grau n e $m_\alpha(x)$ o polinômio minimal de α sobre $\mathbb{K}$, então*

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)),$$

onde $m'_\alpha(x)$ é a derivada de $m_\alpha(x)$.

Demonstração: Sejam $\alpha, \alpha^2, \ldots, \alpha^n$ as raízes de $m_\alpha(x)$ em uma extensão de $\mathbb{K}$, que são conjugados de α. Pela Proposição 1.3.3, segue que $\mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2$, onde σ_i, para $1 \leq i \leq n$, são $\mathbb{K}$-isomorfismos de $\mathbb{K}[\alpha]$. Além disso,

$$\det(\sigma_i(\alpha^j)) = \begin{bmatrix} \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_n(\alpha) \\ \sigma_1(\alpha^2) & \sigma_2(\alpha^2) & \cdots & \sigma_n(\alpha^2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha^n) & \sigma_2(\alpha^n) & \cdots & \sigma_n(\alpha^n) \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha)^1 & \sigma_2(\alpha)^1 & \cdots & \sigma_n(\alpha)^1 \\ \sigma_1(\alpha)^2 & \sigma_2(\alpha)^2 & \cdots & \sigma_n(\alpha)^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha)^n & \sigma_2(\alpha)^n & \cdots & \sigma_n(\alpha)^n \end{bmatrix},$$

que é um determinante de Vandermonde. Logo, $\det(\sigma_i(\alpha^j)) = \prod_{1\leq i<j\leq n}(\alpha^i - \alpha^j)$, e assim,

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1\leq i<j\leq n}(\alpha^i - \alpha^j)^2.$$

Por outro lado, como o polinômio minimal de α é dado por $m_\alpha(x) = \prod_{i=1}^{n}(x - \alpha^i)$, segue que

$$m'_\alpha(x) = \sum_{j=1}^{n}\prod_{i=1, i\neq j}^{n}(x - \alpha^i) \quad \text{e} \quad m'_\alpha(\alpha^j) = \prod_{i=1, i\neq j}^{n}(\alpha^j - \alpha^i).$$

Assim,

$$\prod_{j=1}^{n} m'_\alpha(\alpha_j) = \prod_{i,j=1, i\neq j}^{n} (\alpha^j - \alpha^i),$$

e como $\prod_{j=1}^{n} m'_\alpha(\alpha_j) = N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha))$, segue que

$$N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)) = \prod_{i,j=1, i\neq j}^{n} (\alpha^j - \alpha^i). \tag{1.5}$$

Agora, em $\prod_{i,j=1, i\neq j}^{n} (\alpha^j - \alpha^i)$ cada fator $(\alpha^i - \alpha^j)$ para $i < j$ aparece duas vezes, uma como $(\alpha^i - \alpha^j)$ e outra como $(\alpha^j - \alpha^i)$, e o produto das duas é $-(\alpha^i - \alpha^j)^2$. Assim, no produto da Equação (1.5) aparece o termo $(-1)^s$, onde s é o número de pares (i, j), com $1 \leq i < j \leq n$, ou seja, $N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)) = \prod_{1\leq i<j\leq n} (-1)^s(\alpha^i - \alpha^j)^2$. Mas,

$$\begin{cases} \text{se } i = 1, & \text{então } \ j = 2, 3, \cdots, n \ \ e \ \ s = 1 \\ \text{se } i = 2, & \text{então } \ j = 3, 4, \cdots, n \ \ e \ \ s = 2 \\ \vdots & \\ \text{se } i = n-1, & \text{então } \ j = n \ e \ s = 1. \end{cases}$$

Assim, $(n-1) + (n-2) + \cdots + 1 = \frac{((n-1)+1)n-1}{2} = \frac{1}{2}n(n-1) = s$. Logo $N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)) = (-1)^{\frac{1}{2}n(n-1)} \prod_{1\leq i<j\leq n} (\alpha^i - \alpha^j)^2$. Portanto, $N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)) = (-1)^{\frac{1}{2}n(n-1)}\mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1})$, e deste modo,

$$\mathcal{D}_{\mathbb{L}|\mathbb{K}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}|\mathbb{K}}(m'_\alpha(\alpha)),$$

o que prova a proposição. ■

1.4 Ramificação de ideais

Sejam A um anel de Dedekind de característica zero, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_\mathbb{L}$ o anel de inteiros de $\mathbb{L}$ sobre A. Se $\mathcal{P}$ é um ideal primo não nulo de A, então $\mathcal{P}\mathcal{O}_\mathbb{L}$ é um ideal de $\mathcal{O}_\mathbb{L}$. Como A é Dedekind, pelo Teorema 1.2.3, segue que $\mathcal{O}_\mathbb{L}$ é um anel de Dedekind e um A-módulo finitamente gerado. Além disso, como $\mathcal{O}_\mathbb{L}$ é um anel de Dedekind, do Teorema 1.2.5, segue que $\mathcal{P}\mathcal{O}_\mathbb{L}$ é expresso de modo único como $\mathcal{P}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathcal{B}_i^{e_i}$,

onde $\mathcal{B}_i$ são ideais primos distintos de $\mathcal{O}_{\mathbb{L}}$ e os e_i são inteiros positivos.

Proposição 1.4.1. *Os ideais primos $\mathcal{B}_i$ de $\mathcal{O}_{\mathbb{L}}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{B}_i \cap A = \mathcal{P}$, para $i = 1, \ldots, g$.*

Demonstração: Seja $\mathcal{I}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Assim $\mathcal{I} \cap A = \mathcal{P}$ se, e somente se, $\mathcal{I} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}}$. De fato, se $\mathcal{I} \cap A = \mathcal{P}$, então $\mathcal{P} \subset \mathcal{I}$ e portanto $\mathcal{P}\mathcal{O}_{\mathbb{L}} \subset \mathcal{I}\mathcal{O}_{\mathbb{L}} = \mathcal{I}$. Por outro lado, se $\mathcal{I} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{B}_i^{e_i}$, pela Proposição 1.1.3, segue que $\mathcal{I} \supset \mathcal{B}_i$, para algum i. Como $\mathcal{B}_i$ é maximal, pois $\mathcal{O}_{\mathbb{L}}$ é Dedekind, segue que $\mathcal{B}_i = \mathcal{I}$. Como $\mathcal{I} \subset \mathcal{O}_{\mathbb{L}}$ e $A \subset \mathcal{O}_{\mathbb{L}}$, pelo Proposição 1.2.8, segue que $\mathcal{I} \cap A$ é um ideal primo de A, e também, $\mathcal{I} \cap A \subsetneq A$, pois $1 \notin \mathcal{I}$. Agora, como $\mathcal{P} \subset \mathcal{I}$ e $\mathcal{P} \subset A$, segue que $\mathcal{P} \subset A \cap \mathcal{I}$. Como A é Dedekind, segue que $\mathcal{P} = A \cap \mathcal{I}$, pois $\mathcal{P}$ é maximal. Portanto, $\mathcal{P} = A \cap \mathcal{B}_i$. Assim, $\mathcal{I}$ está na fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{I} \cap A = \mathcal{P}$. ■

Definição 1.4.1. *Se $\mathcal{P} = A \cap \mathcal{I}$, dizemos que $\mathcal{I}$ **está acima de** $\mathcal{P}$.*

Lema 1.4.1.

1. *$A/\mathcal{P}$ e $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$ são corpos e $A/\mathcal{P}$ pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$.*

2. *$\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$ é um espaço vetorial de dimensão finita sobre $A/\mathcal{P}$, para $i = 1, \ldots, n$.*

Demonstração: Como A e $\mathcal{O}_{\mathbb{L}}$ são anéis de Dedekind, segue que $A/\mathcal{P}$ e $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$, para $i = 1, \ldots, g$, são corpos. Agora, consideramos a aplicação $A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$, onde i é a inclusão e π é a projeção. Assim, $\ker(\pi \circ i) = \mathcal{B}_i \cap A = \mathcal{P}$. Pelo Teorema do Homomorfismo, segue que $A/\mathcal{P} \simeq Im(\pi \circ i)$. Portanto, $A/\mathcal{P}$ pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$. Agora, considerando as operações

$$\begin{array}{rcl} + : \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i \times \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i & \longrightarrow & \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i \\ (\bar{x}, \bar{y}) & \longmapsto & \bar{x} + \bar{y} \end{array} \quad \text{e} \quad \begin{array}{rcl} \cdot : A/\mathcal{P} \times \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i & \longrightarrow & \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i \\ (\bar{a}, \bar{x}) & \longmapsto & \bar{a}\bar{x} \end{array}$$

segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$ é um espaço vetorial sobre $A/\mathcal{P}$ e que $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$ tem dimensão finita, pois se $\{x_1, \ldots, x_n\}$ são geradores de $\mathcal{O}_{\mathbb{L}}$ sobre A, e $b \in \mathcal{O}_{\mathbb{L}}$, então $b = a_1x_1 + \cdots + a_nx_n$, com $a_i \in A$, para $i = 1, \ldots, n$. Assim, $\bar{b} = \bar{a}_1\bar{x}_1 + \cdots + \bar{a}_n\bar{x}_n$, com $\bar{a}_i = a_i + \mathcal{P}$. Portanto, $\{\bar{x}_1, \ldots, \bar{x}_n\}$ gera $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$ como um espaço vetorial sobre $A/\mathcal{P}$. ■

Definição 1.4.2. *Seja $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{B}_i^{e_i}$, onde os $\mathcal{B}$'s são ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$.*

1. *O número g é chamado de* ***número de decomposição*** *de $\mathcal{P}$.*

2. *O grau $[\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i : A/\mathcal{P}]$ é chamado de* ***grau de inércia*** *de $\mathcal{B}_i$ sobre A e denotado por $f_i = f(\mathcal{B}_i, \mathcal{P})$.*

3. *O expoente $e_i = e(\mathcal{B}_i, \mathcal{P})$ de $\mathcal{B}_i$ é chamado de* ***índice de ramificação*** *de $\mathcal{B}_i$ sobre A.*

Observação 1.4.1. *Quando $e_i > 1$, para algum $i = 1, 2, \ldots, g$, dizemos que $\mathcal{P}$ se* ***ramifica*** *em $\mathbb{L}$.*

Teorema 1.4.1. *(Teorema da Igualdade Fundamental). [31, pág. 71] Temos que* $\sum_{i=1}^{g} e_i f_i = [\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} : A/\mathcal{P}] = n.$ ■

Corolário 1.4.1. *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos de números tal que $n = [\mathbb{L} : \mathbb{K}]$, $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$ os anéis de inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Se $\mathcal{P} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal primo, então $N(\mathcal{P}\mathcal{O}_{\mathbb{L}}) = N(\mathcal{P})^n$.*

Demonstração: Como $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{n} \mathcal{B}_i^{e_i}$, com $\mathcal{B}_i \cap \mathcal{O}_{\mathbb{K}} = \mathcal{P}$, $[\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i : \mathcal{O}_{\mathbb{K}}/\mathcal{P}] = f_i$, para $i = 1, \ldots, n$ e $\mathcal{B}_i$ ideais primos de $\mathcal{O}_{\mathbb{L}}$, segue que $N_{\mathcal{O}_{\mathbb{L}}}(\mathcal{P}\mathcal{B}) = N_{\mathcal{O}_{\mathbb{L}}}\left(\prod_{i=1}^{n} \mathcal{B}_i^{e_i}\right) = \prod_{i=1}^{n} (N_{\mathcal{O}_{\mathbb{L}}}(\mathcal{B}_i))^{e_i} = \prod_{i=1}^{n} (N_{\mathcal{O}_{\mathbb{K}}}(\mathcal{P})^{f_i})^{e_i} = N_{\mathcal{O}_{\mathbb{K}}}(\mathcal{P})^n$. ■

Definição 1.4.3. *O ideal $\mathcal{P}$ de $\mathcal{O}_{\mathbb{K}}$ é:*

1. ***totalmente decomposto*** *em $\mathbb{L}$, se $g = n$ e assim $e_i = f_i = 1$ para todo $i = 1, 2, \ldots, g$;*

2. ***inerte*** *em $\mathbb{L}$, se $g = 1$, $e_1 = 1$ e consequentemente $f_1 = n$;*

3. ***totalmente ramificado*** *em $\mathbb{L}$, se $g = 1$ e consequentemente $f_1 = 1$ e $e_1 = n$;*

Teorema 1.4.2 (Lema de Kummer)**.** *[1] Suponha que $\mathbb{L}$ é uma extensão finita separável de $\mathbb{K}$, e assuma que $\mathcal{O}_{\mathbb{L}} = A[\alpha]$ para algum elemento α e $f(x)$ o polinômio irredutível de α sobre $\mathbb{K}$. Se $\overline{f}(x)$ é a redução de $f(x)$ sobre $A/\mathcal{P}$,*

$$\overline{f}(x) = \overline{\mu_1}(x)^{e_i} \cdots \overline{\mu_r}(x)^{e_i}$$

é a fatoração de $\overline{f}(x)$ em potências de fatores irredutíveis sobre $A/\mathcal{P}$, com coeficiente dominante 1, então

$$\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{B}_1^{e_1} \cdots \mathcal{B}_r^{e_r} \tag{1.6}$$

é a fatoração de $\mathcal{P}$ em $\mathcal{O}_{\mathbb{L}}$, onde e_i é o índice de ramificação de $\mathcal{B}_i$ sobre $\mathcal{P}$. Além disso,

$$\mathcal{B}_i = \mathcal{P}\mathcal{O}_{\mathbb{L}} + \mu_i(\alpha)\mathcal{O}_{\mathbb{L}}, \tag{1.7}$$

onde $\mu_i(x) \in A[x]$ é um polinômio com coeficiente dominante 1 cuja redução módulo $\mathcal{P}$ é $\overline{\mu_i}(x)$. ■

Teorema 1.4.3. *[31, pág. 74] Se $\mathbb{K}$ é um corpo de números, então um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathbb{K}$ se, e somente se, p divide $\mathcal{D}_{\mathbb{K}}$.* ■

Do Teorema 1.4.3, segue o número de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathbb{K}$ é finito.

Proposição 1.4.2. $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathcal{P}\mathcal{O}_{\mathbb{L}}} \simeq \displaystyle\prod_{i=1}^{g}\left(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{B}_i^{e_i}}\right)$.

Demonstração: O ideal $\mathcal{B}_i$ é o único ideal maximal de $\mathcal{O}_{\mathbb{L}}$ que contém $\mathcal{B}_i^{e_i}$, pois se existir $\mathcal{J}$ um ideal maximal, tal que $\mathcal{J} \supset \mathcal{B}_i^{e_i}$, pela Proposição 1.1.3, segue que $\mathcal{J} \supset \mathcal{B}_i$, para algum i. Como $\mathcal{B}_i$ é maximal, segue que $\mathcal{J} = \mathcal{B}_i$. Vamos mostrar que $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$, para $i \neq j$. Se $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \subsetneq \mathcal{O}_{\mathbb{L}}$, então existe um ideal maximal $\mathcal{J}$ de $\mathcal{O}_{\mathbb{L}}$, tal que $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \subset \mathcal{J} \subset \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{B}_i^{e_i} \subset \mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j}$, segue que $\mathcal{B}_i^{e_i} \subset \mathcal{J}$, ou seja, $\mathcal{B}_i \subset \mathcal{J}$, e como $\mathcal{B}_i$ é maximal, segue que $\mathcal{B}_i = \mathcal{J}$. De modo análogo, como $\mathcal{B}_j^{e_j} \subset \mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j}$, segue que $\mathcal{B}_j^{e_j} \subset \mathcal{J}$, ou seja, $\mathcal{B}_j \subset \mathcal{J}$ e como $\mathcal{B}_j$ é maximal, segue que $\mathcal{B}_j = \mathcal{J}$. Assim, $\mathcal{B}_i = \mathcal{B}_j$, o que é um absurdo. Portanto, $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$. Pelo Lema 1.1.3, segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \simeq \displaystyle\prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}}/\mathcal{B}_i^{e_i}$. ■

Lema 1.4.2. *Seja A um domínio de Dedekind. Sejam $\mathcal{P}_1, \ldots, \mathcal{P}_r$, ideais primos distintos e não nulos de A, e sejam $x_1, \ldots, x_r \in A$ e $e_1, \ldots, e_r$ inteiros positivos. Então existe um elemento $x \in A$ tal que $x - x_i \in \mathcal{P}_i^{e_i}$ e $x - x_i \notin \mathcal{P}_i^{e_i+1}$, para $i = 1, \ldots, r$.*

Demonstração: Para $i = 1, \ldots, r$, segue que $\mathcal{P}_i^{e_i} \supsetneq \mathcal{P}_i^{e_i+1}$. Assim, existe um elemento $a_i \in \mathcal{P}_i^{e_i}$, $a_i \notin \mathcal{P}_i^{e_i+1}$. Pela Proposição 1.4.2, segue que existe $x \in A$ tal que $x-(x_i+a_i) \in \mathcal{P}_i^{e_i+1}$, para $i = 1, \ldots, r$. Desta forma, $x - x_i = [x - (x_i + a_i)] + a_i \in \mathcal{P}_i^{e_i}$, mas $x - x_i \notin \mathcal{P}_i^{e_i+1}$, pois $a_i \notin \mathcal{P}_i^{e_i+1}$. ■

Lema 1.4.3. *Suponha que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão de Galois. Se $\mathcal{B}_1$ e $\mathcal{B}_2$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{B}_1 \cap A = \mathcal{B}_2 \cap A \neq 0$, então existe um $\mathbb{K}$-automorfismo σ de $\mathbb{L}$ tal que $\sigma(\mathcal{B}_1) = \mathcal{B}_2$.*

Demonstração: Seja $G = \{\sigma_1, \ldots, \sigma_n\}$ o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\sigma_i(\mathcal{B}_1) \neq \mathcal{B}_2$, para todo $i = 1, \ldots, n$, pelo Lema 1.4.2, segue que existe $x \in \mathcal{O}_{\mathbb{L}}$ tal que $x \notin \sigma_i(\mathcal{B}_1)$, para

$i = 1, \ldots, n$, e $x \in \mathcal{B}_2$. Seja $a = \prod_{i=1}^{n} \sigma_i(x)$, então $a \in \mathcal{B}_2 \cap A$, e $a \notin \mathcal{B}_1$, pois $\sigma_i(x) \notin \mathcal{B}_1$, para $i = 1, \ldots, n$, o que é uma contradição. Portanto, existe $\sigma \in G$ tal que $\sigma(\mathcal{B}_1) = \mathcal{B}_2$. ■

Teorema 1.4.4. *Suponha que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão de Galois finita de grau n e $\mathcal{P}$ um ideal primo de A. Se $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{B}_i^{e_i}$ e $[\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i : A/\mathcal{P}] = f_i$ então $e_1 = e_2 = \cdots = e_g$, $f_1 = f_2 = \cdots = f_g$ e os corpos $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i$, para $i = 1, \ldots, g$, são isomorfos.*

Demonstração: Pelo Lema 1.4.3, segue que para cada $i = 1, \ldots, g$, existe $\sigma \in G$ tal que $\sigma(\mathcal{B}_1) = \mathcal{B}_i$. Assim, $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \sigma(\mathcal{P}\mathcal{O}_{\mathbb{L}}) = \prod_{i=1}^{g} \sigma(\mathcal{B}_i)^{e_i}$. Pela unicidade da fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$, segue que $e_i = e_1$ para cada $i = 1, \ldots, g$. Finalmente, como $\mathcal{O}_{\mathbb{L}}/\mathcal{B}_i = \mathcal{O}_{\mathbb{L}}/\sigma(\mathcal{B}_1) \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{B}_1$ segue que $f_1 = f_i$ para $i = 1, \ldots, g$, o que prova o teorema. ■

Corolário 1.4.2. *$efg = n$, onde n é o grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$.*

Demonstração: Pelo Teorema 1.4.1, segue que $\sum_{i=1}^{g} e_i f_i = n$. Pelo Teorema 1.4.4, segue que $e_i = e$ e $f_i = f$, para todo $i = 1, \ldots, g$. Portanto, $efg = n$. ■

1.5 Considerações finais do capítulo

Neste capítulo, apresentamos os resultados que são base teórica para o desenvolvimento deste trabalho, resultados sobre módulos livres e noetherianos, os conceitos de traço, normal, anel inteiros, anel de Dedekind, norma de ideais, discriminante e decomposição de um ideal primo. Destacamos a definição e resultados de corpo de números, uma vez que é uma classe de corpos muito importante para o trabalho, em particular os corpos ciclotômicos. Entre os principais resultados, vimos que o anel de inteiros de um corpo de números é um domínio de Dedekind, o discriminante de um corpo, e os resultados sobre norma de ideais e ramificação de ideais.

Capítulo

2

Corpos ciclotômicos

Neste capítulo, apresentamos os corpos ciclotômicos, que são exemplos importantes de corpos de números. Essa classe de corpos desempenha um papel muito importante na teoria algébrica dos números, uma vez que é possível encontrar o anel dos inteiros destes corpos e também podemos obter uma expressão para calcular o seu discriminante, parâmetros que são essenciais para a construção de reticulados algébricos. Por isso, apresentamos alguns resultados fundamentais dessa estrutura, que serão úteis nos capítulos seguintes.

Na Seção 2.1, apresentamos resultados básicos sobre raízes da unidade e corpos ciclotômicos. Em seguida, nas Seções 2.2, 2.3 e 2.4, estudamos os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_n)$, respectivamente. Nestes 3 casos, determinamos o anel de inteiros, uma base e o discriminante desses corpos.

2.1 Raiz da unidade

Nesta seção, apresentamos resultados iniciais sobre raízes da unidade e corpos ciclotômicos.

Definição 2.1.1. *Seja n um inteiro positivo.*

1. *Uma raiz do polinômio $x^n - 1$ é dita uma* ***raiz n-ésima da unidade****, denotada por ζ_n.*

2. *Uma raiz n-ésima da unidade tal que que $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$, é chamada de* ***raiz n-ésima primitiva da unidade****.*

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

4. *O polinômio* $\phi_n(x) = \prod_{j=1}^{n}(x-\zeta_n^j)$*, onde* $mdc(j,n) = 1$*, é chamado de* n***-ésimo polinômio ciclotômico***. *O grau de* $\phi_n(x)$ *é dado pela função de Euler* $\varphi(n) = \#\{0 < m < n \mid mdc(m,n) = 1\}$.

Proposição 2.1.1. *[30, 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.* ■

Sejam $\zeta_1, \ldots, \zeta_n$ as n raízes do polinômio $x^n - 1$. Observe que uma dessas ζ_i é o número 1, pois $1^n - 1 = 0$. Se U_n é o conjunto formado por essas n raízes, então U_n é um grupo multiplicativo cíclico, gerado por uma raiz n-ésima primitiva da unidade ζ. Além disso, os únicos geradores de U_n são as raízes ζ^k, onde $mdc(k,n) = 1$, ou seja, o número possível de geradores de U_n é $\varphi(n)$.

Proposição 2.1.2. *Para* $0 \leq k \leq m-1$ *e* $0 \leq l \leq n-1$*,* $\zeta_m^k\zeta_n^l$ *é uma raiz* mn*-ésima primitiva da unidade se, e somente se,* ζ_m^k *é uma raiz* m*-ésima primitiva da unidade e* ζ_n^l *é uma raiz* n*-ésima primitiva da unidade.*

Demonstração: Se ζ_m^k não é uma raiz m-ésima primitiva da unidade, então $mdc(k,\, m) = d > 1$. Assim, $(\zeta_m^k\zeta_n^l)^{\frac{mn}{d}} = ((\zeta_m^k\zeta_n^l)^{mn})^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1$, o que é um absurdo, pois $\frac{mn}{d} < mn$. Reciprocamente, se ζ_m^k é uma raiz m-ésima primitiva da unidade, de forma análoga, mostra-se que ζ_n^l é uma raiz n-ésima primitiva da unidade, então $mdc(k,\, m) = mdc(l,\, n) = 1$. Assim,

$$(\zeta_m^k\zeta_n^l)^a = 1 \iff \zeta_m^{ka}\zeta_n^{la} = 1 \iff \zeta_m^{ka} = \zeta_n^{-la} \iff \zeta_m^{kan} = \zeta_n^{-lan} \iff (\zeta_m^k)^{na} = (\zeta_n^n)^{-la} \iff$$
$$(\zeta_m^k)^{na} = 1^{-la} \iff (\zeta_m^k)^{na} = 1 \iff m|na.$$

Já que $mdc(m,\, n) = 1$, segue que $m|a$. De maneira análoga, $n|a$. Além disso, usando o fato de que $mdc(m,\, n) = 1$, segue que $mn|a$. Assim, $(\zeta_m^k\zeta_n^l)^{mn} = (\zeta_m^m)^{kn}(\zeta_n^n)^{lm} = 1$. Logo, mn é a menor potência tal que $(\zeta_m^k\zeta_n^l)^{mn} = 1$. Portanto, $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. ■

Proposição 2.1.3. *Se* n *é um inteiro positivo, então* $x^n - 1 = \prod_{d|n}\phi_d(x)$.

Demonstração: Sejam $f(x) = x^n - 1$ e $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ as raízes de $f(x)$. Assim,

$$x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{n-1}).$$

Analisando os períodos de cada raiz de $f(x)$, e escrevendo todas as raízes de mesmo período como um polinômio da forma

$$\phi_d(x) = \prod_{perodo\ \zeta=d} (x-\zeta),$$

segue que $x^n - 1 = \prod_{d|n} \phi_d(x)$. ■

Corolário 2.1.1. *Se n é um inteiro positivo, então*

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

Demonstração: Consequência imediata da Proposição 2.1.3. ■

Observação 2.1.1. *Quando $n = p$, onde p é um número primo, o p-ésimo polinômio ciclotômico é dado por*

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Teorema 2.1.1. *Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde φ denota a função de Euler.*

Demonstração: Considere $f(x)$ um polinômio mônico, irredutível e de menor grau de ζ_n sobre $\mathbb{Q}$. Logo, $x^n - 1 = f(x)g(x)$, com $g(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss, segue que $f(x), g(x) \in \mathbb{Z}(x)$. Se p é um primo tal que $p \nmid n$, então ζ_n^p é uma raiz n-ésima primitiva da unidade. Dessa forma, $(\zeta_n^p)^n - 1 = f(\zeta_n^p)g(\zeta_n^p)$, ou seja, $f(\zeta_n^p)g(\zeta_n^p) = 0$. Logo, se ζ_n^p não é raiz de $f(x)$, então ζ_n^p é raiz de $g(x)$, e ζ_n é raiz de $g(x^p)$. Portanto, $f(x) \mid g(x^p)$, isto é, $g(x^p) = f(x)h(x)$, com $h(x) \in \mathbb{Z}[x]$, pelo Lema de Gauss. Mas, pelo Teorema de Fermat, segue que $a^p \equiv a (mod\ p)$, e então, $g(x^p) \equiv g(x)^p (mod\ p)$. Assim, $f(x)h(x) \equiv g(x)^p (mod\ p)$, ou seja, $g(x)^p \equiv f(x)h(x) (mod\ p)$. Portanto, $g(\bar{\zeta_n})^p = \bar{0}$, já que ζ_n é raiz de $f(x)$. De maneira recursiva, chegamos que $\bar{g}(\zeta_n) = 0$, ou seja, $\bar{f}$ e $\bar{g}$ tem uma raiz em comum. Assim, $x^n - \bar{1} = \bar{f}\bar{g}$, e deste modo $x^n - \bar{1}$ tem raízes múltiplas. Logo, $nx^{n-1} = \bar{0}$ e então, para qualquer $\alpha \in \mathbb{Z}_p$, segue que $n\alpha^{n-1} = \bar{0}$. Como

a característica de $\mathbb{Z}_p$ é p, segue que $p \mid n$, o que é um absurdo, uma vez que supomos que $p \nmid n$. Portanto, ζ_n^p é raiz de $f(x)$ para todo p tal que $p \nmid n$ e $mdc(p,n) = 1$. Portanto, $\partial(f(x)) \geq \partial(g(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x) \mid \phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$. Assim, $\partial(f(x)) = \partial(\phi_n(x)) = \varphi(n)$. ■

Corolário 2.1.2. *Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$, onde φ é a função de Euler.*

Demonstração: Como $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)$, pelo Teorema 2.1.1, segue que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Assim, pelo teorema da multiplicidade de graus, segue que é suficiente mostrar que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Mas isso segue do fato que o polinômio $f(x) = x^2 + (\zeta_n + \zeta_n^{-1})x + 1$ tem ζ_n como raiz e é irredutível sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Portanto, $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$. ■

Proposição 2.1.4. *O n-ésimo polinômio ciclotômico $\phi_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Seja $m_\alpha(x)$ o polinômio minimal de ζ_n. Pelo Teorema 2.1.1, segue que $\partial(m_\alpha(x)) = \partial(\phi_n(x))$ e $\phi_n(\zeta_n) = 0$. Portanto, $m_\alpha \equiv \phi_n$, e dessa forma, $\phi_n(x)$ é irredutível sobre $\mathbb{Q}$. ■

Corolário 2.1.3. *Se $mdc(m,n) = 1$, então $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.*

Demonstração: Como $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m\zeta_n) \subseteq \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ e $mdc(m,n) = 1$, segue, pela Proposição 2.1.2, que $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$. ■

2.2 Corpo ciclotômico $\mathbb{Q}(\zeta_p)$

Sejam $p > 2$ um primo e ζ_p uma raiz p-ésima primitiva da unidade. Como $\zeta_p \neq 1$ é uma raiz de $x^p - 1$ e $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, segue que ζ_p é uma raiz do polinômio

$$\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]. \tag{2.1}$$

Assim, se $\mathcal{O}_\mathbb{K}$ é o anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, segue que $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_\mathbb{K}$. Pela Proposição 2.1.4, segue que $\phi_p(x)$ é o polinômio minimal de ζ_p sobre $\mathbb{Q}$ e $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Como U_p é cíclico, segue que ζ_p^i, para $i = 1, 2, \ldots, p-1$, são as raízes de $\phi_p(x)$, ou seja, $\phi_p(x) = \prod_{i=1}^{p-1}(x - \zeta_p^i)$. Assim, pela Equação (2.1), segue que $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$.

Lema 2.2.1. *Se r e s são inteiros tal que $mdc(p, rs) = 1$, então $(\zeta_p^r - 1)/(\zeta_p^s - 1)$ é um elemento inversível de $\mathbb{Z}[\zeta_p]$, chamado de unidade ciclotômica.*

Demonstração: Como $mdc(p, rs) = 1$, segue que existe um número inteiro t tal que $r \equiv st \ (mod\ p)$. Assim,

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} = \frac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + \cdots + \zeta_p^{s(t-1)} \in \mathbb{Z}[\zeta_p]. \tag{2.2}$$

Analogamente, segue que $\frac{\zeta_p^s - 1}{\zeta_p^r - 1} \in \mathbb{Z}[\zeta_p]$. Portanto, $\frac{\zeta_p^r - 1}{\zeta_p^s - 1}$ é inversível em $\mathbb{Z}[\zeta_p]$. ■

Proposição 2.2.1. *O ideal $(1 - \zeta_p)\mathcal{O}_\mathbb{K}$ é um ideal primo de $\mathcal{O}_\mathbb{K}$ e $((1 - \zeta_p)\mathcal{O}_\mathbb{K})^{p-1} = p\mathcal{O}_\mathbb{K}$. Portanto, p é totalmente ramificado em $\mathbb{Q}(\zeta_p)$.*

Demonstração: Como $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$, pelo Lema 2.2.1, segue que os ideais $(1 - \zeta_p)\mathcal{O}_\mathbb{K}$ e $(1 - \zeta_p^i)\mathcal{O}_\mathbb{K}$, para $i = 1, 2, \ldots, p-1$, são iguais. Portanto, $p\mathcal{O}_\mathbb{K} = ((1 - \zeta_p)\mathcal{O}_\mathbb{K})^{p-1}$. Pelo Teorema 1.4.1, segue que $p\mathcal{O}_\mathbb{K}$ tem no máximo $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ fatores primos em $\mathcal{O}_\mathbb{K}$, e portanto, $(1 - \zeta_p)\mathcal{O}_\mathbb{K}$ é um ideal primo de $\mathcal{O}_\mathbb{K}$. ■

Lema 2.2.2. $(1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.

Demonstração: Pela Proposição 2.2.1, segue que $((1 - \zeta_p)\mathcal{O}_\mathbb{K})^{p-1} = p\mathcal{O}_\mathbb{K}$, e portanto $p \in (1 - \zeta_p)\mathcal{O}_\mathbb{K}$. Assim, $p\mathbb{Z} \subset (1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z}$. Agora, como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, segue que $(1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$ ou $(1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = \mathbb{Z}$. Se $(1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = \mathbb{Z}$, então $1 - \zeta_p$ é um elemento inversível de $\mathcal{O}_\mathbb{K}$. Assim, p é inversível em $\mathcal{O}_\mathbb{K}$. Como p tem inverso em $\mathbb{Q}$, segue que p tem um inverso em $\mathbb{Z} = \mathcal{O}_\mathbb{K} \cap \mathbb{Q}$, o que é um absurdo. Portanto, $(1 - \zeta_p)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z}$. ■

Lema 2.2.3. *Se $j = 1, \ldots, p - 1$, então*

1. $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = -1$.
2. $Tr_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_p^j) = p$.
3. $N_{\mathbb{K}|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$ *e* $N_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_p) = p$.
4. $p = (1 - \zeta_p)(1 - \zeta_p^2)\cdots(1 - \zeta_p^{p-1})$.

Demonstração:

1. Pela Observação 2.1.1, segue que o p-ésimo polinômio ciclotômico de ζ_p é dado por $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. As raízes de $\phi_p(x)$ são $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$. Logo, $0 = \phi_p(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \cdots + \zeta_p^j + 1$, e assim, $\zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \cdots + \zeta_p^j = -1$. Portanto, $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \cdots + \zeta_p^j = -1$, para $j = 1, \ldots, p - 1$.

2. $Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p^j) = Tr_{\mathbb{K}|\mathbb{Q}}(1) - Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j)$. Mas, como $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(1) = 1+1+\cdots+1 = p-1$, e do ítem 1, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = -1$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p^j) = p-1+1 = p$.

3. Como $\zeta_p - 1$ é uma raiz do polinômio $f(x) = x^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} x^{j-1}$, segue que, $N(\zeta_p - 1) = (-1)^{p-1}p$, e $N(1-\zeta_p) = N((-1)(\zeta_p-1)) = N(-1)N(\zeta_p-1) = (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p$.

4. Como $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ são raízes do polinômio mônico $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, segue que $x^{p-1} + x^{p-2} + \cdots + x + 1 = (x-\zeta_p)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1})$. Assim, tomando $x = 1$, então $(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$. ■

Lema 2.2.4. *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in p\mathbb{Z}$.*

Demonstração: Cada conjugado $\alpha_i(1-\zeta_p^i)$ de $\alpha(1-\zeta_p)$ é um múltiplo de $(1-\zeta_p^i)$ em $\mathcal{O}_{\mathbb{K}}$, onde $i = 1, 2, \ldots, p-1$. Como $1-\zeta_p^i = (1-\zeta_p)(\zeta_p^{i-1} + \zeta_p^{i-2} + \cdots + \zeta_p + 1)$, segue que $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathcal{O}_{\mathbb{K}}$. Como o traço é a soma dos conjugados, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) = \alpha_1(1-\zeta_p) + \alpha_2(1-\zeta_p^2) + \cdots + \alpha_p(1-\zeta_p^p) = \beta(1-\zeta_p),$$

onde $\beta \in \mathcal{O}_{\mathbb{K}}$. Portanto, $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é integralmente fechado, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in \mathbb{Z}$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$. ■

Teorema 2.2.1. *$\mathbb{Z}[\zeta_p]$ é o anel de inteiros de $\mathbb{K}$ e $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Como $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_{\mathbb{K}}$, é suficiente mostrar que $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Se $\alpha \in \mathcal{O}_{\mathbb{K}} \subset \mathbb{Q}(\zeta_p)$, então

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

com $a_i \in \mathbb{Q}$, para $i = 0, 1, \ldots, p-2$. Multiplicando por $1-\zeta_p$ em ambos os lados, segue que

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

Pelo Lema 2.2.4, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) = a_0 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) + a_1 Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2} Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^{p-2} - \zeta_p^{p-1}) \in p\mathbb{Z}.$$

Como $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \ldots, p-2$, segue que $a_0 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = a_0 p \in p\mathbb{Z}$, onde $a_0 \in \mathbb{Z}$. Analogamente, como $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_{\mathbb{K}}$, segue que

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

Multiplicando ambos os lados por $1-\zeta_p$, obtemos

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

e assim, pelo Lema 2.2.4, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}((\alpha-a_0)\zeta_p^{-1}(1-\zeta_p)) = a_1 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) + a_2 Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2} Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^{p-3} - \zeta_p^{p-2}) \in p\mathbb{Z}.$$

Logo, $a_1 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = a_1 p \in p\mathbb{Z}$, onde $a_1 \in \mathbb{Z}$. Prosseguindo, desta maneira, segue que $a_i \in \mathbb{Z}$, para cada $i = 1, \ldots, n$. Assim, $\alpha \in \mathbb{Z}[\zeta_p]$. Portanto, $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{K}}$. ■

Proposição 2.2.2. *Se $\mathbb{L} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, então $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ é o anel de inteiros de $\mathbb{L}$ e $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Do Teorema 2.2.1, segue que anel de inteiros de $\mathbb{Q}(\zeta_p)$ é $\mathbb{Z}[\zeta_p]$. Como ζ_p e ζ_p^{-1} são inteiros, segue que $\zeta_p + \zeta_p^{-1}$ também é. Portanto, $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$. Mostremos, agora, que $\mathcal{O}_{\mathbb{L}} \subseteq \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. De fato, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então

$$\alpha = a_1(\zeta_p + \zeta_p^{-1}) + a_2(\zeta_p^2 + \zeta_p^{-2}) + \cdots + a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}})$$

onde $a_i \in \mathbb{Q}$, para $i = 1, 2, \ldots, \frac{p-1}{2}$. Devemos provar que $a_i \in \mathbb{Z}$. Multiplicando α por $\zeta_p^{\frac{p-1}{2}}$, segue que

$$\zeta_p^{\frac{p-1}{2}}\alpha = a_1\zeta_p^{\frac{p+1}{2}} + a_1\zeta_p^{\frac{p-3}{2}} + a_2\zeta_p^{\frac{p+3}{2}} + a_2\zeta_p^{\frac{p-5}{2}} + \cdots + a_{\frac{p-1}{2}}\zeta_p^{p-1} + a_{\frac{p-1}{2}},$$

que é um inteiro algébrico de $\mathbb{Q}(\zeta_p)$, logo pertence a $\mathbb{Z}[\zeta_p]$. Assim, $a_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, \frac{p-1}{2}$. Portanto, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Como $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$ e como $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\} \subseteq \mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que é suficiente mostrar que $\{\zeta_p + \zeta_p^{-1}, \cdots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é linearmente independente. De fato, sejam $a_1, a_2, \ldots, a_{\frac{p-1}{2}} \in \mathbb{Z}$

tais que

$$a_1(\zeta_p+\zeta_p^{-1})+a_2(\zeta_p^2+\zeta_p^{-2})+\cdots+a_{\frac{p-1}{2}}(\zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}})=0.$$

Logo,

$$a_1\zeta_p+a_1\zeta_p^{p-1}+a_2\zeta_p^2+a_2\zeta_p^{p-2}+\cdots+a_{\frac{p-1}{2}}\zeta_p^{\frac{p-1}{2}}+a_{\frac{p-1}{2}}\zeta_p^{\frac{p-1}{2}}=0.$$

Como $\{1,\zeta_p,\ldots,\zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$ sobre $\mathbb{Z}$, segue que estes elementos são linearmente independentes, e deste modo, $a_1=a_2=\cdots=a_{\frac{p-1}{2}}=0$. Assim, $\{\zeta_p+\zeta_p^{-1},\ldots,\zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\}$ é linearmente independente. Portanto, $\{\zeta_p+\zeta_p^{-1},\ldots,\zeta_p^{\frac{p-1}{2}}+\zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_p+\zeta_p^{-1}]$ sobre $\mathbb{Z}$. ■

Proposição 2.2.3. *O discriminante de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é dado por*

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

Demonstração: Pelo Teorema 2.2.1, segue que $\{1,\zeta_p,\ldots,\zeta_p^{p-2}\}$ é uma base integral. Pela Proposição 1.3.6, segue que

$$\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1,\zeta_p,\ldots,\zeta_p^{p-2})=(-1)^{\frac{(p-1)(p-2)}{2}}N_{\mathbb{K}|\mathbb{Q}}(\phi_p'(\zeta_p)),$$

onde $\phi_p'(x)$ é a derivada do p-ésimo polinômio ciclotômico $\phi_p(x)$ que é dado por

$$\phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1=\frac{x^p-1}{x-1}.$$

Derivando-o de ambos os lados, segue que

$$\phi_p'(\zeta_p)=\frac{(\zeta_p-1)p\zeta_p^{p-1}-(\zeta_p^p-1)}{(\zeta_p-1)^2}=\frac{-p\zeta_p^{p-1}}{1-\zeta_p}.$$

Assim, aplicando a norma, usando sua linearidade e o Lema 2.2.3, segue que

$$N_{\mathbb{K}|\mathbb{Q}}(\phi_p'(\zeta_p))=\frac{N_{\mathbb{K}|\mathbb{Q}}(-p)N_{\mathbb{K}|\mathbb{Q}}(\zeta_p)^{p-1}}{N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p)}=\frac{-p^{p-1}1^{p-1}}{p}=p^{p-2}.$$

Além disso, como p é ímpar, segue que $(-1)^{p-2}=-1$, e assim $(-1)^{\frac{(p-1)(p-2)}{2}}=(-1)^{\frac{(p-1)}{2}}$. Portanto,

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

o que prova a proposição. ■

2.3 Corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$

Se $n = p^r$, onde p é um número primo e r é um inteiro maior que 1, então o p^r-ésimo polinômio ciclotômico é dado por

$$\phi_{p^r}(x) = \frac{x^{p^r}-1}{\phi_1(x)\phi_2(x)\cdots\phi_{p^{r-1}}(x)} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1.$$

Lema 2.3.1. *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p^r)$, $\mathcal{O}_\mathbb{K}$ é o anel de inteiros de $\mathbb{K}$ e $\alpha \in \mathcal{O}_\mathbb{K}$, então:*

1. $(1-\zeta_p^r)\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.
2. $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p^r)) \in p\mathbb{Z}$.

Demonstração: Análoga a demonstrações dos Lemas 2.2.2 e 2.2.4. ■

Lema 2.3.2. $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$.

Demonstração: Por definição, segue que $\mathbb{Z}[\alpha] = \{\sum_{i=1}^{n} a_i\alpha^i \mid a_i \in \mathbb{Z}\}$. Assim, se $\alpha \in \mathbb{Z}[1-\zeta_{p^r}]$, então

$$\begin{aligned}\alpha &= a_0 + a_1(1-\zeta_{p^r}) + a_2(1-\zeta_{p^r})^2 + \cdots + a_{(p-1)p^{r-1}}(1-\zeta_{p^r})^{(p-1)p^{r-1}} \\ &= (a_0 + a_1 + \cdots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2)\zeta_{p^r} + \cdots .\end{aligned}$$

Logo, $\alpha = b_0 + b_1\zeta_{p^r} + b_2\zeta_{p^r}^2 + \cdots + b_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$, e portanto, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Agora, se $\alpha \in \mathbb{Z}[\zeta_{p^r}]$, então $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$. Como $\zeta_{p^r} = 1-(1-\zeta_{p^r})$, segue que α pode ser escrito da forma

$$\begin{aligned}\alpha &= a_0 + a_1(1-(1-\zeta_{p^r})) + a_2(1-(1-\zeta_{p^r}))^2 + \cdots + a_{(p-1)p^{r-1}}(1-(1-\zeta_{p^r}))^{(p-1)p^{r-1}} \\ &= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2(1-2(1-\zeta_{p^r}+(1-\zeta_{p^r}))^2)) + \cdots \\ &= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2 - 2a_2(1-\zeta_{p^r}) + a_2(1-\zeta_{p^r})^2 + \cdots \\ &= (a_0 + a_1 + a_2 + \cdots + a_{(p-1)p^{r-1}-1}) + (-a_1 - 2a_2 - \cdots - ((p-1)p^{r-1}-1)a_{(p-1)p^{r-1}-1}) \\ &\quad (1-\zeta_{p^r}) + (a_2 - 3a_3 + \cdots)(1-\zeta_{p^r})^2 + \cdots ,\end{aligned}$$

ou seja, $\alpha = b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}}(1-\zeta_{p^r})^{(p-1)p^{r-1}} \in \mathbb{Z}[1-\zeta_{p^r}]$. Portanto, $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[1-\zeta_{p^r}]$. ■

Proposição 2.3.1. *Se $j = 1, 2, \ldots, p^{r-1}$ e $mdc(j, p^r) = 1$, então*

1. $N_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$.

2. $\prod_j (1 - \zeta_{p^r}^j) = p$, *com* $1 \leq j \leq p^r$, *e tal que* $p \nmid j$. *Em particular,* $N_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_{p^r}) = p$.

Demonstração:

1. Por definição, segue que $N_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r}^j) = \zeta_{p^r}^j \zeta_{p^r}^{j+1} \cdots \zeta_{p^r}^{j+(p-1)p^{r-1}}$. Como $\zeta_{p^r}^j$ e $\zeta_{p^r}^{j+p^{r-1}}$ são elementos conjugados, segue que $\zeta_{p^r} \zeta_{p^r}^{j+1} \cdots \zeta_{p^r}^{j+(p-1)p^{r-1}} = (-1)^{(p-1)p^{r-1}}$. Portanto, $N_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$, para $j = 1, \ldots, p^{r-1}$ e $mdc(j, p^r) = 1$.

2. Como $\phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$, segue que todos os $\zeta_{p^r}^j$, onde $1 \leq j \leq p^r$ e tal que $p \nmid j$ são raízes de $\phi_{p^r}(x)$ uma vez que são raízes de $x^{p^r} - 1$ mas não de $x^{p^{r-1}} - 1$. Deste modo, $\phi_{p^r}(x) = \prod_j (x - \zeta_{p^r}^j)$ e existem exatamente $\varphi(p^r) = (p-1)p^{r-1}$ valores de j pois $\partial(\phi_{p^r}(x)) = (p-1)p^{r-1}$. Tomando $x = 1$, segue que $\phi_{p^r}(1) = \prod_{k=1, p\nmid j}^{p^r} (1 - \zeta_{p^r}^j) = 1 + 1^{p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p$. Portanto, $\prod_{j=1, p\nmid j}^{p^r} (1 - \zeta_{p^r}^j) = p$. Agora, como $N_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_{p^r}) = \prod_{j=1, p\nmid j}^{p^r} (1 - \zeta_{p^r}^j)$, segue que $N_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_{p^r}) = p$. ■

Proposição 2.3.2. *[16, pág. 43] Se $j = 1, 2, \ldots, p^r$, então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r}^j) = \begin{cases} 0, \text{ se } mdc(j, p^r) < p^{r-1}; \\ -p^{r-1}, \text{ se } mdc(j, p^r) = p^{r-1}; \\ p^{r-1}(p-1), \text{ se } mdc(j, p^r) > p^{r-1}. \end{cases}$$

■

Teorema 2.3.1. *Sejam $\mathbb{L}$ uma extensão finita de grau n de $\mathbb{Q}$, $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, onde $\alpha_i \in \mathcal{O}_\mathbb{L}$ e $\mathcal{D}_{\mathbb{L}|\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = d$. Se $\alpha \in \mathcal{O}_\mathbb{L}$, então α pode ser escrito na forma*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d, para $j = 1, 2, \ldots, n$.

Demonstração: Se $\alpha \in \mathcal{O}_\mathbb{L}$, então $\alpha \in \mathbb{L}$, uma vez que $\mathcal{O}_\mathbb{L} \subseteq \mathbb{L}$. Sendo $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, segue que α pode ser escrito na forma

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n,$$

com $x_j \in \mathbb{Q}$, para $j = 1, \ldots, n$. Sejam $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Aplicando σ_i, para $i = 1, \ldots, n$, em α, segue um sistema de n equações dado por

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n),$$

para $i = 1, \ldots, n$. Resolvendo esse sistema pela regra de Cramer, segue que as n raízes são dadas por $x_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Assim, os γ_j, para $j = 1, 2, \ldots, n$, e δ são inteiros algébricos uma vez que são obtidos a partir dos α_i's, que são, por hipótese, inteiros algébricos. Pela Proposição 1.3.3, segue que $\delta^2 = d$, e portanto, $dx_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$ é um inteiro algébrico. Como $\mathbb{Z}$ é integralmente fechado, segue que $dx_j \in \mathbb{Z}$, para $j = 1, 2, \ldots, n$. Seja $m_j = dx_j$, para $j = 1, 2, \ldots n$. Se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, teremos que m_j^2 é divisível por d. Mas, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, segue que é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico. Como $m_j = dx_j = \delta\gamma_j$, segue que $m_j^2 = d^2x_j^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Logo $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j é um inteiro algébrico. Portanto $\frac{m_j^2}{d} \in \mathbb{Z}$, e assim, m_j^2 é divisível por d. Portanto, $\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$, com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d, para $j = 1, 2, \ldots, n$. ■

Lema 2.3.3. *Se* $\mathcal{D}_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$, *então* $d = p^s$ *para algum* $s \in \mathbb{N}$.

Demonstração: Como

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

segue que

$$x^{p^r} - 1 = \phi_{p^r}(x)g(x), \tag{2.3}$$

onde $g(x) = x^{p^{r-1}} - 1$. Derivando ambos os lados da Equação (2.3), segue que

$$p^r x^{p^r-1} = \phi'_{p^r}(x)g(x) + \phi_{p^r}(x)g'(x),$$

e substituindo x por ζ_{p^r}, segue que

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

Como $\phi_{p^r}(\zeta_{p^r}) = 0$, segue que $p^r\zeta_{p^r}^{p^r-1} = \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r})$, ou seja,

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

Logo,

$$p^r = \zeta_{p^r}\phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}),$$

e aplicando a função norma em ambos os lados da última igualdade ficamos com

$$p^{(p-1)p^{r-1}r} = N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r}))N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Assim, pela Proposição 1.3.6, segue que

$$p^{(p-1)p^{r-1}r} = \pm\mathcal{D}_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1,\ldots,\zeta_{p^r}^{(p-1)p^{r-1}-1})N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Portanto, $d|p^{r(p-1)p^{r-1}}$, ou seja, $d = p^s$, para algum inteiro s. ■

Teorema 2.3.2. *O anel de inteiros de* $\mathbb{K}$ *é* $\mathbb{Z}[\zeta_{p^r}]$ *e* $\{1,\zeta_{p^r},\ldots,\zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ *é uma base de* $\mathbb{Z}[\zeta_{p^r}]$ *como um* $\mathbb{Z}$*-módulo.* ■

Demonstração: Mostraremos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}]$. Suponhamos, por absurdo, que $\mathcal{O}_{\mathbb{K}} \neq \mathbb{Z}[1-\zeta_{p^r}]$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então pelo Teorema 2.3.1, segue que

$$\alpha = \frac{m_0 + m_1(1-\zeta_{p^r}) + \cdots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}, \tag{2.4}$$

onde $m_i \in \mathbb{Z}$, para $i = 1,2,\ldots,(p-1)p^{r-1}$. Pelo Lema 2.3.3, segue que $d = p^s$, onde $s \in \mathbb{N}$. Logo, existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que nem todos os m_i's são divisíveis por p^s. Suponhamos que m_j, com $j \leq (p-1)p^{r-1}$, não seja divisível por p^s. Deste modo, existem $q,r \in \mathbb{Z}$ tal que $m_j = p^sq + r$, onde $0 < r < p^s$. Assim, substituindo m_j na Equação (2.4), segue que

$$\alpha = \frac{m_0 + m_1(1-\zeta_{p^r}) + \cdots + (p^sq+r)(1-\zeta_{p^r})^j + \cdots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}.$$

Logo, $\mathcal{O}_{\mathbb{K}}$ possui um elemento da forma

$$\beta = \frac{r(1-\zeta_{p^r})^{j-1} + m_j(1-\zeta_{p^r})^j + \cdots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}.$$

Multiplicando ambos os lados por p^{s-1}, ficamos com

$$\beta p^{s-1} = \frac{r(1-\zeta_{p^r})^{j-1} + m_j(1-\zeta_{p^r})^j + \cdots + m_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p},$$

que pode ser escrito como

$$\gamma = \frac{a_{j-1}(1-\zeta_{p^r})^{j-1} + a_j(1-\zeta_{p^r})^j + \cdots + a_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}}{p},$$

onde $a_i \in \mathbb{Z}$ e a_j não é divisível por p, Agora, pelo ítem 2, da Proposição 2.3.1, segue que $\prod^{p^r}(1-\zeta_{p^r}) = p$. Logo, $\frac{p}{(1-\zeta_{p^r})^n} \in \mathbb{Z}[1-\zeta_{p^r}]$ uma vez que $1-\zeta_{p^r}^k$ é divisível, em $\mathbb{Z}[1-\zeta_{p^r}]$, por $(1-\zeta_{p^r})$. Assim, $\frac{p}{(1-\zeta_{p^r})^j} \in \mathbb{Z}[1-\zeta_{p^r}]$ e daí $\frac{\gamma p}{(1-\zeta_{p^r})^j} \in \mathcal{O}_{\mathbb{K}}$. Subtraindo termos que estão em $\mathcal{O}_{\mathbb{K}}$, segue que $\frac{a_j}{(1-\zeta_{p^r})} \in \mathcal{O}_{\mathbb{K}}$. Assim, $N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_{p^r}) | N_{\mathbb{K}|\mathbb{Q}}(a_j)$. Mas, como $N_{\mathbb{K}|\mathbb{Q}}(a_j) = a_j^n$, segue do ítem 2 da Proposição 2.3.1, que $p \mid a_j^n$, o que é um absurdo pois $p \nmid a_j$. Assim, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}]$. Agora, pelo Lema 2.3.2, segue que $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$e portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$. ■

Proposição 2.3.3. *Se $\mathbb{L} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, então $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ é o anel de inteiros de $\mathbb{L}$ e $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Do Teorema 2.3.1, segue que o anel de inteiros de $\mathbb{Q}(\zeta_{p^r})$ é $\mathbb{Z}[\zeta_{p^r}]$. Como ζ_{p^r} é inteiro, segue que $\zeta_{p^r}^{-1}$ é inteiro e pelo Corolário 1.2.2, segue que $\zeta_{p^r} + \zeta_{p^r}^{-1}$ também é inteiro. Portanto, $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$. Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então

$$\alpha = a_1(\zeta_{p^r} + \zeta_{p^r}^{-1}) + a_2(\zeta_{p^r}^2 + \zeta_{p^r}^{-2}) + \cdots + a_{\frac{(p-1)p^{r-1}}{2}}(\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}),$$

onde $a_i \in \mathbb{Q}$, para $i = 1, 2, \ldots, \frac{(p-1)p^{r-1}}{2}$. Devemos mostrar que $a_i \in \mathbb{Z}$. Multiplicando α por $\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}$, segue que

$$\begin{aligned}\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}}\alpha &= a_1\zeta_p^{\frac{(p-1)p^{r-1}+2}{2}} + a_1\zeta_{p^r}^{\frac{(p-1)p^{r-1}-2}{2}} + a_2\zeta_{p^r}^{\frac{(p-1)p^{r-1}+4}{2}} + a_2\zeta_{p^r}^{\frac{(p-1)p^{r-1}-4}{2}} + \cdots + \\ &+ a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{(p-1)p^{r-1}} + a_{\frac{(p-1)p^{r-1}}{2}},\end{aligned}$$

que é um elemento inteiro algébrico de $\mathbb{Q}(\zeta_{p^r})$. Logo, pertence a $\mathbb{Z}[\zeta_{p^r}]$. Assim, $a_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, \frac{(p-1)p^{r-1}}{2}$. Portanto, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$, ou seja, o anel de inteiros de $\mathbb{L}$ é $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$. Como $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ é uma $\mathbb{Z}$-base de $\mathbb{L}$ sobre $\mathbb{Q}$ e como $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\} \subseteq \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que é suficiente mostrar que

é linearmente independente. Para isso, sejam $a_1, a_2, \ldots, a_{\frac{(p-1)p^{r-1}}{2}} \in \mathbb{Z}$ e suponhamos que

$$a_1(\zeta_{p^r} + \zeta_{p^r}^{-1}) + a_2(\zeta_{p^r}^2 + \zeta_{p^r}^{-2}) + \cdots + a_{\frac{(p-1)p^{r-1}}{2}}(\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}) = 0.$$

Logo

$$a_1\zeta_{p^r} + a_1\zeta_{p^r}^{(p-1)p^{r-1}-1} + a_2\zeta_{p^r}^2 + a_2\zeta_{p^r}^{(p-1)p^{r-1}-2} + \cdots + a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + a_{\frac{(p-1)p^{r-1}}{2}}\zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}} = 0.$$

Como $\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r}]$ sobre $\mathbb{Z}$, segue que estes elementos são linearmente independentes, e assim, $a_1 = a_2 = \cdots = a_{\frac{(p-1)p^{r-1}}{2}} = 0$. Assim $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta^{\frac{(1-p)p^{r-1}}{2}}\}$ é linearmente independente. Portanto, $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \cdots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ sobre $\mathbb{Z}$. ■

Proposição 2.3.4. *O discriminante de $\mathbb{Q}(\zeta_{p^r})$ sobre $\mathbb{Q}$ é dado por*

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

Demonstração: Pelo Teorema 2.3.2, segue que $\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ é uma base integral. Pela Proposição 1.3.6, segue que

$$\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = \pm N_{\mathbb{K}|\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})),$$

onde $\phi'_{p^r}(x)$ é a derivada do p^r-ésimo polinômio ciclotômico que é dado por

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

Derivando ambos os lados, segue que

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

ou seja,

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

Como $\zeta_{p^r}^{p^r}=1$, segue que $\zeta_{p^r}^{p^{r-1}}=(e^{\frac{2\pi i}{p^r}})^{p^{r-1}}=e^{\frac{2\pi i}{p}}=\zeta_p$. Assim,

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

Agora, aplicando a função norma em ambos os membros e usando sua linearidade, segue que

$$N_{\mathbb{K}|\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r}))=\frac{N_{\mathbb{K}|\mathbb{Q}}(-p^r)}{N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p)N_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r})}.$$

Pela Proposição 2.3.1, segue que $N_{\mathbb{K}|\mathbb{Q}}(\zeta_{p^r})=\pm1$, $N_{\mathbb{K}|\mathbb{Q}}(-p^r)=(-p^r)^{(p-1)p^{r-1}}$, e $N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p)=N_{\mathbb{K}|\mathbb{Q}}(N_{\mathbb{K}|\mathbb{Q}(\zeta_p)}(1-\zeta_p))=N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p)^{p^{r-1}}=p^{p^{r-1}}$. Assim, $N_{\mathbb{K}|\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r}))=\dfrac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}}=\pm p^{p^{r-1}(r(p-1)-1)}$. Portanto

$$\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1,\zeta_{p^r},\ldots,\zeta_{p^r}^{(p-1)p^{r-1}-1})=\pm p^{p^{r-1}(r(p-1)-1)},$$

o que prova a proposição. ■

2.4 Corpo ciclotômico $\mathbb{Q}(\zeta_n)$

Nesta seção, nosso objetivo é determinar o anel de inteiros e o discriminante para qualquer corpo ciclotômico $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Esta generalização segue de um resultado mais geral considerando os inteiros algébricos de um corpo composto $\mathbb{KL}$, onde $\mathbb{K}$ e $\mathbb{L}$ são corpos de números. Para isso, se $\mathbb{K}$ e $\mathbb{L}$ são corpos de números, então o corpo composto $\mathbb{KL}$, que é definido como o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e $\mathbb{L}$, consiste de todas as somas finitas

$$\alpha_1\beta_1+\cdots+\alpha_r\beta_r,\ \text{onde}\ \alpha_i\in\mathbb{K},\ \text{e}\ \beta_i\in\mathbb{L},\ \text{para}\ i=1,2,\ldots,r.$$

Se $\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{KL}}$ são os anéis de inteiros algébricos de $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{KL}$, respectivamente, então $\mathcal{O}_{\mathbb{KL}}$ contém o anel

$$\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}=\{\alpha_1\beta_1+\cdots+\alpha_r\beta_r\mid\alpha_i\in\mathcal{O}_{\mathbb{K}},\ \beta_i\in\mathcal{O}_{\mathbb{L}},\ \text{para}\ i=1,2,\ldots,r\}.$$

Geralmente, a igualdade não ocorre, entretanto, pode-se mostrar que $\mathcal{O}_{\mathbb{KL}}=\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$ sob certas condições sobre os corpos. Sejam m e n os graus de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, sobre $\mathbb{Q}$, e seja $d=mdc(d_1,\,d_2)$, onde d_1 e d_2 são os discriminantes de $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$, respectivamente.

Teorema 2.4.1. *Se* $[\mathbb{KL} : \mathbb{Q}] = mn$, *então* $\mathcal{O}_{\mathbb{KL}} \subset \frac{1}{d}\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$.

Demonstração: Sejam $\{\alpha_1, \ldots, \alpha_m\}$ uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $\{\beta_1, \ldots, \beta_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}$. Assim, $B = \{\alpha_i\beta_j \mid i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ é uma base de $\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}$ e também uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$. Se $\alpha \in \mathcal{O}_{\mathbb{KL}}$, então pelo Teorema 2.3.1, segue que α pode ser escrito na forma

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j, \tag{2.5}$$

onde r e todos os m_{ij} estão em $\mathbb{Z}$, e que estes $mn + 1$ inteiros não tem fatores comuns maiores que 1, ou seja, $mdc(r, mdc(m_{ij})) = 1$. Para mostrarmos o teorema, devemos mostrar que $r|d$ para qualquer α. Para isto, devemos mostrar que $r|d_1$ e $r|d_2$ pois assim, pela definição de máximo divisor comum, segue que $r \mid d$. Como todo monomorfismo σ de $\mathbb{K}$ em $\mathbb{C}$ extende a um monomorfismo, que também denotamos por σ, de $\mathbb{KL}$ em $\mathbb{C}$, fixando $\mathbb{L}$, segue que

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j,$$

para cada σ. Se $x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$, para cada $i = 1, \ldots, m$, então obtemos m equações $\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha)$ para cada σ, e resolvendo este sistema pela regra de Cramer, segue que $x_i = \frac{\gamma_i}{\delta}$, onde δ é o determinante da matriz formado pelos coeficientes $\sigma(\alpha_i)$ e γ_i é obtido de δ trocando a i-ésima coluna por $\sigma(\alpha)$, para $i = 1, 2, \ldots, m$. Assim, δ e todos os γ_i são inteiros algébricos, pois todos os $\sigma(\alpha_i)$ e $\sigma(\alpha)$ são, e além disso, $\delta^2 = d_1$. Se $e = d_1$, então $ex_i = \delta\gamma_i \in \mathcal{O}_{\mathbb{C}}$, onde $\mathcal{O}_{\mathbb{C}}$ é o anel de inteiros algébricos de $\mathbb{C}$, e portanto, $ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j \in \mathcal{O}_{\mathbb{C}} \cap \mathbb{L} = \mathcal{O}_{\mathbb{L}}$. Como $\{\beta_1, \ldots, \beta_n\}$ forma uma base integral de $\mathcal{O}_{\mathbb{L}}$, segue que os números racionais $\frac{em_{ij}}{r}$ devem ser inteiros, e deste modo r dividem em_{ij}, para todo i e j. Como assumimos que r é relativamente primo com $mdc(m_{ij})$, segue que $r|e = d_1$. Analogamente mostramos que, $r|d_2$. Assim, $r|d_1$ e $r|d_2$. Portanto, $r|d$ e daí $d = kr$, com $k \in \mathbb{Z}$, ou seja, $r = \frac{d}{k}$. Substituindo na Equação (2.5), segue que

$$\alpha = \sum_{i,j} \frac{km_{ij}}{d}\alpha_i\beta_j = \frac{1}{d}\sum_{i,j} km_{ij}\alpha_i\beta_j.$$

Logo, $\alpha \in \frac{1}{d}\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Portanto, $\mathcal{O}_{\mathbb{KL}} \subset \frac{1}{d}\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. ■

Corolário 2.4.1. *Se* $[\mathbb{KL} : \mathbb{Q}] = mn$ *e* $d = 1$, *então* $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$.

Demonstração: Como $\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{KL}}$, pelo Teorema 2.4.1, segue que $\mathcal{O}_{\mathbb{KL}} \subseteq \frac{1}{d}\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Como

por hipótese $d = 1$, segue que $\mathcal{O}_{\mathbb{KL}} \subseteq \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Portanto, $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. ■

Teorema 2.4.2. *Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então $\mathbb{Z}[\zeta_n]$ é o anel de inteiros de $\mathbb{K}$ e $\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como um $\mathbb{Z}$-módulo.*

Demonstração: O teorema já foi provado para n primo ou potência de um primo, pelos Teoremas 2.2.1 e 2.3.2. Agora, se n não é primo ou não é uma potência de um primo, então podemos escrever $n = n_1n_2$, para inteiros relativamente primos n_1, n_2 maiores que 1. Vamos mostrar por indução que se o resultado é válido para n_1 e n_2, então o resultado é válido para n. Para aplicar o Corolário 2.4.1, devemos mostrar que

1. $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ e como consequência $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}]$.
2. $\varphi(n) = \varphi(n_1)\varphi(n_2)$.
3. $d = 1$.

De fato:

1. Do Corolário 2.1.3, segue que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$.
2. Como n_1 e n_2 são relativamente primos, segue que $\varphi(n) = \varphi(n_1)\varphi(n_2)$.
3. Pela Proposição 1.3.6, segue que $\mathcal{D}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)}N(m'_\alpha(\alpha))$, onde $m_\alpha(x)$ é o polinômio minimal de α sobre $\mathbb{Q}$. Sejam d_{n_1} e d_{n_2} os discriminantes de $\mathbb{Z}[\zeta_{n_1}]$ e $\mathbb{Z}[\zeta_{n_2}]$, respectivamente. Como $m_{\zeta_{n_1}}(x) = x^{n_1} - 1$, segue que $m'_{\zeta_{n_1}}(x) = n_1x^{n_1-1}$, e substituindo x por ζ_{n_1}, segue que $m'_{\zeta_{n_1}}(\zeta_{n_1}) = n_1\zeta_{n_1}^{n_1-1} = \frac{n_1}{\zeta_{n_1}}$. Assim, aplicando a função norma em ambos os lados e usando a sua linearidade, segue que

$$N_{\mathbb{Q}(\zeta_{n_1})|\mathbb{Q}}(m'_{\zeta_{n_1}}(\zeta_{n_1})) = \frac{N_{\mathbb{Q}(\zeta_{n_1})|\mathbb{Q}}(n_1)}{N_{\mathbb{Q}(\zeta_{n_1})|\mathbb{Q}}(\zeta_{n_1})} = \frac{n_1^{\varphi(n_1)}}{\pm 1}.$$

Portanto, $d_{n_1} = \pm n_1^{\varphi(n_1)}$, e isto implica que $d_{n_1}|n_1^{\varphi(n_1)}$. Analogamente, $d_{n_2}|n_2^{\varphi(n_2)}$. Sendo $d = mdc(d_{n_1}, d_{n_2})$, segue que

$$\begin{cases} d|d_{n_1}\, e\, d_{n_1}|n_1^{\varphi(n_1)} \Longrightarrow d|n_1^{\varphi(n_1)} \\ d|d_{n_2}\, e\, d_{n_2}|n_2^{\varphi(n_2)} \Longrightarrow d|n_2^{\varphi(n_2)}. \end{cases}$$

Como $mdc(n_1^{\varphi(n_1)}, n_2^{\varphi(n_2)}) = 1$, segue que $d|1$, e portanto, $d = 1$.

Assim, pelo Corolário 2.4.1, segue que $\mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_n]$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$. ■

Proposição 2.4.1. *Se $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é o anel de inteiros de $\mathbb{L}$ e $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Pelo Teorema 2.4.2 segue que o anel de inteiros de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$. Como ζ_n é inteiro, segue que ζ_n^{-1} é inteiro e pelo Corolário 1.2.2, segue que $\zeta_n + \zeta_n^{-1}$ também é inteiro. Portanto, $\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$, onde $\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros de $\mathbb{L}$. Agora, mostremos que $\mathcal{O}_{\mathbb{L}} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então

$$\alpha = a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{\varphi(n)}{2}}(\zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}),$$

onde $a_i \in \mathbb{Q}$, para $i = 1, 2, \ldots, \frac{\varphi(n)}{2}$. Devemos mostrar que $a_i \in \mathbb{Z}$. Multiplicando α por $\zeta_n^{\frac{\varphi(n)}{2}}$, segue que

$$\zeta_n^{\frac{\varphi(n)}{2}}\alpha = a_1\zeta_n^{\frac{\varphi(n)+2}{2}} + a_1\zeta_n^{\frac{\varphi(n)-2}{2}} + a_2\zeta_n^{\frac{\varphi(n)+4}{2}} + a_2\zeta_n^{\frac{\varphi(n)-4}{2}} + \cdots + a_{\frac{\varphi(n)}{2}}\zeta_n^{\varphi(n)} + a_{\frac{\varphi(n)}{2}},$$

que é um inteiro algébrico em $\mathbb{Q}(\zeta_n)$, logo pertence a $\mathbb{Z}[\zeta_n]$. Assim, $a_i \in \mathbb{Z}$, para $i = 1, 2, \ldots, \frac{\varphi(n)}{2}$. Portanto, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, ou seja, o anel de inteiros de $\mathbb{L}$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Como $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$ e como $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que é suficiente mostrar que é linearmente independente. Para isso, sejam $a_1, a_2, \ldots, a_{\frac{\varphi(n)}{2}} \in \mathbb{Z}$ e suponhamos que

$$a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{\varphi(n)}{2}}(\zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}) = 0.$$

Logo,

$$a_1\zeta_n + a_1\zeta_n^{-1} + a_2\zeta_n^2 + a_2\zeta_n^{-2} + \cdots + a_{\frac{\varphi(n)}{2}}\zeta_n^{\frac{\varphi(n)}{2}} + a_{\frac{\varphi(n)}{2}}\zeta_n^{-\frac{\varphi(n)}{2}} = 0.$$

Como $\{1, \zeta_n, \ldots, \zeta_n^{\frac{\varphi(n)}{2}-2}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ sobre $\mathbb{Z}$, segue que estes elementos são linearmente independentes, e assim, $a_1 = a_2 = \cdots = a_{\frac{\varphi(n)}{2}} = 0$. Assim, $\{\zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\frac{\varphi(n)}{2}} + \zeta_n^{\frac{-\varphi(n)}{2}}\}$ é linearmente independente, e portanto, é uma base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ sobre $\mathbb{Z}$. ■

Nosso objetivo, agora, é o cálculo do discriminante de corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima da unidade.

Teorema 2.4.3. *[33, pág. 12] Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde n é um inteiro maior que 1, então o*

discriminante de $\mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{Q}$ *é dado por*

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

■

2.5 Considerações finais do capítulo

Neste capítulo, desenvolvemos os conceitos básicos envolvendo raízes da unidade e corpos ciclotômicos. Mostramos que o anel de inteiros do corpo ciclotômico $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$, encontramos uma base e explicitamos o discriminante, para os casos em que $n = p$, $n = p^r$ e n qualquer, onde p é um número primo e r um inteiro maior que 1. E também, encontramos o anel de inteiros e uma base para o corpo maximal nestes três casos.

Capítulo

3

Extensões abelianas de grau p

Neste capítulo, apresentamos resultados sobre corpos de números abeliano $\mathbb{K}$ de grau finito p, com p um primo ímpar. Para a obtenção desses resultados dividimos o capítulo em três seções, em cada seção analisamos o condutor do corpo de números abeliano $\mathbb{K}$, segundo sua fatoração em números primos. Na Seção 3.2, consideramos o caso em que o condutor de $\mathbb{K}$ é da forma $\prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i primo para $i = 1, \ldots, s$. Na Seção 3.3, apresentamos o caso em que o condutor de $\mathbb{K}$ é da forma p^2, com p um primo ímpar. E por fim, na Seção 3.4, o caso em que o condutor é da forma $p^2 \prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i's primos, para $i = 1, \ldots, s$.

Em cada uma destas seções, apresentamos um elemento primitivo de $\mathbb{K}$, uma base integral para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, caracterizamos um elemento de $\mathcal{O}_{\mathbb{K}}$ tal que pertença à um ideal primo específico de $\mathcal{O}_{\mathbb{K}}$ e encontramos o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$.

3.1 Corpos de números abelianos

Nesta seção, apresentamos alguns resultados sobre corpos de números abelianos.

Definição 3.1.1. *Se $\mathbb{K}|\mathbb{Q}$ é uma extensão de Galois cujo grupo de Galois é abeliano (cíclico), dizemos que a extensão $\mathbb{K}|\mathbb{Q}$ é abeliana (cíclica).*

Se $\mathbb{K}|\mathbb{Q}$ é uma extensão de Galois de grau p, com p um primo ímpar, segue da Proposição 2.1.1 que $\mathbb{K}$ é uma extensão cíclica, e logo, abeliana.

Teorema 3.1.1. *(Teorema de Kronecker-Weber) [30, pág. 273] Se $\mathbb{Q} \subseteq \mathbb{K}$ é uma extensão abeliana, então existe uma ráiz n-ésima da unidade ζ_n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$.* ■

Definição 3.1.2. *Seja $\mathbb{K}|\mathbb{Q}$ uma extensão abeliana finita. O menor inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado* ***condutor*** *do corpo $\mathbb{K}$, e denotado por $cond(\mathbb{K}) = n$.*

Desta forma, se $\mathbb{K}$ é um corpo de números de grau p, p primo ímpar, então $Gal(\mathbb{K}|\mathbb{Q})$ é um subgrupo de $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*$.

Proposição 3.1.1. *O número de subcorpos $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ de grau p, com $n = p_1^{a_1} \cdots p_u^{a_u}$, é $\frac{p^s-1}{p-1}$, onde $s = \#\{p_i \ ; \ p|\varphi(p_i^{a_i}),\ i = 1, \ldots, u\}$.*

Demonstração: Como existe uma relação bijetora entre os subgrupos de ordem p e os subgrupos de índice p do grupo abeliano $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, é suficiente mostrar que o grupo

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_u^{a_u}\mathbb{Z})^*$$

contem $\frac{p^s-1}{p-1}$ subgrupos de ordem p, ou seja, que contém $p^s - 1$ elementos de ordem p. Pela Proposição 2.1.1, segue que o grupo $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$ é cíclico de ordem $\varphi(p_i^{a_i})$, para cada $i = 1, \ldots, u$. Assim, se p divide $\varphi(p_i^{a_i})$, então $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$ possui um elemento x_i de ordem p e a equação $x_i^p = 1$ tem p soluções em $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$, dadas por $1, x_i, \ldots, x_i^{p-1}$. Se p não divide $\varphi(p_i^{a_i})$, então $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$ não possui um elemento x_i de ordem p e a equação $x_i^p = 1$ tem somente a solução trivial. Desse modo, a equação $(x_1, \ldots, x_u)^p = (1, \ldots, 1)$ tem $p^s - 1$ soluções não triviais, isto é, existem $p^s - 1$ elementos de ordem p em $(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_u^{a_u}\mathbb{Z})^*$. ■

Lema 3.1.1. *[33, pág. 10] Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então um primo p ramifica em $\mathcal{O}_\mathbb{K}$ se, e somente se, $p|n$.* ■

Assim, os possíveis primos que ramificam em $\mathcal{O}_\mathbb{K}$ são os primos que dividem o $cond(\mathbb{K}) = n$.

Proposição 3.1.2. *Seja $\mathbb{K}$ um corpo de números abeliano de grau p, com p primo ímpar. Então,*

1. *p ramifica em $\mathcal{O}_\mathbb{K}$ se, e somente se, $cond(\mathbb{K}) = p^2 p_1 \cdots p_s$;*

2. *p não ramifica em $\mathcal{O}_\mathbb{K}$ se, e somente se, $cond(\mathbb{K}) = p_1 \cdots p_s$;*

onde os p_i's são primos tais que $p_i \equiv 1 \ (mod\ p)$, para $i = 1, \ldots, s$.

Demonstração: Provemos o item 1. Suponha que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$, onde $m = p^a p_1^{a_1} \cdots p_u^{a_u}$, com $a > 0$. Podemos supor que $p_1, \ldots, p_s$ são os primos na fatoração de m tais que $p|\varphi(p_i)$,

com $s \leq u$. Se $n = p^2 p_1 \cdots p_s$, então $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$ e, pela Proposição 3.1.1, ambos contém o mesmo número de p-extensões. Portanto, $n = p^2 p_1 \cdots p_s$ é o condutor de $\mathbb{K}$. A recíproca segue do Lema 3.1.1. Para o item 2, suponha que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$, onde $m = p_1^{a_1} \cdots p_u^{a_u}$, com $p_i \neq p$ para todo $i = 1, \ldots, u$. Temos que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p_1 \cdots p_u})$. De fato, se $\mathbb{K} \nsubseteq \mathbb{Q}(\zeta_{p_1 \cdots p_u})$, então $\mathbb{K} \cap \mathbb{Q}(\zeta_{p_1 \cdots p_u}) = \mathbb{Q}$, o que implica que $[\mathbb{K}\mathbb{Q}(\zeta_{p_1 \cdots p_u}) : \mathbb{Q}] = p\varphi(p_1 \cdots p_u)$ divide $\varphi(m)$, ou seja, p divide $p_1^{a_1 - 1} \cdots p_u^{a_u - 1}$. Se $p_1, \ldots, p_u$ são os primos em m tais que $p | \varphi(p_i)$, para $i = 1, \ldots, s$, então $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p_1 \cdots p_u})$, pois caso contrário p divide $\varphi(p_{s+1} \cdots p_u)$. A recíproca segue do Lema 3.1.1. ■

Neste capítulo, analisamos os resultados sobre corpos de números abelianos de grau p em três casos:

1. $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i primo para $i = 1, \ldots, s$, [28].
2. $cond(\mathbb{K}) = p^2$, [13].
3. $cond(\mathbb{K}) = p^2 \prod_{i=1}^{s} p_i$, com $p_i \equiv 1 \ (mod\ p)$ e p_i primo para $i = 1, \ldots, s$, com enfoque particular no caso $cond(\mathbb{K}) = p^2 q$, com $q \equiv 1 \ (mod\ p)$, [6].

Proposição 3.1.3. *[18] Se $\mathbb{K}$ é um corpo de números abeliano de grau p e condutor n, então $|\mathcal{D}_{\mathbb{K}}| = n^{p-1}$.* ■

3.1.1 Teoremas de Leopoldt

Para encontrarmos um elemento primitivo e um $\mathbb{Z}$-base para o anel de inteiros de um corpo de números abeliano $\mathbb{K}$, vamos fazer uso dos seguintes resultados.

Teorema 3.1.2. *[22] [3] Se $\mathbb{K}$ é um corpo de números abeliano de condutor n, então $\mathbb{K} = \mathbb{Q}[G]T = \bigoplus_{d \in D} \mathbb{Q}[G]\eta_d$, onde*

$$D = \left\{ d \in \mathbb{N};\ (\prod_{p|n,\ p \neq 2} p) | d,\ d|n,\ d \neq 2k,\ k \text{ ímpar} \right\},$$

$\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}$, $\eta_d = Tr_{\mathbb{Q}(\zeta_d)|\mathbb{K}_d}(\zeta_d)$, $T = \sum_{d \in D} \eta_d$ *e* $G = Gal(\mathbb{K}|\mathbb{Q})$. ■

Teorema 3.1.3. *[25] [3] Se $\mathbb{K}$ é um corpo de números abeliano de condutor n, então $\mathcal{O}_{\mathbb{K}} =$*

$\bigoplus_{d\in D} \mathbb{Z}[G]\eta_d$, *onde*

$$D = \left\{ d \in \mathbb{N};\ (\prod_{p|n,\ p\neq 2} p)|d,\ d|n,\ d \neq 2k,\ k\ \textit{ímpar} \right\},$$

$\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}$, $\eta_d = Tr_{\mathbb{Q}(\zeta_d)|\mathbb{K}_d}(\zeta_d)$, $T = \sum_{d\in D} \eta_d$ *e* $G = Gal(\mathbb{K}|\mathbb{Q})$. ■

3.2 Extensões abelianas de grau p, onde p é não ramificado e $cond(\mathbb{K}) = p_1p_2...p_s$

Seja $\mathbb{K}$ um corpo de números abeliano de grau p, onde p é um primo ímpar. Suponha que $n = \prod_{i=1}^{s} p_i$ seja o condutor de $\mathbb{K}$, com $p_i \equiv 1(mod\ p)$ e os p_i's são primos distintos para $i = 1, \ldots, s$. Apresentamos, nesta seção, o número de subcorpos de $\mathbb{L} = \mathbb{Q}(\zeta_n)$, o elemento primitivo de $\mathbb{K}$, uma base integral do anel de inteiros, e por fim apresentamos uma família de $\mathbb{Z}$-submódulos de $\mathcal{O}_{\mathbb{K}}$.

Proposição 3.2.1. *O número de subcorpos* $\mathbb{K}$ *de grau* p *e condutor* n *em* $\mathbb{Q}(\zeta_n)$ *é* $(p-1)^{s-1}$, *onde* $n = \prod_{i=1}^{s} p_i$ *e* $p_i \equiv 1(mod\ p)$.

Demonstração: O resultado segue para $s = 1$, uma vez que o corpo $\mathbb{Q}(\zeta_{p_1})$ contém somente uma p-extensão. Quando $n = p_1p_2$, existem 2 subcorpos de $\mathbb{Q}(\zeta_n)$ que possuem condutor p_i, com $i = 1, 2$. Assim, existem dois subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n, e portanto, existem $\frac{p^2-1}{p-1} = p + 1 - 2 = p - 1$ subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. Para $n = p_1p_2p_3$, consideramos subcorpos de condutor p_i e p_ip_j, para $i \neq j$. Assim, existem 3 subcorpos de condutor p_i e $\frac{3!}{2!(3-2)!}(p-1)$ subcorpos de condutor p_ip_j, com $i \neq j$. Logo, existem $\frac{p^3-1}{p-1} - 3 - 3(p-1) = (p-1)^2$ subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. Fazendo dessa maneira, segue que existem $\frac{p^s-1}{p-1} - s - \frac{s!}{2!(s-2)!}(p-1) - \frac{s!}{3!(s-3)!}(p-1)^2 - \cdots - \frac{s!}{(s-1)!(s-(s-1))!}(p-1)^{s-2} = (p-1)^{s-1}$ subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. ■

Teorema 3.2.1. *[19] Se* $\mathbb{K}$ *é um corpo de números abeliano com condutor* n *ímpar livre de quadrados, então* $\mathbb{Q}(t) = \mathbb{K}$, *onde* $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$ *e* $\mathbb{L} = \mathbb{Q}(\zeta_n)$. ■

Definição 3.2.1. *Seja* $\mathbb{K}|\mathbb{Q}$ *uma extensão de Galois finita. Se os conjugados de um elemento* $t \in \mathbb{K}$ *formam uma* $\mathbb{Q}$*-base de* $\mathbb{K}$, *dizemos que* $\mathbb{K}$ *tem uma* ***base integral normal*** *gerada por* t. *Em outras palavras,* $\mathbb{K} = \mathbb{Q}[G]t$, *onde* $G = Gal(\mathbb{K}|\mathbb{Q})$.

Definição 3.2.2. *Seja $\mathbb{K}|\mathbb{Q}$ uma extensão de Galois finita. Se os conjugados de um elemento $t \in \mathcal{O}_\mathbb{K}$ formam uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$, dizemos que $\mathcal{O}_\mathbb{K}$ tem uma b**ase integral normal** gerada por t. Em outras palavras, $\mathcal{O}_\mathbb{K} = \mathbb{Z}[G]t$, onde $G = Gal(\mathbb{K}|\mathbb{Q})$.*

O Teorema a seguir fornece condições para que $\mathcal{O}_\mathbb{K}$ possua uma base integral normal.

Teorema 3.2.2 (Hilbert-Speiser)**.** *[19] Seja $\mathbb{K}$ um corpo de números abeliano, com condutor n. Assim, $\mathcal{O}_\mathbb{K}$ tem uma base integral normal se, e somente se, n é livre de quadrados.* ■

3.2.1 Forma traço integral

Seja p um primo não ramificado em $\mathbb{K}$. Assim, se θ é um gerador de $Gal(\mathbb{K}|\mathbb{Q})$, então $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base integral normal de $\mathbb{K}$, gerada pelo elemento $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$. Nessa subseção, estamos interessados em calcular $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_\mathbb{K}$.

Como $\mathbb{K}$ é de grau p, segue que $\mathbb{K}$ é totalmente real, $|\mathcal{D}_\mathbb{K}| = n^{p-1}$, $n = p_1 \cdots p_s$ e $p_1, \ldots, p_s$ são primos que ramificam em $\mathbb{K}$. Se $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_\mathbb{K}$, então $x^2 = \sum_{i,j=0}^{p-1} a_ia_j\theta^i(t)\theta^j(t)$. Como

$$Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t)),$$

com $i, j = 1, \ldots, p-1$, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = \sum_{i,j=0}^{p-1} a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t)).$$

Logo, a forma traço canônica de $\mathbb{K}$ pode ser expressa em função de $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t))$, onde $k = 1, \ldots, p-1$.

Seja H um subgrupo de $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ que fixa $\mathbb{K}$. Como $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*$, segue que os elementos de H podem ser representados como s-uplas em $(\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*$.

Lema 3.2.1. *Se $\alpha = (\alpha_1, \ldots, \alpha_s) \in H$, com $1 \leq q < s$ e $\Pi : H \to (\mathbb{Z}/p_{j_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{j_q}\mathbb{Z})^*$ é a projeção definida por $\Pi(\alpha) = (\alpha_{j_1}, \ldots, \alpha_{j_q})$, com $1 \leq j_1 < \cdots < j_q \leq s$, então*

$$|Ker(\Pi)| = \frac{\prod_{l=1}^{r}(p_{i_l} - 1)}{p},$$

onde $1 \leq i_1 < \cdots < i_r \leq s$ são coordenadas de α distintas dos $j_1, \ldots, j_q$.

Demonstração: Se $Z = (\mathbb{Z}/p_{j_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{j_q}\mathbb{Z})^*$ e $Z^c = (\mathbb{Z}/p_{i_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{i_r}\mathbb{Z})^*$, então $H \leq \Pi(H) \times Z^c \leq (\mathbb{Z}/n\mathbb{Z})^*$. Mas, como H tem índice p em $(\mathbb{Z}/n\mathbb{Z})^*$, segue que $\Pi(H) \times Z^c = H$ ou $\Pi(H) \times Z^c = (\mathbb{Z}/n\mathbb{Z})^*$. A primeira igualdade não ocorre, pois caso contrário H teria $\mathbb{Z}^c$ como fator, o que contradiz o fato de $\mathbb{K}$ ter condutor máximo. Desse modo, Π é um homomorfismo sobrejetor, ou seja, $H/Ker(\Pi) \simeq Z$. Portanto,

$$|Ker(\Pi)| = \frac{\varphi(n)/p}{(p_{j_1} - 1) \cdots (p_{j_q} - 1)} = \frac{\prod_{l=1}^{r}(p_{i_l} - 1)}{p},$$

o que prova o lema. ■

Se $z \in \Pi(H)$, então $\Pi^{-1}(z)$ é uma classe lateral de $Ker(\Pi)$ em H, a saber, $\Pi^{-1}(z) = \alpha Ker(\Pi)$, onde $z = \Pi(\alpha)$. Logo, $|\Pi^{-1}(z)| = |Ker(\Pi)|$.

No próximo teorema usamos a notação $q_i = p_i - 1$, para todo $i = 1, \ldots, s$, e

$$A_{i_1,\ldots,i_r} = \frac{(p_{i_1} - 1) \cdots (p_{i_r} - 1)}{p} = \frac{q_{i_1} \cdots q_{i_r}}{p},$$

onde $1 \leq i_1 < \cdots < i_r \leq s$.

Teorema 3.2.3. *Se θ é um gerador de $Gal(\mathbb{K}|\mathbb{Q})$ e $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$, então*

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

com $k = 0, 1, \ldots, p-1$.

Demonstração: Se $h = \varphi(n)/p$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t)) = \frac{1}{h} Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t))$. Como θ é o gerador de $Gal(\mathbb{K}|\mathbb{Q})$, segue que $\theta = \sigma_r|_{\mathbb{K}}$ para algum $\sigma_r \in Gal(\mathbb{L}|\mathbb{Q})$, tal que $\sigma_r(\zeta_n) = \zeta_n^r$. Logo,

$$t\theta^k(t) = \sum_{\alpha,\beta \in H} \zeta_n^{\alpha+\beta r^k}.$$

Agora, se $d = \frac{n}{p_1} + \cdots + \frac{n}{p_s}$, então $\zeta_n^d = \zeta_{p_1} \cdots \zeta_{p_s}$. Assim, $\zeta_n^{\alpha+\beta r^k}$ é uma raíz primitiva da unidade se, e somente se, $\zeta_n^{d(\alpha+\beta r^k)} = \zeta_{p_1}^{\alpha+\beta r^k} \cdots \zeta_{p_s}^{\alpha+\beta r^k}$ também é, pois $mdc(d, n) = 1$. Desta maneira,

$$Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = \sum_{\alpha,\beta \in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n^{\alpha+\beta r^k}) = \sum_{\alpha,\beta \in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p_1}^{\alpha+\beta r^k} \cdots \zeta_{p_s}^{\alpha+\beta r^k}).$$

Se $\alpha = (\alpha_1, \ldots, \alpha_s), \beta = (\beta_1, \ldots, \beta_s) \in H$ e $r = (r_1, \ldots, r_s) \in (\mathbb{Z}/n\mathbb{Z})^*$, então $\alpha + \beta r^k \ (mod\ p_i) = \alpha_i + \beta_i r_i^k$. Assim,

$$Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = \sum_{\alpha,\beta \in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}).$$

E como

$$Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) = Tr_{\mathbb{Q}(\zeta_{n/p_1})|\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_{n/p_1})})(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}),$$

segue que

$$Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_{n/p_1})}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) = (\zeta_{p_2}^{\alpha_2+\beta_2 r_2 k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}).$$

Logo,

$$\begin{aligned} Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) &= \sum_{\alpha,\beta \in H} Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) Tr_{\mathbb{Q}(\zeta_{n/p_1})|\mathbb{Q}}(\zeta_{p_2}^{\alpha_2+\beta_2 r_2^k} \cdots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) \qquad (3.1) \\ &= \sum_{\alpha,\beta \in H} Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})|\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k}), \qquad (3.2) \end{aligned}$$

onde

$$Tr_{\mathbb{Q}(\zeta_{p_i})|\mathbb{Q}}(\zeta_{p_i}^{\alpha_i+\beta_i r_i^k}) = \begin{cases} p_i - 1, \ se\ \alpha_i + \beta_i r_i^k = 0 \\ -1, \ se\ \alpha_i + \beta_i r_i^k \neq 0, \end{cases}$$

para $i = 1, \ldots, s$. Dividiremos a prova em dois casos: o primeiro quando $k = 0$ e o segundo quando $k = 1, \ldots, p-1$.

Caso 1: $k = 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_s) \in H$. Como a extensão $\mathbb{K}|\mathbb{Q}$ é de Galois de grau ímpar, segue que $\mathbb{K}$ é totalmente real. Assim, a conjugação complexa pertence a H e, portanto, $(-1, \ldots, -1) \in H$. Logo, $\beta = (-\alpha_1, \ldots, -\alpha_s) \in H$. Além disso, β é o único elemento de H tal que $\alpha + \beta = 0$, pois $H \leq (\mathbb{Z}/n\mathbb{Z})^* \subseteq \mathbb{Z}/n\mathbb{Z}$. Assim, $\alpha_i + \beta_i = 0$, para $i = 1, \ldots, s$. Logo,

$$Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})|\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) = (p_1 - 1) \cdots (p_s - 1) = \varphi(n).$$

Neste caso, existem $h = \#H$ parcelas iguais a $\varphi(n)$ na Equação (3.2). Deste modo, a soma das parcelas correspondentes aos pares $\alpha, \beta \in H$ tais que $\alpha_i + \beta_i = 0$, para todo $i = 1, ;s$, é igual a $T_0 = h\varphi(n)$. Pelo Lema 3.2.1, para cada $i_1 = 1, \ldots, s$, segue que existem $S_{i_1} = A_{i_1} - 1 = \frac{q_{i_1}}{p} - 1$

elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = -\alpha_i$ para todo $i \neq i_1$ e $\alpha_{i_1} + \beta_{i_1} \neq 0$. Neste caso, cada parcela $Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})|\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k})$ na Equação (3.2) correspondente ao par α, β é igual a $-\frac{\varphi(n)}{q_{i_1}}$. Logo, a soma destas parcelas é igual a

$$T_1 = -h\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}S_{i_1} = -h\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}\left(\frac{q_{i_1}}{p}-1\right) = -h\left(\frac{1}{p}\binom{s}{s-1}\varphi(n) - \sum_{i_1}^{s}\frac{\varphi(n)}{q_{i_1}}\right).$$

Analogamente, existem $S_{i_1,i_2} = A_{i_1,i_2} - S_{i_1} - S_{i_2} - 1 = A_{i_1,i_2} - A_{i_1} - A_{i_2} + 1$ elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = -\alpha_i$ para todo $i \neq i_1, i_2$, onde $\alpha_{i_1} + \beta_{i_1} \neq 0$ e $\alpha_{i_2} + \beta_{i_2} \neq 0$, $i_1, i_2 = 1, \ldots, s$, com $i_1 < i_2$. Nesse caso, cada parcela na Equação (3.2) é igual a $\frac{\varphi(n)}{q_{i_1}q_{i_2}}$, e a soma delas é dada por

$$\begin{aligned} T_2 &= h\sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}S_{i_1,i_2} = h\left(\sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}\frac{(q_{i_1}q_{i_2}-q_{i_1}-q_{i_2})}{p} + \sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}\right) \\ &= h\left[\frac{1}{p}\left(\binom{s}{s-2}\varphi(n) - \binom{s-1}{s-2}\sum_{i_1}^{s}\frac{\varphi(n)}{q_{i_1}}\right) + \sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}\right]. \end{aligned}$$

O caso geral, em que u coordenadas $\alpha_i+\beta_i$ são não nulas, para cada $u = 1, \ldots, s$, é caracterizado da seguinte forma: Existem

$$\begin{aligned} S_{i_1,\ldots,i_u} &= A_{i_1,\ldots,i_u} - \sum_{1\leq l_1<\cdots<l_{u-1}\leq u} S_{i_{l_1},\ldots,i_{l_u}} - \cdots - \sum_{1\leq l_1<l_2\leq u} S_{i_{l_1},i_{l_2}} - \sum_{l=1}^{u} S_{i_l} - 1 \\ &= A_{i_1,\ldots,i_u} - \sum_{1\leq l_1<\cdots<l_{u-1}\leq u} A_{i_{l_1},\ldots,i_{l_u}} + \cdots + (-1)^{u-1}\sum_{l=1}^{u} A_{i_l} + (-1)^u \end{aligned}$$

elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = -\alpha_i$ para todo $i \neq i_1, \ldots, i_u$ e $\alpha_{i_l} + \beta_{i_l} \neq 0$ para todo $l = 1, \ldots, u$. Neste caso, cada parcela na Equação (3.2) é igual a

$$\frac{(-1)^u\varphi(n)}{q_{i_1}q_{i_2}\cdots q_{i_u}}$$

e a respectiva soma é dada por

$$\begin{aligned} T_u &= (-1)^u h\sum_{l_1<\cdots<l_u}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_u}}S_{i_1,\ldots,i_u} \\ &= (-1)^u h\sum_{l_1<\cdots<l_u}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_u}}\left(\frac{q_{i_1}\cdots q_{i_u} - (q_{i_1}\cdots q_{i_{u-1}} + \cdots + q_{i_2}\cdots q_{i_u}) + \cdots}{p}\right. \end{aligned}$$

$$\frac{\cdots+(-1)^{u-2}(q_{i_1}q_{i_2}+\cdots+q_{i_{u-1}}q_{i_u})+(-1)^{u-1}(q_{i_1}+\cdots+q_{i_u})}{p}+(-1)^u\Bigg)$$

$$\begin{aligned}=\ & (-1)^u h\Bigg[\frac{1}{p}\Bigg(\binom{s}{s-u}\varphi(n)-\binom{s-1}{s-u}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\cdots\\ & \cdots+(-1)^{u-1}\binom{s-(u-1)}{s-u}\sum_{l_1<\cdots<l_u}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{u-1}}}\Bigg)+(-1)^u\sum_{l_1<\cdots<l_u}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_u}}\Bigg].\end{aligned}$$

Assim,

$$\begin{aligned}Tr_{\mathbb{L}|\mathbb{Q}}(t^2) &= T_0+T_1+T_2+\cdots+T_{s-1}+T_s\\ &= h\varphi(n)-h\Bigg(\frac{1}{p}\binom{s}{s-1}\varphi(n)-\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}\Bigg)\\ &\quad +h\Bigg[\frac{1}{p}\Bigg(\binom{s}{s-2}\varphi(n)-\binom{s-1}{s-2}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}\Bigg)+\sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}\Bigg]-\cdots\\ &\quad +(-1)^{s-1}h\Bigg[\frac{1}{p}\Bigg(\binom{s}{1}\varphi(n)-\binom{s-1}{1}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\cdots\\ &\quad \cdots+(-1)^{s-2}\binom{2}{1}\sum_{i_1<\cdots<i_{s-2}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-2}}}\Bigg)+(-1)^{s-1}\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\Bigg]\\ &\quad +(-1)^s h\Bigg[\frac{1}{p}\Bigg(\binom{s}{0}\varphi(n)-\binom{s-1}{0}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\cdots\\ &\quad \cdots+(-1)^{s-1}\binom{1}{0}\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\Bigg)+(-1)^s\Bigg].\end{aligned}$$

Deste modo,

$$\begin{aligned}Tr_{\mathbb{L}|\mathbb{Q}}(t^2) &= h\Bigg[\Bigg(1+\frac{-\binom{s}{s-1}+\binom{s}{s-2}-\cdots+(-1)^{s-1}\binom{s}{1}+(-1)^s\binom{s}{0}}{p}\Bigg)\varphi(n)\\ &\quad +\Bigg(1+\frac{-\binom{s-1}{s-2}+\binom{s-1}{s-3}-\cdots+(-1)^{s-2}\binom{s-1}{1}+(-1)^{s-1}\binom{s-1}{0}}{p}\Bigg)\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\cdots\\ &\quad +\Bigg(1+\frac{-\binom{2}{1}+\binom{2}{0}}{p}\Bigg)\sum_{i_1<\cdots<i_{s-2}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-2}}}+\Bigg(1-\frac{\binom{1}{0}}{p}\Bigg)\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}+1\Bigg].\end{aligned}$$

E como

$$-\binom{u}{u-1}+\binom{u}{u-2}-\cdots+(-1)^{u-1}\binom{u}{1}+(-1)^u\binom{u}{0}=-1,$$

para todo $u = 1, \ldots, s$, segue que

$$Tr_{\mathbb{L}|\mathbb{Q}}(t^2) = h\left[\left(1-\frac{1}{p}\right)\left(\varphi(n) + \sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}} + \sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}} + \cdots + \sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right) + 1\right].$$

Finalmente, como

$$\begin{aligned} n = p_1p_2\cdots p_s &= (q_1+1)(q_2+1)\cdots(q_s+1) \\ &= \varphi(n) + \sum_{i_1<\cdots<i_{s-1}} q_{i_1}\cdots q_{i_{s-1}} + \cdots + \sum_{i_1<i_2} q_{i_1}q_{i_2} + \sum_{i_1=1}^{s} q_{i_1} + 1 \\ &= \varphi(n) + \sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}} + \sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}} + \cdots + \sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}} + 1, \end{aligned}$$

segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = \frac{1}{h}Tr_{\mathbb{L}|\mathbb{Q}}(t^2) = \frac{(p-1)(n-1)}{p} + 1 = n - \left(\frac{n-1}{p}\right).$$

Caso 2: $k \neq 0$, ou seja, $k = 1, 2, \ldots, p-1$. Seja $\alpha = (\alpha_1, \ldots, \alpha_s) \in H$. Assim, $\alpha + \beta r^k \neq 0$, para todo $\beta \in H$, uma vez que, se $\beta \in H$ é tal que $\alpha + \beta r^k = 0$, então $\alpha = -\beta r^k \in r^k H$, pois $-1 \in H$. Por outro lado, denotando $G = Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, segue que $G/H \simeq Gal(\mathbb{K}|\mathbb{Q})$. Logo, $G = H \cup \sigma_r H \cup \cdots \cup \sigma_{r^{p-1}} H$, isto é, $(\mathbb{Z}/n\mathbb{Z})^* = H \cup rH \cup \cdots \cup r^{p-1}H$ é uma união de classes laterais disjuntas. Desse modo, $\alpha \notin H$, o que é um absurdo. Portanto, a soma T_0 das parcelas $Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})|\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k})$ na Equação (3.2) correspondentes aos pares $\alpha, \beta \in H$ tais que $\alpha_i + \beta_i r_i^k = 0$, para todo $i = 1, \ldots, s$, é nula, isto é, $T_0 = 0$. Uma vez que $-\alpha r^{-k} = (-\alpha_1 {r_1}^{-k}, \ldots, -\alpha_s {r_s}^{-k}) \in (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*$, segue do Lema 3.2.1 que, para cada $i_1 = 1, \ldots, s$, existem $A_{i_1} = \dfrac{q_{i_1}}{p}$ elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = \alpha_i r_i^{-k}$, para todo $i \neq i_1$. Consequentemente, $\alpha_i + \beta_i r_i^k = 0$, para $i \neq i_1$. Ainda, $\alpha_{i_1} + \beta_{i_1} r_{i_1}^k \neq 0$, pois $\alpha + \beta r^k \neq 0$. Neste caso, a parcela

$$Tr_{\mathbb{Q}(\zeta_{p_1})|\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})|\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k})$$

na Equação (3.2) correspondente ao par α, β é igual a $-\frac{\varphi(n)}{q_{i_1}}$. Então, a soma destas parcelas é igual a

$$T_1 = -h\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}A_{i_1} = -h\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}\left(\frac{q_{i_1}}{p}\right) = \frac{-h}{p}\binom{s}{s-1}\varphi(n).$$

Analogamente, existem $S_{i_1,i_2} = A_{i_1,i_2} - A_{i_1} - A_{i_2}$ elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que

$\beta_i = -\alpha_i r_i^{-k}$ para todo $i \neq i_1, i_2$, onde $\alpha_{i_1} + \beta_{i_1} r_{i_1}^k \neq 0$ e $\alpha_{i_2} + \beta_{i_2} r_{i_2}^k \neq 0$, para $i_1, i_2 = 1, \ldots, s$, com $i_1 < i_2$. Neste caso, a parcela na Equação (3.2) é igual a $\frac{\varphi(n)}{q_{i_1} q_{i_2}}$, e a soma delas é dada por

$$T_2 = h \sum_{i_1<i_2} \frac{\varphi(n)}{q_{i_1}q_{i_2}} S_{i_1,i_2} = h \sum_{i_1<i_2} \frac{\varphi(n)}{q_{i_1}q_{i_2}} \frac{(q_{i_1}q_{i_2} - q_{i_1} - q_{i_2})}{p} = \frac{h}{p}\left(\binom{s}{s-2}\varphi(n) - \binom{s-1}{s-2}\sum_{i_1}^{s} \frac{\varphi(n)}{q_{i_1}}\right).$$

No caso geral, quando u coordenadas $\alpha_i + \beta_i r_i^k$ são não nulas, para cada $u = 1, \ldots, s$, existem

$$\begin{aligned} S_{i_1,\ldots,i_u} &= A_{i_1,\ldots,i_u} - \sum_{1\leq l_1<\cdots<l_{u-1}\leq u} S_{i_{l_1},\ldots,i_{l_u}} - \cdots - \sum_{1\leq l_1<l_2\leq u} S_{i_{l_1},i_{l_2}} - \sum_{l=1}^{u} S_{i_l} \\ &= \frac{q_{i_1}\ldots q_{i_u}}{p} - \sum_{1\leq l_1<\cdots<l_{u-1}\leq u} \frac{q_{i_{l_1}}\cdots q_{i_{l_u}}}{p} + \cdots + (-1)^{u-1}\sum_{l=1}^{u}\frac{q_{i_l}}{p} \end{aligned}$$

elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = -\alpha_i r_i^{-k}$ para todo $i \neq i_1, \ldots, i_u$ e $\alpha_{i_l} + \beta_{i_l} r_{i_l}^{-k} \neq 0$ para todo $l = 1, \ldots, u$. Neste caso, cada parcela na Equação (3.2) é igual a

$$\frac{(-1)^u \varphi(n)}{q_{i_1}q_{i_2}\cdots q_{i_u}},$$

e a soma é dada por

$$\begin{aligned} T_u &= (-1)^u h \sum_{l_1<\cdots<l_u} \frac{\varphi(n)}{q_{i_1}\cdots q_{i_u}} S_{i_1,\ldots,i_u} \\ &= (-1)^u \frac{h}{p}\left(\binom{s}{s-u}\varphi(n) - \binom{s-1}{s-u}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}} + \cdots \right. \\ &\quad \left. \cdots + (-1)^{u-1}\binom{s-(u-1)}{s-u}\sum_{l_1<\cdots<l_u}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{u-1}}}\right). \end{aligned}$$

Assim, $Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = T_0 + T_1 + T_2 + \cdots + T_{s-1} + T_s$, isto é,

$$\begin{aligned} Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) &= -\frac{h}{p}\binom{s}{s-1}\varphi(n) + \frac{h}{p}\left(\binom{s}{s-2}\varphi(n) - \binom{s-1}{s-2}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}\right) + \cdots \\ &+(-1)^{s-1}\frac{h}{p}\left(\binom{s}{1}\varphi(n) - \binom{s-1}{1}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}} + \cdots + (-1)^{s-2}\binom{2}{1}\sum_{i_1<\cdots<i_{s-2}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-2}}}\right) \\ &+(-1)^{s}\frac{h}{p}\left(\binom{s}{0}\varphi(n) - \binom{s-1}{0}\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}} + \cdots + (-1)^{s-1}\binom{1}{0}\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right). \end{aligned}$$

Portanto,

$$\begin{aligned} Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) &= \frac{h}{p}\Bigg[\Bigg(-\binom{s}{s-1}+\binom{s}{s-2}-\cdots+(-1)^{s-1}\binom{s}{1}+(-1)^s\binom{s}{0}\Bigg)\varphi(n) \\ &\quad +\Bigg(-\binom{s-1}{s-2}+\cdots+(-1)^{s-2}\binom{s-1}{1}+(-1)^{s-1}\binom{s-1}{0}\Bigg)\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\cdots \\ &\quad +\Bigg(-\binom{2}{1}+\binom{2}{0}\Bigg)\sum_{i_1<\cdots<i_{s-2}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-2}}}-\binom{1}{0}\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\Bigg] \\ &= \frac{h}{p}\Bigg(\varphi(n)+\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}+\cdots+\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\Bigg). \end{aligned}$$

E como

$$n-1=\varphi(n)+\sum_{i_1=1}^{s}\frac{\varphi(n)}{q_{i_1}}+\sum_{i_1<i_2}\frac{\varphi(n)}{q_{i_1}q_{i_2}}+\cdots+\sum_{i_1<\cdots<i_{s-1}}\frac{\varphi(n)}{q_{i_1}\cdots q_{i_{s-1}}},$$

segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t))=\frac{1}{h}Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t))=-\Bigg(\frac{n-1}{p}\Bigg),$$

o que demonstra o teorema. ■

Com as notações do Teorema 3.2.3, a seguir descrevemos a forma traço sobre o quadrado de um elemento qualquer do anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

Corolário 3.2.1. *Se* $x=\sum_{i=0}^{p-1}a_i\theta^i(t)\in\mathcal{O}_{\mathbb{K}}$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2)=n\Bigg(\sum_{i=0}^{p-1}a_i^2\Bigg)-\frac{n-1}{p}\Bigg(\sum_{i=0}^{p-1}a_i\Bigg)^2.$$

Demonstração: Pelo Teorema 3.2.3, segue que

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x^2) &= \sum_{i,j=0}^{p-1}Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t))=\sum_{i=0}^{p-1}a_i^2Tr_{\mathbb{K}|\mathbb{Q}}(t^2)+\sum_{\substack{i,j=0\\ i\neq j}}^{p-1}a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t)) \\ &= \Bigg(n-\frac{n-1}{p}\Bigg)\Bigg(\sum_{i=0}^{p-1}a_i^2\Bigg)-2\Bigg(\frac{n-1}{p}\Bigg)\Bigg(\sum_{\substack{i,j=0\\ i<j}}^{p-1}a_ia_j\Bigg). \\ &= n\Bigg(\sum_{i=0}^{p-1}a_i^2\Bigg)-\frac{n-1}{p}\Bigg(\sum_{i=0}^{p-1}a_i\Bigg)^2, \end{aligned}$$

o que demonstra o corolário. ■

3.2.2 Mínimo da forma traço integral

Nesta subseção, apresentamos um algoritmo para encontrar o mínimo da forma traço integral $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, dada pelo Corolário 3.2.1, restrita ao $\mathbb{Z}$-módulo livre

$$\mathcal{M}_m = \{a_0t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \ \in \ \mathcal{O}_{\mathbb{K}} \mid a_0 + a_1 + \cdots + a_{p-1} \equiv 0 \ (mod\ m)\}, \quad (3.3)$$

onde m é um inteiro positivo. Com este mínimo será possível construir reticulados algébricos com densidade de centro ótima para as dimensões 3, 5 e 7 no Capítulo 5.

Se $m = 1$, segue que $\mathcal{M}_1 = \mathcal{O}_{\mathbb{K}}$, e assim

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) \geq pN_{\mathbb{K}|\mathbb{Q}}(x^2)^{\frac{1}{p}} \geq p,$$

para todo $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Como $Tr_{\mathbb{K}|\mathbb{Q}}(1) = p$, segue que o mínimo de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}\backslash\{0\}$, é igual a p. Agora, se $m > 1$, para cada par (i, j), com $i, j = 0, 1, \ldots, p-1$ e $i \neq j$, seja a aplicação

$$\begin{array}{rccc} \tau_{ij}: & \mathbb{Z}^p & \longrightarrow & \mathbb{Z}^p \\ & (a_0, \ldots, a_{p-1}) & \longmapsto & (b_0, \ldots, b_{p-1}) \end{array}$$

onde $b_k = \begin{cases} a_i - 1, \ se\ k = i; \\ a_j + 1, \ se\ k = j; \\ a_k, \ caso \text{ contrário.} \end{cases}$

Se $a = (a_0, \ldots, a_{p-1}), b = (b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p$ são tais que $\tau_{ij}(a) = b$, então $\sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k$. Reciprocamente, se $\sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k$, então existe uma composição de τ_{ij}'s que aplica a em b. Se $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$, denotamos a soma $\sum_{k=0}^{p-1} a_k^2$ por $\|a\|^2$.

Proposição 3.2.2. *Se $a, b \in \mathbb{Z}^p$ é tal que $\tau_{ij}(a) = b$, onde $i, j = 1, \ldots, p-1$, então, $\|a\|^2 > \|b\|^2$ se, e somente se, $a_i - a_j > 1$.*

Demonstração: Como $\|a\|^2 > \|b\|^2 \Leftrightarrow a_i^2 + a_j^2 > (a_i - 1)^2 + (a_j + 1)^2 \Leftrightarrow a_i - a_j > 1$, o resultado segue. ■

Definição 3.2.3. *A* ***órbita*** *de $a \in \mathbb{Z}^p$ é definida como o conjunto*

$$O(a) = \left\{ (b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p \mid \sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k \right\}.$$

A ***órbita*** *de um elemento $x \in \mathcal{O}_\mathbb{K}$, é definida como o conjunto*

$$O(x) = \left\{ b_0 t + b_1\theta(t) + \cdots + b_{p-1}\theta^{p-1}(t) \in \mathcal{O}_\mathbb{K} \mid \sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k \right\}.$$

Lema 3.2.2. *Sejam $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$ e $S = a_0 + \cdots + a_{p-1} > 0$. Se q e r são, respectivamente, o quociente e o resto da divisão de S por p, então*

$$\min_{b \in O(a),\ b \neq 0} \|b\|^2 = pq^2 + 2rq + r.$$

E esse mínimo é atingido exatamente nos elementos b de $\mathbb{Z}^p$ tais que r entradas são iguais a $q+1$ e $p-r$ entradas são iguais a q.

Demonstração: Uma vez que $\|b\|^2 > 0$, para todo $b \in O(a)$, segue que existe $\bar{b} = (b_0, \ldots, b_{p-1})$ pertencente à órbita de a tal que

$$\|\bar{b}\|^2 = \min_{b \in O(a),\ b \neq 0} \|b\|^2.$$

Assim, $b_0 + \cdots + b_{p-1} = pq + r > 0$ e, pela Proposição 3.2.2, segue que quaisquer duas entradas de $\bar{b}$ satisfazem $|b_i - b_j| \geq 1$. Logo, $\bar{b}$ deve ser uma permutação $(q+1, \ldots, q+1, q, \ldots, q)$, onde o número de entradas iguais a $q+1$ é r e o número de entradas iguais a q é $p-r$. Portanto, $\|\bar{b}\|^2 = pq^2 + 2rq + r$. ■

Teorema 3.2.4. *Sejam $x = \sum_{k=0}^{p-1} a_k\theta^k(t) \in \mathcal{O}_\mathbb{K}$ e $S = S(x) = a_0 + \cdots + a_{p-1} > 0$. Se q é o quociente e r o resto da divisão de S por p, então*

$$M(S) = \min_{y \in O(x)} Tr_{\mathbb{K}|\mathbb{Q}}(y^2) = pq^2 + 2rq + nr - \frac{n-1}{p} r^2.$$

Demonstração: Pelo Corolário 3.2.1, para cada $y = \sum_{k=0}^{p-1} b_k\theta^k(t) \in \mathcal{O}_\mathbb{K}$, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(y^2) = n\|b\|^2 - \frac{n-1}{p} S^2,$$

onde $b = (b_0, \cdots, b_{p-1}) \in \mathbb{Z}^p$. Portanto, pelo Lema 3.2.2, segue que

$$\min_{y \in O(x)} Tr_{\mathbb{K}|\mathbb{Q}}(y^2) = n(pq^2 + 2rq + r) - \frac{n-1}{p}(pq + r)^2 = pq^2 + 2rq + nr - \frac{n-1}{p}r^2,$$

o que prova o teorema. ■

Corolário 3.2.2. *Se p divide S, então $M(S) = min\{2n, S^2/p\}$.*

Demonstração: Se $S = 0$, pelo Corolário 3.2.1, segue que o mínimo de $Tr_{\mathbb{K}|\mathbb{Q}}(y^2)$, para y não nulo pertencente à órbita de zero, ou seja, é igual a $2n$. Além disso, o mínimo é atingido com o elemento $y = b_0t + b_1\theta(t) + \cdots + b_{p-1}\theta(p-1)(t)$, com $(b_0, b_1, \ldots, b_{p-1}) = (1, -1, 0, \ldots, 0)$, ou uma de sua perturbações. Agora, se $S > 0$, então $S = pq$, isto é, $q = S/p$ e $r = 0$. Portanto, pelo Teorema 3.2.4, segue que $M(S) = S^2/p$. ■

Teorema 3.2.5. *Sejam m um inteiro positivo e $M^* = \min_{x \in \mathcal{M}_m,\ x \neq 0} Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$.*

1. *Se $p|m$, então $M^* = min\{2n, m^2/p\}$.*
2. *Se $p \nmid m$, então $M^* = min\{2n, M(m), \ldots, M(pm)\}$.*

Demonstração: Observe que $M^* = \min_{j \in \mathbb{Z}}\{M(jm)\}$. Supondo que p divide m, segue do Corolário 3.2.2, que se $j = 0$, então $M(jm) = 2n$ e, se $j \neq m$, então $M(jm) = min_{j \neq 0}\{(jm)^2/p\} = m^2/p$. Agora, suponhamos que p não divide m. Para $j = 0$ ainda é válido que $M(jm) = 2n$, pois p divide $jm = 0$. Para $j \neq 0$, segue que $\{jm \mid j = 1, \ldots, p\}$ é um conjunto completo de resíduos módulo p e a expressão $pq^2 + 2rq + nr - \frac{n-1}{p}r^2$ é uma função estritamente crescente de q. Portanto, $mim\{M(mj) \mid j \in \mathbb{Z}^*\} = min\{M(m), \ldots, M(pm)\}$. ■

3.2.3 Caracterização dos ideais primos acima dos ideais $p_i\mathbb{Z}$

Nesta subseção, vamos caracterizar o elemento de $\mathcal{O}_\mathbb{K}$ que pertence a um ideal primo $\mathcal{B}_i$'s acima de $p_i\mathbb{Z}$, onde os p_i's são primos que aparecem na fatoração do $cond(\mathbb{K})$ e $p_i \equiv 1\ (mod\ p)$.

Proposição 3.2.3. *Se $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_\mathbb{K}$, então $x \in \mathcal{B}_i$ se, e somente se, $\sum_{i=0}^{p-1} a_i \equiv 0\ (mod\ p)$.*

Demonstração: Como $t \in \mathcal{O}_\mathbb{K}$, segue que $t \equiv c\ (mod\ \mathcal{B}_i)$, com $c \in \mathbb{Z}$. Assim, $\theta_i(t) \equiv c\ (mod\ \mathcal{B}_i)$, e desse modo, $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \equiv c\sum_{i=0}^{p-1} a_i\ (mod\ \mathcal{B}_i)$. Dessa forma, $x \in \mathcal{B}_i$ se, e somente se, $c\sum_{i=0}^{p-1} a_i \equiv 0\ (mod\ \mathcal{B}_i)$ se, e somente se, $c \in \mathcal{B}_i$ ou $\sum_{i=0}^{p-1} a_i \in \mathcal{B}_i$, uma vez que $\mathcal{B}_i$ é um ideal

primo. Se $c \in \mathcal{B}_i$, então t e $\theta^i(t)$ pertencem a $\mathcal{B}_i$. Logo, $\sum_{i=0}^{p-1} \theta^i(t) \in \mathcal{B}_i$, isto é, $Tr_{\mathbb{K}|\mathbb{Q}}(t) \in \mathcal{B}_i$. Como $Tr_{\mathbb{K}|\mathbb{Q}}(t) = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = (-1)^s$, segue que $\pm 1 \in \mathcal{B}_i$, o que é uma contradição. Portanto, $x \in \mathcal{B}_i$ se, e somente se, $\sum_{i=0}^{p-1} a_i \in \mathcal{B}_i \cap \mathbb{Z} = p_i\mathbb{Z}$, o que demostra o resultado. ■

Proposição 3.2.4. *Os ideais primos $\mathcal{B}_i$'s de $\mathcal{O}_\mathbb{K}$ que estão acima de $p_i\mathbb{Z}$ são da forma $p_i\mathbb{Z}t + \sum_{j=0}^{p-1} p_i\mathbb{Z}(\theta^j(t) - t)$.*

Demonstração: Se $x = \sum_{i=0}^{p-1} \theta^i(t) \in \mathcal{O}_\mathbb{K}$, então $x = \sum_{i=0}^{p-1} \theta^i(t) + \sum_{i=0}^{p-1} a_it - \sum_{i=0}^{p-1} a_it = t\sum_{i=0}^{p-1} a_i + \sum_{i=0}^{p-1} a_i(\theta^i(t) - t)$. Logo, pela Proposição 3.2.3, segue que $x \in \mathcal{B}_i$ se, e somente se, $x = p_i\mathbb{Z}t + p_i\mathbb{Z}(\theta^i(t) - t)$. ■

3.3 Extensões abelianas de grau p, onde p é ramificado e $cond(\mathbb{K}) = p^2$

Nesta seção, vamos considerar p^2 o condutor de um corpo $\mathbb{K}$. O objetivo é explicitar o elemento primitivo de $\mathbb{K}$, uma base integral do anel de inteiros $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$, caracterizar os ideais de $\mathcal{O}_\mathbb{K}$ que estão acima do ideal primo $p\mathbb{Z}$ e calcular o valor $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, para $x \in \mathcal{O}_\mathbb{K}$ não nulo. Desse modo, sejam $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Se $G = Gal(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^*$, então G é um grupo cíclico. Assim, considere θ um gerador de G. Observe que se $\psi \in G$, então $\psi(\zeta_{p^2}) = \zeta_{p^2}^j$, com $mdc(p^2, j) = 1$ e $1 \leq j < p^2$. Se α é tal que $mdc(p^2, \alpha) = 1$, onde $1 \leq \alpha < p^2$ e $\theta(\zeta_{p^2}) = \zeta_{p^2}^\alpha$, com $\langle\theta\rangle = G$, então $\overline{\alpha}$ gera $(\mathbb{Z}/p^2\mathbb{Z})^*$. Como $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$, segue que

$$Gal(\mathbb{L}|\mathbb{Q}) = \{\theta, \theta^2, \ldots, \theta^{p(p-1)} = Id_\mathbb{L}\},$$
$$Gal(\mathbb{K}|\mathbb{Q}) = \{\theta|_\mathbb{K}, \theta^2|_\mathbb{K}, \ldots, \theta^p|_\mathbb{K} = Id_\mathbb{K}\},$$
$$Gal(\mathbb{L}|\mathbb{K}) = \{\theta^p, \theta^{2p}, \ldots, \theta^{p(p-1)} = Id_\mathbb{L}\}.$$

Observação 3.3.1. *Como $Gal(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q})$ é cíclico e $p|\varphi(p^2)$, segue que existe um único subcorpo $\mathbb{K}$ de $\mathbb{Q}(\zeta_{p^2})$ de grau p.*

Proposição 3.3.1. *Se $cond(\mathbb{K}) = p^2$, então $\mathbb{K} = \mathbb{Q}(t)$, com $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$.*

Demonstração: Um vez que $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2}) \in \mathbb{K}$, segue que $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq \mathbb{K}$. Como $[\mathbb{K} : \mathbb{Q}] = p$, com p primo, segue que $\mathbb{Q} = \mathbb{Q}(t)$ ou $\mathbb{K} = \mathbb{Q}(t)$. Pelo Teorema 3.1.3, segue que $\mathbb{K} = \mathbb{Q}[G](t - 1)$. Logo, se $\mathbb{Q} = \mathbb{Q}(t)$, então $t \in \mathbb{Q}$, e assim, $\mathbb{K} = \mathbb{Q}$, gerando uma contradição. Portanto, $\mathbb{K} = \mathbb{Q}(t)$, com $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$. ■

Proposição 3.3.2. *Se $cond(\mathbb{K}) = p^2$, então $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Pelo Teorema 3.1.3, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G]t \oplus \mathbb{Z}$. Logo, $\{1, \theta(t), \ldots, \theta^{p-1}(t), \theta^p(t)\}$ é um conjunto de geradores de $\mathcal{O}_{\mathbb{K}}$ visto como um $\mathbb{Z}$-módulo. Como o posto de $\mathcal{O}_{\mathbb{K}}$ é p, segue que $\{1, \theta(t), \ldots, \theta^{p-1}(t), \theta^p(t)\}$ não é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, uma vez que possui $p+1$ elementos. Porém, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p^2}) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = \sum_{j=1}^{p} \theta^j(t) = 0$, e assim, podemos considerar $\theta^p(t) = t$ uma combinação linear inteira de $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$. Desta maneira, o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é um conjunto gerador de $\mathcal{O}_{\mathbb{K}}$ como $\mathbb{Z}$-módulo e possui p elementos, e portanto, segue que $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. ■

3.3.1 Forma traço integral

Considerando $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$, $\mathbb{K}$ um corpo de números abeliano de grau p e $cond(\mathbb{K}) = p^2$, estamos interessados em calcular $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Sabemos que $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. Assim, consideramos $x = \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$, com $a_i \neq 0$, para algum $i = 0, 1, \cdots, p-1$. Como

$$x^2 = \left(a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t)\right)^2 = a_0^2 + \sum_{i=1}^{p-1} a_i^2(\theta^i(t))^2 + 2\sum_{1\leq i<j\leq p-1} a_ia_j\theta^i(t)\theta^j(t) + a_0\sum_{i=1}^{p-1} a_i\theta^i(t),$$

segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2Tr_{\mathbb{K}|\mathbb{Q}}(1) + \sum_{i=1}^{p-1} a_i^2Tr_{\mathbb{K}|\mathbb{Q}}((\theta^i(t))^2) + 2\sum_{1\leq i<j\leq p-1} a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) + a_0\sum_{i=1}^{p-1} a_iTr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t))$. Além disso, como

1. $Tr_{\mathbb{K}|\mathbb{Q}}((\theta^i(t))^2) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t^2)) = Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$, pois θ^i é um homomorfismo e $\theta^j(t)$ é conjugado de t em $\mathbb{K}|\mathbb{Q}$;

2. $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})) = 0$;

3. $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t\theta^{j-i}(t))) = Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$;

4. $Tr_{\mathbb{K}|\mathbb{Q}}(1) = p$,

segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2p + \sum_{i=1}^{p-1} a_i^2Tr_{\mathbb{K}|\mathbb{Q}}(t^2) + 2\sum_{1\leq i<j\leq p-1} a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$. Portanto, é suficiente conhecermos $Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$ para encontrarmos o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$.

Proposição 3.3.3. *[13, pág. 97] Se $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$ e $\langle\theta\rangle = Gal(\mathbb{L}|\mathbb{Q})$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = p(p-1)$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t)) = -p$, onde $1 \leq i < j \leq p-1$.* ■

E assim, pela Proposição 3.3.3, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 + (p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_i a_j\right).$$

Proposição 3.3.4. *[15, pág. 64] O mínimo da forma quadrática dada por* $Q_n(a_1,\ldots,a_n) = n\sum_{i=1}^{n} a_i^2 - 2\sum_{1\leq i<j\leq n} a_i a_j$, *com entradas inteiras, é* n *e esse mínimo é atingido em* $\pm(1,\ldots,1)$ *ou* $\pm e_i$, *onde* $\{e_i\}$ *é a base canônica de* $\mathbb{Z}^n$. ■

Proposição 3.3.5. *O* $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ 0 \neq x \in \mathcal{O}_{\mathbb{K}}\} = p$ *e é atingido com* $(a_0,\ldots,a_{p-1}) = (1,0,0,\ldots,0)$.

Demonstração: Segue diretamente da Proposição 3.3.4 ■

3.3.2 Caracterização do ideal primos acima de $p\mathbb{Z}$

Sejam $\mathcal{B}_{\mathbb{K}}$ o ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$ e $\mathcal{B}_{\mathbb{L}}$ o ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$, com $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$. O nosso objetivo é caracterizar o ideal $\mathcal{B}_{\mathbb{K}} = \mathcal{B}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$.

Proposição 3.3.6. *Se* $\zeta_{p^2} = \zeta$, *então* $\mathcal{B}_{\mathbb{K}}$ *é gerado por* $N_{\mathbb{L}|\mathbb{K}}(1-\zeta)$.

Demonstração: Sabemos que $p\mathcal{O}_{\mathbb{L}} = \mathcal{B}_{\mathbb{L}}^{p(p-1)}$, isto é, p ramifica totalmente em $\mathcal{O}_{\mathbb{L}}$, onde $\mathcal{B}_{\mathbb{L}} = (1-\zeta)\mathbb{Z}[\zeta]$. Seja $\lambda = N_{\mathbb{L}|\mathbb{K}}(1-\zeta) = \prod_{j=1}^{p-1}(1-\zeta^{\alpha^{jp}})$. Como $\mathbb{K}$ é um corpo de números, segue que o ideal $\langle\lambda\rangle$ em $\mathcal{O}_{\mathbb{K}}$ se decompõe em produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$. Uma vez que $1-\zeta$ é o conjugado de $1-\zeta^{\alpha^{jp}}$, segue que $(1-\zeta)\mathcal{O}_{\mathbb{L}} = (1-\zeta^{\alpha^{jp}})\mathcal{O}_{\mathbb{L}}$, o que implica que $\prod_{j=1}^{p-1}(1-\zeta^{\alpha^{jp}})\mathcal{O}_{\mathbb{L}} = (1-\zeta)^{p-1}\mathcal{O}_{\mathbb{L}}$, e assim, $\lambda\mathcal{O}_{\mathbb{L}} = \mathcal{B}_{\mathbb{L}}^{p-1} = \mathcal{B}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Portanto, $\lambda\mathcal{O}_{\mathbb{L}} = \mathcal{B}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$, ou seja, $\mathcal{B}_{\mathbb{K}} = \langle\lambda\rangle = \langle N_{\mathbb{L}|\mathbb{K}}(1-\zeta)\rangle = \mathcal{B}_{\mathbb{K}}^{p-1}$. ■

3.4 Extensões abelianas de grau p, onde p é ramificado e $cond(\mathbb{K}) = p^2p_1p_2...p_s$

Nesta seção, primeiramente vamos considerar $n = p^2\prod_{i=1}^{s} p_i$, com os p_i's primos distintos e $p_i \equiv 1\ (mod\ p)$, o condutor de $\mathbb{K}$. O objetivo é explicitar o elemento primitivo de $\mathbb{K}$ e uma base integral do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Desse modo, nesta seção, consideramos $n = p^2\prod_{i=1}^{s} p_i$, $\mathbb{L} = \mathbb{Q}(\zeta_n)$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p e p_i's primos distintos e $p_i \equiv 1\ (mod\ p)$. Em seguida, vamos considerar $s = 1$, ou seja, $cond(K) = p^2q$, com q primo e $q \equiv 1\ (mod\ p)$, e caracterizar o ideal primo $\mathcal{Q}$ de $\mathcal{O}_{\mathbb{K}}$ que está acima do ideal primo $q\mathbb{Z}$, calcular o valor $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, para $x \in \mathcal{O}_{\mathbb{K}}$ não nulo e, por fim, calcular $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ 0 \neq x \in \mathcal{Q}\}$.

Proposição 3.4.1. *Existem* $(p-1)^s$ *subcorpos de grau* p *em* $\mathbb{Q}(\zeta_n)$ *de condutor* n.

Demonstração: Consideramos primeiramente $n = p^2p_1$. Como $\mathbb{Q}(\zeta_{p^2})$ e $\mathbb{Q}(\zeta_{p_1})$ são extensões cíclicas de $\mathbb{Q}$, $p|\varphi(p^2)$ e $p|\varphi(p_1)$, segue que existem apenas dois corpos de grau p contidos em $\mathbb{Q}(\zeta_n)$ os quais não tem condutor n. Desta forma, existem $\frac{p^2-1}{p-1} - 2 = p-1$ subcorpos de $\mathbb{Q}(\zeta_n)$ que possuem condutor n. Agora, consideramos n $= p^2p_1p_2$. Logo, existem 3 subcorpos de $\mathbb{Q}(\zeta_n)$ os quais tem condutor p^2, p_1 e p_2. Também, existem $\frac{3!}{2!(3-2)!}(p-1) = 3(p-1)$ subcorpos de condutor p^2p_i ou p_ip_j, com $i, j = 1, 2$. Portanto, existem $\frac{p^3-1}{p-1} - 3 - 3(p-1) = (p-1^2)$ subcorpos de condutor n. Repetindo este processo, segue que existem $\frac{p^{s+1}-1}{p-1} - (s+1) - \frac{(s+1)!}{2!(s+1-2)!}(p-1) - \frac{(s+1)!}{3!(s+1-3)!}(p-1)^2 - \cdots - \frac{(s+1)!}{s!(s+1-s)!}(p-1)^{s-1} = (p-1)^s$ subcorpos de condutor n. ■

Proposição 3.4.2. *Se* $cond(\mathbb{K}) = n$, *então* $\mathbb{K} = \mathbb{Q}(t)$, *onde* $t = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n)$.

Demonstração: Pelo Teorema 3.1.2, segue que $D = \{d_1 = p\prod_{i=1}^{s} p_i, d_2 = n\}$. Assim, $\mathbb{K}_{d_1} = \mathbb{Q}$ e $\mathbb{K}_{d_2} = \mathbb{K}$. Logo, $T = Tr_{\mathbb{Q}(\zeta_{d_1})|\mathbb{Q}}(\zeta_{d_1}) + Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n) = (-1)^{s+1} + t$. Como $t \in \mathbb{K}$, segue que $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq \mathbb{K}$. Logo, $\mathbb{Q} = \mathbb{Q}(t)$ ou $\mathbb{K} = \mathbb{Q}(t)$, uma vez que $[\mathbb{K}\colon \mathbb{Q}] = p$. Assim, se $\mathbb{Q} = \mathbb{Q}(t)$, ou seja, $t \in \mathbb{Q}$, então $\mathbb{K} = \mathbb{Q}[G]T = \mathbb{Q}[G](\pm 1 + t)$, com $T \in \mathbb{Q}$ o gerador da base normal de $\mathbb{K}$. Agora, se $x \in \mathbb{K}$, então $x = \sum_{g\in G} a_g g(\pm 1 + t)$, ou seja, $\mathbb{K} \subseteq \mathbb{Q}$, o que é uma contradição. Portanto $t \notin \mathbb{Q}$ e $\mathbb{K} = \mathbb{Q}(t)$. ■

Proposição 3.4.3. *Se* $n = p^2\prod_{i=1}^{s} p_i$ *e* $\mathbb{L} = \mathbb{Q}(\zeta_n)$, *então* $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$.

Demonstração: Seja $n' = \prod_{i=1}^{s} p_i$. Como $\mathbb{Q}(\zeta_{p^2}) \cap \mathbb{Q}(\zeta_{n'}) = \mathbb{Q}$, segue que $Gal(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}) \simeq Gal(\mathbb{L}|\mathbb{Q}(\zeta_{n'}))$. Como $mdc(p^2, n') = 1$, segue que existem $a, b \in \mathbb{Z}$ tais que $ap^2 + bn' = 1$. Logo, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n^{ap^2+bn'}) = Tr_{\mathbb{Q}(\zeta_{n'})|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{Q}(\zeta_{n'})}(\zeta_{n'}^a\zeta_{p^2}^b) = Tr_{\mathbb{Q}(\zeta_{n'})|\mathbb{Q}}(\zeta_{n'}^a Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^b)) = 0$, uma vez que $Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^b)) = 0$, para $mdc(b, p^2) = 1$. Portanto, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$. ■

Proposição 3.4.4. *Se* $cond(\mathbb{K}) = n$, *então* $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ *é uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Pelo Teorema 3.1.3, segue que $\mathcal{O}_{\mathbb{K}} = \bigoplus_{d\in D} \mathbb{Z}[G]\eta_d$. Logo, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G](\pm 1) \bigoplus \mathbb{Z}[G](t)$, onde $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$. Como $\mathbb{Z}[G](\pm 1) = \sum_{g\in G} a_g g(\pm 1) = \pm \sum_{g\in G} a_g$, com $a_g \in \mathbb{Z}$, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} \bigoplus \mathbb{Z}[G](t)$. Desta maneira, o conjunto $\{1, \theta(t), \ldots, \theta^p(t)\}$ gera $\mathcal{O}_{\mathbb{K}}$ e possui $p + 1$ elementos. Agora, observe que $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$, uma vez que n não é livre de quadrados. Logo, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = \sum_{i=1}^{p} \sigma^i(t) = 0$, o que implica que $-\sum_{i=1}^{p-1} \theta^i(t) = \theta^p(t)$, ou seja, $\theta^p(t)$ é uma combinação linear inteira de $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$,

e assim, $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ gera $\mathbb{Z}[G](t)$. Assim, o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é um conjunto com p elementos que gera $\mathcal{O}_{\mathbb{K}}$. Já que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto p, segue que $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{K}}$. ■

3.4.1 Forma traço integral

Nesta subseção, consideramos $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2\prod_{i=1}^{s} p_i$, com p e p_i's primos distintos e $p_i \equiv 1 \ (mod\ p)$, para $i = 1, \ldots, s$. Pela Proposição 3.4.4, segue que o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, onde $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$ e $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$. O objetivo é calcular o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Para isso, seja $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ não nulo, com $a_i \in \mathbb{Z}$, para $i = 1, \ldots, p-1$. Assim,

$$\begin{aligned}
Tr_{\mathbb{K}|\mathbb{Q}}(x^2) &= Tr_{\mathbb{K}|\mathbb{Q}}\left(\left(a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t)\right)^2\right) \\
&= Tr_{\mathbb{K}|\mathbb{Q}}\left(a_0^2 + a_0\sum_{i=1}^{p-1} a_i\theta^i(t) + 2\sum_{1\le i<j\le p-1} a_ia_j\theta^i(t)\theta^j(t) + \sum_{i=1}^{p-1} a_i^2(\theta^i(t))^2\right) \\
&= a_0^2p + a_0\sum_{i=1}^{p-1} a_iTr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)) + 2\sum_{1\le i<j\le p-1} a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) \\
&+ \sum_{i=1}^{p-1} a_i^2Tr_{\mathbb{K}|\mathbb{Q}}((\theta^i(t))^2).
\end{aligned}$$

Note que $\theta^i(t)$, para $i = 1, 2, \ldots, p-1$ é um conjugado de t em $\mathbb{K}|\mathbb{Q}$, assim, $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)) = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$, uma vez que n não é livre de quadrados. Além disso, $Tr_{\mathbb{K}|\mathbb{Q}}((\theta^i(t))^2) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t^2)) = Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$, uma vez que θ^i é um automorfismo e $\theta^i(t^2)$ é um conjugado de t^2 em $\mathbb{K}|\mathbb{Q}$. Ainda, para $1 \le i < j \le p-1$, segue que $\theta^i(t)\theta^j(t) = \theta^i(t\theta^{i-j}(t))$, e assim, $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t\theta^{i-j}(t))) = Tr_{\mathbb{K}|\mathbb{Q}}((t\theta^{i-j}(t))$. Desta forma, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2p + 2\sum_{1\le i<j\le p-1} a_ia_jTr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t)) + \sum_{i=1}^{p-1} a_i^2Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$.

Nosso objetivo, agora, é calcular o $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$ para $s = 1$, ou seja, consideramos $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2q$, com $q \equiv 1 \ (mod\ p)$ e q primo.

Proposição 3.4.5. *Se $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = pq(p-1)$.*

Demonstração: Inicialmente, note que $t^2 \in \mathbb{K}$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = \frac{p}{\varphi(n)}Tr_{\mathbb{L}|\mathbb{Q}}(t^2)$. Considerando $G = Gal(\mathbb{L}|\mathbb{Q}) = \{\tau_r\colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)|\ \tau_r \text{ é um automorfismo, } \tau_r(\zeta_n) = \zeta_n^r,\ mdc(r,n) = 1\}$, segue que $\theta = \tau_r|_{\mathbb{K}}$, para algum $\tau_r \in G$. Se $H = Gal(\mathbb{L}|\mathbb{K})$, então $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n) = \sum_{\alpha\in H} \tau_\alpha(\zeta_n) =$

$\sum_{\alpha\in H}\zeta_n^{\alpha}$. Assim, $t^2 = \sum_{\alpha,\beta\in H}\zeta_n^{\alpha+\beta}$. Agora, observe que H é um subgrupo de G e $G \simeq \mathbb{Z}_{p^2}^* \times \mathbb{Z}_q^*$. Desta forma, escrevemos $\alpha, \beta \in H$ como $\alpha = (\alpha_0, \alpha_1)$ e $\beta = (\beta_0, \beta_1)$, onde $\alpha_0, \beta_0 \in \mathbb{Z}_{p^2}^*$ e $\alpha_1, \beta_1 \in \mathbb{Z}_q^*$. Se $d = \frac{n}{p^2} + \frac{n}{q}$, então $\zeta_n^d = \zeta_{p^2}\zeta_q$, e ainda, $\zeta_n^{\alpha+\beta}$ é uma raiz primitiva da unidade se, e somente se, ζ_n^d é uma raiz primitiva da unidade. Logo,

$$Tr_{\mathbb{L}|\mathbb{Q}}(\sum_{\alpha,\beta\in H}\zeta_n^{\alpha+\beta}) = \sum_{\alpha,\beta\in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n^{\alpha+\beta}) = \sum_{\alpha,\beta\in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n^{d(\alpha+\beta)}) \tag{3.4}$$

$$= \sum_{\alpha,\beta\in H} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}\zeta_q^{\alpha_1+\beta_1}) \tag{3.5}$$

$$= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}) Tr_{\mathbb{Q}(\zeta_q)|\mathbb{Q}}(\zeta_q^{\alpha_1+\beta_1}), \tag{3.6}$$

onde $Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}) = \begin{cases} 0, \ se\ mdc(\alpha_0+\beta_0, p^2) = 1 \\ -p, \ se\ mdc(\alpha_0+\beta_0, p^2) = p \\ p(p-1), \ se\ mdc(\alpha_0+\beta_0, p^2) = p^2 \end{cases}$

e $Tr_{\mathbb{Q}(\zeta_q)|\mathbb{Q}}(\zeta_q^{\alpha_1+\beta_1}) = \begin{cases} -1, \ se\ mdc(\alpha_1+\beta_1, q) = 1 \\ q-1, \ se\ mdc(\alpha_1+\beta_1, q) = q. \end{cases}$

Agora, se $\alpha = (\alpha_0, \alpha_1) \in H$, então vamos analisar os seguintes casos:

1. $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 (mod\ q)$
2. $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$
3. $\beta_0 \equiv -\alpha_0 (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 (mod\ q)$
4. $\beta_0 \equiv -\alpha_0 (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$
5. $\beta_0 \not\equiv -\alpha_0 (mod\ p)$ e $\beta_1 \equiv -\alpha_1 (mod\ q)$
6. $\beta_0 \not\equiv -\alpha_0 (mod\ p)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$

Caso 1: Como $\mathbb{K}$ é um corpo de números totalmente real, segue que a conjugação complexa pertence ao grupo H. Desta forma, se $\alpha \in H$, então existe um único elemento $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação (3.6) correspondente a esses elementos é igual a

$$P_1 = o(H)p(p-1)(q-1).$$

Caso 2: Se $\alpha \in H$, segue que o número de elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0$ é dado pela ordem da imagem inversa da seguinte projeção:

$$\begin{aligned} \pi_2 : H &\longrightarrow \mathbb{Z}_{p^2}^* \\ \beta &\longmapsto \beta_0. \end{aligned}$$

π_2 é sobrejetora, pois caso contrário, teríamos que $H \subseteq \pi_2(H) \times \mathbb{Z}_q^* \subseteq G$ com $o(G/h) = p$, o que implica que $H = \pi_2(H) \times \mathbb{Z}_q^*$ ou $G = \pi_2(H) \times \mathbb{Z}_q^*$ e se tivéssemos $H = \pi_2(H) \times \mathbb{Z}_q^*$ o condutor de $\mathbb{K}$ não seria n. Logo, pelo Teorema do Núcleo e da Imagem, segue que $\frac{o(H)}{o(Ker(\pi_2))} = o(\mathbb{Z}_{p^2}^*)$, ou seja, $o(Ker(\pi_2)) = \frac{q-1}{p}$. Desconsiderando o elemento $\beta \in \pi_2^{-1}(\alpha_0)$ tal que $\beta_1 = -\alpha_1$, segue que existem $\frac{q-1}{p}$ elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação (3.6) que corresponde a esses elementos é igual a

$$P_2 = o(H)\left(\frac{q-1}{p} - 1\right)p(p-1)(-1) = -o(H)\left(\frac{\varphi(n)}{p} - p(p-1)\right).$$

Caso 3: Vamos considerar, neste caso, o isomorfismo existente entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Desta forma, se $\alpha \in H$, então existe um único $\beta \in H$ tal que $\beta \in \{\phi^{-1}(\overline{-\alpha_0}, -\alpha_1)\}$. Como já sabemos que $\beta = (-\alpha_0, -\alpha_1) \in H$ e $\phi^{-1}(-\alpha_0, -\alpha_1) = (\overline{-\alpha_0}, -\alpha_1)$, segue que não existem elementos $\beta \in H$ diferente do conjugado complexo de α em $\{\phi^{-1}(\overline{-\alpha_0}, -\alpha_1)\}$. Assim, a parcela da Equação (3.6) correspondente a esses elementos é nula.

Caso 4: De modo análogo ao caso 2, consideramos a projeção

$$\begin{aligned} \pi_4 : H &\longrightarrow \mathbb{Z}_p^* \\ \beta &\longmapsto \overline{\beta_0}, \end{aligned}$$

a qual é sobrejetora, uma vez que é compostas de sobrejetoras. Se $\alpha \in H$, então o número de elementos $\beta \in H$ tal que $\beta \in \{\pi_4^{-1}(\overline{-\alpha_0})\}$ é dado pela cardinalidade do $Ker(\pi_4)$, a qual é $q-1$. Porém, é necessário excluirmos os β tal que $\beta \in \{\pi_2^{-1}(-\alpha_0, \alpha_1)\}$. Dessa forma, segue que existem $\dfrac{(p-1)(q-1)}{p}$ elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação (3.6) que corresponde a esses elementos é igual a

$$P_4 = o(H)\frac{(p-1)(q-1)}{p}(-p)(-1) = o(H)(p-1)(q-1).$$

Casos 5 e 6: Neste caso, as parcelas da Equação 3.6 correspondentes são nulos, uma vez que $Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}) = 0$.

Finalmente, como $Tr_{\mathbb{L}|\mathbb{Q}}(t^2) = P_1 + P_2 + P_4 = o(H)(p(p-1)(q-1) - (p-1)(q-1) + p(p-1) + (p-1)(q-1)) = o(H)pq(p-1)$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = pq(p-1)$. ■

Proposição 3.4.6. *Se $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$ e $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t)) = -pq$.*

Demonstração: Consideramos $\theta = \tau_r$, com τ_r como na demonstração da Proposição 3.2.2. Como $r \in \mathbb{Z}_n^*$, segue que podemos considerar $r = (r_0, r_1) \in \mathbb{Z}_{p^2}^* \times \mathbb{Z}_q$. Vamos calcular $Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = \dfrac{p}{\varphi(n)} Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t))$. De modo análogo, segue que

$$Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0 + r_0^k\beta_0}) Tr_{\mathbb{Q}(\zeta_q)|\mathbb{Q}}(\zeta_q^{\alpha_1 + r_1^k\beta_1}). \tag{3.7}$$

Assim, se $\alpha \in H$, então vamos analisar os seguintes casos:

1. $\beta_0 \equiv -\alpha_0 r_0^{-k} (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 r_1^{-k} (mod\ q)$
2. $\beta_0 \equiv -\alpha_0 r_0^{-k} (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 r_1^{-k} (mod\ q)$
3. $\beta_0 \equiv -\alpha_0 r_0^{-k} (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 r_0^{-k} (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 r_1^{-k} (mod\ q)$
4. $\beta_0 \equiv -\alpha_0 r_0^{-k} (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 r_0^{-k} (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 r_1^{-k} (mod\ q)$
5. $\beta_0 \not\equiv -\alpha_0 r_0^{-k} (mod\ p)$ e $\beta_1 \equiv -\alpha_1 r_1^{-k} (mod\ q)$
6. $\beta_0 \not\equiv -\alpha_0 r_0^{-k} (mod\ p)$ e $\beta_1 \not\equiv -\alpha_1 r_1^{-k} (mod\ q)$

Caso 1: Se $\alpha \in H$, então queremos analisar o número de elementos $\beta \in H$ tal que $\beta = -\alpha r^{-k}$. Observamos que r é uma raiz primitiva módulo n, e assim, $\mathbb{Z}_n^* \simeq H \cup rH \cup r^2H \cup \cdots \cup r^{p-1}H$, as quais são classes laterais disjuntas. Note que $\beta = -\alpha r^{-k} \in r^{-k}H$, pois $-\alpha \in H$. Portanto, não existe $\beta \in H$ tal que $\beta = -\alpha r^{-k}$.

Caso 2: Consideramos a projeção π_2 dada na demonstração da Proposição 3.4.5. Se $\beta_0 \equiv -\alpha_0 r_0^{-k}$, então existem $\frac{q-1}{p}$ elementos $\beta \in H$ tal que $\pi_2(\beta) = -\alpha_0 r_0^{-k}$. Assim, a parcela da Equação 3.7 correspondente a esses elementos é igual a

$$P_2 = o(H)\left(\frac{q-1}{p}\right)p(p-1)(-1) = -o(H)(p-1)(q-1).$$

Caso 3: Utilizando o isomorfismo ϕ entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$, segue que se $(\overline{\alpha_0 r_0^{-k}}, -\alpha_1 r_1^{-k}) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, então existe um único $\beta \in H$ tal que $\phi(\beta) = (\overline{\alpha_0 r_0^{-k}}, -\alpha_1 r_1^{-k})$, o qual é diferente de $-\alpha r^{-k}$.

Assim, a parcela da Equação (3.7) correspondente a esses elementos é igual a

$$P_3 = o(H)(-p)(q-1).$$

Caso 4: Consideramos a projeção sobrejetora

$$\begin{aligned} \pi_4 : H &\longrightarrow \mathbb{Z}_p^* \\ \beta &\longmapsto \overline{\beta_0}, \end{aligned}$$

Logo, existem $q-1$ elementos $\beta \in H$ tal que $\pi_4(\beta) = \overline{-\alpha_0 r_0^{-k}}$. Porém, devemos excluir o elementos β tal que $\pi_4(\beta) = -\alpha_0 r_0^{-k}$. Assim, existem $\frac{(p-1)(q-1)}{p}$ elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 r_0^{-k}(mod\ p)$, $\beta_0 \not\equiv -\alpha_0 r_0^{-k}(mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 r_1^{-k}(mod\ q)$. É necessário também excluir os elementos contados no item 3. Assim, a parcela da Equação (3.7) correspondente a esses elementos é igual a

$$P_4 = o(H)\left(\frac{(p-1)(q-1)}{p} - 1\right)(-1)(-p) = o(H)((p-1)(q-1)-p).$$

Caso 5 e 6: Nestes casos as parcelas da Equação 3.7 correspondentes a esses casos são nulas. Finalmente, como $Tr_{\mathbb{L}|\mathbb{Q}}(t\theta^k(t)) = P_2 + P_3 + P_4 = o(H)(-(p-1)(q-1) - p(q-1) + (p-1)(q-1) - p) = o(H)(-pq)$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t)) = -pq$. ■

Proposição 3.4.7. *Se $x \in \mathcal{O}_{\mathbb{K}}$ é não nulo, então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q \sum_{1\le i<j\le p-1} a_i a_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right).$$

Demonstração: Como $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2 p - 2 \sum_{1\le i<j\le p-1} a_i a_j Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t)) + \sum_{i=1}^{p-1} a_i^2 Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$, pelas Proposições 3.4.5 e 3.4.6, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q \sum_{1\le i<j\le p-1} a_i a_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right),$$

o que prova o resultado. ■

3.4.2 Mínimo da forma traço integral

Nesta subseção, consideramos $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2\prod_{i=1}^{s} p_i$ com p e p_i's primos distintos e $p_i \equiv 1\ (mod\ p)$, para $i = 1, \ldots, s$. Vamos analisar uma família de $\mathbb{Z}$-submódulos B_m de $\mathcal{O}_{\mathbb{K}}$, onde é possível encontrar $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ x \in B_m, x \neq 0\}$. Com este mínimo será possível a construção de alguns reticulados algébricos. Pela Proposição 3.4.7, se $x \in \mathcal{O}_{\mathbb{K}}$ é não nulo, então

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q\sum_{1\leq i<j\leq p-1} a_ia_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right),$$

e portanto,

$$Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = pa_0^2 + pq\left((p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_ia_j\right).$$

Considerando $\underline{a} = (a_1, \ldots, a_{p-1})$ e $Q(\underline{a}) = (p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_ia_j$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = pa_0^2 + pqQ(\underline{a})$.

Definição 3.4.1. *Sejam $Gal(\mathbb{K}|\mathbb{Q}) = \langle\theta\rangle$ e $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$. Definimos o seguinte $\mathbb{Z}$-submódulo de $\mathcal{O}_{\mathbb{K}}$*

$$B_m = \{a_0 + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{O}_{\mathbb{K}}|\ a_0 + a_1 + \cdots + a_{p-1} \equiv 0(mod\ m)\},$$

onde m é um inteiro positivo.

Se $m = 1$, então $B_1 = \mathcal{O}_{\mathbb{K}}$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) \geq pN_{\mathbb{K}|\mathbb{Q}}(x^2)^{\frac{1}{p}} \geq p$, para todo $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Logo, $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ x \in \mathcal{O}_{\mathbb{K}},\ x \neq 0\} = p$ é atingido com $(1, 0, \ldots, 0) \in \mathcal{O}_{\mathbb{K}}$.

3.4.3 Caracterização dos ideais primos acima dos ideais $p_i\mathcal{O}_{\mathbb{K}}$

Seja $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2\prod_{i=1}^{s} p_i$ com p e p_i's primos distintos e $p_i \equiv 1\ (mod\ p)$, para $i = 1, \ldots, s$. Desta forma, os ideais $p\mathcal{O}_{\mathbb{K}}, p_1\mathcal{O}_{\mathbb{K}}, \ldots, p_s\mathcal{O}_{\mathbb{K}}$ ramificam em $\mathcal{O}_{\mathbb{K}}$, uma vez que todos dividem o discriminante do corpo $\mathbb{K}$. Como $\mathbb{K}|\mathbb{Q}$ é uma extensão de galoisiana de grau p, com p um primo ímpar, segue que os ideias $p\mathcal{O}_{\mathbb{K}}, p_1\mathcal{O}_{\mathbb{K}}, \ldots, p_s\mathcal{O}_{\mathbb{K}}$ ramificam totalmente em $\mathcal{O}_{\mathbb{K}}$. Logo, $p\mathcal{O}_{\mathbb{K}} = \mathcal{B}^p, p_1\mathcal{O}_{\mathbb{K}} = \mathcal{B}_1^p, \ldots, p_s\mathcal{O}_{\mathbb{K}} = \mathcal{B}_s^p$, onde $\mathcal{B} \cap \mathbb{Z} = p, \mathcal{B}_1 \cap \mathbb{Z} = p_1, \ldots, \mathcal{B}_s \cap \mathbb{Z} = p_s$.

Seja $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ não nulo. Como $t \in \mathcal{O}_{\mathbb{K}}$, segue que $t \equiv c\ (mod\ \mathcal{B}_i)$, uma vez que $\mathcal{O}_{\mathbb{K}}/\mathcal{B}_1 \simeq \mathbb{Z}/p_i\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p_i - 1}\}$. Assim, $\theta^i(t) \equiv \theta^i(c) \equiv c\ (mod\ \mathcal{B}_i)$, para

$i = 1, \ldots, p-1$. Desse maneira, para qualquer $x \in \mathcal{O}_{\mathbb{K}}$, segue que $x = a_0 + c\sum_{i=1}^{p-1} a_i \ (mod\ \mathcal{B}_i)$. Observe que $t + \theta(t) + \cdots + \theta^{p-i}(t) = 0$, um vez que $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$. Logo, $pc \equiv 0 \ (mod\ \mathcal{B}_i)$, o que implica que, $pc \equiv 0 \ (mod\ p_i)$, e assim, $c \equiv 0 \ (mod\ p_i)$. Portanto, $x \equiv a_0 \ (mod\ \mathcal{B}_i)$, ou seja, $x \in \mathcal{B}_i$ se, e somente se, $a_0 \equiv 0 \ (mod\ p_i)$.

Proposição 3.4.8. *Sejam $\mathbb{K}$ um corpo de números de grau p e condutor $n = p^2q$ com $q \equiv 1 \ (mod\ p)$, p e q primos ímpares, $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ e $\mathcal{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $q\mathbb{Z}$. Se $x \in \mathcal{Q}$, então $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ x \in \mathcal{Q},\ x \neq 0\} = pq(p-1)$.*

Demonstração: Se $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{Q}$, ou seja, $a_0 \equiv 0 \ (mod\ q)$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q\sum_{1\leq i<j\leq p-1} a_ia_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right)$. Suponhamos, primeiramente, que $a_0 = 0$. Como $x \in \mathcal{Q}$ é não nulo, segue que $a_i \neq 0$, para algum $i = 1, \ldots, p-1$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(-2q\sum_{1\leq i<j\leq p-1} a_ia_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right) = pq\left(-2\sum_{1\leq i<j\leq p-1} a_ia_j + (p-1)\sum_{i=1}^{p-1} a_i^2\right)$. Logo, pela Proposição 3.3.4, segue que $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ x \in \mathcal{Q},\ x \neq 0\} = pq(p-1)$. Agora, suponhamos que $a_0 = qk$, com $k \in \mathbb{Z}^*$ e $a_i = 0$ para todo $i = 1, \ldots, p-1$. Logo, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = pq^2k^2 \geq pq^2 > pq(p-1)$. E se, $a_i \neq 0$ para algum $i = 1, \ldots, p-1$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q\sum_{1\leq i<j\leq p-1} a_ia_j + q(p-1)\sum_{i=1}^{p-1} a_i^2\right) \geq pq^2k^2 + pq(p-1) > pq(p-1)$. Assim, se $a_0 = qk$, com $k \in \mathbb{Z}^*$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) > pq(p-1)$. Desta forma, $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)|\ x \in \mathcal{Q},\ x \neq 0\} = pq(p-1)$ e este mínimo é atingido com $a_0 = 0$ e $a_i = \pm e_i$, para $i = 1, \ldots, p-1$. ■

3.5 Considerações finais do capítulo

Neste capítulo, apresentamos resultados sobre extensões abelianas de grau p, com p um número primo ímpar. Exibimos o elemento primitivo, uma base para o anel de inteiros, o valor do $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $0 \neq x \in \mathcal{O}_{\mathbb{K}}$, e caracterizamos os ideais primos acima do ideal $p_i\mathcal{O}_{\mathbb{K}}$. Estes resultados são utilizados para a construção de exemplos de reticulados com densidade de centro ótimas para as dimensões 3, 5 e 7, feita no Capítulo 5.

Capítulo

4

Reticulados

Reticulados são subgrupos discretos de pontos do $\mathbb{R}^n$ que aparecem em diversas aplicações, com destaque na teoria de códigos corretores de erros e na criptografia. O estudo dos reticulados surgiu a partir do problema geométrico de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem o maior espaço possível.

Neste capítulo, apresentamos conceito e resultados sobre a teoria dos reticulados via corpos de números. Na Seção 4.1, apresentamos a definição e principais parâmetros sobre reticulados no $\mathbb{R}^n$, tais como, matriz geradora, matriz de Gram, determinante de um reticulado, volume de um reticulado, raio de empacotamento e densidade de centro. Em seguida, na Seção 4.2, apresentamos exemplos de reticulados com maiores densidades de centro conhecidas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12, 16 e 24. Por fim, na Seção 4.3, apresentamos os reticulados algébricos e seus principais resultados, descrevendo algumas maneiras de se obter reticulados no $\mathbb{R}^n$ via teoria algébrica dos números, fornecendo propriedades e fórmulas para alguns parâmetros desses reticulados.

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

Nesta seção, apresentamos o conceito de reticulado no $\mathbb{R}^n$, algumas propriedades e parâmetros importantes que serão muito utilizados nas seções seguintes.

Definição 4.1.1. *Sejam $\beta = \{v_1, \ldots, v_m\}$ um conjunto de vetores do $\mathbb{R}^n$ linearmente*

independentes sobre $\mathbb{R}$ *com* $m \leq n$. *Um* ***reticulado*** *com base* β *e dimensão* m *é o subconjunto do* $\mathbb{R}^n$ *da forma*

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

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

Observação 4.1.1. *Em outras palavras, o reticulado* Λ *pode ser expresso como*

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

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 4.1.1. *Se* $\beta = \{(1,0),(0,1)\}$ *é uma base canônica de* $\mathbb{Z}^2$, *então* $\Lambda = \mathbb{Z}^2$ *é um reticulado gerado por* β, *conforme a Figura 4.1.*

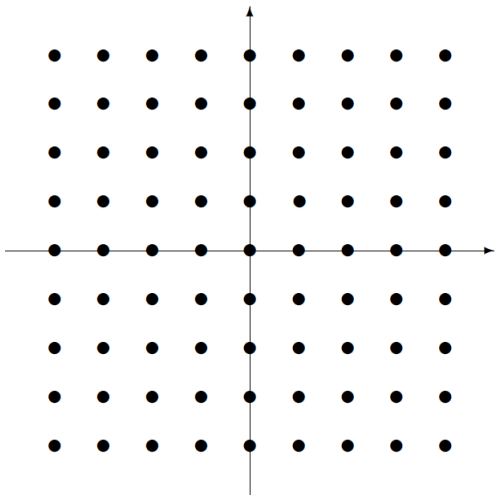

Figura 4.1: Reticulado $\mathbb{Z}^2$.

A base de um reticulado não é única, no Exemplo 4.1.1, $\beta' = \{(2,1),(-1,3)\}$ também é uma base do reticulado $\mathbb{Z}^2$.

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

Proposição 4.1.1. *Sejam $\{v_1, \ldots, v_n\} \subset \mathbb{R}^n$ uma base de um reticulado Λ e $\{u_1, \ldots, u_n\}$ um conjunto de vetores de Λ linearmente independentes sobre $\mathbb{R}$ tal que $u_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Assim, $\{u_1, \ldots, u_n\}$ é uma base de Λ se, e somente se, $det(a_{ij}) = \pm 1$.*

Demonstração: Sejam $\{v_1, \ldots, v_n\} \subset \mathbb{R}^n$ uma base de um reticulado Λ e $\{u_1, \ldots, u_n\}$ um conjunto de vetores de Λ linearmente independentes sobre $\mathbb{R}$ tal que

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Assim, $\{u_1, \ldots, u_n\}$ é uma base de Λ quando (a_{ij}) é a matriz de mudança de base, isto é, $det(a_{ij}) = \pm 1$. ■

Definição 4.1.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, com base $\beta = \{v_1, \ldots, v_n\}$. O conjunto*

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

*é chamado de **região fundamental** de Λ com relação a base $\{v_1, \ldots, v_n\}$.*

Exemplo 4.1.2. *O reticulado Λ gerado por $e_1 = (1, 0)$ e $e_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ tem região fundamental dada pela Figura 4.2.*

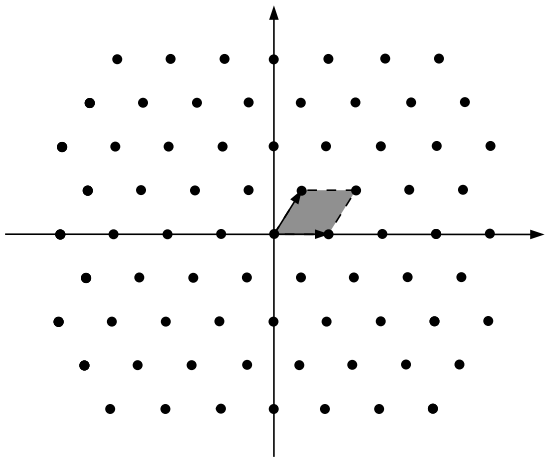

Figura 4.2: Região fundamental do reticulado Λ.

Definição 4.1.3. *Um subgrupo H do $\mathbb{R}^n$ é **discreto** se, para qualquer subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, tivermos $H \cap \mathbb{K}$ finito.*

Teorema 4.1.1. *[1, pág. 110] Se H é um subgrupo discreto do $\mathbb{R}^n$, então H é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.* ■

Logo, do Teorema 4.1.1, segue que um reticulado Λ é um conjunto discreto do $\mathbb{R}^n$.

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

Nesta subseção apresentamos os conceitos de matriz geradora, matriz de Gram e determinante de um reticulado.

Definição 4.1.4. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, com base $\beta = \{v_1, \ldots, v_n\}$. A **matriz geradora** do reticulado Λ é definida como sendo a matriz*

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

onde $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, para $i = 1, \ldots, n$.

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

$$\Lambda = \{\lambda M \mid \lambda \in \mathbb{Z}\}.$$

Definição 4.1.5. *Sejam Λ um reticulado e M sua matriz geradora. A **matriz de Gram** associada a matriz geradora é definida por $G = M^t M$.*

A proposição seguir nos diz que o determinante da matriz de Gram G de um reticulado não depende da base escolhida.

Proposição 4.1.2. *Sejam $\{v_1, \ldots, v_n\}, \{u_1, \ldots, u_n\} \subset \mathbb{R}^n$ duas bases de um reticulado Λ. Se $G = MM^t$ e $G' = M'M'^t$, onde $M = (v_{ij})$ e $M' = (u_{ij})$, então $det(G) = det(G')$.*

Demonstração: Como $|det(M)| = |det(M')|$, segue que $det(G) = det(M)det(M^t) = det(M)^2 = det(M')^2 = det(M')det(M'^t) = det(G')$. ■

Definição 4.1.6. *O **determinante** de $\Lambda \subset \mathbb{R}^n$ é definido como o determinante de uma matriz de Gram de Λ, isto é, $det(\Lambda) = det(G)$. Assim, $det(\Lambda) = det(M)^2$*

Definição 4.1.7. *Sejam Λ um reticulado, M sua matriz geradora e B uma matriz inteira $n \times n$. Um **sub-reticulado** de Λ é um reticulado dado por*

$$\Lambda' = \{\lambda BM |\ \lambda \in \mathbb{Z}^n\}.$$

4.1.2 Volume de um reticulado

Definição 4.1.8. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \ldots, v_n\}$ uma base de Λ e $\mathcal{P}_\beta$ a região fundamental. O **volume da região fundamental** $\mathcal{P}_\beta$ é definido como $\mathcal{V}ol(\mathcal{P}_\beta) = |det(M)|$, onde M é uma matriz geradora de Λ.*

Se $\{v_1, \ldots, v_n\}, \{u_1, \ldots, u_n\} \subset \mathbb{R}^n$ são duas bases de um reticulado Λ, pela Proposição 4.1.1, segue que $|det(v_{ij})| = |det(u_{ij})|$, ou seja, o módulo do determinante da matriz geradora não depende da base escolhida. Assim, é possível definir o volume de um reticulado.

Definição 4.1.9. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com $\mathbb{Z}$-base $\beta = \{v_1, \ldots, v_n\}$. O **volume do reticulado** Λ é definido como $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P}_\beta)$.*

Observação 4.1.2. *Se $\Lambda \subset \mathbb{R}^n$ é um reticulado, então $det(\Lambda) = det(G) = det(M^tM) = det(M^t)det(M) = \mathcal{V}ol(\Lambda)^2$.*

4.1.3 Raio de empacotamento e densidade de centro

O problema de empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço n-dimensional de forma que a parte do espaço coberto por essas esferas seja a maior possível. Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo de fácil manuseio. Desse modo, o estudo de empacotamentos reticulados equivale ao estudo dos reticulados.

Definição 4.1.10. *Um **empacotamento esférico**, ou simplesmente um **empacotamento** no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto e que este arranjo de esferas ocupe o "maior espaço possível".*

Definição 4.1.11. *Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros das esferas formam um reticulado no $\mathbb{R}^n$.*

Observação 4.1.3. *Podemos descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Definição 4.1.12. *Seja um empacotamento no $\mathbb{R}^n$, associado a um reticulado Λ, com $\beta = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base. A* ***densidade de empacotamento*** *de Λ, $\Delta(\Lambda)$, é definida como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.*

Como queremos que este arranjo de esferas ocupe o "maior espaço possível" no $\mathbb{R}^n$, o interessante é estudar empacotamentos associados a um reticulado Λ em que as esferas tenham raio máximo. Como Λ é um conjunto discreto do $\mathbb{R}^n$, se $k > 0$, então a interseção do conjunto compacto $\{x \in \mathbb{R}^n \mid |x| \leq k\}$ com o reticulado Λ é um conjunto finito. Assim, faz sentido definirmos o número $\Lambda_{min} = \min\{|\lambda| \mid \lambda \in \Lambda,\ \lambda \neq 0\}$, onde $|\cdot|$ é a norma euclidiana no $\mathbb{R}^n$.

Definição 4.1.13. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\Lambda_{min} = \min\{|\lambda| \mid \lambda \in \Lambda,\ \lambda \neq 0\}$. O número $(\Lambda_{min})^2$ é chamado de* ***norma mínima*** *de Λ.*

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

Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado com raio de empacotamento ρ e $B(\rho)$ a esfera com centro na origem e raio ρ. Com base na Definição 4.1.12 a densidade de empacotamento de Λ é dada por

$$\Delta(\Lambda) = \frac{\text{Volume da esfera}}{\text{Volume da região fundamental}} = \frac{\mathcal{V}ol(B(\rho))}{\mathcal{V}ol(\Lambda)} = \frac{\mathcal{V}ol(B(1))\rho^n}{\mathcal{V}ol(\Lambda)},$$

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

Definição 4.1.14. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. A* ***densidade de centro*** *de Λ é definida por*

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

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

Como o valor de $\mathcal{V}ol(B(1))$ é conhecido, segue que nosso foco de analise será a densidade de centro de um reticulado.

4.2 Reticulados importantes e melhores densidades de centro

Nesta seção, apresentamos os reticulados conhecidos na literatura que possuem densidade de cento ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12, 16 e 24.

4.2.1 Reticulado n-dimensional A_n

O reticulado n-dimensional A_n, para $n \geq 1$, é definido como:

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

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

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

Assim, o $det(A_n) = n + 1$, o raio de empacotamento é $\rho = \sqrt{2}/2$ e a densidade de centro é $\delta = \dfrac{2^{(\frac{-n}{2})}}{\sqrt{n+1}}$.

Exemplo 4.2.1 (Reticulado 2-dimensional A_2)**.** *O reticulado A_2 é formado por todos os pontos (x_0, x_1, x_2) de $\mathbb{Z}^3$ que pertencem ao plano $x_0 + x_1 + x_2 = 0$, contido em $\mathbb{R}^3$. A Figura 4.3 mostra a disposição dos pontos do reticulado no espaço tridimensional, assim como o empacotamento associado. Assim, uma matriz geradora para o reticulado A_2 é dada por*

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$ e a densidade de centro é dada por

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

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

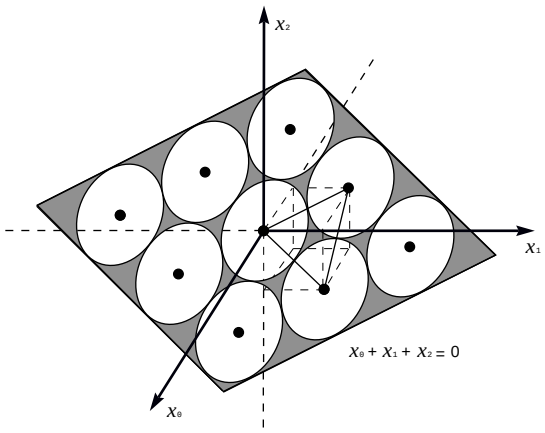

Figura 4.3: Empacotamento associado a A_2.

4.2.2 Reticulado n-dimensional D_n

O reticulado n-dimensional D_n, para $n \geq 3$, é definido como:

$$D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : \sum x_i \equiv 0 \ (mod\ 2)\}.$$

Uma matriz geradora M do reticulado D_n é dada por

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

Assim, o raio de empacotamento é $\rho = \sqrt{2}/2$ e a densidade de centro é $\delta = 2^{-(\frac{n+2}{2})}$.

Exemplo 4.2.2 (Reticulado 3-dimensional D_3)**.** *O reticulado D_3 é formado por todos os pontos $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_1 + x_2 + x_3$ é um número par. A Figura 4.4 mostra o arranjo das esferas do empacotamento associado a D_3.*

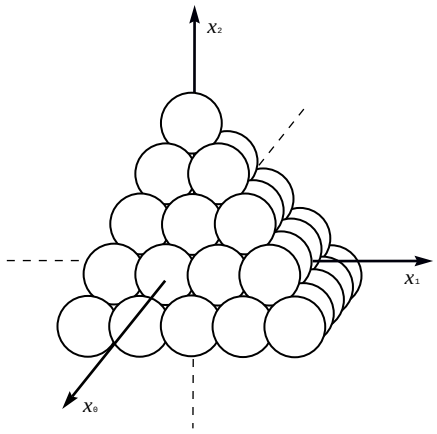

Figura 4.4: Esferas do empacotamento associado a D_3.

Uma matriz geradora do reticulado D_3 é dada por

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$ e a densidade de centro é dada por

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

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

Exemplo 4.2.3 (Reticulado 4-dimensional D_4)**.** *O reticulado D_4 é formado por todos os pontos $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ tal que $x_1+x_2+x_3+x_4$ é um número par. Uma matriz geradora do reticulado D_4 é dada por*

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$, a densidade de centro é

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

e cada esfera do empacotamento é tangenciada por exatamente 24 esferas. O reticulado D_4 possui densidade de centro ótima para a dimensão 4.

Exemplo 4.2.4 (Reticulado 5-dimensional D_5)**.** *O reticulado D_5 é formado por todos os pontos $(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$ tal que $x_1 + x_2 + x_3 + x_4 + x_5$ é um número par. Uma matriz geradora do reticulado D_5 é dada por*

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$ e a densidade de centro é dada por

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

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

4.2.3 Reticulado 8-dimensional E_8

O reticulado 8-dimensional E_8 é definido como

$$E_8 = \{(x_1, x_2, \ldots, x_8) \in \mathbb{R}^8 : \forall x_i,\ x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + 1/2,\ \sum x_i \equiv 0 (mod\ 2)\}.$$

Uma matriz geradora do reticulado E_8 é dada por

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$, a densidade de centro é dada por

$$\delta(E_8) = \frac{1}{16} = 0,0625,$$

e cada esfera do empacotamento é tangenciada por exatamente 240 esferas. O reticulado E_8 possui densidade de centro ótima para a dimensão 8.

Podemos definir reticulados de dimensão 6 e 7 a partir do reticulado E_8, que são dados nos exemplos a seguir.

Exemplo 4.2.5 (Reticulado 6-dimensional E_6)**.** *O reticulado E_6 é definido por*

$$E_6 = \{x \in E_8 : xv = 0,\ \forall v \in V\},\ \textit{onde } V \textit{ é um } A_2 \textit{ subreticulado em } E_8.$$

Uma matriz geradora do reticulado E_6 é dada por

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$, a densidade de centro é dada por

$$\delta(E_6) = \frac{1}{8\sqrt{3}} = 0,07217,$$

e cada esfera do empacotamento é tangenciada por exatamente 72 esferas. O reticulado E_6 possui densidade de centro ótima para a dimensão 6.

Exemplo 4.2.6 (Reticulado 7-dimensional E_7)**.** *O reticulado E_7 é definido por*

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

Uma matriz geradora do reticulado E_7 é dada por

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

o raio de empacotamento é $\rho = \frac{\sqrt{2}}{2}$ e a densidade de centro é dada por

$$\delta(E_7) = \frac{1}{16} = 0,0625.$$

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

4.2.4 Reticulado 12-dimensional K_{12}

O reticulado 12-dimensional K_{12} foi descrito por Coxeter e Todd em 1954. Uma matriz geradora para este reticulado é dada por

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

o raio de empacotamento é $\rho = 1$ e a densidade de centro é dada por

$$\delta(K_{12}) = \frac{1}{27} \simeq 0,03704.$$

O reticulado K_{12} é o mais denso conhecido para dimensão 12.

4.2.5 Reticulado laminado Λ_n

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

Exemplo 4.2.7 (Reticulado 16-dimensional Λ_{16})**.** *O reticulado* 16*-dimensional* Λ_{16} *foi descrito por Barnes e Wall em 1959. Uma matriz geradora para este reticulado é dada por*

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

o raio de empacotamento é $\rho = 1$ *e a densidade de centro é dada por*

$$\delta(\Lambda_{16}) = \frac{1}{16} = 0,0625.$$

O reticulado Λ_{16} *é o mais denso conhecido para dimensão 16.*

Exemplo 4.2.8 (Reticulado 24-dimensional Λ_{24})**.** *O reticulado* 24*-dimensional* Λ_{24} *foi descrito por Leech em 1965. Uma matriz geradora para este reticulado é dada por*

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

o raio de empacotamento é $\rho = 1$ *e a densidade de centro é dada por*

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

O reticulado Λ_{24} *é o mais denso conhecido para dimensão 24.*

Até a dimensão 8 podemos estabelecer relações entre os reticulados vistos nos exemplos desta seção e os reticulados laminados. A tabela abaixo representa as maiores densidades de centros conhecidas para as dimensões 1, 2, 3, 4, 5, 6, 7, 8, 12, 16 e 24.

dim	densidade de centro	reticulado
1	$1/2 = 0.50000$	$\Lambda_1 \cong A_1 \cong \mathbb{Z}$
2	$1/2\sqrt{3} \simeq 0.28868$	$\Lambda_2 \cong A_2$
3	$1/4\sqrt{2} \simeq 0.17678$	$\Lambda_3 \cong A_3 \cong D_3$
4	$1/8 = 0.12500$	$\Lambda_4 \cong D_4$
5	$1/8\sqrt{2} \simeq 0.08839$	$\Lambda_5 \cong D_5$
6	$1/8\sqrt{3} \simeq 0.07217$	$\Lambda_6 \cong E_6$
7	$1/16 = 0.06250$	$\Lambda_7 \cong E_7$
8	$1/16 = 0.06250$	$\Lambda_8 \cong E_8$
12	$1/27 \simeq 0.03704$	K_{12}
16	$1/16 = 0.06250$	Λ_{16}
24	1	Λ_{24}

Tabela 4.1: Densidades de centro de reticulados conhecidos.

4.3 Reticulados algébricos

Na Seção 4.1, vimos o conceito de reticulados no $\mathbb{R}^n$ e apresentamos parâmetros que nos ajudam a classificar os reticulados de acordo com a sua densidade de centro na Seção 4.2. Nesta seção, identificamos um $\mathbb{Z}$-módulo livre de posto finito contido num corpo de números $\mathbb{K}$ com um reticulado no $\mathbb{R}^n$, que chamamos de reticulado algébrico. Com essa identificação é possível apresentar algumas características do reticulado algébrico 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. Os resultados desta seção serão úteis no Capitulo 5, onde apresentamos exemplos de construções de reticulados algébricos utilizando o homomorfismo canônico.

4.3.1 Homomorfismo canônico

Seja $\mathbb{K}$ um corpo de números finito de grau n. Sabemos da Teoria de Galois que existem exatamente n $\mathbb{Q}$-monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$, com $i = 1, \ldots, n$. 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 $\mathbb{C}$. Assim, existem um número par de monomorfismos imaginários. Denotando por r_1 o número de monomorfismos reais e por $2r_2$ o número de monomorfismos imaginários, segue que $n = r_1 + 2r_2$, 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 $j = 1, \ldots, r_2$.

Definição 4.3.1. *O homomorfismo injetivo de anéis $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ dado 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 as partes real e imaginária de um número complexo, respectivamente.*

Teorema 4.3.1. *[31, pág. 56] 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 $\mathbb{R}^n$, com base $\{\sigma_{\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{K}}(x_n)\}$ cujo volume é dado por*

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

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 M 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 permutando as linhas da matriz M de forma conveniente, obtemos

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

Pela Proposição 1.3.3, segue que $det(\sigma_i(x_j)) \neq 0$. Logo, $det(M) \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j) \in \mathbb{R}^n$ são linearmente independentes sobre $\mathbb{R}$, ou seja,

$$\sigma_{\mathbb{K}}(M) = \mathbb{Z}\sigma_{\mathbb{K}}(x_1) + \cdots + \mathbb{Z}\sigma_{\mathbb{K}}(x_n)$$

é um reticulado no $\mathbb{R}^n$, do qual M é uma matriz geradora, e

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

o que prova o resultado. ■

Corolário 4.3.1. *[31, pág. 57] Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$, $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{I})$ são reticulados em $\mathbb{R}^n$ com volumes dados, respectivamente, por*

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

onde $N(\mathcal{I})$ é a norma de $\mathcal{I}$.

Demonstração: Pelo Teorema 4.3.1, segue que $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{I})$ são reticulados no $\mathbb{R}^n$ e, dada uma $\mathbb{Z}$-base $\{x_1, \ldots, x_n\}$ de $\mathcal{O}_{\mathbb{K}}$, o seu volume é dado por

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

uma vez que o discriminante $\mathcal{D}_{\mathbb{K}} = det(\sigma_i(x_j))^2$. Pelo Teorema 1.1.2, segue que existe uma $\mathbb{Z}$-base $\{w_1, \ldots, w_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros não nulos $a_1, \ldots, a_n$ tais que $\{a_1w_1, \ldots, a_nw_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$. Assim,

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

Pela Proposição 1.2.13, segue que $N(\mathcal{I}) = |a_1 \cdots a_n|$, e portanto,

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

como queríamos. ■

Observação 4.3.1. *Seja $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. Pelo Corolário 4.3.1, segue que a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{I})$ é dada por*

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

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

Proposição 4.3.1. *Se $\mathbb{K}$ é um corpo de números de grau n e $x \in \mathbb{K}$, então*

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

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

Demonstração: Sejam $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ tal que $r_1 + 2r_2 = n$, onde r_1 são os monomorfismos reais e r_2 a metade dos monomorfismos imaginários. Se $x \in \mathbb{K}$, então

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

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

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

Note que

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

para $r_1 + 1 \leq j \leq r_1 + r_2$. Logo,

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

Se $r_1 = 0$, isto é, $\mathbb{K}$ for totalmente imaginário, então

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

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

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

e, como os $\sigma_i(x\overline{x})$ são conjugados de $x\overline{x}$, segue que $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}Tr(x\overline{x})$. Agora, se $r_2 = 0$, isto é, $\mathbb{K}$ for um corpo totalmente real, então

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

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

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

Logo,

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

ou seja, $|\sigma_{\mathbb{K}}(x)|^2 = \begin{cases} Tr_{\mathbb{K}|\mathbb{Q}}(x^2), \ \textit{se } \mathbb{K} \text{ for totalmente real,} \\ \frac{1}{2}Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}), \ \textit{se } \mathbb{K} \text{ for totalmente imaginário,} \end{cases}$

o que prova o resultado. ■

Note que se $\mathbb{K}|\mathbb{Q}$ é galoisiana, então $\mathbb{K}$ é, necessariamente, totalmente real ou totalmente imaginário. Em particular, quando n é ímpar, segue que $\mathbb{K}$ é totalmente real.

Proposição 4.3.2. *Seja $\mathbb{K}$ um corpo de números totalmente real ou totalmente imaginário. Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$, $\mathcal{D}_{\mathbb{K}}$ o discriminante de $\mathbb{K}$ e $\mathcal{I}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é dada por*

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

onde $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})| \ x \in \mathcal{I}, \ x \neq 0\}$ e $N(\mathcal{I})$ é a norma do ideal $\mathcal{I}$.

Demonstração: Primeiro, vamos supor que $\mathbb{K}$ seja totalmente real, ou seja, $r_2 = 0$, e assim

$$\rho = \frac{1}{2} \min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})}| \ x \in \mathcal{I}, \ x \neq 0\}.$$

Como $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})|\ x \in \mathcal{I},\ x \neq 0\}$, segue que $\rho = 1/2\sqrt{t}$, e portanto,

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

Agora, suponhamos que $\mathbb{K}$ seja um corpo totalmente imaginário. Desta forma,

$$\rho = \frac{1}{2}\min\{\sqrt{\frac{1}{2}Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})|}\ x \in \mathcal{I},\ x \neq 0\} = \frac{1}{2}\sqrt{\frac{1}{2}t}.$$

Além disso, $r_1 = 0$ e $r_2 = n/2$, e portanto,

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

o que prova a proposição. ■

4.4 Considerações finais do capítulo

Neste capítulo, apresentamos o conceito principal do trabalho, os reticulados e principais propriedades. Na primeira seção, demos noções gerais e básicas sobre reticulados no $\mathbb{R}^n$, tais como, matriz geradora, matriz de Gram, determinante, volume, raio de empacotamento e densidade de centro. Na segunda, apresentamos os reticulados clássicos da literatura que possuem densidade de centro ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12, 16 e 24. E na Seção 4.3, apresentamos resultados sobre reticulados algébricos via homomorfismo canônico (ou Minkowski), fazendo uma ligação entre reticulados e a teoria dos números, explicitando a formula de densidade de centro de reticulados algébricos obtidos por ideais de anéis de inteiros de corpos de números.

Capítulo

5

Construções de reticulados

Neste capítulo, utilizamos os resultados vistos nos capítulos anteriores para construir exemplos de reticulados algébricos via homomorfismo canônico, que são versões rotacionadas dos reticulados vistos no Capítulo 4 e que possuem densidade de centro ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 12 e 24.

5.1 Dimensão 2

Nesta seção, apresentamos exemplos de reticulados com dimensão 2. Primeiramente, na Subseção 5.1.1, apresentamos uma construção via polinômios. Em seguida, na Subseção 5.1.2, apresentamos a construção via homomorfismo canônico.

5.1.1 Construção via polinômios

O objetivo desta subseção é obter versões rotacionados do reticulado Λ_2 via polinômios de grau 2 para os casos em que $\Delta > 0$ e $\Delta < 0$, ou seja, polinômio de duas raízes reais e com de raízes complexas.

Caso em que $\Delta > 0$.

Seja $f(x) = x^2 + ax + b$, onde $a, b \in \mathbb{Z}$ e $a \neq 0$, e sejam $\alpha, \beta \in \mathbb{R}$ as raízes de f. Logo, como $\Delta > 0$, temos que $\Delta = a^2 - 4b > 0$, e portanto as raízes de f são reais e distintas. Das equações de Newton-Girard temos que

$$\begin{cases} \alpha + \beta = -a \\ \alpha\beta = b. \end{cases}$$

Se $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$, seja $\Lambda_f \subset \mathbb{R}^2$ o reticulado gerado pela base $\{v_1, v_2\}$. A matriz geradora de Λ_f será dada por

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

Como vimos no Capítulo 4, se $\Lambda \subseteq \mathbb{R}^n$ é um reticulado a densidade de Λ é dada por

$$\delta(\Lambda) = \frac{\rho^n}{Vol(\Lambda)} = \frac{\rho^n}{|det(M)|},$$

onde ρ é o raio de empacotamento de Λ. Desta forma, para calcularmos a densidade de centro precisamos encontrar expressões para o calculo de ρ e o $det(M)$.

Agora, como $\alpha = \dfrac{-a + \sqrt{\Delta}}{2}$ e $\beta = \dfrac{-a - \sqrt{\Delta}}{2}$ temos que

$$|detM| = |\alpha^2 + \beta^2| = |a|\sqrt{\Delta} = |a|\sqrt{a^2 - 4b},$$

e resta encontrar o valor de ρ. Mas, segue da Subseção 4.1.3 que o maior raio de empacotamento de um reticulado Λ é $\rho = \Lambda_{min}/2$, onde $(\Lambda_{min})^2$ é a norma mínima de Λ.

Proposição 5.1.1. *Se $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes $\alpha, \beta \in \mathbb{R}$, Λ_f é o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Z}$, então*

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

Demonstração: Calculando o quadrado do módulo de v temos que $|v|^2 = z_1^2v_1v_1 + z_2^2v_2v_2 + z_1z_2(v_1v_2 + v_2v_1)$. E como $v_1v_1 = v_2v_2 = \alpha^2 + \beta^2 = (a^2 + 2b)$ e $v_1v_2 = v_2v_1 = 2\alpha\beta = 2b$, então

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

o que prova o resultado. ■

Desta forma, temos uma expressão para calcular a norma de um vetor de Λ_f e resta saber onde este vetor atinge norma mínima para termos o valor do raio de empacotamento do reticulado e assim calcularmos efetivamente a densidade de centro do reticulado Λ_f.

Teorema 5.1.1. *Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes $\alpha, \beta \in \mathbb{R}$, Λ_f o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$. Se $a^2 = 6b$, então o reticulado $\Lambda_f = \{z_1v_1 + z_2v_2 \mid z_1, z_2 \in \mathbb{Z}\}$ possui densidade de centro $\frac{1}{2\sqrt{3}}$, que é ótima em dimensão 2.*

Demonstração: Seja $f(x) = x^2 + ax + b$ com $a, b \in \mathbb{Z}$ tal que $a^2 = 6b$ e seja $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Z}$, um vetor de Λ_f. Pela Proposição 5.1.1 temos que $|v|^2 = a^2(z_1^2 + z_2^2) - 2b(z_1 - z_2)^2 = 6b(z_1^2 + z_2^2) - 2b(z_1 - z_2)^2$. Observe que esta forma quadrática assume valor mínimo $4b$ quando $z_1 = 1$ e $z_2 = 0$. Logo

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

Agora, como $|detM| = |a|\sqrt{\Delta} = |a|\sqrt{a^2 - 4b}$, temos

$$|detM| = |a|\sqrt{\Delta} = |a|\sqrt{a^2 - 4b} = \sqrt{6b}\sqrt{2b} = 2\sqrt{3}b.$$

Assim, a densidade de centro de Λ_f será dada por

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

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

Caso em que $\Delta < 0$.

Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, onde $a \neq 0$ e $\gamma_1 = \alpha + i\beta, \gamma_2 = \alpha - i\beta \in \mathbb{C}$ as raízes de f, com $\alpha, \beta \in \mathbb{R}$ e $\beta \neq 0$. Com $\Delta = a^2 - 4b < 0$, temos que as raízes são complexas. Se $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$, seja $\Lambda_f \subset \mathbb{R}^2$ o reticulado gerado pela base $\{v_1, v_2\}$. A matriz geradora de Λ_f será dada por

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

Portanto, $detM = \dfrac{a\sqrt{-\Delta}}{2} = \dfrac{a\sqrt{4b - a^2}}{2}$.

Proposição 5.1.2. *Se $f(x) = x^2+ax+b \in \mathbb{Z}[x]$ com raízes conjugadas $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$, Λ_f é o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Z}$, então*

$$|v|^2 = \tfrac{a^2}{4}(z_1^2 + z_2^2) + \tfrac{4b-a^2}{4}(z_1 - z_2)^2.$$

Demonstração: Sejam $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, as raízes de f e $v = z_1v_1 + z_2v_2$, com $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$ e $z_1, z_2 \in \mathbb{Z}$. Temos que

$$v = z_1(\alpha, \beta) + z_2(\alpha, -\beta) = (\alpha(z_1 + z_2), \beta(z_1 - z_2)).$$

Logo,

$$\begin{aligned} |v|^2 &= \alpha^2(z_1 + z_2)^2 + \beta^2(z_1 - z_2)^2 = \left(\frac{-a}{2}\right)^2 (z_1 + z_2)^2 + \left(\frac{\sqrt{-\Delta}}{2}\right)^2 (z_1 - z_2)^2 \\ &= \frac{a^2}{4}(z_1 + z_2)^2 + \frac{4b - a^2}{4}(z_1 - z_2)^2. \end{aligned}$$

o que prova o resultado. ■

Teorema 5.1.2. *Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com raízes conjugadas $\alpha \pm i\beta$, $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$, Λ_f o reticulado de dimensão 2 gerado pela base $\{v_1, v_2\}$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$. Se $a^2 = b$, então o reticulado $\Lambda_f = \{z_1v_1 + z_2v_2 \mid z_1, z_2 \in \mathbb{Z}\}$ possui densidade de centro $\frac{1}{2\sqrt{3}}$, que é ótima em dimensão 2.*

Demonstração: Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ tal que $a^2 = b$ e seja $v = z_1v_1 + z_2v_2$, com $z_1, z_2 \in \mathbb{Z}$ um vetor de Λ_f. Pela Proposição 5.1.2 temos que

$$|v|^2 = \frac{a^2}{4}(z_1 + z_2)^2 + \frac{4b - a^2}{4}(z_1 - z_2)^2 = \frac{b}{4}(z_1 + z_2)^2 + \frac{3b}{4}(z_1 - z_2)^2.$$

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

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

Agora, como $detM = \frac{a\sqrt{-\Delta}}{2} = \frac{a\sqrt{4b-a^2}}{2}$, temos

$$|detM| = \frac{a\sqrt{-\Delta}}{2} = \left|\frac{a\sqrt{4b - a^2}}{2}\right| = \sqrt{b}\sqrt{3b} = b\sqrt{3}.$$

Assim, a densidade de centro de Λ_f será dada por

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

que é a mesma densidade de centro do reticulado Λ_2. ■

Exemplo 5.1.1. *Sejam $f(x) = x^2 + x + 1$, $\alpha \pm i\beta \in \mathbb{C}$ as raízes de f e $v = z_1v_1 + z_2v_2 \in \Lambda_f$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\alpha, -\beta)$. Temos que $|v|^2 = \frac{1}{4}(z_1^2 + z_2^2) + \frac{3}{4}(z_1 - z_2)^2$, que possui o valor mínimo 1 quando tomamos $z_1 = 1$ e $z_2 = 0$. Logo $\rho = \frac{1}{2}$, e mais,*

$$|detM| = \left| \frac{a\sqrt{-(a^2 - 4b)}}{2} \right| = \frac{\sqrt{3}}{2}.$$

Portanto,

$$\delta(\Lambda_f) = \frac{\rho^2}{|det(M)|} = \frac{\frac{1}{2}}{\frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}} \cong 0,28868.$$

5.1.2 Construção via homomorfismo

Nesta subseção, apresentamos uma construção através do homomorfismo canônico.

Exemplo 5.1.2. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$, então $[\mathbb{K} : \mathbb{Q}] = 2$. Seja $\mathcal{P}$ um ideal primo de $\mathcal{O}_\mathbb{K}$, onde $\mathcal{P} = (1 - \zeta_3)\mathcal{O}_\mathbb{K}$. Pelo Teorema 2.2.1, segue que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_3]$, e assim se $x \in \mathcal{P}$, então existem $a, b \in \mathbb{Z}$ tal que $x = (1-\zeta_3)(a+b\zeta_3)$. Agora, como $\overline{\zeta_3} = \zeta_3^{-1}$, segue que $\overline{x} = (1-\zeta_3^{-1})(a+b\zeta_3^{-1})$. Logo,*

$$x\overline{x} = a^2 + b^2 + (b-a)^2 + (ab-a^2)(\zeta_3 + \zeta_3^{-1}) + (ab-b^2)(\zeta_3 + \zeta_3^{-1}) + (-ab)((\zeta_3^2 + \zeta_3^{-2}).$$

Usando a linearidade do traço, a propriedade que $Tr_{\mathbb{K}|\mathbb{Q}}(a_i) = 2a_i$ e o Lema 2.2.3, temos que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = 2a^2 + 2b^2 + 2(b-a)^2 - 2(ab-a^2) - 2(ab-b^2) - 2(-ab) = 6a^2 + 6b^2 - 6ab.$$

Fazendo $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) \mid x \in \mathcal{P} \text{ e } x \neq 0\}$, segue que $t = 6$, com $a = 0$ e $b = 1$. Agora, Pela Proposição 2.2.3, temos que $\mathcal{D}(1, \zeta_3) = -3$, e pelas Proposições 1.2.15 e 1.2.16, segue que $N(\mathcal{P}) = N((1-\zeta_3)\mathcal{O}_\mathbb{K}) = N(1-\zeta_3)N(\mathcal{O}_\mathbb{K}) = N(1-\zeta_3)$. Logo, pelo Lema 2.2.3,

$N(\mathcal{P}) = N(1-\zeta_3) = 3$. *Portanto, pela Observação 4.3.1, segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{(\frac{t}{4})^{\frac{n}{2}}}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}N(\mathcal{P})} = \frac{\frac{6}{4}}{\sqrt{33}} = \frac{1}{2\sqrt{3}} \simeq 0,288675,$$

que é a maior densidade conhecida para dimensão 2, que corresponde a densidade de centro do reticulado Λ_2.

5.2 Dimensão 3

Nesta seção, apresentamos exemplos de versões rotacionados do reticulado Λ_3 que possuem densidade de centro ótimas. Primeiramente, na Subseção 5.2.1, apresentamos uma construção via polinômios de grau 3 e raízes reais. Em seguida, na Subseção 5.2.2, apresentamos a construção via homomorfismo canônico.

5.2.1 Construção via polinômios

Sejam $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, onde $a \neq 0$ e $\alpha, \beta, \gamma \in \mathbb{R}$ as raízes de f.

Proposição 5.2.1. *[10, pág. 48] Um polinômio f de grau 3 com coeficientes reais possui três raízes reais distintas se o discriminante de f for maior que zero, uma raiz real e duas complexas se o discriminante de f for menor que zero.* ■

Desta forma, como queremos raízes reais, segue da Proposição 5.2.1 que $c(27c+4a^3-18ab) < b^2(a^2-ab)$. Se $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$ e $v_3 = (\beta, \gamma, \alpha)$, seja $\Lambda_f \subset \mathbb{R}^3$ o reticulado gerado pela base $\{v_1, v_2, v_3\}$. A matriz geradora de Λ_f será dada por

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

O resultado a seguir nos dá o valor do determinante da matriz M.

Lema 5.2.1. *O determinante de M é dado por*

$$detM = -a(a^2 - 3b).$$

Demonstração: Temos que o $detM = \alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma$. Das equações de Newton-Girard segue que

$$\begin{cases} \alpha+\beta+\gamma=-a \\ \alpha\beta+\alpha\gamma+\beta\gamma=b \\ \alpha\beta\gamma=c, \end{cases}$$

e assim, $(\alpha+\beta+\gamma)^2=\alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\alpha\gamma+\beta\gamma)=a^2$ e portanto,

$$\alpha^2+\beta^2+\gamma^2=a^2-2b. \tag{5.1}$$

Uma vez que $\alpha+\beta+\gamma=-a$, multiplicando o lado esquerdo da Equação (5.1) por $\alpha+\beta+\gamma$ e o lado direito por $-a$ segue que

$$\alpha^3+\beta^3+\gamma^3+\alpha\beta^2+\beta\alpha^2+\beta\gamma^2+\gamma\alpha^2+\gamma\beta^2=-a(a^2-2b).$$

Logo

$$\alpha^3+\beta^3+\gamma^3+3\alpha\beta\gamma=-a^3+3ab,$$

e portanto, $detM=-a(a^2-3b)$. ■

Proposição 5.2.2. *Se $f(x)=x^3+ax^2+bx+c\in\mathbb{Z}[x]$ com raízes $\alpha,\beta,\gamma\in\mathbb{R}$, Λ_f é o reticulado de dimensão 3 gerado pela base $\{v_1,v_2,v_3\}$, onde $v_1=(\alpha,\beta,\gamma)$, $v_2=(\gamma,\alpha,\beta)$ e $v_3=(\beta,\gamma,\alpha)$, e $v\in\Lambda_f$, tal que $v=z_1v_1+z_2v_2+z_3v_3$, com $z_1,z_2,z_3\in\mathbb{Z}$. Então*

$$|v|^2=(a^2-2b)(z_1^2+z_2^2+z_3^2)+2b(z_1z_2+z_1z_3+z_2z_3).$$

Demonstração: Temos que

$$\begin{aligned} v &= z_1v_1+z_2v_2+z_3v_3=z_1(\alpha,\beta,\gamma)+z_2(\gamma,\alpha,\beta)+z_3(\beta,\gamma,\alpha) \\ &= (\alpha z_1+\gamma z_2+\beta z_3,\beta z_1+\alpha z_2+\gamma z_3,\gamma z_1+\beta z_2+\alpha z_3). \end{aligned}$$

Então,

$$\begin{aligned} |v|^2 &= (\alpha z_1+\gamma z_2+\beta z_3)^2+(\beta z_1+\alpha z_2+\gamma z_3)^2+(\gamma z_1+\beta z_2+\alpha z_3)^2 \\ &= (\alpha^2+\beta^2+\gamma^2)(z_1^2+z_2^2+z_3^2)+2(\alpha\beta+\alpha\gamma+\beta\gamma)(z_1z_2+z_1z_3+z_2z_3) \\ &= (a^2-2b)(z_1^2+z_2^2+z_3^2)+2b(z_1z_2+z_1z_3+z_2z_3). \end{aligned}$$

o que prova o resultado. ■

Teorema 5.2.1. *Sejam $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$ com raízes $\alpha, \beta, \gamma \in \mathbb{R}$, Λ_f é o reticulado de dimensão 3 gerado pela base $\{v_1, v_2, v_3\}$, onde $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$ e $v_3 = (\beta, \gamma, \alpha)$. Se $(\frac{a}{2})^2 = b$ e $c(27c+4a^3-18ab) < 0$, então o reticulado $\Lambda_f = \{z_1v_1+z_2v_2+z_3v_3 \mid z_1, z_2, z_3 \in \mathbb{Z}\}$ possui densidade de centro $\frac{\sqrt{2}}{8}$, que é ótima em dimensão 3.*

Demonstração: Pela Proposição 5.2.2 temos que

$$\begin{aligned} |v|^2 &= (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_1z_3 + z_2z_3) \\ &= 2b(z_1^2 + z_2^2 + z_3^3 + z_1z_2 + z_1z_3 + z_2z_3). \end{aligned}$$

Observe que esta forma quadrática assume valor mínimo $2b$ quando $z_1 = 1$ e $z_2 = z_3 = 0$. Logo

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

Agora, como $detM = \dfrac{a\sqrt{-\Delta}}{2} = \dfrac{a\sqrt{4b-a^2}}{2}$, temos

$$|detM| = |-a(a^2 - 3b)| = |ab|.$$

Assim, a densidade de centro de Λ_f será dada por

$$\delta(\Lambda_f) = \frac{\rho^3}{|det(M)|} = \frac{(\frac{\sqrt{2b}}{2})^3}{|ab|} = \frac{1}{4\sqrt{2}} \cong 0,17678,$$

que é a mesma densidade de centro do reticulado Λ_3. ■

5.2.2 Construção via homomorfismo

Nesta subseção, apresentamos uma construção através do homomorfismo canônico, utilizando os resultados vistos no Capítulo 3.

Seja $\mathbb{K}$ um corpo de números de grau p. Os Teoremas 3.2.4 e 3.2.5 fornecem o mínimo M^* do $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $0 \neq x \in \mathcal{M}_m$. Para determinar em quais elementos esse mínimo é atingido, utilizamos o Lema 3.2.2 e o Corolário 3.2.2. Mais especificamente, quando $M^* = 2n$, o mínimo é atingido nos elementos

$$x = a_0t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathcal{O}_{\mathbb{K}},$$

tais que $(a_0, a_1, \ldots, a_{p-1}) = (1, -1, 0, \ldots, 0)$, ou alguma de suas permutações. Se p divide m e $M^* = m^2/p$, segue que o mínimo é atingido em $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t)$, com $(a_0, a_1, \ldots, a_{p-1}) = (m/p, m/p, \ldots, m/p)$. E se p não divide m, o mínimo é atingido em $x = a_0 t + a_1\theta(t) + \cdots a_{p-1}\theta^{p-1}(t)$, com

$$(a_0, a_1, \ldots, a_{p-1}) = (\underbrace{q_j + 1, \ldots, q_j + 1}_{r_j \ \ coordenadas}, q_j, \ldots, q_j),$$

ou uma de suas permutações, onde q_j e r_j são o quociente de resto da divisão de jm por p, com $j = 1, \ldots, p$, respectivamente.

Exemplo 5.2.1. *Sejam $p = 3$, $n = 1123$ e $m = 67$. Assim, como p não divide m, segue do Teorema 3.2.5 que*

$$M^* = min\{2n, M(m), M(2m), M(3m)\} = \{2246, 2245, 6734, 13467\} = 2245.$$

Desta forma, temos que $q_1 = 22$ e $r_1 = 1$, isto é, $67 = 3 \cdot 22 + 1$. Logo, o mínimo é atingido no elemento

$$x = a_0 t + a_1\theta(t) + a_2\theta^2(t) \in \mathcal{O}_{\mathbb{K}},$$

tal que $(a_0, a_1, a_2) = (23, 22, 22)$, ou em uma de suas permutações, onde $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$ e $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$. Logo, segue da Observação 4.3.1 que o reticulado $\sigma_{\mathbb{K}}(\mathcal{M}_{67})$ de dimensão 3 tem densidade de centro igual a

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{67})) = \frac{\rho^3}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} N(\mathcal{M}_{67})} = \frac{(\sqrt{M^*}/2)^3}{nm} = \frac{(\sqrt{2245}/2)^3}{1123 \cdot 67} \simeq 0,17672.$$

Note que a maior densidade de centro de um reticulado de dimensão 3 é obtida pelo reticulado A_3, dada por $\delta(A_3) = \frac{1}{4\sqrt{2}} \simeq 0,17678$.

5.3 Dimensão 4

Nesta seção, apresentamos uma versão rotacionada do reticulado D_4.

Exemplo 5.3.1. *Se $\mathbb{K} = \mathbb{Q}(\zeta_8)$, então $[\mathbb{K} : \mathbb{Q}] = 4$. Seja $\mathcal{P}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$, onde $\mathcal{P} = (1 - \zeta_8)\mathcal{O}_{\mathbb{K}}$. Pelo Teorema 2.3.2, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$, e assim se $x \in \mathcal{P}$, então existem $a_i \in \mathbb{Z}$, $i = 0, 1, 2, 3$, tal que $x = (1 - \zeta_8)(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3)$. Agora, se $\overline{x}$ é o conjugado*

de x, *então* $\overline{x} = (1-\zeta_8^{-1})(a_0 + a_1\zeta_8^{-1} + a_2\zeta_8^{-2} + a_3\zeta_8^{-3})$. *Assim,*

$$\begin{aligned} x\overline{x} &= (2a_0 - 2a_0a_1 - 2a_1^2 - 2a_1a_2 + 2a_2^2 + 2a_0a_3 - 2a_2a_3 + 2a_3^2) + \\ &+ (-a_0^2 + 2a_0a_1 - a_1^2 + 2a_1a_2 - a_2^2 - 2a_2a_3 - a_3^2)\zeta_8 + \\ &+ (a_0^2 - 2a_0a_1 + a_1^2 - 2a_1a_2 + a_2^2 + 2a_0a_3 - 2a_2a_3 + a_3^2)\zeta_8^3 \end{aligned}$$

Pela Proposição 2.3.2, uma vez que $mdc(1,8) = mdc(3,8) = 1 < 4$, *segue que* $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_8) = Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_8^3) = 0$, *logo*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = 4(2a_0 - 2a_0a_1 - 2a_1^2 - 2a_1a_2 + 2a_2^2 + 2a_0a_3 - 2a_2a_3 + 2a_3^2).$$

Fazendo $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) | x \in \mathcal{P} \text{ e } x \neq 0\}$, *segue que* $t = 8$, *com* $a_0 = a_1 = 1$ *e* $a_2 = a_3 = 0$. *Agora, Pela Proposição 2.3.4, temos que* $\mathcal{D}(1, \zeta_8, \zeta_8^2, \zeta_8^3) = 2^8$, *e pelas Proposições 1.2.15, 1.2.16 e1.3.3, segue que* $N(\mathcal{P}) = N(1-\zeta_8) = 2$. *Portanto, pela Observação 4.3.1, segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{1}{2^n|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}}\frac{t^{\frac{n}{2}}}{N(\mathcal{P})} = \frac{1}{2^4|2^8|^{\frac{1}{2}}}\frac{8^2}{2} = \frac{1}{2^3} \simeq 0,125,$$

que é a maior densidade conhecida para dimensão 4, que corresponde a densidade de centro do reticulado Λ_4.

5.4 Dimensão 5

Nesta seção, apresentamos uma versão rotacionada do reticulado D_5.

Exemplo 5.4.1. *Sejam* $p = 5$, $n = 92111$ *e* $m = 607$. *Como* p *não divide* m, *segue do Teorema 3.2.5 que*

$$\begin{aligned} M^* &= min\{2n, M(m), M(2m), M(3m), M(4m), M(5m)\} \\ &= \{184222, 736897, 184223, 1289570, 295245, 1842245\} = 184222. \end{aligned}$$

O mínimo é atingido no elemento

$$x = a_0t + a_1\theta(t) + a_2\theta^2(t) + a_3\theta^3(t) + a_4\theta^4(t) \in \mathcal{O}_{\mathbb{K}},$$

tal que $(a_0, a_1, a_2, a_3, a_4) = (1, -1, 0, 0, 0)$, *ou em uma de suas permutações, onde* $t =$

$Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$ *e* $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$.

Logo, segue da Observação 4.3.1 que o reticulado $\sigma_{\mathbb{K}}(\mathcal{M}_{607})$ *de dimensão 5 tem densidade de centro igual a*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{607})) = \frac{\rho^5}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} N(\mathcal{M}_{607})} = \frac{(\sqrt{M^*}/2)^5}{n^2 m} = \simeq 0,08839.$$

Note que a maior densidade de centro de um reticulado de dimensão 5 é obtida pelo reticulado D_3, *dada por* $\delta(D_5) = \frac{1}{8\sqrt{2}} \simeq 0,08839$.

5.5 Dimensão 6

Nesta seção, apresentamos uma versão rotacionada do reticulado E_6.

Exemplo 5.5.1. *Se* $\mathbb{K} = \mathbb{Q}(\zeta_9)$, *então* $[\mathbb{K} : \mathbb{Q}] = 6$ *e seu anel de inteiros é* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_9]$. *Seja* $\mathcal{P}$ *um ideal primo de* $\mathcal{O}_{\mathbb{K}}$, *onde* $\mathcal{P} = (1-\zeta_9)^2\mathcal{O}_{\mathbb{K}}$. *Se* $x \in \mathcal{P}$, *então existem* $a_i \in \mathbb{Z}$, $i = 0, 1, \ldots, 5$, *tal que* $x = (1 - 2\zeta_9 + \zeta_9^2)(a_0 + a_1\zeta_9 + a_2\zeta_9^2 + a_3\zeta_9^3 + a_4\zeta_9^4 + a_5\zeta_9^5)$. *Agora, se* $\overline{x}$ *é o conjugado de* x, *então*

$$\overline{x} = (1 - 2\zeta_9^{-1} + \zeta_9^{-2})(a_0 + a_1\zeta_9^{-1} + a_2\zeta_9^{-2} + a_3\zeta_9^{-3} + a_4\zeta_9^{-4} + a_5\zeta_9^{-5}).$$

Assim,

$$\begin{aligned} x\overline{x} &= (6a_0^2 - 9a_0a_1 + 6a_1^2 + \cdots + 6a_5^2) + (-5a_0^2 + 11a_0a_1 - 5a_1^2 + \cdots - 5a_5^2)\zeta_9 + \\ &+ (5a_0^2 - 11a_0a_1 + 5a_1^2 + \cdots + 5a_5^2)\zeta_9^2 + (-a_0^2 + 4a_0a_1 - a_1^2 + \cdots - a_2^2)\zeta_9^4 + \\ &+ (4a_0^2 - 7a_0a_1 + 4a_1^2 + \cdots + 4a_5^2)\zeta_9^5. \end{aligned}$$

Pela Proposição 2.3.2, uma vez que $mdc(1,9) = mdc(2,9) = mdc(4,9) = mdc(5,9) = 1 < 3$, *segue que*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = 6(6a_0^2 - 9a_0a_1 + 6a_1^2 + \cdots + 6a_5^2).$$

Fazendo $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) | x \in \mathcal{P} \text{ e } x \neq 0\}$, *segue que* $t = 18$, *com* $a_0 = 1$, $a_4 = a_5 = -1$ *e* $a_1 = a_2 = a_3 = 0$. *Agora, como* $\mathcal{D}_{\mathbb{K}} = -3^9$ *e* $N(\mathcal{P}) = 3^2$, *pela Observação 4.3.1, segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{3^6}{2^2 3^{\frac{13}{2}}} = \frac{1}{8\sqrt{3}} \simeq 0,07217,$$

que é a maior densidade conhecida para dimensão 6, que corresponde a densidade de centro do

reticulado Λ_6.

5.6 Dimensão 7

Nesta seção, apresentamos uma versão rotacionada do reticulado E_7.

Exemplo 5.6.1. *Sejam* $p = 7$, $n = 600601$ *e* $m = 1096$. *Como* p *não divide* m, *segue do Teorema 3.2.5 que*

$$\begin{aligned} M^* &= min\{2n, M(m), M(2m), M(3m), M(4m), M(5m), M(6m), M(7m)\} \\ &= \{1201202, 1201210, 3603638, 7207284, 1201204, 2402422, 4804858, 8408512\} \\ &= 1201202. \end{aligned}$$

O mínimo é atingido no elemento

$$x = a_0 t + a_1\theta(t) + a_2\theta^2(t) + \cdots + a_6\theta^6(t) \in \mathcal{O}_{\mathbb{K}},$$

tal que $(a_0, a_1, \ldots, a_4) = (1, -1, 0, 0, 0, 0, 0)$, *ou em uma de suas permutações, onde* $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$ *e* $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$.

Logo, segue da Observação 4.3.1 que o reticulado $\sigma_{\mathbb{K}}(\mathcal{M}_{1096})$ *de dimensão 7 tem densidade de centro igual a*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{1096})) = \frac{\rho^7}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}} N(\mathcal{M}_{607})} = \frac{(\sqrt{M^*}/2)^7}{n^3 m} =\simeq 0,0625.$$

Note que a maior densidade de centro de um reticulado de dimensão 7 é obtida pelo reticulado E_3, *dada por* $\delta(E_7) = \frac{1}{16} = 0,0625$.

5.7 Dimensão 8

Nesta seção, apresentamos exemplos de versões rotacionados do reticulado E_8

5.7.1 Construção 1

Exemplo 5.7.1. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ *e* $\mathcal{P} = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)\mathcal{O}_{\mathbb{K}}$ *um ideal primo de* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$. *Então,* $[\mathbb{K} : \mathbb{Q}] = 8$, $\mathcal{D}_{\mathbb{K}} = \pm 2^8 5^6$ *e* $N(\mathcal{P}) = 80$. *Se* $x \in \mathcal{P}$, *então*

$$x = (-1 - \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4)(\sum_{i=0}^{7} a_1 \zeta_{20}^i),$$

onde $a_i \in \mathbb{Z}$, *para* $i = 0, 1, \ldots, 7$. *Assim,*

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) &= 40(\sum_{i=1}^{7} a_i^2 + a_0a_1 + a_1a_2 - a_0a_3 + a_2a_3 - a_0a_4 - a_1a_4 + a_3a_4 - a_1a_5 - a_2a_5 \\ &+ a_4a_5 + a_0a_6 - a_2a_6 - a_3a_6 + a_5a_6 + a_0a_7 + a_1a_7 - a_3a_7 - a_4a_7 + a_6a_7). \end{aligned}$$

Então $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})|\ x \in \mathcal{P},\ x \neq 0\} = 40$ *com* $a_0 = a_1 = a_4 = -1$, $a_2 = a_6 = 1$ $a_3 + a_5 + a_7 = 0$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathcal{P})$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{1}{2^n |\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}} \frac{t^{\frac{1}{2}}}{N(\mathcal{P})} = \frac{1}{16} = 0,0625,$$

que é a maior densidade conhecida para dimensão 8, que corresponde a densidade de centro do reticulado E_8.

5.7.2 Construção 2

Nesta subseção, faremos a construção feita por André Luiz Flores, J. Carmelo Interlano, Trajano Pires da Nóbrega Neto e André Luís Contiero em [17]. A seguir fornecemos alguns conceitos e resultados necessários para tal construção.

Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ onde $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana e $G = Gal(\mathbb{L}|\mathbb{Q})$ é um grupo abeliano. Sejam $\mathcal{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ e $S = \{\mathcal{B}_1, \ldots, \mathcal{B}_s\}$ o conjunto de ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathcal{Q}$, e assuma que $q\mathbb{Z} = \mathcal{Q} \cap \mathbb{Z}$. O grupo de decomposição de $\mathcal{Q}$ em $\mathbb{K}|\mathbb{Q}$ é $D_{\mathbb{K}} = \{\theta \in Gal(\mathbb{K}|\mathbb{Q})|\ \theta(\mathcal{Q}) = \mathcal{Q}\}$. E por fim, seja $E = \{\sigma \in G|\ \sigma(S) = S\}$.

Proposição 5.7.1. *Temos que*

1. E *é um subgrupo de* G.

2. E *é composto pelo automorfismos de* $D_{\mathbb{K}}$ *estendidos a* $\mathbb{L}$.

3. Se $\sigma \in G$ e $\sigma(S) \cap S = \emptyset$, então $\sigma \in E$.

Demonstração:

1. Segue diretamente que E é um subgrupo de G.

2. Sejam $\psi \in E$ e $\mathcal{B}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathcal{Q}$. Segue que $\psi(\mathcal{B})$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathcal{Q}$, de onde $\psi(\mathcal{B}) \subset \mathcal{B}_j$, para algum $j = 1, \ldots, s$. Assim, $\psi(\mathcal{Q}) \subset \mathcal{Q}$, logo $\psi(\mathcal{Q}) = \mathcal{Q}$. Consequentemente, $\psi|_{\mathbb{K}} \in D_{\mathbb{K}}$. Por outro lado, sejam $\psi \in G$ tal que $\psi|_{\mathbb{K}}(\mathcal{Q}) = \mathcal{Q}$ e $\mathcal{B}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathcal{Q}$. Observe que $\psi(\mathcal{B})$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ e $\psi(\mathcal{Q}) \subset \psi(\mathcal{B})$, e assim $\psi(\mathcal{B})$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathcal{Q}$, isto é, $\psi \in E$.

3. Seja $\sigma \in G$ tal que $\sigma(\mathcal{B}) = \mathcal{B}'$ para algum $\mathcal{B}, \mathcal{B}' \in S$. Neste caso, $\sigma(\mathcal{Q})$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ abaixo de $\mathcal{B}'$. Contudo, já que $\mathcal{B}' \in S$, o único ideal primo de $\mathcal{O}_{\mathbb{L}}$ contido em $\mathcal{B}'$ é um $\mathcal{Q}$, tal que $\sigma(\mathcal{Q}) = \mathcal{Q}$. Portanto, $\sigma|_{\mathbb{K}} \in D_{\mathbb{K}}$, e pelo item 2, segue que $\sigma \in E$.

■

Agora, suponha que $\mathbb{L}$ é totalmente real e seja $\gamma : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Se $\gamma|_{\mathbb{L}} \notin D_{\mathbb{L}} = \{\sigma \in Gal(\mathbb{L}|\mathbb{Q})|\ \sigma(\mathcal{B}) = \mathcal{B},\ \forall \mathcal{B} \in S\}$, então exite um ideal $\mathcal{I}$ de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q}\mathcal{O}_{\mathbb{L}} = \mathcal{I}\overline{\mathcal{I}}$.

Corolário 5.7.1. *Suponha que $[\mathbb{L} : \mathbb{K}]$ seja ímpar. Então $\gamma|_{\mathbb{L}} \in D_{\mathbb{L}}$ se, e somente se, $\gamma|_{\mathbb{K}} \in D_{\mathbb{K}}$.*

Demonstração: Segue direto que $\gamma|_{\mathbb{L}} \in D_{\mathbb{L}}$ implica que $\gamma|_{\mathbb{K}} \in D_{\mathbb{K}}$. Agora, $\gamma|_{\mathbb{K}} \in D_{\mathbb{K}}$ implica que $\gamma|_{\mathbb{K}} \in E$, ou seja, $\gamma|_{\mathbb{L}}(S) = S$. Suponha por absurdo que $\gamma|_{\mathbb{L}} \notin D_{\mathbb{L}}$, isto é, $\gamma(\mathcal{B}_i) \neq \mathcal{B}_i$, para todo $i \in \{1, \ldots, s\}$. O que faz com que s seja par, mas como s divide $[\mathbb{L} : \mathbb{K}]$, chegamos em uma contradição. Portanto, $\gamma|_{\mathbb{L}} \in D_{\mathbb{L}}$. ■

Seja m e n dois inteiros relativamente primos. A ordem de n módulo m será denotada por $ord_m n$. A partir de agora, considere $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ e $\mathbb{K} = \mathbb{Q}(\zeta_p)$.

Teorema 5.7.1. *[33, Teorema 2.13, pag. 14] O numero de ideais primos distintos acima de $\mathcal{Q}$ em $\mathcal{O}_{\mathbb{L}}$ é igual a $\dfrac{p-1}{ord_p q}$.* ■

Corolário 5.7.2. *$\gamma|_{\mathbb{L}} \in D_{\mathbb{L}}$ se, e somente se, $ord_p q \equiv 0 \ (mod\ 2)$.*

Demonstração: Pelo Corolário 5.7.1, $\gamma|_{\mathbb{L}} \in D_{\mathbb{L}}$ se, e somente se, $\gamma|_{\mathbb{K}} \in D_{\mathbb{K}}$. O número de ideais primos em $\mathcal{O}_{\mathbb{K}}$ acima de q é igual a $\dfrac{p-1}{ord_p q}$, então $|D_{\mathbb{K}}| = ord_p q$. Contudo, o grupo de

Galois de $\mathbb{K}|\mathbb{Q}$ possui exatamente um elemento de ordem 2, $\gamma|_{\mathbb{K}}$. Por outro lado, suponha que $ord_p q \equiv 0 \ (mod\ 2)$. Já que $D_{\mathbb{K}}$ é um grupo cíclico de ordem par, segue que existe exatamente um subgrupo de ordem 2. ■

Corolário 5.7.3. *Se p e q satisfazem a condição $ord_p q \equiv ord_q p \equiv 1 \ (mod\ 2)$, então eles se decompoem em ideais primos em $\mathcal{O}_{\mathbb{L}}$ como*

$$p\mathcal{O}_{\mathbb{L}} = (\mathcal{P}_1 \cdots \mathcal{P}_r \overline{\mathcal{P}_1 \cdots \mathcal{P}_r})^{p-1} \ e \ p\mathcal{O}_{\mathbb{L}} = (\mathcal{Q}_1 \cdots \mathcal{Q}_s \overline{\mathcal{Q}_1 \cdots \mathcal{Q}_s})^{q-1},$$

onde $r = \dfrac{q-1}{2ord_q p}$ *e* $s = \dfrac{p-1}{2ord_p q}$.

Demonstração: Segue diretamente do Teorema 5.7.1 e do Corolário 5.7.2 ■

Lema 5.7.1. *Sejam p e q satisfazendo a condição $ord_p q \equiv ord_q p \equiv 1 \ (mod\ 2)$, e $p\mathcal{O}_{\mathbb{L}}$, $q\mathcal{O}_{\mathbb{L}}$ como no Corolário 5.7.3. Seja $\mathcal{I} = \mathcal{P}_1 \cdots \mathcal{P}_{r_p/2} \mathcal{Q}_1 \cdots \mathcal{Q}_{r_q/2}$. Então, para todo $x \in \mathcal{I}$, $Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x}) \equiv 0 \ (mod\ 2pq)$.*

Demonstração: Primeiramente, mostremos que $Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x})$ é par. De fato, para $x \in \mathbb{Z}[\zeta_{pq}]$, segue que $x\overline{x} \in \mathbb{Q}(\zeta_{pq} + \zeta_{pq}^{-1}) = \mathbb{L}^+$. Já que $x\overline{x} \in \mathbb{L}^+$, segue que $Tr_{\mathbb{L}|\mathbb{L}^+}(x\overline{x}) = 2x\overline{x}$. Então,

$$Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{L}^+|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{L}^+}(x\overline{x})) = 2Tr_{\mathbb{L}^+|\mathbb{Q}}(x\overline{x}).$$

Por fim mostremos que $Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x})$ é múltiplo de pq. De fato, já que $x \in \mathcal{I}$, então $x\overline{x} \in \mathcal{I}\overline{\mathcal{I}} = \mathcal{J}$, que por sua vez é igual ao produto de todos os ideais de $\mathbb{Z}[\zeta_{pq}]$ acima de pq. Para $x\overline{x} \in \mathcal{J}$, segue que $\tau(x\overline{x}) \in \tau(\mathcal{J}) = \mathcal{J}$, onde τ é qualquer automorfismo de $\mathbb{L}$. Assim, todos os conjugados de $x\overline{x}$ estão em $\mathcal{J}$. Como consequência, a sua soma, que é $Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x})$, pertence a $\mathcal{J} \cap \mathbb{Z} = pq\mathbb{Z}$. ■

No exemplo seguinte, usando os resultados vistos nesta subseção, construímos reticulados de densidade de centro ótimas para dimensão 8.

Exemplo 5.7.2. *Sejam p e q dois primos ímpares distintos com*

$$ord_p q \equiv ord_q p \equiv 1 \ (mod\ 2).$$

Seja $\mathbb{K}_1 \subseteq \mathbb{Q}(\zeta_p)$ e $\mathbb{K}_2 \subseteq \mathbb{Q}(\zeta_q)$ tais que $h_p = [\mathbb{Q}(\zeta_p) : \mathbb{K}_1]$ e $h_q = [\mathbb{Q}(\zeta_q) : \mathbb{K}_2]$ são ímpares. Defina $n_1 = [\mathbb{K}_1 : \mathbb{Q}]$ e $n_2 = [\mathbb{K}_2 : \mathbb{Q}]$. Assim, o corpo $\mathbb{M} = \mathbb{K}_1\mathbb{K}_2$ tem grau $n_1 n_2$. E como $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos, temos que

$$|\mathcal{D}_{\mathbb{M}}| = p^{n_2(n_1-1)} q^{n_1(n_2-1)}.$$

Em $\mathbb{M}$, seja r_p e r_q o número de primos acima de p e q, respectivamente. Uma vez que h_p e h_q são ímpares, p e q se decompõem em $\mathcal{O}_{\mathbb{M}}$ com segue:

$$p\mathcal{O}_{\mathbb{M}} = (\mathcal{P}_1 \cdots \mathcal{P}_{r_p/2}\overline{\mathcal{P}_1 \cdots \mathcal{P}_{r_p/2}})^{n_2} \text{ e } q\mathcal{O}_{\mathbb{M}} = \mathcal{Q}_1 \cdots \mathcal{Q}_{r_q/2}\overline{\mathcal{Q}_1 \cdots \mathcal{Q}_{r_q/2}})^{n_1}.$$

Seja $\mathcal{J} = \mathcal{P}_1 \cdots \mathcal{P}_{r_p/2}\mathcal{Q}_1 \cdots \mathcal{Q}_{r_q/2}$, logo sua norma é dada por

$$N(\mathcal{J}) = (p^{h_p})^{r_p/2}(q^{h_q})^{r_q/2} = p^{n_2/2}q^{n_1/2},$$

e para $x \in \mathcal{J}$, $Tr_{\mathbb{M}|\mathbb{Q}}(x\overline{x}) = \frac{1}{h_p h_q} Tr_{\mathbb{L}|\mathbb{Q}}(x\overline{x})$. Por hipótese, ambos h_p e h_q são ímpares e menores que p e q, respectivamente. Pelo Lema 5.7.1, $Tr_{\mathbb{M}|\mathbb{Q}}(x\overline{x}) \equiv 0 \pmod{2pq}$. Desses fatos, temos que $Tr_{\mathbb{M}|\mathbb{Q}}(x\overline{x}) \geq 2pq$, sempre que $x \neq 0$. Usando isto e a Proposição 4.3.1, o raio de empacotamento do reticulado $\sigma_{\mathbb{M}}(\mathcal{J})$ pode ser limitado inferiormente como

$$\rho \geq \frac{\sqrt{pq}}{2}.$$

Finalmente, observe que $\mathbb{K}_1 \nsubseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, uma vez que h_p é ímpar. Já que $\mathbb{K}_1|\mathbb{Q}$ é de Galois, $\mathbb{K}_1$ é um corpo totalmente complexo. A extensão $\mathbb{M}|\mathbb{Q}$ também é de Galois, e então $\mathbb{M}$ é um corpo totalmente complexo e assim $r_1 = 0$ e $r_2 = n_1n_2/2$. Com tudo isso, seque que a densidade de centro do reticulado

$$\sigma_{\mathbb{M}}(\mathcal{J}) \geq \frac{(2pq)^{\frac{n_1n_2}{2}}}{p^{\frac{n_2(n_1-1)}{2}}q^{\frac{n_1(n_2-1)}{2}}p^{\frac{n_2}{2}}q^{\frac{n_1}{2}}2^{n_1n_2}} = \frac{1}{2^{n_1n_2/2}}.$$

Quando n_1n_2 é igual a 8, a densidade de centro $\delta = 1/16$, que é a mesma do E_8. Observamos que qualquer reticulado de dimensão 8 com densidade de centro $\delta = 1/16$ deve ser igual ao E_8.

5.8 Dimensão 12

Nesta seção, apresentamos uma versão rotacionada do reticulado K_{12}.

Exemplo 5.8.1. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{21})$ e $\mathcal{P} = (\zeta_{21}^2 - \zeta_{21}^4 + \zeta_{21}^8)\mathcal{O}_{\mathbb{K}}$ um ideal primo de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{21}]$. Então, $[\mathbb{K} : \mathbb{Q}] = 12$, $\mathcal{D}_{\mathbb{K}} = 3^6 7^{10}$ e $N(\mathcal{P}) = 7$. Se $x \in \mathcal{P}$, então*

$$x = (\zeta_{21}^2 - \zeta_{21}^4 + \zeta_{21}^8)(\sum_{i=0}^{11} a_1\zeta_{21}^i),$$

onde $a_i \in \mathbb{Z}$, *para* $i = 0, 1, \ldots, 11$. *Assim,*

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) &= 28a_0^2 + 28a_1^2 + 28a_0a_{10} - 14a_1a_{10} + 28a_{10}^2 + 28a_0a_{11} + 28a_1a_{11} + 28a_{11}^2 \\ &- 14a_0a_2 - 14a_11a_2 + 28a_2^2 - 14a_0a_3 - 14a_1a_3 - 28a_{10}a_3 + 28a_3^2 - 14a_0a_4 \\ &- 14a_1a_4 - 28a_{11}a_4 - 14a_2a_4 + 28a_4^2 + 28a_0a_5 - 14a_1a_5 + 28a_{10}a_5 - 14a_2a_5 \\ &- 14a_3a_5 + 28a_5^2 + 28a_1a_6 - 14a_{10}a_6 + 28a_{11}a_6 - 14a_2a_6 - 14a_3a_6 - 14a_4a_6 \\ &+ 28a_6^2 - 28a_0a_7 - 14a_{10}a_7 - 14a_{11}a_7 + 28a_2a_7 - 14a_3a_7 - 14a_4a_7 - 14a_5a_7 \\ &+ 28a_1^2 - 28a_1a_8 - 14a_{10}a_8 - 14a_{11}a_8 + 28a_3a_8 - 14a_4a_8 - 14a_5a_8 - 14a_6a_8 \\ &+ 28a_8^2 - 14a_0a_9 - 14a_{11}a_9 - 28a_2a_9 + 28a_4a_9 - 14a_5a_9 - 14a_6a_9 - 14a_7a_9 + 28a_9^2. \end{aligned}$$

Então $t = \min\{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})|\ x \in \mathcal{P},\ x \neq 0\} = 28$ *com* $a_1 = 0$, *para* $i = 1, \ldots, 11$ *e* $i \neq 7$, *e* $a_7 = -1$. *Portanto, a densidade de centro do reticulado* $\sigma_{\mathbb{K}}(\mathcal{P})$ *é dada por*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{1}{2^n|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}}\frac{t^{\frac{1}{2}}}{N(\mathcal{P})} = \frac{1}{27} \simeq 0,03704,$$

que é a maior densidade conhecida para dimensão 12, que corresponde a densidade de centro do reticulado K_{12}.

5.9 Dimensão 24

Nesta seção, apresentamos uma versão rotacionada do reticulado Λ_{24}.

Proposição 5.9.1. *[1] Se* p *e* q *são números primos distintos,* $m = \varphi(pq)$ *e* $x \in \mathbb{Z}[\zeta_{pq}]$ *é tal que* $x = a_0 + a_1\zeta_{pq} + \cdots + a_{n-1}\zeta_{pq}^{m-1}$, *então*

$$Tr_{\mathbb{Q}(\zeta_{pq})|\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)\alpha_0 + 2(1-p)\sum_{p|i}\alpha_i + 2(1-q)\sum_{q|i}\alpha_i + 2\sum_{p\not|i, q\not|i}\alpha_i,$$

onde $\alpha_i = \sum_{j=0}^{m-(i+1)} a_j a_{i+1}$, *para* $i = 0, 1, \ldots, m-1$. ■

Exemplo 5.9.1. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_{39})$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{39}]$ *seu anel de inteiros e* $f(x)$ *o polinômio minimal de* ζ_{39} *sobre* $\mathbb{Q}$. *Estudemos a fatoração dos ideais* $3\mathcal{O}_{\mathbb{K}}$ *e* $13\mathcal{O}_{\mathbb{K}}$ *como produto de ideais primos em* $\mathcal{O}_{\mathbb{K}}$. *Assim, como*

$$f(x) = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1,$$

segue que

$$f(x) \equiv (x^3+2x+2)^2 + (x^3+x^2+x+2)^2(x^3+2x^2+2x+2)^2(x^3+x^2+2) \ (mod\ (\mathbb{Z}/3\mathbb{Z})[x]).$$

Assim $g = 4$, $e_1 = e_2 = e_3 = e_4 = 2$, $f_1 = f_2 = f_3 = f_4 = 3$, $\overline{\mu_1(x)} = x^3+2x+2$, $\overline{\mu_2(x)} = x^3+x^2+x+2$, $\overline{\mu_3(x)} = x^3+2x^2+2x+2$, $\overline{\mu_4(x)} = x^3+x^2+2$. *Logo, pelo Teorema 1.4.2,*

$$\begin{aligned}
\mathcal{P}_1 &= 3\mathcal{O}_{\mathbb{K}} + ({\zeta_{39}}^3 + 2\zeta_{39} + 2)\mathcal{O}_{\mathbb{K}} \\
\mathcal{P}_2 &= 3\mathcal{O}_{\mathbb{K}} + ({\zeta_{39}}^3 + {\zeta_{39}}^2 + \zeta_{39} + 2)\mathcal{O}_{\mathbb{K}} \\
\mathcal{P}_3 &= 3\mathcal{O}_{\mathbb{K}} + ({\zeta_{39}}^3 + 2{\zeta_{39}}^2 + 2\zeta_{39} + 2)\mathcal{O}_{\mathbb{K}} \\
\mathcal{P}_4 &= 3\mathcal{O}_{\mathbb{K}} + ({\zeta_{39}}^3 + 2{\zeta_{39}}^2 + 2)\mathcal{O}_{\mathbb{K}}.
\end{aligned}$$

Portanto $3\mathcal{O}_{\mathbb{K}} = (\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4)^2$, *com* $N(\mathcal{P}_i) = 3^3$, *para* $i = 1,2,3,4$. *Como* $ord_{13}3 = 3 \equiv 1\ (mod\ 2)$, *segue do Corolário 5.7.2 que* $\overline{\sigma} = \sigma_{38} \notin D_{\mathbb{K}}(3) = \{\sigma_1, \sigma_{14}, \sigma_{16}, \sigma_{22}, \sigma_{29}, \sigma_{35}\}$. *Neste caso, temos que* $\mathcal{P}_4 = \overline{\mathcal{P}_1}$ *e* $\mathcal{P}_3 = \overline{\mathcal{P}_2}$.
Para o ideal $13\mathcal{O}_{\mathbb{K}}$ *temos que*

$$f(x) \equiv (x+4)^2(x+10)^{12} \ (mod\ \mathbb{Z}/13\mathbb{Z}[x]).$$

Assim $g = 2$, $\overline{\mu_1(x)} = x+4$, $\overline{\mu_2(x)} = x+10$, $e_1 = e_2 = 12$, $f_1 = f_2 = 1$. *Logo,*

$$\begin{aligned}
\mathcal{Q}_1 &= 13\mathcal{O}_{\mathbb{K}} + (\zeta_{39} + 4)\mathcal{O}_{\mathbb{K}} \\
\mathcal{Q}_2 &= 13\mathcal{O}_{\mathbb{K}} + (\zeta_{39} + 10)\mathcal{O}_{\mathbb{K}}.
\end{aligned}$$

Portanto $13\mathcal{O}_{\mathbb{K}} = (\mathcal{Q}_1\mathcal{Q}_2)^{12}$, *com* $N(\mathcal{Q}_i) = 13$, *para* $i = 1,2$. *Como* $ord_3 13 = 13 \equiv 1\ (mod\ 2)$, *segue que* $\overline{\sigma} = \notin D_{\mathbb{K}}(13) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{10}, \sigma_{16}, \sigma_{19}, \sigma_{22}, \sigma_{25}, \sigma_{28}, \sigma_{31}, \sigma_{34}, \sigma_{37}\}$. *Neste caso, temos que* $\mathcal{Q}_2 = \overline{\mathcal{Q}_1}$.

Considerando o ideal $\mathcal{P} = \mathcal{P}_1\mathcal{P}_2\mathcal{Q}_1$, *vamos calcular a densidade de centro de* $\sigma_{\mathbb{K}}(\mathcal{P})$. *Como* $\mathcal{D}_{\mathbb{K}} = 3^{12}13^{22}$ *e* $N(\mathcal{P}) = N(\mathcal{P}_1)N(\mathcal{P}_2)N(\mathcal{Q}_1) = 3^6 13$, *segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{2^{12}\rho^{24}}{3^{12}13^{12}}.$$

Então, precisamos determinar agora

$$\rho = \frac{1}{2}\min\left\{\sqrt{\frac{Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x})}{2}} \mid x \in \mathcal{P},\ x \neq 0\right\}.$$

Veremos que se $x \in \mathcal{P}$, *então* $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) \geq 4 \cdot 39$. *Visto que* $mdc(p,q) = 1$, *para* $x \in \mathcal{P}$, *podemos escrever* $x = a_0 + a_1\zeta_3$ *com* $a_0, a_1 \in \mathbb{Z}[\zeta_{13}]$. *Também, do Teorema 5.7.1, temos que se* $x \in \mathcal{P}$, *então* $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) \equiv 0\ (mod\ 2 \cdot 39)$. *Assim,*

$$Tr_{\mathbb{K}|\mathbb{Q}(\zeta_{13})} = a_0\overleftarrow{a_0} + a_1\overline{a_1} + (a_0 - a_1)(\overline{a_0 - a_1}),$$

e assim, aplicando o $Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}$, *temos que*

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) &= Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(Tr_{\mathbb{K}|\mathbb{Q}(\zeta_{13})}(x\overline{x}) \\ &= Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}a_1\overline{a_0} + Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(a_1\overline{a_1}) + Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}[(a_0 - a_1)(\overline{a_0 - a_1})]. \end{aligned}$$

Assim, na soma, para que o valor $2 \cdot 39$ *seja atingido as únicas possibilidades são, a menos de ordem,* $Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}a_0\overline{a_0} = 12$, $Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(a_1\overline{a_1}) = 30$ *e* $Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}[(a_0 - a_1)(\overline{a_0 - a_1})] = 36$, *a menos de ordem. as possibilidades para* a_0 *e* a_1 *são*
$a_0 = \pm\zeta_{13}^{i_0}$, $i_0 = 0, \ldots, 12$;
$a_1 = \pm(\zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})$,
onde i_1, i_2, i_3, *são distintos dois a dois. Sejam* $a_0 = -\zeta_{13}^{i_0}$ *e* $a_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$. *Se* $i_0 \neq i_k$, *com* $k = 1, 2, 3$, *então* $Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}[(a_0 - a_1)(\overline{a_0 - a_1})] = 36$. *Se* $x \in \mathcal{P}$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(a_0\overline{a_0} + a_1\overline{a_1}) - (a_0 + a_1)(\overline{a_0 + a_1}) \in 3\mathbb{Z}[\zeta_{13}],$$

e portanto, se $y = (a_0 + a_1)(\overline{a_0 + a_1})$, $y \equiv 0\ (mod\ 3)$. *Seja* $\phi : \mathbb{Z}[\zeta_{13}] \to \mathbb{Z}$ *o homomorfismo de anéis definido por* $\phi\left(\sum_{i=0}^{11} b_i\zeta_{13}^i\right) = \sum_{i=0}^{11} b_i$. *Já que* $y \in 3\mathbb{Z}[\zeta_{13}]$, *segue que* $\phi(y) \equiv 0\ (mod\ 3)$. *Reescrevendo* y *substituindo* a_0 *e* a_1 *pelos valores fixados acima temos que*

$$y = (-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) = 4 - \alpha + \beta \equiv 0\ (mod\ 3\mathbb{Z}[\zeta_{13}]),$$

onde $\alpha = \sum_{j=1}^{3}(\zeta_{13}^{i_0 - i_j} + \zeta_{13}^{i_j - i_0})$ *e* $\beta = \sum_{j,l}^{3}\zeta_{13}^{i_l - i_j}$. *Fazendo* n_α *o número de expoentes tais que* $i_0 - i_j = -1$ *ou* $i_j - i_0 = -1$ *e* n_β *o número de expoentes tais que* $i_l - i_j = -1$, *segue que as possibilidades*

para n_α são 0 ou 1, uma vez que i_1, i_2, i_3 são disjuntos dois a dois. Agora, as possibilidades para n_β são 1, 0 ou 2. Note que $\phi(\zeta_{13}^{-1}) = \phi(-1-\zeta_{13}-\cdots-\zeta_{13}^{11}) = -12 \equiv 0 \ (mod\ 3)$. Assim, $\phi(\alpha) = 6 - n_\alpha$ e $\phi(\beta) = 6 - n_\beta$. Logo, $\phi(y) = 4 - \phi(\alpha) + \phi(\beta) \equiv 1 + n_\alpha - n_\beta \equiv 0 \ (mod\ 3\mathbb{Z}[\zeta_{13}])$ e as únicas soluções possíveis são

$$n_\alpha = 0 \text{ e } n_\beta = 1$$

$$ou$$

$$n_\alpha = 1 \text{ e } n_\beta = 2.$$

Suponha $n_\alpha = 0$ e $n_\beta = 1$. Dado $0 < c \leq 11$, por hipótese, o coeficiente de ζ_{13}^c é múltiplo de 3. Logo

$$\beta = \zeta_{13}^{-1} + \sum_{l,j}^{3} \zeta_{13}^{i_l - i_j}, \text{ com } i_l - i_j \neq -1.$$

Se existem l e j tais que $i_l - i_j = c$, então o coeficiente ζ_{13}^c na equação acima é nulo, pois $\zeta_{13}^{-1} = -1 - \zeta_{13} - \cdots - \zeta_{13}^{11}$. Desta forma, ζ_{13}^c aparece também com coeficiente nulo na expansão de α na base integral $\{1, \ldots, \zeta_{13}^{11}\}$. Se existem l e j tais que $i_l - i_j = c$, novamente ζ_{13}^c aparece com coeficiente nulo na decomposição de y. Assim, a única possibilidade é $c = 0$ e $y = 3$. Portanto, como

$$Tr_{\mathbb{K}|\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(a_0\overline{a_0} + a_1\overline{a_1}) - (a_0 + a_1)(\overline{a_0 + a_1}),$$

temos que $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(3(a_0\overline{a_0} + a_1\overline{a_1}) - (a_0 + a_1)(\overline{a_0 + a_1})) = 3Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(a_0\overline{a_0}) + 3Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}(a_1\overline{a_1}) - Tr_{\mathbb{Q}(\zeta_{13})|\mathbb{Q}}((a_0+a_1)(\overline{a_0 + a_1})) = 3\cdot 12 + 3\cdot 30 - 36 = 90$, e isto não pode ocorrer pois 90 não é múltiplo de $2\cdot 39$. Quando $n_\alpha = 1$ e $n_\beta = 2$ a verificação é feita de maneira análoga. Portanto, $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) \geq 4 \cdot 39 = 156$. O elemento $x = 1 - \zeta_{39}^3 - \zeta_{39}^1 3 + \zeta_{39}^{16} \in \mathcal{P}$ e observando que $\underline{x} = (1,0,0,-1,0,0,0,0,0,0,0,0,0,-1,0,0,1,0,0,0,0,0,0,0,0)$, pela Proposição 5.9.1, temos que $Tr_{\mathbb{K}|\mathbb{Q}}(x\overline{x}) = 156$. Portanto $\rho = \sqrt{39/2}$ e a densidade de centro é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{P})) = \frac{2^{12}\sqrt{39/2}^{24}}{3^{12}13^{12}} = 1,$$

que é a maior densidade conhecida para dimensão 20, que corresponde a densidade de centro do reticulado Λ_{24}.

5.10 Considerações finais do capítulo

Por fim, concluímos a dissertação apresentando neste capítulo com exemplos de reticulados com densidade de centro ótimas usando toda teoria desenvolvida ao logo deste trabalho. Construímos exemplos de reticulados algébricos com densidade de centro ótimas para as dimensões 2, 3, 4, 5, 6, 7, 8, 10, 12 e 24, através do homomorfismo canônico e via polinômios para as dimensões 2 e 3.

Conclusões

Este trabalho foi dedicado ao estudo de métodos para a construção de reticulados algébricos que possuem densidade de centro ótimas para determinadas dimensões. Para isto, inicialmente, abordamos os conceitos e resultados básicos necessários para o desenvolvimento do trabalho, módulos, anel de inteiros, traço, norma, anel de Dedekind, norma de ideais, discriminante e decomposição de ideais.

Em seguida, no Capítulo 2, desenvolvemos um estudo sobre o corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para os casos em que $n = p$, $n = p^r$ e n qualquer, onde p é um número primo e r um inteiro maior que 1, onde o objetivo foi determinar o anel de inteiros, uma base para o anel de inteiros e o discriminante desses corpos.

No capítulo seguinte, o foco foi os corpos de números abelianos de grau p, com p um número primo ímpar, dividindo o capítulo em três casos, de acordo com o condutor. Exibimos o elemento primitivo, uma base para o anel de inteiros, o valor do $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $0 \neq x \in \mathcal{O}_{\mathbb{K}}$, e caracterizamos os ideais primos acima do ideal $p_i\mathcal{O}_{\mathbb{K}}$. Esse capítulo do trabalho foi um dos principais, pois através da teoria desenvolvida nele, foi possível construir reticulados com densidade de centro ótimas para dimensões 3, 5 e 7.

O conceito principal do trabalho foi apresentado no Capítulo 4, os reticulados algébricos. Além de apresentar as principais propriedades de reticulados no $\mathbb{R}^n$ e os reticulados A_n, D_n, E_8, K_{12} e Λ_n, apresentamos resultados sobre reticulados algébricos via homomorfismo canônico, fazendo uma ligação entre reticulados e a teoria dos números, explicitando a formula de densidade de centro de reticulados algébricos obtidos por ideais de anéis de inteiros de corpos de números.

Finalmente, no último capítulo, chegamos de fato nas construções de reticulados algébricos, onde construímos exemplos de reticulados algébricos com densidade de centro ótimas, onde

foi utilizados dois métodos, o primeiro através do homomorfismo canônico e o segundo via polinômios.

Tais construções, tem implicações em outras áreas do conhecimento, especialmente na Teoria da Informação, quando se constrói codificadores de fonte baseados em reticulados algébricos, uma vez que existe relação entre a densidade de um empacotamento de esferas e a eficiência de um código corretor de erros.

Referências

[1] Alves, C. *Reticulados via corpos ciclotômicos*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2014.

[2] Andrade, A., Ferrari, A. J., Benedito, C., and Costa, S. I. R. Constructions of algebraic lattices. *Computational & Applied Mathematics 29*, 3 (2010), 493–505.

[3] Araujo, R. R. d. *Anéis de inteiros de corpos de números e aplicações*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2015.

[4] Benedito, C. W. d. O. *Famílias de reticulados algébricos e reticulados ideais*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2010.

[5] Boutros, J., Viterbo, E., Rastello, C., and Belfiore, J.-C. Good lattice constellations for both rayleigh fading and gaussian channels. *IEEE Transactions on Information Theory 42*, 2 (1996), 502–518.

[6] Chagas, A. C. M. M. *Uma contribuição a teoria dos números e reticulados*. Tese de doutorado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2015.

[7] Conway, J. H., and Sloane, N. J. A. *Sphere packings, lattices and groups*, vol. 290. Springer Science & Business Media, 2013.

[8] da Nóbrega Neto, T. P., Interlando, J. C., and Lopes, J. O. D. On computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$. *Journal of Number Theory 96*, 2 (2002), 319–325.

[9] da Nóbrega Neto, T. P., Interlando, J. C., Lopes, J. V. N., and Fores, A. L. Optimal families of two and three-dimensional lattice packings from polynomials with integer coefficients. *JP Journal of Algebra, Number Theory and Applications 15* (2009), 54–51.

[10] Dickson, L. E. *First course in the theory of equations*. J. Wiley & sons, Incorporated, 1922.

[11] Domingues, H. H., and Iezzi, G. *Álgebra moderna*. Atual, 1982.

[12] Endler, O. *Teoria dos números algébricos*, vol. 15. Instituto de Matemática Pura e Aplicada, CNPq, 1986.

[13] Fávaro, E. R. *Corpos cujo condutor é potência de primo: caracterização e reticulados ideais associados*. Tese de doutorado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2012.

[14] Ferrari, A. J. *Reticulados algébricos via corpos abelianos*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2008.

[15] Flores, A. L. *Representação geométrica de ideais de corpos de números*. Dissertação de mestrado, Imeec - Unicamp, Campinas - SP, 1996.

[16] Flores, A. L. *Reticulados em corpos abelianos*. Tese de doutorado, Feec –Unicamp, Campinas - SP, 2000.

[17] Flores, A. L., Interlando, J. C., da Nóbrega Neto, T. P., and Contiero, A. L. A new number field construction of the lattice E_8. *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry* (2013), 1–6.

[18] Interlando, J. C., Lopes, J. O. D., and NETO, T. P. D. N. The discriminant of abelian number fields. *Journal of Algebra and its Applications 5*, 01 (2006), 35–41.

[19] Johnston, H. Notes on galois modules. *Notes accompanying the course Galois Modules given in Cambridge in* (2011).

[20] Jorge, G. C., de Andrade, A. A., Costa, S. I., and Strapasson, J. E. Algebraic constructions of densest lattices. *Journal of Algebra 429* (2015), 218–235.

[21] Lang, S. *Algebra*. Addison-Wesley Publishing Company, 1972.

[22] Leopoldt, H.-W. Über die hauptordnung der ganzen elemente eines abelschen zahlkörpers. *Journal für die reine und angewandte Mathematik 201* (1959), 119–149.

[23] Lopes, J. O. D. The discriminant of subfields of $\mathbb{Q}(\zeta_{2^r})$. *Journal of Algebra and its Applications 2*, 04 (2003), 463–469.

[24] Marcus, D. *Numbers fields*. Springer-Verlag, 1977.

[25] nter Lettl, G. The ring of integers of an abelian number field. *J. reine angew. Math 404* (1990), 162–170.

[26] Nunes, J. V. L. *p-extensões galoisianas e aplicações*. Tese de doutorado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2015.

[27] Oliveira, E. L. d. *Construções de Reticulados via Extensoes Cıclicas de Grau Ímpar*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2011.

[28] Oliveira, E. L. d. *Torres de extensões abelianas de grau primo ímpar não ramificado*. Tese de doutorado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2015.

[29] Rayzaro, O. S. *Corpos abelianos com aplicações*. Dissertação de mestrado, Ibilce, UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto - SP, 2009.

[30] Ribenboim, P. *Classical theory of algebraic numbers*. Springer-Verlag, 2001.

[31] Samuel, P. *Algebraic theory of numbers*. Hermann, Paris, 1970.

[32] Stewart, I., and Tall, D. *Algebraic number theory*. Chapman & Hall, London, 1987.

[33] Washington, L. *Introduction to ciclotomic fields*. Springer-Verlag, 1982.