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

Instituto de Biociências, Letras e Ciências Exatas

Torres de Extensões Abelianas de grau primo ímpar não ramificado

Everton Luiz de Oliveira

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

Coorientador: Prof. Dr. José Carmelo Interlando

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - IBILCE / UNESP, como requisito parcial para obtenção do título de Doutor em Matemática.

São José do Rio Preto
Fevereiro - 2015

Everton Luiz de Oliveira

Torres de Extensões Abelianas de grau primo ímpar não ramificado

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

BANCA EXAMINADORA

Prof. Dr. Trajano Pires da Nóbrega Neto
Professor Adjunto
UNESP – São José do Rio Preto
Orientador

Prof. Dr. André Luiz Flores
Professor Adjunto
Universidade Federal de Alagoas

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

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

Prof. Dr. José Othon Dantas Lopes
Professor Associado
Universidade Federal do Ceará

São José do Rio Preto, 27 de fevereiro de 2015.

Luiz de Oliveira, Everton.
Torres de extensões abelianas de grau primo ímpar não ramificado / Everton Luiz de Oliveira. – São José do Rio Preto, 2015
63 f. : il.

Orientador: Trajano Pires da Nóbrega Neto
Coorientador: José Carmelo Interlando
Tese (doutorado) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas

1. Matemática. 2. Álgebra comutativa. 3. Teoria dos números. 4. Teoria dos reticulados. I. Nóbrega Neto, Trajano Pires da. II. Interlando, José Carmelo. III. Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas. IV. Título.

CDU – 512.71

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

Agradecimentos

Agradeço a todos que, direta ou indiretamente, contribuíram para o desenvolvimento deste trabalho, em especial:

Ao Professor Dr. Trajano Pires da Nóbrega Neto pela orientação, pela confiança depositada e pelo rico conhecimento compartilhado.

Ao Professor Dr. José Carmelo Interlando pela orientação, por seu interesse e envolvimento na pesquisa e pela imprescindível colaboração.

Aos professores membros da Banca Examinadora pelas valiosas sugestões na correção final do trabalho.

Ao Corpo Docente e amigos do Departamento de Matemática do IBILCE pela proximidade e humanidade nas relações cotidianas.

À Christina pela solicitude e companheirismo.

Aos amigos de estrada, de infância e de vida. Ao Janeiro Chuvoso.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, pelo apoio financeiro durante todo período de desenvolvimento deste trabalho.

Aos meus pais
Claudio e Cleide
e ao meu irmão Beto.

Resumo

Seja $\mathbb{L}/\mathbb{Q}$ uma extensão abeliana de grau primo ímpar p e condutor n, onde p é não ramificado em $\mathbb{L}$. Neste trabalho, explicitamos a forma traço integral $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)|_{\mathfrak{O}_{\mathbb{L}}}$ e obtemos algumas de suas propriedades, entre as quais determinamos o mínimo não nulo por ela assumido em uma classe de $\mathbb{Z}$-módulos do anel de inteiros $\mathfrak{O}_{\mathbb{L}}$. Estudamos o comportamento das torres obtidas através da composição dos corpos de números de grau p contidos em $\mathbb{Q}(\zeta_n)$ e, finalmente, descrevemos a forma traço integral do compósito de duas quaisquer dessas p-extensões, quando os respectivos condutores são relativamente primos.

Palavras-Chave: extensões abelianas, corpos ciclotômicos, forma traço integral, reticulados algébricos, corpo de gêneros.

Abstract

Let $\mathbb{L}/\mathbb{Q}$ be an abelian extension of odd prime degree p and conductor n, and assume that p is unramified in $\mathbb{L}/\mathbb{Q}$. In this work the integral trace form $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)|_{\mathfrak{O}_{\mathbb{L}}}$ is given explicitly and some of its properties are derived, in particular the determination of its nonzero minima in certain $\mathbb{Z}$-submodules of the ring of algebraic integers $\mathfrak{O}_{\mathbb{L}}$. An analysis of the field towers obtained as the composita of number fields of degree p, contained in $\mathbb{Q}(\zeta_n)$, is presented. Finally, the integral trace form of the compositum of any two of those p-extensions, when the respective conductors are relatively prime, is described as well.

Keywords: abelian extensions, cyclotomic fields, integral trace forms, algebraic lattices, genus field.

Índice de Símbolos

$\mathbb{N}$: conjunto dos números naturais
$\mathbb{Z}$: conjunto dos números inteiros
$\mathbb{Q}$: conjunto dos números racionais
$\mathbb{R}$: conjunto dos números reais
$\mathbb{C}$: conjunto dos números complexos
$\sum$: somatório
$\prod$: produtório
$\#B$: cardinalidade do conjunto B
$M = (a_{ij})$: matriz
$\det(M)$: determinante da matriz M
$a|b$: a divide b
$\text{mdc}(a, b)$: máximo divisor comum de a e b
$\text{mmc}(a, b)$: mínimo múltiplo comum de a e b
$a \equiv b \pmod{m}$: a congruente a b módulo m
$\text{ord}_m a$: ordem de a módulo m
$\phi(n)$: função de Euler aplicada a n
$\binom{s}{k}$: binomial de s sobre k
$Ker(f)$: núcleo da aplicação f
$Im(f)$: imagem da aplicação f
H, G: grupos
$\circ$(G): ordem do grupo G
H $\leq$ G: H é subgrupo de G
A, B: anéis

$A[x]$: anel de polinômios com coeficientes em A
AG: anel de grupo de G sobre A
$\mathfrak{a}$, $\mathfrak{p}$,$\mathfrak{P}$, ...: ideais
$A/\mathfrak{a}$: anel quociente
$\mathcal{M}, \mathcal{N}$: módulos
$\mathbb{F}$, $\mathbb{K}$, $\mathbb{L}$, $\mathbb{M}$, ...: corpos
$\mathbb{L}/\mathbb{K}$: extensão de corpos
$\mathbb{KL}$: compósito dos corpos $\mathbb{K}$ e $\mathbb{L}$
$[\mathbb{L} : \mathbb{K}]$: grau da extensão $\mathbb{L}/\mathbb{K}$
$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$: grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$: traço relativo do elemento α de $\mathbb{L}$
$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha)$: norma relativa do elemento α de $\mathbb{L}$
$\mathrm{N}(\mathfrak{a})$: norma do ideal $\mathfrak{a}$
$\mathfrak{O}_{\mathbb{K}}$: anel dos inteiros do corpo de números $\mathbb{K}$
$\mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n)$: discriminante de $(\alpha_1, \ldots, \alpha_n) \subset \mathbb{L}^n$
$\mathrm{Disc}(\mathbb{K})$: discriminante do corpo de números $\mathbb{K}$
$\mathbb{Z}/n\mathbb{Z}$: grupo das classes residuais módulo n
$(\mathbb{Z}/n\mathbb{Z})^*$: grupo das classes residuais invertíveis módulo n
ζ_n: raiz n-ésima primitiva da unidade
$\phi_n(x)$: n-ésimo polinômio ciclotômico
$\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico
$\mathrm{cond}(\mathbb{K})$: condutor do corpo $\mathbb{K}$
$\mathrm{H}(\mathbb{K})$: Corpo de Classes de Hilbert de $\mathbb{K}$
Λ: reticulado
$\mathcal{V}ol(\Lambda)$: volume do reticulado Λ
$\Delta(\Lambda)$: densidade de empacotamento do reticulado Λ
$\delta(\Lambda)$: densidade de centro de Λ
$\sigma_{\mathbb{K}}$: homomorfismo canônico
$\sigma_{\mathbb{K}}(\mathcal{M})$: reticulado algébrico

Sumário

Introdução

A descrição de reticulados algébricos densos via torres de corpos de números é assunto recorrente na Teoria Algébrica dos Números. Em 1964, Golod e Shafarevich [5] provaram que uma torre infinita de corpos totalmente complexos

$$\mathbb{Q} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}_3 \cdots \tag{1}$$

pode ser obtida por uma escolha adequada de $\mathbb{K}_1$, onde $\mathbb{K}_{i+1}$ é a extensão abeliana não ramificada maximal de $\mathbb{K}_i$, ou seja, é o Corpo de Classes de Hilbert $\mathrm{H}(\mathbb{K}_i)$. Alguns anos depois, Martinet [8] e Roquet [14] obtiveram reticulados utilizando torres como em (1). Martinet, por exemplo, define $\mathbb{K}_1 = \mathbb{K}(\sqrt{-q})$, onde $\mathbb{K}$ é um corpo totalmente real com $[\mathbb{K} : \mathbb{Q}] \geq 10$ e q é um primo totalmente decomposto em $\mathbb{K}$. Todos os reticulados apresentados nestas referências são imersões do anel de inteiros dos corpos que compõem essas torres e apresentam boa densidade; vide [2], 7.4. No entanto, apesar de provada sua existência, esses reticulados não são descritos explicitamente, visto que os parâmetros fundamentais desses corpos não são conhecidos, como a dimensão, base integral, o discriminante e a forma traço integral.

Seja $\mathbb{K}/\mathbb{Q}$ uma extensão galoisiana de grau m. A forma quadrática $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x})$, com $x \in \mathfrak{O}_{\mathbb{K}}$, é chamada de forma traço integral de $\mathbb{K}$. Quando $\mathbb{K}$ é totalmente real e $\{w_1, \ldots, w_m\}$ é uma base integral de $\mathbb{K}$, ela é dada por

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) = \sum_{i,j=1}^{m} a_i a_j \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_i w_j),$$

onde $x = a_1 w_1 + \ldots + a_n w_m \in \mathfrak{O}_{\mathbb{K}}$. O traço $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(w_i w_j)$, com $i, j = 1, \ldots, m$, é chamado de forma traço canônica de $\mathbb{K}$, com respeito à base $\{w_1, \ldots, w_m\}$.

Sejam $\mathcal{M} \subseteq \mathfrak{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto m e $\sigma_{\mathbb{K}}$ a imersão canônica de $\mathbb{K}$ em $\mathbb{R}^m$. O raio de empacotamento do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é obtido pelo mínimo da forma traço integral de $\mathbb{K}$ restrita aos elementos de $\mathcal{M}$. Este parâmetro nos permite calcular a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{M})$. Por outro lado, as entradas da matriz de Gram do reticulado $\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})$, associada à base $\{w_1, \ldots, w_m\}$, são dadas pela forma traço canônica de $\mathbb{K}$. Consequentemente, $\det(\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})) = \mathrm{Disc}(\mathbb{K})$, vide [2], pág. 225. Dada sua aplicabilidade, as formas traço canônica e integral são parâmetros de suma relevância. Conner and Perlis [1] apresentam um abrangente tratado sobre o assunto e Epkenhans [4] e Scharlau [16] contêm generalizações de alguns resultados obtidos em [1]. Nota-se, porém, que em raros casos estes parâmetros são descritos explicitamente.

Um corpo de números $\mathbb{L}$ de grau primo ímpar p será chamado de p-extensão. Quando $\mathbb{L}/\mathbb{Q}$ é abeliana, temos pelo Teorema de Kronecker-Weber que existe um inteiro positivo n tal que $\mathbb{L} \subset \mathbb{Q}(\zeta_n)$. Suponhamos que n é o condutor de $\mathbb{L}$ e que p não divide n. Nesse caso, o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ contém $(p^s - 1)/(p - 1)$ p-extensões, onde s é o número de primos na fatoração de n (veja a Seção 2.1), as quais são galoisianas, totalmente reais (vide Observação 1.1.1) e, para fins de contagem, serão denotadas por $\mathbb{L}_i$, com $1 \leq i \leq (p^s - 1)/(p - 1)$. Consideramos, então, as torres de compósitos de p-extensões da forma

$$\mathbb{Q} \subset \mathbb{L}_1 \subset \mathbb{L}_1\mathbb{L}_2 \subset \mathbb{L}_1\mathbb{L}_2\mathbb{L}_3 \subset \cdots \subset \mathbb{Q}(\zeta_n). \tag{2}$$

Na Seção 3.1 provamos que todas as torres assim definidas têm o mesmo topo (ou limite superior) e ele coincide com o Corpo de Gêneros, o qual denotamos por $\mathbb{L}^*$, e é o corpo de números abeliano maximal contendo $\mathbb{L}$, de modo que $\mathbb{L}^*/\mathbb{L}$ seja não ramificada, vide [19]. Em outras palavras, $\mathbb{L}^*$ é um subcorpo do Corpo de Classes de Hilbert $\mathrm{H}(\mathbb{L})$ tal que, quando $\mathrm{H}(\mathbb{L})$ é abeliano sobre $\mathbb{Q}$, temos $\mathbb{L}^* = \mathrm{H}(\mathbb{L})$.

Os conceitos preliminares utilizados neste trabalho são todos apresentados no primeiro capítulo. Abordamos os resultados fundamentais da Teoria de Galois e da Teoria Algébrica dos Números, de modo a tornar o texto auto suficiente nos capítulos subsequentes. Introduzimos conceitos básicos como traço, norma, discriminante, anel de inteiros e a decomposição de ideais; para tal, utilizamos basicamente as referências [3], [6], [13] e [15]. Na Seção 1.2 definimos reticulado algébrico via imersão canônica e descrevemos alguns de seus parâmetros, como volume, matriz de Gram e a densidade de centro; utilizamos principalmente as referências [2] e [15]. Os resultados obtidos na Seção 1.3 compõem uma demonstração alternativa para a recíproca do Teorema de Hilbert-Speiser, vide [11]. Em outras palavras, descrevemos uma base normal integral para os corpos de números abelianos, cujo condutor é ímpar livre de quadrados. Como

veremos, esse resultado é utilizado para descrever o anel de inteiros de qualquer corpo intermediário da torre de p-extensões (2), vide Proposição 2.1.2.

No segundo capítulo apresentamos os parâmetros e propriedades das p-extensões abelianas de condutor n. Existem dois casos a serem analisados. Neste trabalho, consideramos especialmente o caso em que p não divide n. Vemos, na Seção 2.1, que n é impar livre de quadrados e $\mathbb{Q}(\zeta_n)$ contém $(p-1)^{s-1}$ p-extensões de condutor n, as quais admitem uma base normal integral. Descrevemos explicitamente as formas traço canônica e integral dessas p-extensões e encontramos o mínimo da forma traço integral restrita a determinados $\mathbb{Z}$-módulos de posto p em $\mathfrak{O}_{\mathbb{L}}$. Desse modo, obtemos os reticulados algébricos via imersão canônica desses $\mathbb{Z}$-módulos em $\mathbb{R}^p$, nas dimensões $p = 3$, 5 e 7, os quais apresentam boa densidade de centro. Na Seção 2.4 apresentamos uma terminologia dos casos de ramificação, onde citamos os resultados já existentes na literatura quando n é múltiplo de p.

No terceiro capítulo são apresentadas as propriedades dos compósitos de p-extensões abelianas. Analisamos o comportamento das torres de p-extensões, através da contagem dos subcorpos de uma composição e da escolha dos condutores dos corpos que a definem. Garantimos, assim, a unicidade do Corpo de Gêneros e o representamos pelo compósito $\mathbb{L}^* = \mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_s$, de p-extensões linearmente disjuntas. Na Seção 3.2 descrevemos as formas traço canônica e integral de $\mathbb{L}_1\mathbb{L}_2$, quando $\mathbb{L}_1$ e $\mathbb{L}_2$ têm condutores relativamente primos. Nesse contexto, provamos que a forma traço canônica de $\mathbb{L}_1\mathbb{L}_2$ preserva o produto, o que também ocorre nos resultados já conhecidos sobre o anel de inteiros e o discriminante, a saber, $\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2} = \mathfrak{O}_{\mathbb{L}_1}\mathfrak{O}_{\mathbb{L}_2}$ e $\mathrm{Disc}(\mathbb{L}_1\mathbb{L}_2) = \mathrm{Disc}(\mathbb{L}_1)^{[\mathbb{L}_2:\mathbb{Q}]}\mathrm{Disc}(\mathbb{L}_2)^{[\mathbb{L}_1:\mathbb{Q}]}$, vide [6], pág.68. Desse modo, estendemos esses resultados e também obtemos a forma traço canônica do Corpo de Gêneros. Por fim, na Seção 3.3 apresentamos nossas perspectivas a partir dos resultados aqui obtidos, entre as quais a minimização da forma traço integral descrita no Corolário 3.2.4 e a investigação da formas traço do compósito de p-extensões, quando os respectivos condutores não são relativamente primos.

CAPÍTULO 1

Conceitos Preliminares

1.1 Teoria Algébrica dos Números

Nesta seção introduzimos os resultados fundamentais da Teoria de Galois e da Teoria Algébrica dos Números utilizados neste trabalho. São abordados conceitos como traço, norma, anel de inteiros e discriminante de um corpo de números e a decomposição de ideais. A prova de determinados resultados é omitida. Alguns por se tratarem de resultados clássicos e outros pela extensa demonstração. Todavia, inserimos a referência nos que seguem sem demonstração. Quando citado um anel, ele é comutativo e possui unidade.

Teoria de Galois

Sejam $\mathbb{K}, \mathbb{L}$ corpos tais que $\mathbb{K} \subseteq \mathbb{L}$. Dizemos que o corpo $\mathbb{L}$ é uma extensão de $\mathbb{K}$, ou ainda, que $\mathbb{L}/\mathbb{K}$ é uma extensão. O grau da extensão $\mathbb{L}/\mathbb{K}$ é a dimensão de $\mathbb{L}$ como espaço vetorial sobre $\mathbb{K}$, e o denotamos por $\dim_{\mathbb{K}} \mathbb{L} = [\mathbb{L} : \mathbb{K}]$. No caso em que $[\mathbb{L} : \mathbb{K}]$ é finito, dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão finita.

Definição 1.1.1. *Uma extensão finita $\mathbb{K}$ do corpo $\mathbb{Q}$ dos números racionais é chamada de corpo de números. Se $[\mathbb{K} : \mathbb{Q}] = n$, dizemos que $\mathbb{K}$ é um corpo de números de grau n. Um corpo de números de grau primo p será chamado de p-extensão.*

Sejam $\mathbb{L}/\mathbb{K}$ uma extensão e $\mathrm{Aut}(\mathbb{L})$ o grupo dos automorfismos de $\mathbb{L}$. O conjunto

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

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

Definição 1.1.2. *Uma extensão finita $\mathbb{L}/\mathbb{K}$ que satisfaz $[\mathbb{L} : \mathbb{K}] = \circ(\mathrm{Gal}(\mathbb{L}/\mathbb{K}))$ é chamada de extensão de Galois, ou galoisiana. Nesse caso, se $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ é abeliano, dizemos que $\mathbb{L}/\mathbb{K}$ é abeliana e se $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ é cíclico, dizemos que $\mathbb{L}/\mathbb{K}$ é cíclica.*

Teorema 1.1.3. *([17],Teo.12.1)(Teorema da Correspondência de Galois) Seja $\mathbb{L}/\mathbb{K}$ uma extensão galoisiana.*

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

(ii) Se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, então $\mathbb{L}/\mathbb{M}$ é galoisiana e $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ é o único subgrupo de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ que satisfaz

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

(iii) Se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, então $\mathbb{M}/\mathbb{K}$ é galoisiana se, e somente se, $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ é um subgrupo normal de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Nesse caso

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

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

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

de n-ésimo polinômio ciclotômico. O corpo $\mathbb{Q}(\zeta_n)$ é dito o n-ésimo corpo ciclotômico. Considere $(\mathbb{Z}/n\mathbb{Z})^*$ o grupo das classes residuais invertíveis módulo n. Temos que

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

Desse modo, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ via o isomorfismo natural $\sigma_i \mapsto \overline{i}$.

Teorema 1.1.4. *([13],pág.44) O grupo $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico se, e somente se, $n = 2$, 4, p^r ou $2p^r$, onde p é um primo ímpar e $r \geq 1$.*

Exemplo 1.1.1. *Se p é um primo ímpar, segue do Teorema 1.1.4 que o corpo ciclotômico $\mathbb{Q}(\zeta_p)$ é uma extensão cíclica de grau $p-1$ sobre $\mathbb{Q}$, cujo grupo de Galois é dado por* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{p-1}\}$, *onde $\sigma_i : \zeta_p \mapsto \zeta_p^i$, para $i = 1, \ldots, p-1$. Além disso, o p-ésimo polinômio ciclotômico é dado por*

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

Teorema 1.1.5. *([13], página 273)(Teorema de Kronecker-Weber) Se $\mathbb{K}/\mathbb{Q}$ é uma extensão abeliana finita, então existe uma raíz n-ésima da unidade ζ_n, tal que*

$$\mathbb{K} \subseteq \mathbb{Q}(\zeta_n).$$

Definição 1.1.6. *Seja $\mathbb{K}/\mathbb{Q}$ uma extensão abeliana finita. O menor inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado de condutor do corpo $\mathbb{K}$, e o denotamos por* $\mathrm{cond}(\mathbb{K}) = n$.

Se $\mathbb{L}/\mathbb{K}$ é uma extensão finita, então existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. O elemento α é chamado de elemento primitivo (Teorema do Elemento Primitivo, [15], pág. 34).

Proposição 1.1.7. *([15],pág.33) Se $\mathbb{L}/\mathbb{K}$ é uma extensão finita de grau n e $\mathbb{F}$ é um corpo algebricamente fechado contendo $\mathbb{K}$, então existem exatamente n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{F}$.*

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

Definição 1.1.8. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$.*

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

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

Observação 1.1.1. *Se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana de grau n, então os $\mathbb{Q}$-monomorfismos σ_i, com $i = 1, \ldots, n$, definidos na Proposição 1.1.7 compõem o grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$. Nesse caso, $\mathbb{K}$ será, necessariamente, totalmente real ou totalmente complexo, pois $\sigma_i(\mathbb{K}) = \mathbb{K}$, para todo $i = 1, \ldots, n$. Em particular, se n é ímpar então $\mathbb{K}$ é totalmente real, pois os monomorfismos complexos, quando existem, os são aos pares.*

Teorema 1.1.9. *([13],pág.20)(Lema de Dedekind) Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ num corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$. Então, $\{\sigma_1, \ldots, \sigma_n\}$ é linearmente independente sobre $\mathbb{F}$.*

Traço e norma

Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos de $\mathbb{L}$. Definimos o traço e a norma de um elemento $\alpha \in \mathbb{L}$, com respeito à extensão $\mathbb{L}/\mathbb{K}$, como sendo respectivamente

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

Seja $\mathbb{M}$ um corpo tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Se $a \in \mathbb{K}$, $\alpha, \beta \in \mathbb{L}$ e $\gamma \in \mathbb{M}$, então valem as seguintes propriedades:

1. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\beta)$
2. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a\alpha) = a \cdot \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$
3. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a) = n \cdot a$
4. $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha) \cdot \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\beta)$
5. $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n \cdot \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha)$
6. $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(a) = a^n$
7. $\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\gamma) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\gamma))$
8. $\mathrm{N}_{\mathbb{M}/\mathbb{K}}(\gamma) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathrm{N}_{\mathbb{M}/\mathbb{L}}(\gamma))$
9. $\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\alpha) = [\mathbb{M} : \mathbb{L}] \cdot \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$
10. $\mathrm{N}_{\mathbb{M}/\mathbb{K}}(\alpha) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(a)^{[\mathbb{M}:\mathbb{L}]}$.

Módulos

Seja A um anel. Um grupo abeliano aditivo $(\mathcal{M}, +)$ munido de um produto

$$\cdot : \mathrm{A} \times \mathcal{M} \to \mathcal{M}$$

é dito um A-módulo quando satisfaz as seguintes propriedades:

(i) $a \cdot (x + y) = a \cdot x + a \cdot y$;

(ii) $(a + b) \cdot x = a \cdot x + b \cdot x$;

(iii) $(ab) \cdot x = a \cdot (b \cdot x)$;

(iv) $1 \cdot x = x$;

para todo $a, b \in \mathrm{A}$ e $x, y \in \mathcal{M}$. Denotamos o produto $a \cdot x$ simplesmente por ax.

Um subgrupo $\mathcal{N}$ de $\mathcal{M}$ é chamado de um A-submódulo de $\mathcal{M}$, se para todo $a \in \mathrm{A}$ e $x \in \mathcal{N}$ tivermos $ax \in \mathcal{N}$.

Definição 1.1.10. *Seja $\mathcal{M}$ um* A*-módulo.*

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

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

Teorema 1.1.11. *([15],pág.21) Sejam* A *um anel principal, $\mathcal{M}$ um* A*-módulo livre de posto n e $\mathcal{N}$ um* A*-submódulo de $\mathcal{M}$. Então,*

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

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

Proposição 1.1.12. *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$ e $\mathcal{M} \subseteq \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n. Se $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, então $\det(\sigma_i(x_j))_{i,j=1}^n \neq 0$.*

Demonstração. Suponha $\det(\sigma_i(x_j))_{i,j=1}^n = 0$. Então as colunas da matriz $(\sigma_i(x_j))_{i,j=1}^n$ são linearmente dependentes. Assim, existem $a_1, \ldots, a_n \in \mathbb{C}$, não todos nulos, tais que $\sum_{i=1}^n a_i\sigma_i(x_j) = 0$, para todo $j = 1, \ldots, n$. Desse modo, teríamos $\sum_{i=1}^n a_i\sigma_i(x) = 0$, para todo $x \in M$, o que contradiz o Teorema 1.1.9 (Lema de Dedekind). □

Inteiros Algébricos

Sejam A $\subseteq$ B anéis. Dizemos que um elemento $\alpha \in$ B é inteiro sobre A se existe um polinômio mônico não nulo $f(x) \in$ A$[x]$ tal que $f(\alpha) = 0$, isto é, existem $a_0, \ldots, a_{n-1} \in A$ tais que

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

O conjunto dos elementos de B que são inteiros sobre A é um subanel de B, o qual denotamos por $\mathfrak{O}_{\mathrm{B}}$(A). Chamamos $\mathfrak{O}_{\mathrm{B}}$(A) de anel de inteiros de B sobre A. Se todo elemento de B é inteiro sobre A, dizemos que B é inteiro sobre A e, nesse caso, $\mathfrak{O}_{\mathrm{B}}$(A) = B.

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

Proposição 1.1.13. *([15],pág.38) Se $\mathbb{K}$ é um corpo de números e $\alpha \in \mathfrak{O}_{\mathbb{K}}$, então* $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ *e* $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ *são números inteiros.*

Teorema 1.1.14. *([15],pág.40) Sejam* A *um anel principal, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$. Nessas condições,*

(i) $\mathfrak{O}_{\mathbb{L}}$(A) *é um* A*-módulo livre de posto n.*

(ii) Se $\mathfrak{a}$ é um ideal não nulo de $\mathfrak{O}_{\mathbb{L}}$(A)*, então $\mathfrak{a}$ é um* A*-módulo livre de posto n.*

Se $\mathbb{K}$ é um corpo de números, então segue do Teorema 1.1.14 que $\mathfrak{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto finito. Nesse caso, uma $\mathbb{Z}$-base de $\mathfrak{O}_{\mathbb{K}}$ é dita uma base integral de $\mathbb{K}$.

Teorema 1.1.15. *([18],Teo.2.16) O conjunto*

$$\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}\}$$

é uma base integral de $\mathbb{Q}(\zeta_n)$, cujo anel de inteiros é dado por $\mathbb{Z}[\zeta_n]$.

Definição 1.1.16. *Seja $\mathbb{K}/\mathbb{Q}$ uma extensão galoisiana finita, com*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}.$$

Se existe $\alpha \in \mathfrak{O}_{\mathbb{K}}$ tal que $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ é uma base integral de $\mathbb{K}$, então ela é dita uma base normal integral de $\mathbb{K}$. O elemento α é dito um gerador dessa base.

Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{M} \subseteq \mathfrak{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. A cardinalidade do quociente $\mathfrak{O}_{\mathbb{K}}/\mathcal{M}$ é dita norma de $\mathcal{M}$, a qual denotamos por $[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}]$. Em particular, se $\mathfrak{a}$ é um ideal de $\mathfrak{O}_{\mathbb{K}}$, denotamos $\mathrm{N}(\mathfrak{a}) = [\mathfrak{O}_{\mathbb{K}} : \mathfrak{a}]$; vide Teorema 1.1.14.

Proposição 1.1.17. *([15], Seção 3.5) Se* $\{w_1, \ldots, w_n\}$ *é uma base integral de* $\mathbb{K}$ *e* $\{a_1 w_1, \ldots, a_n w_n\}$ *uma* $\mathbb{Z}$*-base de* $\mathcal{M}$*, onde* $a_1, \ldots, a_n$ *são inteiros não nulos, então* $[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}] = |a_1 \ldots a_n|$.

Discriminante

Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita de grau n e $(\alpha_1, \ldots, \alpha_n)$ uma n-upla de elementos em $\mathbb{L}$. Definimos o discriminante, em $\mathbb{L}/\mathbb{K}$, dessa n-upla por

$$\mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)),$$

isto é, o determinante da matriz cuja (i, j)-ésima entrada é $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)$, para $i, j = 1, \ldots, n$.

Proposição 1.1.18. *([15],pág.39) Se* $\sigma_1, \ldots, \sigma_n$ *são os* $\mathbb{K}$*-monomorfismos de* $\mathbb{L}$ *num corpo algebricamente fechado* $\mathbb{F}$*, contendo* $\mathbb{K}$*, então*

$$\mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = [\det(\sigma_i(\alpha_j))]^2.$$

Demonstração. Para cada $i, j = 1, \ldots, n$, temos que

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Desse modo,

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

□

Proposição 1.1.19. *([15],pág.38) Seja* $(\beta_1, \ldots, \beta_n)$ *uma n-upla de elementos em* $\mathbb{L}$*, tais que* $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$*, com* $a_{ij} \in \mathbb{K}$*, para* $j = 1, \ldots, n$*. Então*

$$\mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\beta_1, \ldots, \beta_n) = [\det(a_{ij})]^2 \mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n).$$

Demonstração. Se $\sigma_1, \ldots, \sigma_n$ são os $\mathbb{K}$-monomorfismos de $\mathbb{L}$, então

$$\begin{aligned} \mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\beta_1, \ldots, \beta_n) &= \det(\sigma_k(\beta_j))^2 \\ &= \det(\sigma_k(\sum_{i=1}^{n} a_{ij}\alpha_i))^2 \\ &= \det((a_{ij})(\sigma_k(\alpha_i)))^2 \\ &= \det(a_{ij})^2 \mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

□

Sejam $\mathbb{K}$ um corpo de números de grau n e $\{\alpha_1, \ldots, \alpha_n\}$ uma base integral de $\mathbb{K}$. Segue da Proposição 1.1.19 que um conjunto $\{\beta_1, \ldots, \beta_n\} \subset \mathbb{K}$ também é uma base integral de $\mathbb{K}$ se, e somente se,

$$\mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n).$$

Definição 1.1.20. *Seja $\mathbb{K}$ um corpo de números. O discriminante, em $\mathbb{K}/\mathbb{Q}$, de qualquer base integral de $\mathbb{K}$ é chamado de discriminante do corpo $\mathbb{K}$, e denotado por* $\mathrm{Disc}(\mathbb{K})$.

Proposição 1.1.21. *([12]) Seja $\mathbb{K}$ um corpo de números abeliano de grau primo p e condutor m. Então,*

$$|\mathrm{Disc}(\mathbb{K})| = m^{p-1}.$$

Teorema 1.1.22. *([12]) Seja $\mathbb{K}$ um corpo de números abeliano de condutor $m = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$. Então,*

$$|\mathrm{Disc}(\mathbb{K})| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{s} p_i^{\sum_{k=1}^{a_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^k}) : \mathbb{Q}]}}.$$

Observação 1.1.2. *Note que,*

$$\sum_{k=1}^{a_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^k}) : \mathbb{Q}] < a_i [\mathbb{K} : \mathbb{Q}],$$

para todo $i = 1, \ldots, s$. Logo,

$$|\mathrm{Disc}(\mathbb{K})| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s},$$

onde

$$\alpha_i = a_i [\mathbb{K} : \mathbb{Q}] - \sum_{k=1}^{a_i} [\mathbb{K} \cap \mathbb{Q}(\zeta_{m/p_i^k}) : \mathbb{Q}] > 0.$$

Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos de números de grau n_1 e n_2, respectivamente. Dizemos que $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos quando $[\mathbb{K}_1\mathbb{K}_2 : \mathbb{Q}] = n_1 n_2$. Quando $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos e seus discriminantes relativamente primos, eles são ditos linearmente disjuntos.

Observação 1.1.3. *Se $\mathbb{K}_1/\mathbb{Q}$ e $\mathbb{K}_2/\mathbb{Q}$ são extensões galoisianas, segue pelo Teorema da Correspondência de Galois que $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos se, e somente se, $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$.*

Proposição 1.1.23. *([6], página 68) Se $\mathbb{K}_1$ e $\mathbb{K}_2$ são corpos de números linearmente disjuntos, de grau n_1 e n_2, respectivamente, então*

(i) $\mathfrak{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathfrak{O}_{\mathbb{K}_1}\mathfrak{O}_{\mathbb{K}_2}$.

(ii) $\mathrm{Disc}(\mathbb{K}_1\mathbb{K}_2) = \mathrm{Disc}(\mathbb{K}_1)^{n_2}\mathrm{Disc}(\mathbb{K}_2)^{n_1}$.

Decomposição de Ideais

Sejam $\mathbb{K}$ um corpo de números e $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$. Se $\mathfrak{p}$ é um ideal primo não-nulo de $\mathfrak{O}_{\mathbb{K}}$, então o ideal $\mathfrak{p}\mathfrak{O}_{\mathbb{L}}$ de $\mathfrak{O}_{\mathbb{L}}$ pode ser unicamente expresso na forma

$$\mathfrak{p}\mathfrak{O}_{\mathbb{L}} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i},$$

onde cada $\mathfrak{P}_i$ é um ideal primo de $\mathfrak{O}_{\mathbb{L}}$ e e_i é um inteiro positivo, para $i = 1, \ldots, r$, com $r > 0$. Os ideais $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os únicos ideais primos de $\mathfrak{O}_{\mathbb{L}}$ tais que $\mathfrak{P}_i \cap \mathfrak{O}_{\mathbb{K}} = \mathfrak{p}$. Além disso, $\mathfrak{p}\mathfrak{O}_{\mathbb{L}} \cap \mathfrak{O}_{\mathbb{K}} = \mathfrak{p}$. Nesse caso dizemos que $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os ideais de $\mathfrak{O}_{\mathbb{L}}$ que estão acima de $\mathfrak{p}$. Vide Samuel, [15], páginas 50 e 71.

Temos que $\mathfrak{p}$ e $\mathfrak{P}_i$ são ideais maximais de $\mathfrak{O}_{\mathbb{K}}$ e $\mathfrak{O}_{\mathbb{L}}$, respectivamente. Dessa forma, o corpo $\mathfrak{O}_{\mathbb{L}}/\mathfrak{P}_i$ pode ser considerado como uma extensão finita do corpo $\mathfrak{O}_{\mathbb{K}}/\mathfrak{p}$, para cada $i = 1, \ldots, r$. Vide [3], pág. 103.

Definição 1.1.24. *O grau* $[\mathfrak{O}_{\mathbb{L}}/\mathfrak{P}_i : \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}]$ *é chamado de grau de inércia de* $\mathfrak{P}_i$ *e é denotado por* $f_i = f(\mathfrak{P}_i \mid \mathfrak{p})$. *O expoente* $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ *é chamado de índice de ramificação de* $\mathfrak{P}_i$, *para cada* $i = 1, \ldots, r$.

Definição 1.1.25. *Quando pelo menos um dos índices de ramificação* e_i *é maior do que um, dizemos que* $\mathfrak{p}$ *se ramifica, ou é ramificado, em* $\mathbb{L}$.

Dizemos que $\mathbb{L}/\mathbb{K}$ é não ramificada quando todos ideais primos de $\mathfrak{O}_{\mathbb{K}}$ são não ramificados em $\mathbb{L}$. A extensão abeliana não ramificada maximal sobre $\mathbb{K}$ é chamada de Corpo de Classes de Hilbert de $\mathbb{K}$, o qual denotamos por H($\mathbb{K}$); vide [7], pág. 232.

Teorema 1.1.26. *([3],pág.104)(Teorema da Igualdade Fundamental)*

$$\sum_{i=1}^{r} e_i f_i = [\mathfrak{O}_{\mathbb{L}}/\mathfrak{p}\mathfrak{O}_{\mathbb{L}} : \mathfrak{O}_{\mathbb{K}}/\mathfrak{p}] = n.$$

Utilizando a Igualdade Fundamental podemos estimar as várias possibilidades de decomposição do ideal $\mathfrak{p}$ em $\mathfrak{O}_{\mathbb{L}}$. No que segue, damos nomes aos casos extremos. Dizemos que $\mathfrak{p}$ é:

(a) Totalmente decomposto em $\mathbb{L}$, quando $r = n$, ou seja, $e_i = f_i = 1$, para todo $i = 1, \ldots, r$.

(c) Totalmente ramificado em $\mathbb{L}$, quando $e_i = n$ para algum $i = 1, \ldots, r$, nesse caso, $r = f_i = 1$.

(b) Inerte em $\mathbb{L}$, quando $f_i = n$ para algum $i = 1, \ldots, r$, isto é, $r = e_i = 1$.

Quando $\mathbb{L}/\mathbb{K}$ é galoisiana, temos que $e(\mathfrak{P}_1 \mid \mathfrak{p}) = \ldots = e(\mathfrak{P}_r \mid \mathfrak{p})$ e $f(\mathfrak{P}_1 \mid \mathfrak{p}) = \ldots = f(\mathfrak{P}_r \mid \mathfrak{p})$; vide [3], Teorema (20.2). Denotamos, então, $e = e(\mathfrak{P}_i \mid \mathfrak{p})$ e $f = f(\mathfrak{P}_i \mid \mathfrak{p})$, para todo $i = 1, \ldots, r$. E, nesse caso, a Igualdade Fundamental é dada por

$$efr = n.$$

Desse modo, quando n é primo, os três casos extremos de decomposição de $\mathfrak{p}$ em $\mathfrak{O}_{\mathbb{L}}$ serão os únicos possíveis.

A seguinte proposição apresenta a multiplicatividade do índice de ramificação e do grau de inércia, resultado fundamental no estudo da decomposição de ideais em torres de corpos de números.

Proposição 1.1.27. *([7],pág.65) Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ corpos de números e $\mathfrak{p}$, $\mathfrak{P}$ e $\mathfrak{P}'$ ideais primos de $\mathfrak{O}_{\mathbb{K}}$, $\mathfrak{O}_{\mathbb{L}}$ e $\mathfrak{O}_{\mathbb{M}}$, respectivamente. Se $\mathfrak{P}'$ está acima de $\mathfrak{P}$, então*

(i) $\mathfrak{P}$ está acima de $\mathfrak{p}$ se, e somente se, $\mathfrak{P}'$ está acima de $\mathfrak{p}$.

(ii) Nesse caso, $e(\mathfrak{P}' \mid \mathfrak{p}) = e(\mathfrak{P}' \mid \mathfrak{P}) \cdot e(\mathfrak{P} \mid \mathfrak{p})$ e $f(\mathfrak{P}' \mid \mathfrak{p}) = f(\mathfrak{P}' \mid \mathfrak{P}) \cdot f(\mathfrak{P} \mid \mathfrak{p})$.

Quando $\mathbb{K} = \mathbb{Q}$, temos que $\mathfrak{O}_{\mathbb{K}} = \mathbb{Z}$ e $\mathbb{L}$ é um corpo de números de grau n. Nesse caso, se um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ ramifica em $\mathbb{L}$, dizemos que o número primo p ramifica em $\mathbb{L}$.

Teorema 1.1.28. *([15],pág.74) Seja $\mathbb{L}$ um corpo de números. Um número primo p ramifica em $\mathbb{L}$ se, e somente se, p divide o discriminante* Disc($\mathbb{L}$).

Se $\mathbb{L}$ é um corpo de números abeliano de condutor m, então, segue do Teorema 1.1.22, que os primos que dividem m são exatamente os mesmos que dividem o discriminante Disc($\mathbb{L}$).

Corolário 1.1.29. *Seja $\mathbb{L}$ um corpo de números abeliano de condutor m. Um número primo p ramifica em $\mathbb{L}$ se, e somente se, p divide m.*

Sejam $m > 1$ e p um primo não ramificado em $\mathbb{Q}(\zeta_m)$, isto é, p não divide m. Como $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ é galoisiana, segue que $e = e(\mathfrak{P}_i \mid p) = 1$ e $f = f(\mathfrak{P}_i \mid p)$, para todo $i = 1, \ldots, r$, onde $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os ideais de $\mathfrak{O}_{\mathbb{Q}(\zeta_m)}$ que estão acima de p. Nesse caso, a Igualdade Fundamental se escreve como

$$fr = \phi(m),$$

e além disso:

Teorema 1.1.30. *([3],pág.119) Com as notações acima, temos que*

$$r = \frac{\phi(m)}{f},$$

onde f é a ordem de $\overline{p}$ no grupo multiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$.

Corolário 1.1.31. *Seja $\mathbb{L}$ um corpo de números abeliano de grau primo p e condutor m. Se $\mathrm{ord}_m p = 1$, ou seja $p \equiv 1 \pmod{m}$, então p é totalmente decomposto em $\mathbb{L}$. Agora, se $\mathrm{ord}_m p = \phi(m)$, então p é inerte em $\mathbb{L}$.*

Demonstração. Segue do Teorema 1.1.30 e da Proposição 1.1.27. □

1.2 Reticulados Algébricos

Apresentamos o conceito de reticulado no $\mathbb{R}^n$ e alguns de seus parâmetros, como volume, matriz de Gram e densidade de centro. Identificamos um $\mathbb{Z}$-módulo livre de posto finito contido num corpo de números $\mathbb{K}$ com um reticulado no $\mathbb{R}^n$, o qual chamamos de reticulado algébrico. Essa imersão nos permite descrever algumas propriedades do reticulado obtido, através das propriedades do corpo $\mathbb{K}$.

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

Sejam n um inteiro positivo e $\{v_1, \ldots, v_m\}$ um conjunto de vetores no $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. Definimos o reticulado Λ de dimensão m e base $\{v_i\}_{i=1}^m$ como sendo o conjunto

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

Em outras palavras, um reticulado é um $\mathbb{Z}$-módulo livre de posto finito contido no $\mathbb{R}^n$, cuja base é linearmente independente sobre $\mathbb{R}$. Denotamos também $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$.

Consideramos, nesta seção, somente os reticulados no $\mathbb{R}^n$ cuja base apresenta n vetores, ou seja, os reticulados n-dimensionais no $\mathbb{R}^n$.

Proposição 1.2.1. *Sejam $\{v_1, \ldots, v_n\}$ uma base de Λ e $\{w_1, \ldots, w_n\} \subset \Lambda$ um conjunto de vetores linearmente independentes sobre $\mathbb{R}$, tais que $w_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Tem-se que $\{w_i\}_{i=1}^n$ é uma base de Λ se, e somente se, $\det(a_{ij}) = \pm 1$.*

Demonstração. Como

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

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

Seja $\beta = \{v_1, \ldots, v_n\}$ uma base de Λ. Dizemos que a matriz $M = (v_{ij})$ é geradora do reticulado Λ, onde $v_i = (v_{i1}, \ldots, v_{in}) \in \mathbb{R}^n$, para $i = 1, \ldots, n$. Nesse caso, denotamos $\Lambda = \{\alpha M;\ \alpha \in \mathbb{Z}^n\}$. O conjunto

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

é chamado de região fundamental de Λ com relação à base β. Definimos o volume da região fundamental $\mathcal{P}_\beta$ por

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

Sejam $\{w_1, \ldots, w_n\} \subset \mathbb{R}^n$ uma outra base de Λ e $N = (w_{ij})$ a matriz geradora de Λ associada a essa base. Pela Proposição 1.2.1, temos que $|\det(M)| = |\det(N)|$ e, consequentemente, $\det(MM^t) = \det(NN^t)$. Isto permite as seguintes definições:

Definição 1.2.2. *Seja β uma base de Λ. Definimos o volume do reticulado Λ como sendo o volume da região fundamental $\mathcal{V}ol(\mathcal{P}_\beta)$, o qual denotamos por $\mathcal{V}ol(\Lambda)$.*

Seja M uma matriz geradora de Λ. Definimos a matriz de Gram de Λ, associada a M, como sendo a matriz

$$G = MM^t.$$

Definição 1.2.3. *Seja G uma matriz de Gram do reticulado Λ. Definimos o determinante de Λ como sendo o determinante de G, e o denotamos por* $\det(\Lambda)$.

Um empacotamento esférico do reticulado Λ é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$, cujos centros são os elementos de Λ, de modo que a intersecção de quaisquer duas esferas tenha no máximo um ponto. O maior raio para o qual é possível definir um empacotamento de Λ é obtido pelo número

$$\rho = \frac{\min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\}}{2},$$

chamado raio de empacotamento de Λ.

A densidade de empacotamento $\Delta(\Lambda)$ de Λ é a proporção do espaço $\mathbb{R}^n$ recoberto pelo empacotamento de esferas de raio ρ. Equivalentemente, se $\mathcal{B}(\rho)$ é a esfera de centro na origem e raio ρ, temos que

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(\rho))}{\mathcal{V}ol(\mathcal{P}_\beta)} = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Definição 1.2.4. *Definimos a densidade de centro $\delta(\Lambda)$ do reticulado Λ como sendo*

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

Exemplo 1.2.1. *Seja Λ o reticulado no $\mathbb{R}^2$ gerado pela base $\{(1,0),(1/2,\sqrt{3}/2)\}$, isto é,*

$$\Lambda = \mathbb{Z}(1,0) + \mathbb{Z}(1/2,\sqrt{3}/2).$$

Temos que $\min\{|\lambda|;\ \lambda \in \Lambda,\ \lambda \neq 0\} = 1$. Logo, $\rho = 1/2$ é o maior raio para o qual é possível obter um empacotamento de Λ. Por outro lado,

$$\mathcal{V}ol(\Lambda) = \left|\det \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}\right| = \sqrt{3}/2.$$

Portanto,

$$\Delta(\Lambda) = \frac{\pi}{\sqrt{12}} \simeq 0,9069 \quad e$$

$$\delta(\Lambda) = \frac{1}{\sqrt{12}} \simeq 0,2886751.$$

Este reticulado é conhecido como A_2 ou reticulado hexagonal e tem a maior densidade de centro no $\mathbb{R}^2$; vide [2], seções 1.2 e 1.4.

1.2.2 Reticulados Algébricos via Homomorfismo Canônico

Seja $\mathbb{K}$ um corpo de números de grau n. Existem exatamente n $\mathbb{Q}$-monomorfismos $\sigma_i : \mathbb{K} \to \mathbb{C}$, com $i = 1,\ldots,n$ (vide Proposição 1.1.7). Se σ_j é um monomorfismo complexo, o seu conjugado $\overline{\sigma}_j$ também pertence ao conjunto dos n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde $\overline{\sigma}_j \neq \sigma_j$. Desse modo, temos um número par de monomorfismos complexos. Assim, denotando por r_1 o número de monomorfismos reais e por $2r_2$ o número de monomorfismos complexos, podemos reordená-los de modo que $\sigma_1,\ldots,\sigma_{r_1}$ sejam reais e $\sigma_{r_1+1},\ldots,\sigma_{r_1+2r_2}$ sejam complexos, com $n = r_1 + 2r_2$ e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1,\ldots,r_2$.

O homomorfismo injetivo $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por

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

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

Exemplo 1.2.2. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_3)$, onde $\zeta_3 = e^{\frac{2\pi i}{3}}$. Os $\mathbb{Q}$-monomorfismos σ_1 e σ_2 de $\mathbb{K}$ em $\mathbb{C}$, são dados por $\sigma_i(\zeta_3) = \zeta_3^i$, com $i = 1, 2$. Desse modo, $\mathbb{K}$ é totalmente complexo, com $r_1 = 0$ e $r_2 = 1$. Se $x = a + b\zeta_3 \in \mathbb{K}$, então $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^2$ é dado por*

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

Teorema 1.2.5. *([15],pág.56) Se $\mathcal{M} \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, então $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado no $\mathbb{R}^n$, com base $\{\sigma_{\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{K}}(x_n)\}$ e volume dado por*

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

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

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

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 convenientemente, obtemos

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

Pela Proposição 1.1.12, temos 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 $\mathbb{R}$. Isto é,

$$\sigma_{\mathbb{K}}(\mathcal{M}) = \mathbb{Z}\sigma_{\mathbb{K}}(x_1) + \ldots + \mathbb{Z}\sigma_{\mathbb{K}}(x_n)$$

é um reticulado no $\mathbb{R}^n$, do qual M^t é uma matriz geradora, e

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

□

Corolário 1.2.6. *([15],pág.57) Seja $\mathcal{M} \subseteq \mathfrak{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. Então $\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{M})$ são reticulados no $\mathbb{R}^n$, cujos volumes são, respectivamente,*

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})) = 2^{-r_2} |\mathrm{Disc}(\mathbb{K})|^{\frac{1}{2}} \quad e \quad \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{M})) = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}}))[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}].$$

Demonstração. Pelo Teorema 1.2.5, temos que $\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{M})$ são reticulados no $\mathbb{R}^n$ e, dada uma base integral $\{x_1, \ldots, x_n\}$ de $\mathbb{K}$, segue que

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

pois $\mathrm{Disc}(\mathbb{K}) = \det(\sigma_i(x_j))^2$. Pelo Teorema 1.1.11, existem uma base integral $\{w_1, \ldots, w_n\}$ de $\mathbb{K}$ e inteiros não-nulos $a_1, \ldots, a_n$, tais que $\{a_1w_1, \ldots, a_nw_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$. Logo,

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

Porém, pela Proposição 1.1.17, temos que $[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}] = |a_1 \ldots a_n|$. Portanto,

$$\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{M})) = 2^{-r_2}|\mathrm{Disc}(\mathbb{K})|^{\frac{1}{2}}[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}] = \mathcal{V}ol(\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}}))[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}].$$

□

Seja $\mathcal{M} \subseteq \mathfrak{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. Segue do Corolário 1.2.6 que a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{M})) = \frac{2^{r_2}\rho^n}{|\mathrm{Disc}(\mathbb{K})|^{\frac{1}{2}}[\mathfrak{O}_{\mathbb{K}} : \mathcal{M}]}, \tag{1.1}$$

onde $\rho = \frac{1}{2}\min\{|\sigma_{\mathbb{K}}(x)|;\ x \in \mathcal{M},\ x \neq 0\}$ e

$$|\sigma_{\mathbb{K}}(x)|^2 = \begin{cases} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2)\ , & \text{se } \mathbb{K} \text{ é totalmente real;} \\ \frac{1}{2}\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x})\ , & \text{se } \mathbb{K} \text{ é totalmente imaginário.} \end{cases}$$

Vide [2], pág. 225. Note que se $\mathbb{K}/\mathbb{Q}$ é galoisiana então $\mathbb{K}$ é, necessariamente, totalmente real ou totalmente imaginário. Em particular, quando n é impar temos que $\mathbb{K}$ é totalmente real; vide Observação 1.1.1.

Observação 1.2.1. *Sejam $\mathbb{K}$ totalmente real e $\{w_1, \ldots, w_n\}$ uma base integral de $\mathbb{K}$. A matriz $(\sigma_i(w_j))_{i,j=1}^n$ é geradora do reticulado algébrico $\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})$. Desse modo, a matriz de Gram associada é dada pela forma traço canônica de $\mathbb{K}$, com respeito a essa base, isto é,*

$$G = (\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(w_iw_j))_{i,j=1}^n.$$

Nesse caso, o determinante $\det(\sigma_{\mathbb{K}}(\mathfrak{O}_{\mathbb{K}})) = \mathrm{Disc}(\mathbb{K})$.

1.3 Base Normal Integral de uma Extensão Abeliana

Nesta seção descrevemos uma base normal integral para os corpos de números abelianos contidos em $\mathbb{Q}(\zeta_n)$, quando n é um inteiro positivo ímpar livre de quadrados, ou seja, $n = p_1 \dots p_s$, onde $p_1, \dots, p_s$ são primos ímpares distintos. Em particular, tais condições são satisfeitas pelo condutor de uma p-extensão abeliana $\mathbb{L}$, quando p é um primo ímpar não ramificado, vide Proposição 2.1.2. Isto garante a existência de uma base normal integral para $\mathbb{L}$, com a qual geramos o anel de inteiros $\mathfrak{O}_{\mathbb{L}}$ na Seção 2.2.

Proposição 1.3.1. *Se n é um inteiro positivo ímpar livre de quadrados, então*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = (-1)^s.$$

Demonstração. Temos que $n = p_1 \dots p_s$, onde $p_1, \dots, p_s$ são primos ímpares distintos. Faremos a prova por indução sobre s. O caso $s = 1$ segue do fato de que $x^{p_1-1} + x^{p_1-2} + \cdots + 1$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}$. Suponha agora que a asserção seja verdadeira para $q = p_1 \dots p_{s-1}$. Afirmamos que ela é verdadeira para $n = qp_s$. De fato,

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{qp_s}) &= \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_q)}(\zeta_q\zeta_{p_s})) = \mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_q)}(\zeta_{p_s})) \\ &= (-1)\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q) = (-1)^s. \end{aligned}$$

□

Proposição 1.3.2. *Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_n)$ e $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então $\mathbb{K} = \mathbb{Q}(t)$.*

Demonstração. É claro que $\mathbb{Q}(t) \subseteq \mathbb{K}$. Então, pela Proposição 1.3.1, segue que

$$\begin{aligned} (-1)^s = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) &= \mathrm{Tr}_{\mathbb{Q}(t)/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}(t)}(\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n))) = \mathrm{Tr}_{\mathbb{Q}(t)/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}(t)}(t)) \\ &= \mathrm{Tr}_{\mathbb{Q}(t)/\mathbb{Q}}([\mathbb{K} : \mathbb{Q}(t)]t) = [\mathbb{K} : \mathbb{Q}(t)]\mathrm{Tr}_{\mathbb{Q}(t)/\mathbb{Q}}(t). \end{aligned}$$

Porém, $[\mathbb{K} : \mathbb{Q}(t)]$ e $\mathrm{Tr}_{\mathbb{Q}(t)/\mathbb{Q}}(t)$ são inteiros. Logo, $[\mathbb{K} : \mathbb{Q}(t)] = 1$. □

O Teorema 1.1.15 apresenta uma base integral de $\mathbb{Q}(\zeta_n)$. Alternativamente, no seguinte lema descrevemos uma base normal integral de $\mathbb{Q}(\zeta_n)$.

Lema 1.3.3. *O conjunto*

$$\{\zeta_n^i \ ; \ i = 1, \dots, n, \ \mathrm{mdc}(i, n) = 1\}$$

é uma base normal integral do corpo ciclotômico $\mathbb{Q}(\zeta_n)$.

Demonstração. Por indução sobre s. Quando $s = 1$, temos que ζ_{p_1} é raiz do polinômio minimal $x^{p_1-1} + x^{p_1-2} + \cdots + 1$ e $\{1, \zeta_{p_1}, \ldots, \zeta_{p_1}^{p-2}\}$ é uma base integral de $\mathbb{Q}(\zeta_{p_1})$. Logo, $\{\zeta_{p_1}, \zeta_{p_1}^2, \ldots, \zeta_{p_1}^{p-1}\}$ também o é. Suponhamos, agora, que

$$\{\zeta_{n/p_s}^i \ ; \ i = 1, \ldots, n/p_s, \ \text{mdc}(i, n/p_s) = 1\}$$

seja uma base integral de $\mathbb{Q}(\zeta_{n/p_s})$. Como $\mathbb{Q}(\zeta_{n/p_s})$ e $\mathbb{Q}(\zeta_{p_s})$ são linearmente disjuntos e $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/p_s})\mathbb{Q}(\zeta_{p_s})$, então uma base integral de $\mathbb{Q}(\zeta_n)$ é dada por

$$\mathcal{B} = \{\zeta_{n/p_s}^i \zeta_{p_s}^j \ ; \ i = 1, \ldots, n/p_s, \ j = 1, \ldots, p_s - 1, \ \text{mdc}(i, n/p_s) = 1\}.$$

Note que, $\zeta_{n/p_s}^i \zeta_{p_s}^j = \zeta_n^{ip_s} \zeta_n^{j\frac{n}{p_s}} = \zeta_n^{ip_s + j\frac{n}{p_s}}$. Porém, $\text{mdc}(ip_s + j\frac{n}{p_s}, n) = 1$ e $\mathcal{B}$ tem cardinalidade $\phi(\frac{n}{p_s})\phi(p_s) = \phi(n)$, pois $ip_s + j\frac{n}{p_s} \equiv i'p_s + j'\frac{n}{p_s} \pmod{n}$ implica $i = i'$ e $j = j'$. Portanto, $\mathcal{B} = \{\zeta_n^i \ ; \ i = 1, \ldots, n, \ \text{mdc}(i, n) = 1\}$. □

Teorema 1.3.4. *Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_n)$, $[\mathbb{K} : \mathbb{Q}] = r$ e $\text{Gal}(\mathbb{K}/\mathbb{Q}) = \{\theta_1, \ldots, \theta_r\}$, então*

$$\{\theta_1(t), \ldots, \theta_r(t)\}$$

é uma base normal integral de $\mathbb{K}$, cujo gerador é $t = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$.

Demonstração. Temos que $\theta_i = \sigma_{u_i}|_{\mathbb{L}}$, para cada $i = 1, \ldots, r$, onde $\sigma_{u_i} \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Seja, então, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}) = \{\sigma_{v_j} \ ; \ j = 1, \ldots, q\}$ onde $q = \phi(n)/r$. Logo,

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_{u_i} \circ \sigma_{v_j} \ ; \ i = 1, \ldots, r, j = 1, \ldots, q\}.$$

De fato, se $\sigma_{u_{i_1}} \circ \sigma_{v_{j_1}} = \sigma_{u_{i_2}} \circ \sigma_{v_{j_2}}$, então $\sigma_{u_{i_1}}^{-1} \circ \sigma_{u_{i_2}} = \sigma_{v_{j_1}} \circ \sigma_{v_{j_2}}^{-1} \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$, o que implica $\sigma_{u_{i_1}}^{-1} \circ \sigma_{u_{i_2}}|_{\mathbb{K}} = Id$, isto é, $\sigma_{u_{i_1}}|_{\mathbb{K}} = \sigma_{u_{i_2}}|_{\mathbb{K}}$ donde $i_1 = i_2$. Assim, também $j_1 = j_2$.

Seja $x \in \mathfrak{O}_{\mathbb{K}}$. É claro que $x \in \mathfrak{O}_{\mathbb{Q}(\zeta_n)}$. Assim, do Lema 1.3.3 temos que

$$\begin{aligned} x &= \sum_{\substack{k=1 \\ (k,n)=1}}^{n} a_k \zeta_n^k \\ &= \sum_{i=1}^{r} \sum_{j=1}^{q} a_{u_i,v_j} (\sigma_{u_i} \circ \sigma_{v_j})(\zeta_n) \\ &= \sigma_{u_1} \left(\sum_{j=1}^{q} a_{u_1,v_j} \sigma_{v_j}(\zeta_n) \right) + \cdots + \sigma_{u_r} \left(\sum_{j=1}^{q} a_{u_r,v_j} \sigma_{v_j}(\zeta_n) \right). \end{aligned}$$

Afirmamos que $a_{u_i,v_1} = a_{u_i,v_j}$, para $i = 1, \ldots, r$ e $j = 1, \ldots, q$. De fato, dado $\sigma_{v_j} \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$, existe $\ell \in \{1, \ldots, q\}$ tal que $\sigma_{v_\ell} \circ \sigma_{v_1} = \sigma_{v_j}$. Assim, como $\sigma_{v_\ell}(x) = x \in \mathbb{K}$

segue, da unicidade da representação de x na base integral, que $a_{u_i,v_1} = a_{u_i,v_j}$ para cada $i = 1, \ldots, r$. Logo, $x = a_{u_1,v_1}\sigma_{u_1}(t) + \cdots + a_{u_r,v_1}\sigma_{u_r}(t)$. Além disso, a independência linear de $\{\zeta_n^i \ ; \ i = 1, \ldots, n, \ \text{mdc}(i,n) = 1\}$ sobre $\mathbb{Z}$ implica que $\{\sigma_{u_1}(t), \ldots, \sigma_{u_r}(t)\}$ também o é.

□

O Lema 1.3.3 e o Teorema 1.3.4 compõem uma demonstração alternativa para a recíproca do Teorema de Hilbert-Speiser, o qual diz que uma extensão abeliana finita $\mathbb{K}/\mathbb{Q}$ tem uma base normal integral se, e somente se, o condutor de $\mathbb{K}$ é ímpar livre de quadrados; vide [11].

CAPÍTULO 2

Extensões Abelianas de grau p não ramificado

Seja $\mathbb{L}/\mathbb{Q}$ uma extensão abeliana de grau primo ímpar p e condutor n. Na Seção 2.1 vemos que a fatoração de n é determinada segundo a ramificação de p em $\mathbb{L}$, isto é, pela divisibilidade de n por p, vide Corolário 1.1.29. Todavia, a partir da Seção 2.2 consideramos especialmente o caso em que p é não ramificado. Nesse caso, existe uma base normal integral para $\mathbb{L}$ (vide Seção 1.3), sobre a qual descrevemos as formas traço canônica e integral de $\mathbb{L}$, em termos de p e n. Na Seção 2.3 desenvolvemos um algoritmo para encontrar o mínimo da forma traço integral restrita a uma classe de $\mathbb{Z}$-módulos livres contidos em $\mathfrak{O}_{\mathbb{L}}$. Com isso, obtemos a densidade de centro da imersão canônica de alguns desses $\mathbb{Z}$-módulos em $\mathbb{R}^p$, nas dimensões $p = 3$, 5 e 7. Por fim, na Seção 2.4 apresentamos a terminologia dos casos de ramificação e algumas propriedades de $\mathbb{L}$ quando p é ramificado.

2.1 Caracterização e contagem das p-extensões via condutor

Na Proposição 2.1.1 avaliamos quantos corpos de números de grau p um corpo ciclotômico contém e, na Proposição 2.1.3, obtemos o número de p-extensões de condutor n contidas em $\mathbb{Q}(\zeta_n)$, quando p não divide n. Estes resultados são fundamentais no estudo das torres de p-extensões abelianas da Seção 3.1.

Proposição 2.1.1. *Sejam $m = p_1^{a_1} \dots p_u^{a_u}$ um inteiro positivo e*

$$s = \#\{p_i \ ; \ p | \phi(p_i^{a_i}), \ i = 1, \dots, u\}.$$

Então, $\mathbb{Q}(\zeta_m)$ contém $(p^s - 1)/(p - 1)$ extensões de grau p sobre $\mathbb{Q}$.

Demonstração. Uma vez que existe uma relação biunívoca entre os subgrupos de ordem p e os subgrupos de índice p do grupo abeliano finito $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, é suficiente mostrar que o grupo

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

contém $(p^s - 1)/(p - 1)$ subgrupos de ordem p, isto é, que contém $p^s - 1$ elementos de ordem p. O grupo $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$ é cíclico de ordem $\phi(p_i^{a_i})$, para cada $i = 1, \dots, u$; vide Teorema 1.1.4. Assim, se p divide $\phi(p_i^{a_i})$, 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 $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$, a saber são elas $1, x_i, \dots, x_i^{p-1}$. Se p não divide $\phi(p_i^{a_i})$, então $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$ não possui elementos de ordem p e a equação $x_i^p = 1$ tem somente a solução trivial. Desse modo, a equação $(x_1, \dots, x_u)^p = (1, \dots, 1)$ tem $p^s - 1$ soluções não triviais, ou seja, existem $p^s - 1$ elementos de ordem p em $(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_u^{a_u}\mathbb{Z})^*$. □

Proposição 2.1.2. *Seja $\mathbb{L}$ uma p-extensão abeliana de condutor n. Então,*

(i) p se ramifica em $\mathbb{L}$ se, e somente se, o condutor $n = p^2 p_1 \dots p_s$;

(ii) p não se ramifica em $\mathbb{L}$ se, e somente se, o condutor $n = p_1 p_2 \dots p_s$;

onde $p_1, p_2, \dots, p_s$ são primos ímpares distintos tais que $p_i \equiv 1 \pmod{p}$, $i = 1, \dots, s$.

Demonstração. (i) Suponha $\mathbb{L} \subseteq \mathbb{Q}(\zeta_m)$, onde $m = p^a p_1^{a_1} \dots p_u^{a_u}$, com $a > 0$. Podemos supor que $p_1, \dots, p_s$ são os primos na fatoração de m tais que $p | \phi(p_i)$, com $s \leq u$. Se $n = p^2 p_1 \dots p_s$, então $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$ e, pela Proposição 2.1.1, ambos contém o mesmo número de p-extenões. Logo $n = p^2 p_1 \dots p_s$ é o condutor de $\mathbb{L}$. (ii) Suponha $\mathbb{L} \subseteq \mathbb{Q}(\zeta_m)$, onde $m = p_1^{a_1} p_2^{a_2} \dots p_u^{a_u}$ com $p_i \neq p$ para todo $i = 1, \dots, u$. Afirmamos que $\mathbb{L} \subseteq \mathbb{Q}(\zeta_{p_1 \dots p_u})$. De fato, se fosse $\mathbb{L} \nsubseteq \mathbb{Q}(\zeta_{p_1 \dots p_u})$, teríamos $\mathbb{L} \cap \mathbb{Q}(\zeta_{p_1 \dots p_u}) = \mathbb{Q}$, o que implica que $[\mathbb{L}\, \mathbb{Q}(\zeta_{p_1 \dots p_u}) : \mathbb{Q}] = p \cdot \phi(p_1 \dots p_u)$ divide $\phi(m)$, isto é, teríamos que p divide $p_1^{a_1 - 1} \dots p_u^{a_u - 1}$. Se $p_1, \dots, p_s$ são os primos em m tais que $p | \phi(p_i)$, $i = 1, \dots s$, então $\mathbb{L} \subseteq \mathbb{Q}(\zeta_{p_1 \dots p_s})$, pois caso contrário teríamos que p divide $\phi(p_{s+1} \dots p_u)$. As recíprocas dos ítens (i) e (ii) seguem do Corolário 1.1.29. □

A demonstração do ítem (ii) da Proposição 2.1.2 é alternativa. Ela pode também ser feita de maneira análoga ao ítem (i), utilizando a Proposição 2.1.1.

Proposição 2.1.3. *Se $n = p_1 \dots p_s$, com $p_i \equiv 1 (mod\ p)$ para $i = 1, \dots, s$, então o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ contém $(p-1)^{s-1}$ p-extensões de condutor n.*

Demonstração. Indução sobre s. O resultado é imediato para $s = 1$, pois o corpo $\mathbb{Q}(\zeta_{p_1})$ contém somente uma p-extensão. Suponha a asserção verdadeira para $k = 2, \dots, s-1$, isto é, $\mathbb{Q}(\zeta_{p_{i_1} p_{i_2} \dots p_{i_k}})$ contém $(p-1)^{k-1}$ p-extensões de condutor $p_{i_1} p_{i_2} \dots p_{i_k}$, com $1 \leq i_1 < i_2 < \dots < i_k \leq s$, para cada $k = 2, \dots, s-1$. Desse modo, o número de p-extensões de condutor menor que n contidas em $\mathbb{Q}(\zeta_n)$ é

$$\sum_{k=1}^{s-1} \binom{s}{k} (p-1)^{k-1}.$$

Portanto, como $\mathbb{Q}(\zeta_n)$ contém $(p^s-1)/(p-1)$ p-extensões (veja Proposição 2.1.1), segue que o número de p-extensões de condutor n é

$$\frac{p^s - 1}{p-1} - \sum_{k=1}^{s-1} \binom{s}{k} (p-1)^{k-1} = (p-1)^{s-1}.$$

□

2.2 Forma Traço Integral de uma p-Extensão

Seja p não ramificado em $\mathbb{L}$. Nesse caso, o condutor de $\mathbb{L}$ é da forma $n = p_1 \dots p_s$, onde $p_1, \dots, p_s$ são primos ímpares distintos, com $p_i \equiv 1 \pmod{p}$, para $i = 1, \dots, s$; vide Proposição 2.1.2. Desse modo, se θ é um gerador de $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, então, pelo Teorema 1.3.4, o conjunto

$$\{t, \theta(t), \dots, \theta^{p-1}(t)\}$$

é uma base normal integral de $\mathbb{L}$, gerada pelo elemento $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$. Nesta seção, temos como objetivo exibir uma expressão para a forma traço integral $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)$, $x \in \mathfrak{O}_{\mathbb{L}}$, com respeito a tal base. Note que $\mathbb{L}$ é totalmente real, $|\mathrm{Disc}(\mathbb{L})| = n^{p-1}$ e $p_1, \dots, p_s$ são os primos que se ramificam em $\mathbb{L}$ (vide Observação 1.1.1, Proposição 1.1.21 e Corolário 1.1.29).

Dado $x = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathfrak{O}_{\mathbb{L}}$, temos que $x^2 = \sum_{i,j=0}^{p-1} a_i a_j \theta^i(t) \theta^j(t)$. Porém,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\theta^i(t)\theta^j(t)) = \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\theta^{i-j}(t)),$$

com $i, j = 0, 1, \dots, p-1$. Desse modo,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2) = \sum_{i,j=0}^{p-1} a_i a_j \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ \theta^{i-j}(t)).$$

Sendo assim, a forma traço canônica de $\mathbb{L}$ pode ser expressa em função de $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\,\theta^k(t))$, com $k = 0, 1, \ldots, p-1$, a qual apresentamos explicitamente no Teorema 2.2.2.

Seja H o subgrupo de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{L}$. Uma vez que

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*,$$

os elementos de H serão representados como s-uplas em $(\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^*$.

Lema 2.2.1. *Sejam $\alpha = (\alpha_1, ..., \alpha_s) \in \mathrm{H}$, $1 \leq q < s$ e $\Pi : \mathrm{H} \longrightarrow (\mathbb{Z}/p_{j_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{j_q}\mathbb{Z})^*$ a projeção definida por $\Pi(\alpha) = (\alpha_{j_1}, \ldots, \alpha_{j_q})$, com $1 \leq j_1 < \ldots < j_q \leq s$. Então*

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

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

Demonstração. Sejam $Z = (\mathbb{Z}/p_{j_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{j_q}\mathbb{Z})^*$ e $Z^c = (\mathbb{Z}/p_{i_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_{i_r}\mathbb{Z})^*$. Assim,

$$\mathrm{H} \leq \Pi(\mathrm{H}) \times Z^c \leq (\mathbb{Z}/n\mathbb{Z})^*.$$

Porém, H tem índice p em $(\mathbb{Z}/n\mathbb{Z})^*$. Logo, $\Pi(\mathrm{H}) \times Z^c = \mathrm{H}$ ou $\Pi(\mathrm{H}) \times Z^c = (\mathbb{Z}/n\mathbb{Z})^*$. A primeira não é possível, pois H teria Z^c como fator, o que contraria $\mathbb{L}$ ter condutor cheio. Desse modo, Π é um homomorfismo sobrejetivo, ou seja, $\mathrm{H}/Ker\ \Pi \simeq Z$. Portanto,

$$|Ker\ \Pi| = \frac{\phi(n)/p}{(p_{j_1} - 1)\ldots(p_{j_q} - 1)} = \frac{\prod_{\ell=1}^{r}(p_{i_\ell} - 1)}{p}.$$

□

Dado $z \in \Pi(\mathrm{H})$, temos que $\Pi^{-1}(z)$ é uma classe lateral de $Ker\ \Pi$ em H, a saber, $\Pi^{-1}(z) = \alpha(Ker\ \Pi)$, onde $z = \Pi(\alpha)$. Logo, $|\Pi^{-1}(z)| = |Ker\ \Pi|$. Quando conveniente, denotaremos $q_i = p_i - 1$, para todo $i = 1, \ldots, s$, e

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

com $1 \leq i_1 < \ldots < i_r \leq s$.

Teorema 2.2.2. *Se θ é um gerador de $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ e $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$, então*

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ \theta^k(t)) = \begin{cases} n - (\frac{n-1}{p})\ , & se\ k = 0 \\ -(\frac{n-1}{p})\ , & se\ k \neq 0\ , \end{cases}$$

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

Demonstração. Se $h = \phi(n)/p$, então $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ \theta^k(t)) = \frac{1}{h}\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t))$. Trabalhamos com o traço sobre $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Temos que $\theta = \sigma_r|_{\mathbb{L}}$, para algum $\sigma_r \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, tal que $\sigma_r(\zeta_n) = \zeta_n^r$. Logo,

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

Porém, pondo $d = \frac{n}{p_1} + \cdots + \frac{n}{p_s}$, temos $\zeta_n^d = \zeta_{p_1} \ldots \zeta_{p_s}$. Assim, $\zeta_n^{\alpha+\beta r^k}$ é raíz n-ésima primitiva da unidade se, e somente se, $\zeta_n^{d(\alpha+\beta r^k)} = \zeta_{p_1}^{\alpha+\beta r^k} \ldots \zeta_{p_s}^{\alpha+\beta r^k}$ também o é, pois $\mathrm{mdc}(d, n) = 1$. Deste modo,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) = \sum_{\alpha,\beta\in \mathrm{H}} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{\alpha+\beta r^k}) = \sum_{\alpha,\beta\in \mathrm{H}} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{p_1}^{\alpha+\beta r^k} \ldots \zeta_{p_s}^{\alpha+\beta r^k}).$$

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

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) = \sum_{\alpha,\beta\in \mathrm{H}} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \ldots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}).$$

Mas,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \ldots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{n/p_1})/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/p_1})}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k} \ldots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k})),$$

em que,

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

Logo,

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) &= \sum_{\alpha,\beta\in \mathrm{H}} \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \mathrm{Tr}_{\mathbb{Q}(\zeta_{n/p_1})/\mathbb{Q}}(\zeta_{p_2}^{\alpha_2+\beta_2 r_2^k} \ldots \zeta_{p_s}^{\alpha_s+\beta_s r_s^k}) \\ &= \sum_{\alpha,\beta\in \mathrm{H}} \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \ldots \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k}), \qquad (*) \end{aligned}$$

onde

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}}(\zeta_{p_i}^{\alpha_i+\beta_i r_i^k}) = \begin{cases} p_i - 1\ , & \text{se}\ \ \alpha_i + \beta_i r_i^k = 0 \\ -1\ , & \text{se}\ \ \alpha_i + \beta_i r_i^k \neq 0\ , \end{cases}$$

para cada $i = 1, \ldots, s$.

No que segue, a prova será dividida em dois casos, a saber, $k = 0$ e $k = 1, \ldots, p-1$.

Caso (i): $k = 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathrm{H}$ fixo. A extensão $\mathbb{L}/\mathbb{Q}$ é galoisiana de grau ímpar, logo é totalmente real. Assim, a conjugação complexa pertence a H e, portanto, $(-1, ..., -1) \in \mathrm{H}$. Logo, $\beta = (-\alpha_1, \ldots, -\alpha_s) \in \mathrm{H}$. Além disso, β é o único

elemento de H tal que $\alpha+\beta=0$, pois $\mathrm{H}\leq(\mathbb{Z}/n\mathbb{Z})^*\subseteq\mathbb{Z}/n\mathbb{Z}$. Sendo assim, $\alpha_i+\beta_i=0$ para todo $i=1,\ldots,s$. Logo,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1})\ldots\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s})=(p_1-1)\ldots(p_s-1)=\phi(n).$$

Nesse caso, $h=|\mathrm{H}|$ parcelas são iguais a $\phi(n)$ em $(*)$. Então, a soma das parcelas correspondentes aos pares $\alpha,\beta\in\mathrm{H}$ tais que $\alpha_i+\beta_i=0$, para todo $i=1,\ldots,s$, é igual a $\mathrm{T}_0=h\phi(n)$.

Pelo Lema 2.2.1, para cada $i_1=1,\ldots,s$, existem $S_{i_1}=A_{i_1}-1=\frac{q_{i_1}}{p}-1$ elementos $\beta=(\beta_1,\ldots,\beta_s)\in\mathrm{H}$, tais que $\beta_i=-\alpha_i$ para todo $i\neq i_1$ e $\alpha_{i_1}+\beta_{i_1}\neq 0$. Nesse caso, a parcela $\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1})\ldots\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s})$ em $(*)$ correspondente ao par α,β é igual a $-\frac{\phi(n)}{q_{i_1}}$. Logo, a soma destas parcelas é igual a

$$\begin{aligned}\mathrm{T}_1 &= -h\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}S_{i_1}\\ &= -h\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}\left(\frac{q_{i_1}}{p}-1\right)\\ &= -h\left(\frac{1}{p}\binom{s}{s-1}\phi(n)-\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}\right).\end{aligned}$$

De maneira análoga, 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 $\alpha_{i_2}+\beta_{i_2}\neq 0$, para $i_1,i_2=1,\ldots,s$, com $i_1<i_2$. Nesse caso, a parcela em $(*)$ é igual a $\frac{\phi(n)}{q_{i_1}q_{i_2}}$, e a soma destas é dada por

$$\begin{aligned}\mathrm{T}_2 &= h\sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}}S_{i_1,i_2}\\ &= h\left(\sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}}\frac{(q_{i_1}q_{i_2}-q_{i_1}-q_{i_2})}{p}+\sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}}\right)\\ &= h\left[\frac{1}{p}\left(\binom{s}{s-2}\phi(n)-\binom{s-1}{s-2}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}\right)+\sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}}\right].\end{aligned}$$

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

$$\begin{aligned}S_{i_1,\ldots,i_u} &= A_{i_1,\ldots,i_u}-\sum_{1\leq\ell_1<\ldots<\ell_{u-1}\leq u}S_{i_{\ell_1},\ldots,i_{\ell_{u-1}}}-\cdots-\sum_{1\leq\ell_1<\ell_2\leq u}S_{i_{\ell_1},i_{\ell_2}}-\sum_{\ell=1}^{u}S_{i_\ell}-1\\ &= A_{i_1,\ldots,i_u}-\sum_{1\leq\ell_1<\ldots<\ell_{u-1}\leq u}A_{i_{\ell_1},\ldots,i_{\ell_{u-1}}}+\cdots+(-1)^{u-1}\sum_{\ell=1}^{u}A_{i_\ell}+(-1)^u\end{aligned}$$

elementos $\beta = (\beta_1, \ldots, \beta_s) \in \mathrm{H}$, tais que $\beta_i = -\alpha_i$ para todo $i \neq i_1, \ldots, i_u$ e $\alpha_{i_\ell} + \beta_{i_\ell} \neq 0$ para todo $\ell = 1, \ldots, u$. Nesse caso, cada parcela em $(*)$ é igual a

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

e a respectiva soma é dada por

$$\begin{aligned}
\mathrm{T}_u &= (-1)^u h \sum_{i_1<\ldots<i_u} \frac{\phi(n)}{q_{i_1}\cdots q_{i_u}} S_{i_1,\ldots,i_u} \\
&= (-1)^u h \sum_{i_1<\ldots<i_u} \frac{\phi(n)}{q_{i_1}\cdots q_{i_u}} \left(\frac{q_{i_1}\ldots q_{i_u} - (q_{i_1}\ldots q_{i_{u-1}} + \cdots + q_{i_2}\ldots q_{i_u}) + \cdots}{p} \right. \\
&\quad \left. \frac{\cdots + (-1)^{u-2}(q_{i_1}q_{i_2} + \cdots + q_{i_{u-1}}q_{i_u}) + (-1)^{u-1}(q_{i_1} + \cdots + q_{i_u})}{p} + (-1)^u \right) \\
&= (-1)^u h \left[\frac{1}{p} \left(\binom{s}{s-u} \phi(n) - \binom{s-1}{s-u} \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} + \cdots \right. \right. \\
&\quad \left. \left. \cdots + (-1)^{u-1} \binom{s-(u-1)}{s-u} \sum_{i_1<\ldots<i_{u-1}} \frac{\phi(n)}{q_{i_1}\cdots q_{i_{u-1}}} \right) + (-1)^u \sum_{i_1<\ldots<i_u} \frac{\phi(n)}{q_{i_1}\cdots q_{i_u}} \right].
\end{aligned}$$

Desse modo,

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) &= \mathrm{T}_0 + \mathrm{T}_1 + \mathrm{T}_2 + \cdots + \mathrm{T}_{s-1} + \mathrm{T}_s \\
&= h\phi(n) - h\left(\frac{1}{p} \binom{s}{s-1} \phi(n) - \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} \right) \\
&\quad + h\left[\frac{1}{p} \left(\binom{s}{s-2} \phi(n) - \binom{s-1}{s-2} \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} \right) + \sum_{i_1<i_2} \frac{\phi(n)}{q_{i_1}q_{i_2}} \right] - \cdots \\
&\quad + (-1)^{s-1} h \left[\frac{1}{p} \left(\binom{s}{1} \phi(n) - \binom{s-1}{1} \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} + \cdots \right. \right. \\
&\quad \left. \left. \cdots + (-1)^{s-2} \binom{2}{1} \sum_{i_1<\ldots<i_{s-2}} \frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-2}}} \right) + (-1)^{s-1} \sum_{i_1<\ldots<i_{s-1}} \frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}} \right] \\
&\quad + (-1)^s h \left[\frac{1}{p} \left(\binom{s}{0} \phi(n) - \binom{s-1}{0} \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} + \cdots \right. \right. \\
&\quad \left. \left. \cdots + (-1)^{s-1} \binom{1}{0} \sum_{i_1<\ldots<i_{s-1}} \frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}} \right) + (-1)^s \right].
\end{aligned}$$

Assim, $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é igual a

$$h\Bigg[\left(1+\frac{-\binom{s}{s-1}+\binom{s}{s-2}-\cdots+(-1)^{s-1}\binom{s}{1}+(-1)^s\binom{s}{0}}{p}\right)\phi(n)$$
$$+\left(1+\frac{-\binom{s-1}{s-2}+\binom{s-1}{s-3}-\cdots+(-1)^{s-2}\binom{s-1}{1}+(-1)^{s-1}\binom{s-1}{0}}{p}\right)\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}+\cdots$$
$$+\left(1+\frac{-\binom{2}{1}+\binom{2}{0}}{p}\right)\sum_{i_1<\ldots<i_{s-2}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-2}}}+\left(1-\frac{\binom{1}{0}}{p}\right)\sum_{i_1<\ldots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}+1\Bigg].$$

Porém,

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

para todo $u=1,\ldots,s$. Logo, $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é igual a

$$h\left[\left(1-\frac{1}{p}\right)\left(\phi(n)+\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}+\sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}}+\cdots+\sum_{i_1<\ldots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right)+1\right].$$

No entanto,

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

Portanto,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t^2)=\frac{1}{h}\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)=\frac{(p-1)(n-1)}{p}+1=n-\left(\frac{n-1}{p}\right).$$

Caso (ii): $k\neq 0$. Como no caso anterior, seja $\alpha=(\alpha_1,\ldots,\alpha_s)\in \mathrm{H}$ fixo. Afirmamos que $\alpha+\beta r^k\neq 0$, para todo $\beta\in\mathrm{H}$. De fato, se $\beta\in\mathrm{H}$ é tal que $\alpha+\beta r^k=0$, então $\alpha=-\beta r^k\in r^k\mathrm{H}$, pois $-1\in\mathrm{H}$. Por outro lado, denotando $\mathrm{G}=\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, temos que $\mathrm{G}/\mathrm{H}\simeq\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Logo, $\mathrm{G}=\mathrm{H}\cup\sigma_r\mathrm{H}\cup\ldots\cup\sigma_{r^{p-1}}\mathrm{H}$, isto é, $(\mathbb{Z}/n\mathbb{Z})^*=\mathrm{H}\cup r\mathrm{H}\cup\ldots\cup r^{p-1}\mathrm{H}$ é uma união de classes laterais disjuntas. Desse modo, $\alpha\notin\mathrm{H}$, o que é uma contradição. Portanto, a soma T_0 das parcelas $\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1r_1^k})\ldots\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_sr_s^k})$ em $(*)$ correspondentes aos pares $\alpha,\beta\in\mathrm{H}$ tais que $\alpha_i+\beta_ir_i^k=0$, para todo $i=1,\ldots,s$, é nula. Logo, $\mathrm{T}_0=0$.

Uma vez que $-\alpha r^{-k} = (-\alpha_1 r_1^{-k}, \ldots, -\alpha_s r_s^{-k}) \in (\mathbb{Z}/p_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_s\mathbb{Z})^*$, segue do Lema 2.2.1 que, para cada $i_1 = 1, \ldots, s$, existem $A_{i_1} = \frac{q_{i_1}}{p}$ elementos $\beta = (\beta_1, \ldots, \beta_s) \in H$, tais que $\beta_i = -\alpha_i r_i^{-k}$ para todo $i \neq i_1$. Sendo assim, $\alpha_i + \beta_i r_i^k = 0$, para todo $i \neq i_1$. Além disso, $\alpha_{i_1} + \beta_{i_1} r_{i_1}^k \neq 0$, pois $\alpha + \beta r^k \neq 0$. Nesse caso, a parcela

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^k}) \ldots \mathrm{Tr}_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^k})$$

em $(*)$ correspondente ao par α, β é igual a $-\frac{\phi(n)}{q_{i_1}}$. Logo, a soma destas parcelas é igual a

$$\mathrm{T}_1 = -h \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} A_{i_1} = -h \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} \left(\frac{q_{i_1}}{p}\right) = -\frac{h}{p} \binom{s}{s-1} \phi(n).$$

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 $i_1 < i_2$. Nesse caso, a parcela em $(*)$ é igual a $\frac{\phi(n)}{q_{i_1} q_{i_2}}$, e a soma destas é dada por

$$\begin{aligned}
\mathrm{T}_2 &= h \sum_{i_1<i_2} \frac{\phi(n)}{q_{i_1} q_{i_2}} S_{i_1,i_2} \\
&= h \sum_{i_1<i_2} \frac{\phi(n)}{q_{i_1} q_{i_2}} \frac{(q_{i_1} q_{i_2} - q_{i_1} - q_{i_2})}{p} \\
&= \frac{h}{p} \left(\binom{s}{s-2} \phi(n) - \binom{s-1}{s-2} \sum_{i_1=1}^{s} \frac{\phi(n)}{q_{i_1}} \right).
\end{aligned}$$

Quando u coordenadas $\alpha_i + \beta_i r_i^k$ são não-nulas, para cada $u = 1, \ldots, s$, existem

$$\begin{aligned}
S_{i_1,\ldots,i_u} &= A_{i_1,\ldots,i_u} - \sum_{1 \leq \ell_1 < \ldots < \ell_{u-1} \leq u} S_{i_{\ell_1},\ldots,i_{\ell_{u-1}}} - \cdots - \sum_{1 \leq \ell_1 < \ell_2 \leq u} S_{i_{\ell_1},i_{\ell_2}} - \sum_{\ell=1}^{u} S_{i_\ell} \\
&= \frac{q_{i_1} \ldots q_{i_u}}{p} - \sum_{1 \leq \ell_1 < \ldots < \ell_{u-1} \leq u} \frac{q_{i_{\ell_1}} \ldots q_{i_{\ell_{u-1}}}}{p} + \cdots + (-1)^{u-1} \sum_{\ell=1}^{u} \frac{q_{i_\ell}}{p}
\end{aligned}$$

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 $\alpha_{i_\ell} + \beta_{i_\ell} r_{i_\ell}^{-k} \neq 0$ para todo $\ell = 1, \ldots, u$. Nesse caso, cada parcela em $(*)$ é igual a

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

e a respectiva soma é dada por

$$\mathrm{T}_u = (-1)^u h \sum_{i_1<\ldots<i_u} \frac{\phi(n)}{q_{i_1} \ldots q_{i_u}} S_{i_1,\ldots i_u}.$$

Logo,

$$\mathrm{T}_u = (-1)^u \frac{h}{p}\left(\binom{s}{s-u}\phi(n) - \binom{s-1}{s-u}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \cdots\right.$$

$$\left. +(-1)^{u-1}\binom{s-(u-1)}{s-u}\sum_{i_1<\ldots<i_{u-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{u-1}}}\right).$$

Sendo assim, $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) = \mathrm{T}_1 + \mathrm{T}_2 + \cdots + \mathrm{T}_{s-1} + \mathrm{T}_s$, isto é,

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) = -\frac{h}{p}\binom{s}{s-1}\phi(n) + \frac{h}{p}\left(\binom{s}{s-2}\phi(n) - \binom{s-1}{s-2}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}}\right) + \cdots$$

$$+(-1)^{s-1}\frac{h}{p}\left(\binom{s}{1}\phi(n) - \binom{s-1}{1}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \cdots + (-1)^{s-2}\binom{2}{1}\sum_{i_1<\ldots<i_{s-2}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-2}}}\right)$$

$$+(-1)^{s}\frac{h}{p}\left(\binom{s}{0}\phi(n) - \binom{s-1}{0}\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \cdots + (-1)^{s-1}\binom{1}{0}\sum_{i_1<\ldots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right).$$

Desse modo, $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t))$ é igual a

$$\begin{aligned}
&\frac{h}{p}\left[\left(-\binom{s}{s-1} + \binom{s}{s-2} - \cdots + (-1)^{s-1}\binom{s}{1} + (-1)^{s}\binom{s}{0}\right)\phi(n)\right.\\
&+\left(-\binom{s-1}{s-2} + \cdots + (-1)^{s-2}\binom{s-1}{1} + (-1)^{s-1}\binom{s-1}{0}\right)\sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \cdots\\
&\left.+\left(-\binom{2}{1} + \binom{2}{0}\right)\sum_{i_1<\ldots<i_{s-2}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-2}}} - \binom{1}{0}\sum_{i_1<\ldots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right]\\
&= -\frac{h}{p}\left(\phi(n) + \sum_{i_1=1}^{s}\frac{\phi(n)}{q_{i_1}} + \sum_{i_1<i_2}\frac{\phi(n)}{q_{i_1}q_{i_2}} + \cdots + \sum_{i_1<\ldots<i_{s-1}}\frac{\phi(n)}{q_{i_1}\cdots q_{i_{s-1}}}\right).
\end{aligned}$$

No entanto,

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

Portanto,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ \theta^k(t)) = \frac{1}{h}\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\ \theta^k(t)) = -\left(\frac{n-1}{p}\right).$$

□

Pelo Teorema 2.2.2, a matriz de Gram $G = (g_{ij})$ do reticulado algébrico $\sigma_{\mathbb{L}}(\mathfrak{O}_{\mathbb{L}})$, com respeito à base $\{\sigma_{\mathbb{L}}(t), \sigma_{\mathbb{L}}(\theta(t)), \ldots, \sigma_{\mathbb{L}}(\theta^{p-1}(t))\} \subset \mathbb{R}^p$, é dada por

$$g_{ij} = \begin{cases} n - (\frac{n-1}{p}) \ , & \text{se } i = j \\ -(\frac{n-1}{p}) \ , & \text{se } i \neq j \ , \end{cases}$$

com $i, j = 1, \ldots, p$. Nesse caso, $|\det(G)| = |\mathrm{Disc}(\mathbb{L})| = n^{p-1}$; vide Observação 1.2.1.

Com as notações do Teorema 2.2.2 descrevemos a forma traço sobre o quadrado de um elemento arbitrário do anel de inteiros $\mathfrak{O}_{\mathbb{L}}$, isto é, a forma traço integral de $\mathbb{L}$:

Corolário 2.2.3. *Se* $x = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathfrak{O}_{\mathbb{L}}$, *então*

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2) = n \left(\sum_{i=0}^{p-1} a_i^2 \right) - \frac{n-1}{p} \left(\sum_{i=0}^{p-1} a_i \right)^2 . \tag{2.1}$$

Demonstração. De fato, segue do Teorema 2.2.2 que

$$\begin{aligned} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2) &= \sum_{i,j=0}^{p-1} a_i a_j \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\theta^{i-j}(t)) = \sum_{i=0}^{p-1} a_i^2 \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t^2) + \sum_{\substack{i,j=0 \\ i \neq j}}^{p-1} a_i a_j \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\theta^{i-j}(t)) \\ &= \left(n - \frac{n-1}{p} \right) \left(\sum_{i=0}^{p-1} a_i^2 \right) - 2 \left(\frac{n-1}{p} \right) \left(\sum_{\substack{i,j=0 \\ i<j}}^{p-1} a_i a_j \right) \\ &= n \left(\sum_{i=0}^{p-1} a_i^2 \right) - \frac{n-1}{p} \left(\sum_{i=0}^{p-1} a_i \right)^2 . \end{aligned}$$

□

2.3 Mínimo da Forma Traço de uma p-Extensão

Considere as mesmas notações da Seção 2.2. Nesta seção, descrevemos um algoritmo para encontrar o mínimo da forma traço integral $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)$, dada pelo Corolário 2.2.3, restrita ao $\mathbb{Z}$-módulo livre

$$\mathcal{M}_m := \{a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_{\mathbb{L}} \, ; \, a_0 + a_1 + \cdots + a_{p-1} \equiv 0 \pmod{m}\}, \tag{2.2}$$

onde m é um inteiro positivo. Por fim, apresentamos a densidade de centro do reticulado algébrico $\sigma_{\mathbb{L}}(\mathcal{M}_m)$, para alguns valores de m e n, nas dimensões 3, 5 e 7.

Primeiramente, considere o caso $m = 1$, ou seja, $\mathcal{M}_1 = \mathfrak{O}_{\mathbb{L}}$. Temos que

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2) \geq p\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x^2)^{\frac{1}{p}} \geq p$$

para todo $x \in \mathfrak{O}_{\mathbb{L}}$, com $x \neq 0$. Porém, $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(1) = p$. Logo, o mínimo de $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)$, com $x \in \mathfrak{O}_{\mathbb{L}} \setminus \{0\}$, é igual a p.

Considere $m > 1$. Para cada par (i, j), com $i, j \in \{0, 1, \ldots, p-1\}$ e $i \neq j$, definimos

$$\begin{array}{rccc} \tau_{ij}: & \mathbb{Z}^p & \longrightarrow & \mathbb{Z}^p \\ & (a_0, \ldots, a_{p-1}) & \longmapsto & (b_0, \ldots, b_{p-1}) \end{array} \quad \text{onde } b_k = \begin{cases} a_i - 1\ , & \text{se } k = i \\ a_j + 1\ , & \text{se } k = j \\ a_k\ , & \text{caso contrário .} \end{cases}$$

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 é válida a última igualdade, então existe uma composição de τ_{ij}'s que aplica a em b. Para cada $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$, a soma $\sum_{k=0}^{p-1} a_k^2$ será denotada por $||a||^2$.

Proposição 2.3.1. *Sejam $a = (a_0, \ldots, a_{p-1}), b = (b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p$ tais que $\tau_{ij}(a) = b$. Então, $||a||^2 > ||b||^2$ se, e somente se, $a_i - a_j > 1$.*

Demonstração. De fato, $||a||^2 > ||b||^2 \iff a_i^2 + a_j^2 > (a_i - 1)^2 + (a_j + 1)^2 \iff a_i - a_j > 1$. □

Definimos a órbita de um elemento $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$ como sendo o conjunto

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

Analogamente, definimos a órbita de $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_{\mathbb{L}}$ por

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

Lema 2.3.2. *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*

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

Além disso, 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. Como $||b||^2 > 0$, para todo $b \in \mathcal{O}(a)$, segue que existe $\overline{b} = (b_0, \ldots, b_{p-1})$ pertencente à órbita de a tal que

$$||\overline{b}||^2 = \min_{b \in \mathcal{O}(a)} ||b||^2.$$

Assim, $b_0 + \cdots + b_{p-1} = pq + r > 0$ e, pela Proposição 2.3.1, quaisquer duas entradas de $\overline{b}$ satisfazem $|b_i - b_j| \leq 1$. Desse modo, $\overline{b}$ deve ser uma permutação

$$(q+1, \ldots, q+1, q, \ldots, q),$$

onde o número de entradas iguais a $q+1$ é r e de entradas iguais a q é $p-r$. Portanto, $||\overline{b}||^2 = pq^2 + 2rq + r$. □

Para cada $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_{\mathbb{L}}$, denotamos $S = S(x) = a_0 + \cdots + a_{p-1}$ e

$$M(S) = \min_{y \in \mathcal{O}(x)} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(y^2).$$

Teorema 2.3.3. *Sejam $x = a_0 t + a_1\theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_{\mathbb{L}}$ 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*

$$M(S) = pq^2 + 2rq + nr - \frac{n-1}{p} r^2. \tag{2.3}$$

Demonstração. Pelo Corolário 2.2.3, para cada $y = b_0 t + b_1\theta(t) + \cdots + b_{p-1}\theta^{p-1}(t) \in \mathcal{O}(x)$, temos que

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(y^2) = n||b||^2 - \frac{n-1}{p} S^2,$$

onde $b = (b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p$. Portanto, segue do Lema 2.3.2 que

$$\begin{aligned} \min_{y \in \mathcal{O}(x)} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(y^2) &= n(pq^2 + 2rq + r) - \frac{n-1}{p}(pq + r)^2 \\ &= pq^2 + 2rq + nr - \frac{n-1}{p} r^2. \end{aligned}$$

□

Corolário 2.3.4. *Considere as mesmas hipóteses do Teorema 2.3.3. Se p divide S, então*

$$M(S) = \min\{2n, S^2/p\}.$$

Demonstração. Suponha $S = 0$. Pelo Corolário 2.2.3, o mínimo de $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(y^2)$, para y não nulo pertencente à órbita de zero, é igual a $2n$. A saber, ele é atingido no elemento $y = b_0 t + b_1\theta(t) + \ldots + b_{p-1}\theta^{p-1}(t)$, com $(b_0, b_1, \ldots, b_{p-1}) = (1, -1, 0, \ldots, 0)$, ou uma de suas permutações. Suponha, agora, $S > 0$. Temos que $S = pq$, isto é, $q = S/p$ e $r = 0$. Logo, o resultado segue do Teorema 2.3.3. □

Teorema 2.3.5. *Sejam m um inteiro positivo e*

$$M^* = \min_{\substack{x \in \mathcal{M}_m \\ x \neq 0}} \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2). \tag{2.4}$$

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

(ii) Se $p \not| m$, então $M^* = \min\{2n, M(m), \ldots, M(pm)\}$.

Demonstração. Observe que

$$M^* = \min_{j \in \mathbb{Z}} M(jm).$$

Suponhamos que p divide m. Pelo Corolário 2.3.4, se $j = 0$, então $M(jm) = 2n$ e , se for $j \neq 0$, teremos

$$M(jm) = \min_{j \neq 0} \frac{(jm)^2}{p} = \frac{m^2}{p}.$$

Suponha, agora, que p não divide m. Para $j = 0$, ainda é válido $M(jm) = 2n$, pois p divide $jm = 0$. Consideremos $j \neq 0$. Temos que $\{jm\,;\, j = 1, \ldots, p\}$ é um conjunto completo de resíduos módulo p e a expressão no lado direito em (2.3) é uma função estritamente crescente de q. Portanto,

$$\min\{M(jm)\,;\, j \in \mathbb{Z}^*\} = \min\{M(m), M(2m), \ldots, M(pm)\}.$$

□

Os Teoremas 2.3.3 e 2.3.5 fornecem o mínimo M^* do traço $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(x^2)$, com $x \neq 0$, restrito ao $\mathbb{Z}$-módulo livre $\mathcal{M}_m$. Para determinar em quais elementos esse mínimo é atingido, utilizamos as demonstrações do Lema 2.3.2 e do Corolário 2.3.4. Mais precisamente, quando $M^* = 2n$, esse mínimo é atingido nos elementos

$$x = a_0 t + a_1 \theta(t) + \cdots + a_{p-1}\theta^{p-1}(t) \in \mathfrak{O}_{\mathbb{L}},$$

tais que $(a_0, a_1, \ldots, a_{p-2}) = (1, -1, 0, \ldots, 0)$, ou uma de suas permutações. Se $p|m$ e $M^* = m^2/p$, então o mínimo é atingido em $x = a_0 t + a_1\theta(t) + \ldots + a_{p-1}\theta^{p-1}(t)$, com $(a_0, a_1 \ldots, a_{p-1}) = (m/p, \ldots, m/p)$. Por fim, quando 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

$$(a_0, a_1 \ldots, a_{p-1}) = (\underbrace{q_j + 1, \ldots, q_j + 1}_{r_j \text{ coordenadas}}, q_j, \ldots, q_j),$$

ou uma de suas permutações, onde q_j e r_j são, respectivamente, o quociente e o resto da divisão de jm por p, com $j = 1, \ldots, p$. Nesse caso, $M^* = \min\{M(m), \ldots, M(pm)\}$. No que segue, apresentamos alguns exemplos para ilustrar esse procedimento.

Exemplo 2.3.1. *Sejam $p = 3$, $n = 1123$ e $m = 67$. Como $p \nmid m$, segue que*

$$M^* = \min\{2n, M(m), M(2m), M(3m)\} = \min\{2246, 2245, 6734, 13467\} = 2245.$$

Temos que $q_1 = 22$ e $r_1 = 1$ ($67 = 3 \times 22 + 1$). Logo, o mínimo é atingido no elemento

$$x = a_0 t + a_1\theta(t) + a_2\theta^2(t) \in \mathfrak{O}_{\mathbb{L}},$$

tal que $(a_0, a_1, a_2) = (23, 22, 22)$, ou em uma de suas permutações, onde $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$ e $\langle\theta\rangle = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Pela Equação (1.1), o reticulado $\sigma_{\mathbb{L}}(\mathcal{M}_{67})$, de dimensão 3, tem densidade de centro igual a

$$\delta(\sigma_{\mathbb{L}}(\mathcal{M}_{67})) = \frac{\rho^3}{|\mathrm{Disc}(\mathbb{L})|^{\frac{1}{2}}[\mathfrak{O}_{\mathbb{L}} : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^3}{nm} \simeq 0,17672.$$

Note que a maior densidade de centro de um reticulado de posto 3 é obtida pelo reticulado A_3, dada por $\delta(A_3) = \frac{1}{4\sqrt{2}} \simeq 0,17678$.

Exemplo 2.3.2. *Sejam $p = 5$, $n = 92111$ e $m = 607$. Temos que $p \nmid m$, logo*

$$\begin{aligned} M^* &= \min\{2n, M(m), M(2m), M(3m), M(4m), M(5m)\} \\ &= \min\{184222, 736897, 184223, 1289570, 295245, 1842245\} = 184222. \end{aligned}$$

O mínimo é obtido no elemento

$$x = a_0 t + a_1\theta(t) + a_2\theta^2(t) + a_3\theta^3(t) + a_4\theta^4(t) \in \mathfrak{O}_{\mathbb{L}},$$

com $(a_0, a_1, a_2, a_3, a_4) = (1, -1, 0, 0, 0)$, ou em uma permutação deste. A densidade de centro do reticulado 5-dimensional $\sigma_{\mathbb{L}}(\mathcal{M}_{607})$ é dada por

$$\delta(\sigma_{\mathbb{L}}(\mathcal{M}_{607})) = \frac{\rho^5}{|\mathrm{Disc}(\mathbb{L})|^{\frac{1}{2}}[\mathfrak{O}_{\mathbb{L}} : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^5}{n^2 m} \simeq 0,08839.$$

O reticulado D_5 tem a maior densidade de centro na dimensão 5, a saber, $\frac{1}{8\sqrt{2}} \simeq 0,08839$.

Exemplo 2.3.3. *Sejam $p = 7$, $n = 600601$ e $m = 1096$. Como $p \nmid m$, segue que*

$$\begin{aligned} M^* &= \min\{2n, M(m), M(2m), M(3m), M(4m), M(5m), M(6m), M(7m)\} \\ &= \min\{1201202, 1201210, 3603638, 7207284, 1201204, 2402422, 4804858, 8408512\} \\ &= 1201202. \end{aligned}$$

O mínimo é atingido nas permutações do elemento

$$x = a_0 t + a_1\theta(t) + \cdots + a_5\theta^5(t) + a_6\theta^6(t) \in \mathfrak{O}_{\mathbb{L}},$$

com

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (1, -1, 0, 0, 0, 0, 0).$$

O reticulado $\sigma_{\mathbb{L}}(\mathcal{M}_{1096})$ *tem dimensão* 7 *e densidade de centro dada por*

$$\delta(\sigma_{\mathbb{L}}(\mathcal{M}_{1096})) = \frac{\rho^7}{|\mathrm{Disc}(\mathbb{L})|^{\frac{1}{2}}[\mathfrak{O}_{\mathbb{L}} : \mathcal{M}_m]} = \frac{(\sqrt{M^*}/2)^7}{n^3 m} \simeq 0,0625.$$

A maior densidade de centro na dimensão 7 *é obitida pelo reticulado* E_7*, a qual é dada por* $\frac{1}{16} = 0,0625$*. Vide Conway e Sloane, [2], páginas 12 e 13.*

2.4 Terminologia

Seja $\mathbb{L}/\mathbb{Q}$ uma extensão abeliana de grau primo ímpar p e $\mathrm{G} = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Quando p não ramifica em $\mathbb{L}$, dizemos que $\mathbb{L}/\mathbb{Q}$ é brandamente ramificada ([1], IV.7). Nesse caso, o conjunto $\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma base normal integral de $\mathbb{L}$, onde $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$ e θ é um gerador de G. Desse modo, podemos expressar o anel de inteiros de $\mathbb{L}$ como

$$\mathfrak{O}_{\mathbb{L}} = \mathbb{Z}\mathrm{G}[t] = \mathbb{Z}t + \mathbb{Z}\theta(t) + \cdots + \mathbb{Z}\theta^{p-1}(t).$$

Em outras palavras, $\mathfrak{O}_{\mathbb{L}}$ é um $\mathbb{Z}$G-módulo livre de posto um, onde $\{t\}$ é linearmente independente sobre o anel de grupo $\mathbb{Z}$G, vide [9]. Segue, então, da Proposição 1.3.1 e do Teorema 2.2.2 que

(i) $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\theta^i(t)) = (-1)^s$;

(ii) $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}((\theta^i(t))^2) = n - (\frac{n-1}{p})$;

(iii) $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\theta^i(t)\theta^j(t)) = -(\frac{n-1}{p})$, se $i \neq j$;

para $i, j = 0, 1, \ldots, p-1$. Nessas condições dizemos que a base normal

$$\{t, \theta(t), \ldots, \theta^{p-1}(t)\}$$

é uma base lagrangiana. Essa base, quando existe, é única a menos de reordenação ([1], Def. IV.8.1 e Prop. IV.8.2). P. E. Conner e R. Perlis utilizaram essa terminologia, introduzida por Hilbert, para o caso particular em que um único primo ramifica em $\mathbb{L}$ (vide [1], IV.12).

Quando p é ramificado em $\mathbb{L}$, dizemos que $\mathbb{L}/\mathbb{Q}$ é severamente ramificada[1] ([1], IV.9). Nesse caso, o condutor de $\mathbb{L}$ é da forma $m = p^2 n$, onde $n = p_1 \ldots p_s$ e $p_1, \ldots, p_s$

[1]As expressões "brandamente ramificada" e "severamente ramificada" são traduções livres das originais "tamely ramified" e "wildly ramified", respectivamente; vide [1], Capítulo IV.

são primos ímpares distintos, com $p_k \equiv 1 \pmod{p}$, $k = 1, \ldots, s$ (vide Proposição 2.1.2) e

$$\mathrm{Disc}(\mathbb{L}) = n^{p-1}p^{2r+2},$$

para algum $r \geq 0$. Estas são condições iniciais para uma possível investigação da forma traço integral no caso ramificado. Contudo, não existe uma base normal integral para $\mathbb{L}$; vide Seção 1.3. A saber, $\mathfrak{O}_{\mathbb{L}}$ é um $\mathbb{Z}G$-módulo isomorfo à soma direta $\mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$ (vide [1], Seção IV.9).

CAPÍTULO 3

O Compósito de Extensões Abelianas de grau p não ramificado

Sejam p um primo ímpar e $n = p_1 \dots p_s$, onde $p_1, \dots, p_s$ são primos ímpares distintos tais que $p_i \equiv 1 \pmod{p}$, para $i = 1, \dots, s$. Chamaremos simplesmente por p-extensão a um corpo de números abeliano de grau p contido em $\mathbb{Q}(\zeta_n)$. Nesse caso, $\mathbb{Q}(\zeta_n)$ contém $(p^s - 1)/(p - 1)$ p-extensões, das quais $(p-1)^{s-1}$ têm condutor n, vide Seção 2.1. Considere as torres de compósitos de p-extensões da forma

$$\mathbb{Q} \subset \mathbb{L}_1 \subset \mathbb{L}_1\mathbb{L}_2 \subset \mathbb{L}_1\mathbb{L}_2\mathbb{L}_3 \subset \cdots \subset \mathbb{Q}(\zeta_n).$$

Na Seção 3.1 apresentamos as propriedades dos corpos intermediários e do topo dessas torres. Quando $\mathbb{L}_1$ e $\mathbb{L}_2$ são duas p-extensões linearmente disjuntas, provamos na Seção 3.2 que a forma traço canônica de $\mathbb{L}_1\mathbb{L}_2$ preserva o produto. Isto nos permite utilizar, por recorrência, o Teorema 2.2.2 para obter explicitamente a forma traço integral de $\mathbb{L}_1\mathbb{L}_2$. Na Seção 3.3, abordamos sobre possíveis aplicações e generalizações dos resultados neste capítulo obtidos, entre eles as investigações da forma traço do compósito de p-extensões, quando os respectivos condutores não são relativamente primos.

3.1 Torres de p-Extensões Abelianas

Nesta seção provamos que o corpo abeliano que representa o topo de qualquer torre de p-extensões é único e coincide com o Corpo de Gêneros. Em outras palavras, ele é unicamente determinado pelos parâmetros p e n. Apresentamos suas propriedades e,

na Seção 3.2, explicitamos sua forma traço canônica, como generalização do Teorema 3.2.2. Esse corpo já é conhecido na literatura no estudo das extensões não ramificadas, considerada sua estreita relação com o Corpo de Classes de Hilbert, vide [19].

Proposição 3.1.1. *Se $\mathbb{L}_1, \ldots, \mathbb{L}_u$ são p-extensões tais que $\mathbb{L}_1 \ldots \mathbb{L}_{k-1} \cap \mathbb{L}_k = \mathbb{Q}$, para todo $k = 2, \ldots, u$, então o compósito $\mathbb{L}_1 \ldots \mathbb{L}_u$ tem grau p^u e contém $(p^u - 1)/(p - 1)$ p-extensões.*

Demonstração. Temos que,

$$\begin{aligned} \mathrm{Gal}(\mathbb{L}_1 \ldots \mathbb{L}_u/\mathbb{Q}) &\simeq \mathrm{Gal}(\mathbb{L}_1 \ldots \mathbb{L}_{u-1}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{L}_u/\mathbb{Q}) \\ &\simeq \mathrm{Gal}(\mathbb{L}_1/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{L}_2/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{L}_u/\mathbb{Q}) \\ &\simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \ . \end{aligned}$$

Assim, a extensão galoisiana $\mathbb{L}_1 \ldots \mathbb{L}_u/\mathbb{Q}$ tem grau p^u e todo elemento não nulo de $H = \mathrm{Gal}(\mathbb{L}_1 \ldots \mathbb{L}_u/\mathbb{Q})$ tem ordem p, isto é, H possui $p^u - 1$ elementos de ordem p. Portanto, H contem $(p^u-1)/(p-1)$ subgrupos de ordem p, ou seja, existem exatamente $(p^u - 1)/(p - 1)$ p-extensões contidas em $\mathbb{L}_1 \ldots \mathbb{L}_u$. □

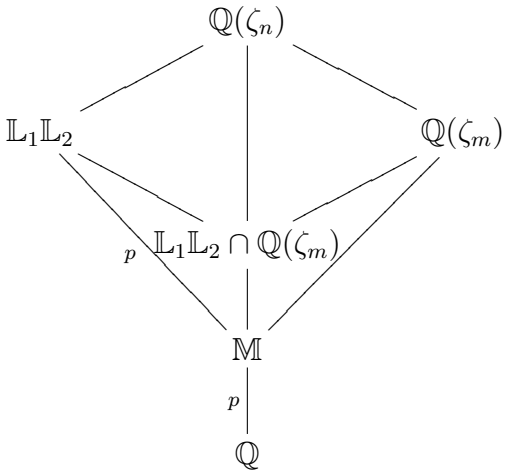
Se $\mathbb{L}_1$ e $\mathbb{L}_2$ são p-extensões distintas, então $\mathbb{L}_1\mathbb{L}_2$ contém $p + 1$ p-extensões; vide Proposição 3.1.1. Sejam m_1 e m_2 os condutores de $\mathbb{L}_1$ e $\mathbb{L}_2$, respectivamente. Nesse caso, o condutor de $\mathbb{L}_1\mathbb{L}_2$ é igual a n se, e somente se, $\mathrm{mmc}(m_1, m_2) = n$.

Proposição 3.1.2. *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões distintas, tais que $\mathbb{L}_1\mathbb{L}_2$ tem condutor n, e $\mathbb{M} \subset \mathbb{L}_1\mathbb{L}_2$ uma p-extensão de condutor $m < n$.*

(i) Então $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m)$ é a única p-extensão de condutor m contida em $\mathbb{L}_1\mathbb{L}_2$.

(ii) Seja d um divisor próprio de n. Então, $m|d$ se, e somente se, $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_d)$.

Demonstração. (i) Como $\mathbb{M} \subseteq \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m) \subseteq \mathbb{L}_1\mathbb{L}_2$ e $[\mathbb{L}_1\mathbb{L}_2 : M] = p$, segue que $\mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m) = M$ ou $\mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m) = \mathbb{L}_1\mathbb{L}_2$. O segundo não é possível, pois se ocorresse teríamos $\mathbb{L}_1\mathbb{L}_2 \subset \mathbb{Q}(\zeta_m)$. Logo, $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m)$. Além disso, essa representação garante que $\mathbb{M}$ é a única p-extensão de condutor m em $\mathbb{L}_1\mathbb{L}_2$. (ii) Suponha que m divide d, isto é, $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_d)$. Nesse caso, $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m) \subseteq \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_d) \subseteq \mathbb{L}_1\mathbb{L}_2$. Como $[\mathbb{L}_1\mathbb{L}_2 : M] = p$, segue que $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_d)$, pois $d < n$. Reciprocamente, suponha $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_d)$. Assim, $\mathbb{M} \subset \mathbb{Q}(\zeta_d)$ tem condutor m. Logo, os primos que dividem m também dividem d. □

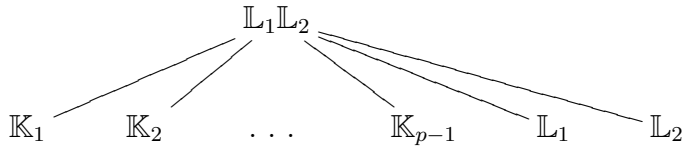


Lema 3.1.3. *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões de condutores m_1 e m_2, respectivamente, tais que $m_1 m_2 = n$. Então $\mathbb{L}_1$ e $\mathbb{L}_2$ são as únicas p-extensões de condutor menor que n contidas no compósito $\mathbb{L}_1\mathbb{L}_2$.*

Demonstração. Podemos supor $m_1 = p_1 \dots p_k$ e $m_2 = p_{k+1} \dots p_s$, para algum $k = 1, \dots, s-1$. Seja $\mathbb{L}_3 \subset \mathbb{L}_1\mathbb{L}_2$ uma p-extensão distinta de $\mathbb{L}_1$ e $\mathbb{L}_2$. Assim, $\mathbb{L}_1\mathbb{L}_3 = \mathbb{L}_1\mathbb{L}_2$, o que implica $\text{cond}(\mathbb{L}_1\mathbb{L}_3) = n$. Desse modo, $m_3 = \text{cond}(\mathbb{L}_3)$ deve conter no mínimo os primos $p_{k+1}, \dots, p_s$ em sua fatoração. Analogamente, os primos $p_1, \dots, p_k$ dividem m_3, pois $\mathbb{L}_2\mathbb{L}_3 = \mathbb{L}_1\mathbb{L}_2$. Logo, n divide m_3, ou seja, $\mathbb{L}_3$ tem condutor n. □

Observação 3.1.1. *Com as notações do Lema 3.1.3, temos que $m_1 m_2 = n$ se, e somente se, o condutor de $\mathbb{L}_1\mathbb{L}_2$ é igual a n e m_1 e m_2 são relativamente primos.*

Segue do Lema 3.1.3 que todas as p-extensões $\mathbb{K}_1, \dots, \mathbb{K}_{p-1}$ não triviais contidas no compósito $\mathbb{L}_1\mathbb{L}_2$ têm condutor n:



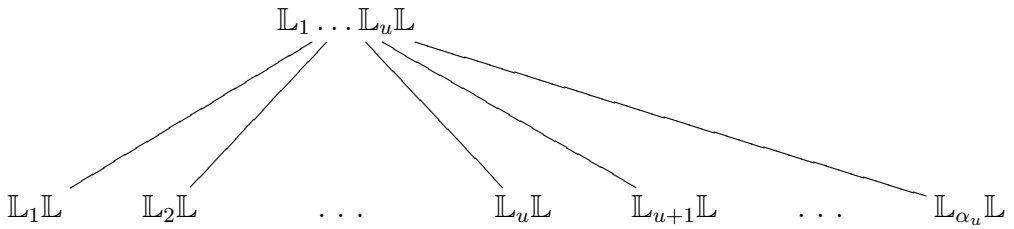
Lema 3.1.4. *Sejam $\mathbb{L}_1 \dots \mathbb{L}_u$ um compósito de p-extensões de grau p^u, com $u < s$ e $\mathbb{L} \not\subseteq \mathbb{L}_1 \dots \mathbb{L}_u$. Então toda p-extensão contida em $\mathbb{L}_1 \dots \mathbb{L}_u\mathbb{L}$ é também um subcorpo de $\mathbb{L}_i\mathbb{L}$, para algum $i = 1, \dots, \alpha_u$, onde os $\mathbb{L}_i$'s são as p-extensões contidas em $\mathbb{L}_1 \dots \mathbb{L}_u$ e $\alpha_u = (p^u - 1)/(p-1)$.*

Demonstração. Temos que $\mathbb{L}_1 \dots \mathbb{L}_u\mathbb{L}$ tem grau p^{u+1}, pois $\mathbb{L} \not\subseteq \mathbb{L}_1 \dots \mathbb{L}_u$. Toda p-extensão contida em $\mathbb{L}_i\mathbb{L}$ também está contida em $\mathbb{L}_1 \dots \mathbb{L}_u\mathbb{L}$. Basta então mostrar que a união $\bigcup_{i=1}^{\alpha_u} \mathbb{L}_i\mathbb{L}$ contém o mesmo número de p-extensões que $\mathbb{L}_1 \dots \mathbb{L}_u\mathbb{L}$, isto é,

contém $\alpha_{u+1} = (p^{u+1} - 1)/(p - 1)$ p-extensões. Note que cada compósito $\mathbb{L}_i\mathbb{L}$ contém $p + 1$ p-extensões. Mostremos que $\mathbb{L}$ é a única p-extensão contida em mais de um compósito $\mathbb{L}_i\mathbb{L}$. De fato, suponha que exista outra p-extensão $\mathbb{L}'$ tal que $\mathbb{L}' \subset \mathbb{L}_i\mathbb{L}$ e $\mathbb{L}' \subset \mathbb{L}_j\mathbb{L}$, com $i \neq j$. Daí, $\mathbb{L}_i\mathbb{L} = \mathbb{L}'\mathbb{L} = \mathbb{L}_j\mathbb{L}$, o que implica $\mathbb{L}_i(\mathbb{L}_j\mathbb{L}) = \mathbb{L}_i(\mathbb{L}_i\mathbb{L}) = \mathbb{L}_i\mathbb{L}$. Desse modo, o compósito $\mathbb{L}_1 \dots \mathbb{L}_u\mathbb{L}$ teria grau p^u, contradição. Sendo assim, com excessão de $\mathbb{L}$, todas as p-extensões contidas em $\mathbb{L}_i\mathbb{L}$, para $i = 1, \dots, \alpha_u$, são distintas. Portanto, temos no total

$$(p + 1) + p(\alpha_u - 1) = (p^{u+1} - 1)/(p - 1) = \alpha_{u+1}$$

p-extensões distintas em $\bigcup_{i=1}^{\alpha_u} \mathbb{L}_i\mathbb{L}$. □



Teorema 3.1.5. *Sejam $\mathbb{L}_1, \mathbb{L}_2, \dots, \mathbb{L}_u$ p-extensões tais que $\prod_{i=1}^{u} m_i = n$, onde $m_i = \text{cond}(\mathbb{L}_i)$, $i = 1, \dots, u$, com $u \in \{2, \dots, s\}$. Então, o compósito $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_u$ contém $(p - 1)^{u-1}$ p-extensões de condutor n.*

Demonstração. Seja $u \in \{2, \dots, s\}$. Mostremos que o compósito $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_k$ contém $(p - 1)^{k-1}$ p-extensões de condutor $m_1m_2 \dots m_k$, para todo $k = 2, \dots, u$. O faremos por indução sobre k. Para $k = 2$ temos que $\text{mdc}(m_1, m_2) = 1$. Logo, pelo Lema 3.1.3, o compósito $\mathbb{L}_1\mathbb{L}_2$ contém $p - 1$ p-extensões de condutor m_1m_2. Suponha a asserção válida para $k = u - 1$. Sejam $\mathbb{M}_1, \dots, \mathbb{M}_\alpha$ as p-extensões de condutor $m_1m_2 \dots m_{u-1}$ e $\mathbb{L}_1, \dots, \mathbb{L}_\beta$ as p-extensões de condutor menor que $m_1m_2 \dots m_{u-1}$ contidas em $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_{u-1}$, onde $\alpha = (p-1)^{u-2}$ e $\beta = \alpha_{u-1} - \alpha$, com $\alpha_{u-1} = (p^{u-1}-1)/(p-1)$. Como $\text{mdc}(m_u, m_1 \dots m_{u-1}) = 1$, segue que $\mathbb{L}_u \not\subseteq \mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_{u-1}$. Assim, pelo Lema 3.1.4, toda p-extensão contida em $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_u$ pode ser obtida como subcorpo de um dos compósitos

$$\mathbb{M}_1\mathbb{L}_u, \dots, \mathbb{M}_\alpha\mathbb{L}_u, \mathbb{L}_1\mathbb{L}_u, \dots, \mathbb{L}_\beta\mathbb{L}_u.$$

Para cada $i = 1, \dots, \alpha$ o compósito $\mathbb{M}_i\mathbb{L}_u$ contém $p - 1$ p-extensões de condutor $m_1m_2 \dots m_u$ e todas as p-extensões contidas em $\mathbb{L}_j\mathbb{L}_u$ têm condutor menor que $m_1m_2 \dots m_u$, com $j = 1, \dots, \beta$. Portanto, o compósito $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_u$ contém $\alpha(p - 1) = (p - 1)^{u-1}$ p-extensões de condutor $m_1m_2 \dots m_u = n$. □

Corolário 3.1.6. *Se um corpo $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ contém todas as p-extensões de condutor n, então conterá todas as p-extensões em $\mathbb{Q}(\zeta_n)$.*

Demonstração. Suponha que o corpo $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ contém todas as p-extensões de condutor n. Dada $\mathbb{M}$ uma p-extensão de condutor $m < n$, considere $\mathbb{M}'$ uma p-extensão de condutor n/m. Assim, pelo Teorema 3.1.5, o compósito $\mathbb{M}\mathbb{M}'$ contém $p-1$ p-extensões de condutor n. Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ duas delas. Como $\mathbb{L}_1, \mathbb{L}_2 \subset \mathbb{K}$, teremos que $\mathbb{K}$ contém $\mathbb{L}_1\mathbb{L}_2 = \mathbb{M}\mathbb{M}'$. Logo, $\mathbb{K}$ contém $\mathbb{M}$. Portanto, $\mathbb{K}$ contém também todas as p-extensões de condutor menor que n. □

Com as notações do Teorema 3.1.5, seja $u = s$, isto é, considere o compósito

$$\mathbb{L}^* = \mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_s \subset \mathbb{Q}(\zeta_n),$$

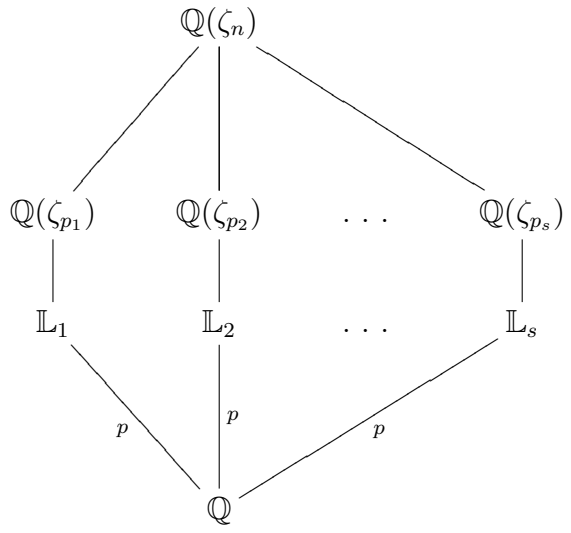
onde $\mathbb{L}_i$ é a única p-extensão de condutor p_i, com $i = 1, 2, \dots, s$ (vide Proposição 2.1.3). Como p_i é o único primo que ramifica em $\mathbb{L}_i$, segue que $\mathbb{L}^*$ tem grau p^s sobre $\mathbb{Q}$ e, pela Proposição 1.1.23, seu anel de inteiros é dado pelo produto

$$\mathfrak{O}_{\mathbb{L}^*} = \mathfrak{O}_{\mathbb{L}_1}\mathfrak{O}_{\mathbb{L}_2} \dots \mathfrak{O}_{\mathbb{L}_s}$$

e $|\mathrm{Disc}(\mathbb{L}^*)| = n^{p^{s-1}(p-1)}$. Pelo Teorema 3.1.5, temos que $\mathbb{L}^*$ contém $(p-1)^{s-1}$ p-extensões de condutor n. Logo, contém todas as p-extensões em $\mathbb{Q}(\zeta_n)$, vide Corolário 3.1.6. Desse modo, $\mathbb{L}^*$ é o topo de qualquer torre de p-extensões:

$$\mathbb{Q} \subset \mathbb{L}_1 \subset \mathbb{L}_1\mathbb{L}_2 \subset \dots \subset \mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_s = \mathbb{L}^* \subset \mathbb{Q}(\zeta_n).$$

Além disso, ele é único nessas condições, pois qualquer compósito de p-extensões que contém todas elas, contém cada $\mathbb{L}_i$ em particular, ou seja, pode ser representado por $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_s$.



O corpo de números $\mathbb{L}^*$ é já conhecido na literatura como o Corpo de Gêneros[1], com respeito a uma p-extensão $\mathbb{L}$ de condutor n. Ele é originalmente definido como sendo o corpo de números abeliano maximal contendo $\mathbb{L}$, de modo que $\mathbb{L}^*/\mathbb{L}$ seja não ramificada. Sob essa terminologia, Zhang Xianke demonstrou, em [19], que o Corpo de Gêneros tem a representação $\mathbb{L}^* = \mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_s$ descrita acima. Note que

$$\mathbb{L}^* = \mathrm{H}(\mathbb{L}) \cap \mathbb{Q}(\zeta_n),$$

isto é, $\mathbb{L}^*$ é um subcorpo do Corpo de Classes de Hilbert $\mathrm{H}(\mathbb{L})$ tal que, quando $\mathrm{H}(\mathbb{L})$ é abeliano sobre os racionais, temos $\mathbb{L}^* = \mathrm{H}(\mathbb{L})$.

Observação 3.1.2. *Note que, pelo Corolário 3.1.6, o Corpo de Gêneros pode também ser representado como* $\mathbb{L}^* = \mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_s$, *onde* $\mathrm{cond}(\mathbb{K}_i) = n$, *para cada* $i = 1, \dots, s$.

3.2 Forma Traço Integral do Compósito de p-Extensões linearmente disjuntas

Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões de condutores m_1 e m_2, respectivamente, com m_1 e m_2 relativamente primos e $\mathrm{cond}(\mathbb{L}_1\mathbb{L}_2) = n$ (ou seja, $m_1m_2 = n$, vide Observação 3.1.1). Se $\theta_1|_{\mathbb{L}_1}$ e $\theta_2|_{\mathbb{L}_2}$ são geradores de $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q})$ e $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$, respectivamente (com $\theta_1, \theta_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$) e $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$, então

$$\{(\theta_1^i \circ \theta_2^j)(t) \ ; \ i, j = 0, 1, \dots, p-1\}$$

é uma base normal integral de $\mathbb{L}_1\mathbb{L}_2$; vide Teorema 1.3.4. O objetivo desta seção é apresentar uma expressão para a forma traço integral $\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2)$, com respeito a essa base.

Dado

$$x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t) \in \mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2},$$

temos que

$$x^2 = \sum_{i,j=0}^{p-1} \sum_{u,v=0}^{p-1} a_{ij}a_{uv}(\theta_1^i \circ \theta_2^j)(t)(\theta_1^u \circ \theta_2^v)(t).$$

Logo,

$$\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) = \sum_{i,u=0}^{p-1} \sum_{j,v=0}^{p-1} a_{ij}a_{uv}\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t\ (\theta_1^{i-u} \circ \theta_2^{j-v})(t)).$$

[1] O termo "Corpo de Gêneros" é tradução livre do original "Genus Field", vide [19].

Desse modo, a forma traço canônica de $\mathbb{L}_1\mathbb{L}_2$ pode ser expressa como

$$\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t)),$$

com $k_1, k_2 = 0, 1, \ldots, p-1$.

As caracterizações acima não exigem que os condutores m_1 e m_2 sejam relativamente primos. Todavia, tal condição é necessária no que segue.

Lema 3.2.1. *Sejam* $\mathrm{H}_1 = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{Q}(\zeta_{m_2}))$ *e* $\mathrm{H}_2 = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_2\mathbb{Q}(\zeta_{m_1}))$. *Então,*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2) = \{\ \gamma_1 \circ \gamma_2\ ;\ \gamma_1 \in \mathrm{H}_1,\ \gamma_2 \in \mathrm{H}_2\ \}.$$

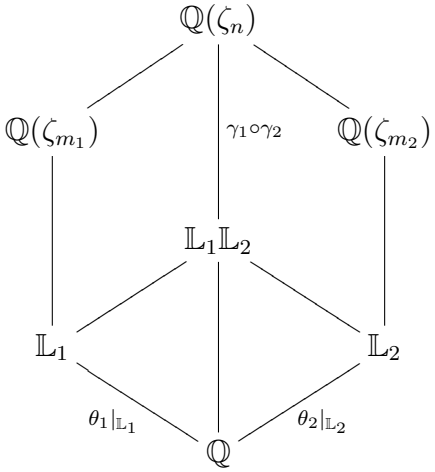
Demonstração. Denotemos $\mathrm{H}' = \{\gamma_1 \circ \gamma_2\ ;\ \gamma_1 \in \mathrm{H}_1,\ \gamma_2 \in \mathrm{H}_2\}$. Temos que $\mathrm{H}_1, \mathrm{H}_2 \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2)$. Logo, H' é um subgrupo de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2)$. Sejam $\gamma_1\circ\gamma_2, \gamma_3\circ\gamma_4 \in \mathrm{H}'$ tais que $\gamma_1 \circ \gamma_2 = \gamma_3 \circ \gamma_4$. Assim,

$$\gamma_1 \circ \gamma_3^{-1} = \gamma_2^{-1} \circ \gamma_4 \in \mathrm{H}_1 \cap \mathrm{H}_2 \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{m_2})) \cap \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{m_1})).$$

Porém, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{m_2})) \cap \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{m_1})) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{m_2})\mathbb{Q}(\zeta_{m_1})) = \{Id\}$. Logo, $\gamma_1 = \gamma_3$ e $\gamma_2 = \gamma_4$. Ou seja, os elementos descritos em H' são todos distintos. Desse modo,

$$\circ(\mathrm{H}') = \frac{\phi(m_1)}{p}\frac{\phi(m_2)}{p} = \frac{\phi(n)}{p^2} = \circ(\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2)).$$

Portanto, $\mathrm{H}' = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2)$. □



Teorema 3.2.2. *Sejam* $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$, $t_1 = \mathrm{Tr}_{\mathbb{Q}(\zeta_{m_1})/\mathbb{L}_1}(\zeta_{m_1})$, $t_2 = \mathrm{Tr}_{\mathbb{Q}(\zeta_{m_2})/\mathbb{L}_2}(\zeta_{m_2})$ *e* $\theta_1|_{L_1}$ *e* $\theta_2|_{L_2}$ *geradores de* $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q})$ *e* $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$ *respectivamente, onde* $\theta_1, \theta_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. *Então,*

$$\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t)) = \mathrm{Tr}_{\mathbb{L}_1/\mathbb{Q}}(t_1\theta_1^{k_1}(t_1))\ \mathrm{Tr}_{\mathbb{L}_2/\mathbb{Q}}(t_2\theta_2^{k_2}(t_2)),$$

com $k_1, k_2 = 0, 1, \ldots, p-1$.

Demonstração. Denotemos $\mathbb{K} = \mathbb{Q}(\zeta_n)$, $\mathbb{L} = \mathbb{L}_1\mathbb{L}_2$ e $\mathrm{H} = \mathrm{Gal}(\mathbb{K}/\mathbb{L})$. Temos que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \{(\theta_1^{k_1} \circ \theta_2^{k_2})|_{\mathbb{L}} \ ; \ k_1, k_2 = 0, 1, \ldots, p-1\}$. Pondo $r = m_1 + m_2$, temos $\zeta_n^r = \zeta_{m_1}\zeta_{m_2}$, onde $(r, n) = 1$. Ou seja, $\sigma_r(\zeta_n) = \zeta_{m_1}\zeta_{m_2}$, onde $\sigma_r \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ é definido por $\sigma_r(\zeta_n) = \zeta_n^r$. Assim,

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t)) &= \sigma_r(\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t))) \\
&= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\sigma_r(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t))) \\
&= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\sigma_r(t)(\theta_1^{k_1} \circ \theta_2^{k_2})(\sigma_r(t))).
\end{aligned}$$

Note que,

$$\sigma_r(t) = \sigma_r(\sum_{\gamma \in \mathrm{H}} \gamma(\zeta_n)) = \sum_{\gamma \in \mathrm{H}} \gamma(\sigma_r(\zeta_n)) = \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\zeta_{m_1}\zeta_{m_2}).$$

Porém, pelo Lema 3.2.1, temos que $\mathrm{H} = \{\gamma_1 \circ \gamma_2 \ ; \ \gamma_1 \in \mathrm{H}_1, \ \gamma_2 \in \mathrm{H}_2\}$, onde $\mathrm{H}_1 = \mathrm{Gal}(\mathbb{K}/\mathbb{L}_1\mathbb{Q}(\zeta_{m_2}))$ e $\mathrm{H}_2 = \mathrm{Gal}(\mathbb{K}/\mathbb{L}_2\mathbb{Q}(\zeta_{m_1}))$. Logo,

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\zeta_{m_1}\zeta_{m_2}) &= \sum_{\gamma_1 \in \mathrm{H}_1, \gamma_2 \in \mathrm{H}_2} (\gamma_1 \circ \gamma_2)(\zeta_{m_1}\zeta_{m_2}) \\
&= \sum_{\gamma_1 \in \mathrm{H}_1, \gamma_2 \in \mathrm{H}_2} \gamma_1(\zeta_{m_1})\gamma_2(\zeta_{m_2}) \\
&= \sum_{\gamma_1 \in \mathrm{H}_1} \gamma_1(\zeta_{m_1}) \sum_{\gamma_2 \in \mathrm{H}_2} \gamma_2(\zeta_{m_2}) \\
&= \mathrm{Tr}_{\mathbb{K}/\mathbb{L}_1\mathbb{Q}(\zeta_{m_2})}(\zeta_{m_1})\mathrm{Tr}_{\mathbb{K}/\mathbb{L}_2\mathbb{Q}(\zeta_{m_1})}(\zeta_{m_2}) \\
&= \mathrm{Tr}_{\mathbb{Q}(\zeta_{m_1})/\mathbb{L}_1}(\zeta_{m_1})\mathrm{Tr}_{\mathbb{Q}(\zeta_{m_2})/\mathbb{L}_2}(\zeta_{m_2}).
\end{aligned}$$

Ou seja, $\sigma_r(t) = \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\zeta_{m_1}\zeta_{m_2}) = t_1t_2$. Portanto,

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t)) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t_1t_2\ (\theta_1^{k_1} \circ \theta_2^{k_2})(t_1t_2)) \\
&= \mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(t_1\theta_1^{k_1}(t_1)\ t_2\theta_2^{k_2}(t_2)) \\
&= \sum_{i,j=0}^{p-1} (\theta_1^i \circ \theta_2^j)(t_1\theta_1^{k_1}(t_1)\ t_2\theta_2^{k_2}(t_2)) \\
&= \sum_{i=0}^{p-1} \theta_1^i(t_1\theta_1^{k_1}(t_1)) \sum_{j=0}^{p-1} \theta_2^j(t_2\theta_2^{k_2}(t_2)) \\
&= \mathrm{Tr}_{\mathbb{L}_1/\mathbb{Q}}(t_1\theta_1^{k_1}(t_1))\ \mathrm{Tr}_{\mathbb{L}_2/\mathbb{Q}}(t_2\theta_2^{k_2}(t_2)),
\end{aligned}$$

com $k_1, k_2 = 0, 1, \ldots, p-1$. □

Corolário 3.2.3. *Com as mesmas hipóteses do Teorema 3.2.2, temos que*

$$\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t\ (\theta_1^{k_1}\circ\theta_2^{k_2})(t)) = \begin{cases} \left(m_1-\frac{m_1-1}{p}\right)\left(m_2-\frac{m_2-1}{p}\right), & k_1=k_2=0 \\ -\left(m_1-\frac{m_1-1}{p}\right)\left(\frac{m_2-1}{p}\right), & k_1=0 \text{ e } k_2\neq 0 \\ -\left(\frac{m_1-1}{p}\right)\left(m_2-\frac{m_2-1}{p}\right), & k_1\neq 0 \text{ e } k_2=0 \\ \left(\frac{m_1-1}{p}\right)\left(\frac{m_2-1}{p}\right), & k_1\neq 0 \text{ e } k_2\neq 0 \end{cases}$$

com $k_1, k_2 = 0, 1, \ldots, p-1$.

Demonstração. Segue dos Teoremas 2.2.2 e 3.2.2. □

Corolário 3.2.4. *Se* $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i\circ\theta_2^j)(t)$ *é um elemento do anel de inteiros* $\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2}$, *então*

$$\begin{aligned}\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= m_1m_2\left(\sum_{i,j=0}^{p-1}a_{ij}^2\right) - \frac{m_1(m_2-1)}{p}\left(\sum_{i=0}^{p-1}A_i^2\right) \\ &\quad -\frac{m_2(m_1-1)}{p}\left(\sum_{i=0}^{p-1}B_i^2\right) + \frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1}a_{ij}\right)^2,\end{aligned}$$

onde $A_i = \sum_{j=0}^{p-1} a_{ij}$ *e* $B_i = \sum_{j=0}^{p-1} a_{ji}$, *para cada* $i = 0, 1, \ldots, p-1$.

Demonstração. Vimos que

$$\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) = \sum_{i,u=0}^{p-1}\sum_{j,v=0}^{p-1} a_{ij}a_{uv}\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t\ (\theta_1^{i-u}\circ\theta_2^{j-v})(t)).$$

Logo, denotando

$$a_1 = \sum_{i,j=0}^{p-1} a_{ij}^2\ , \quad a_2 = \sum_{i=0}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{iv}\ ,$$

$$a_3 = \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{j=0}^{p-1} a_{ij}a_{uj} \quad e \quad a_4 = \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{uv}\ ,$$

segue que

$$
\begin{aligned}
\mathrm{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= \left(m_1-\frac{m_1-1}{p}\right)\left(m_2-\frac{m_2-1}{p}\right)a_1-\left(m_1-\frac{m_1-1}{p}\right)\left(\frac{m_2-1}{p}\right)a_2 \\
&\quad -\left(\frac{m_1-1}{p}\right)\left(m_2-\frac{m_2-1}{p}\right)a_3+\left(\frac{m_1-1}{p}\right)\left(\frac{m_2-1}{p}\right)a_4 \\
&= m_1m_2\ a_1-\frac{m_1(m_2-1)}{p}(a_1+a_2) \\
&\quad -\frac{m_2(m_1-1)}{p}(a_1+a_3)+\frac{(m_1-1)(m_2-1)}{p^2}(a_1+a_2+a_3+a_4) \\
&= m_1m_2\left(\sum_{i,j=0}^{p-1}a_{ij}^2\right)-\frac{m_1(m_2-1)}{p}\left(\sum_{i=0}^{p-1}A_i^2\right) \\
&\quad -\frac{m_2(m_1-1)}{p}\left(\sum_{i=0}^{p-1}B_i^2\right)+\frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1}a_{ij}\right)^2,
\end{aligned}
$$

onde $A_i=\sum_{j=0}^{p-1}a_{ij}$ e $B_i=\sum_{j=0}^{p-1}a_{ji}$, para cada $i=0,1,\ldots,p-1$.

□

Observação 3.2.1. *Note que, para $s=2$ temos $m_i=p_i$, com $i=1,2$. Logo, o compósito $\mathbb{L}_1\mathbb{L}_2$ é o Corpo de Gêneros de uma p-extensão de condutor $n=p_1p_2$.*

De modo geral, considere o Corpo de Gêneros $\mathbb{L}^*=\mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_s$ (com respeito a qualquer uma das $(p-1)^{s-1}$ p-extensões de condutor n), onde $\mathbb{L}_i$ é o único corpo de números de grau p e condutor p_i, para cada $i=1,\ldots,s$. Se $\theta_i|_{\mathbb{L}_i}$ é um gerador de $\mathrm{Gal}(\mathbb{L}_i/\mathbb{Q})$, com $\theta_i\in\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, então

$$
\{(\theta_1^{k_1}\circ\cdots\circ\theta_s^{k_s})(t)\ ;\ k_i=0,1,\ldots,p-1\ ,i=1,\ldots,s\}
$$

é uma base normal integral de $\mathbb{L}^*$, onde $t=\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}^*}(\zeta_n)$, vide Teorema 1.3.4. Nesse caso, se $t_i=\mathrm{Tr}_{\mathbb{Q}(\zeta_{p_i})/\mathbb{L}_i}(\zeta_{p_i})$, então, analogamente ao Teorema 3.2.2, a forma traço canônica do Corpo de Gêneros $\mathbb{L}^*$ é dada pelo produto

$$
\mathrm{Tr}_{\mathbb{L}^*/\mathbb{Q}}(t\ (\theta_1^{k_1}\circ\ldots\circ\theta_s^{k_s})(t))=\prod_{i=1}^{s}\mathrm{Tr}_{\mathbb{L}_i/\mathbb{Q}}(t_i\ \theta_i^{k_i}(t_i)),
$$

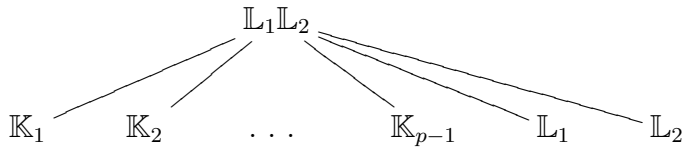
onde

$$
\mathrm{Tr}_{\mathbb{L}_i/\mathbb{Q}}(t_i\ \theta_i^{k_i}(t_i))=\begin{cases} p_i-(\frac{p_i-1}{p})\ , & \text{se } k_i=0 \\ -(\frac{p_i-1}{p})\ , & \text{se } k_i\neq 0\ , \end{cases}
$$

com $k_i=0,1,\ldots,p-1$, para cada $i=1,\ldots,s$. Assim, temos 2^s possíveis valores de $\mathrm{Tr}_{\mathbb{L}^*/\mathbb{Q}}(t\ (\theta_1^{k_1}\circ\ldots\circ\theta_s^{k_s})(t))$ dados explicitamente.

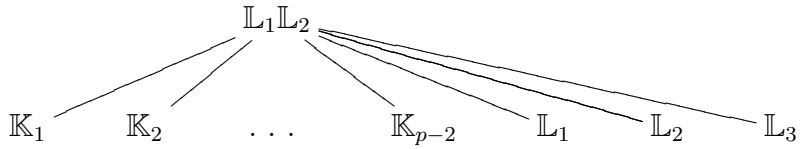
3.3 Perspectivas e a Intersecção de Condutores

Sejam $\mathbb{L}_1, \mathbb{L}_2 \subset \mathbb{Q}(\zeta_n)$ p-extensões de condutores m_1 e m_2, respectivamente, tais que $\text{cond}(\mathbb{L}_1\mathbb{L}_2) = n$ ($\text{mmc}(m_1, m_2) = n$). O compósito $\mathbb{L}_1\mathbb{L}_2$ contém $p+1$ p-extensões. Consideramos primeiramente m_1 e m_2 relativamente primos. Segue do Lema 3.1.3 que $\mathbb{L}_1$ e $\mathbb{L}_2$ são as únicas p-extensões de condutor menor que n contidas no compósito $\mathbb{L}_1\mathbb{L}_2$, isto é, as demais p-extensões $\mathbb{K}_1, \ldots, \mathbb{K}_{p-1}$ contidas em $\mathbb{L}_1\mathbb{L}_2$ têm condutor n. Nesse caso, pelo Teorema 3.2.2, a forma traço canônica do compósito $\mathbb{L}_1\mathbb{L}_2$ preserva o produto.



Note que $\mathbb{L}_1\mathbb{L}_2 = \mathbb{K}_i\mathbb{K}_j$, para quaisquer $i, j = 1, \ldots, p-1$. Porém, ao trabalhar com um compósito da forma $\mathbb{K}_i\mathbb{K}_j$, estaríamos omitindo os condutores m_1 e m_2, o que torna essa representação inconveniente para fins computacionais.

Quando $\text{mdc}(m_1, m_2) \neq 1$, existem múltiplas possibilidades. Considere a mais simples delas. Se $\text{mdc}(m_1, m_2) = p_k$, para algum $k = 1, \ldots, s$, e existe uma p-extensão $\mathbb{L}_3 \subset \mathbb{L}_1\mathbb{L}_2$ de condutor menor que n, distinta de $\mathbb{L}_1$ e $\mathbb{L}_2$, então $\mathbb{L}_3$ tem condutor n/p_k. Nesse caso, $\mathbb{L}_1, \mathbb{L}_2$ e $\mathbb{L}_3$ são as únicas p-extensões de condutor menor que n contidas em $\mathbb{L}_1\mathbb{L}_2$.



Sejam, por exemplo, $\mathbb{L} = \mathbb{L}_1\mathbb{L}_2$, $n = p_1p_2p_3$ e $t = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{L}}(\zeta_n)$. Iremos estimar a forma traço canônica parcial $\text{Tr}_{\mathbb{L}/\mathbb{Q}}(t^2)$ em ambos os casos, $\text{mdc}(m_1, m_2) = 1$ e $\neq 1$. Considere primeiramente $m_1 = p_1p_2$ e $m_2 = p_3$ ($\mathbb{L}_1$ e $\mathbb{L}_2$ linearmente disjuntos). Pelo Corolário 3.2.3, temos que

$$\text{Tr}_{\mathbb{L}/\mathbb{Q}}(t^2) = \frac{n - (p_1p_2 + p_3) + 1}{p^2}(p-1)^2 + \frac{p_1p_2 + p_3 - 2}{p}(p-1) + 1.$$

Suponha, agora, $m_1 = p_1p_2$ e $m_2 = p_2p_3$. Utilizando contagem e combinatória obtemos, de maneira análoga ao Teorema 2.2.2, que

$$\text{Tr}_{\mathbb{L}/\mathbb{Q}}(t^2) = \frac{n - (p_1 + p_2 + p_3) + 2}{p^2}(p-1)^2 + \left(\frac{p_1 + p_2 + p_3 - 3}{p} - \frac{\phi(n)}{p^2}\right)(p-1) + 1.$$

Esses dois casos ilustram como a intersecção de condutores se comporta na expressão da forma traço canônica. As estimativas acima fazem parte de uma possível generalização do caso não linearmente disjunto.

Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ linearmente disjuntos e suponha que $m_1 = p_1 \dots p_r$ e $m_2 = p_{r+1} \dots p_s$. Considere o número primo p_1. Ele é totalmente ramificado em $\mathbb{L}_1$, isto é, existe um ideal primo $\mathfrak{p}$ de $\mathfrak{O}_{\mathbb{L}_1}$ tal que $p_1\mathfrak{O}_{\mathbb{L}_1} = \mathfrak{p}^p$ e $[\mathfrak{O}_{\mathbb{L}_1}/\mathfrak{p} : \mathbb{Z}/p_1\mathbb{Z}] = 1$. Sejam $t_1 = \mathrm{Tr}_{\mathbb{Q}(\zeta_{m_1})/\mathbb{L}_1}(\zeta_{m_1})$ e θ_1 é um gerador de $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q})$. Desse modo, $\mathfrak{p}$ é descrito explicitamente como um caso particular do $\mathbb{Z}$-módulo livre $\mathcal{M}_m$ definido em (2.2), a saber,

$$\mathfrak{p} = \mathcal{M}_{p_1} = \{a_0 t_1 + a_1\theta_1(t_1) + \cdots + a_{p-1}\theta_1^{p-1}(t_1) \in \mathfrak{O}_{\mathbb{L}_1} \,;\, a_0 + a_1 + \cdots + a_{p-1} \equiv 0 \pmod{p_1}\}.$$

Suponhamos que $\mathrm{ord}_{m_2} p_1 = 1$. Nesse caso, p_1 é totalmente decomposto em $\mathbb{L}_2$; vide Corolário 1.1.31. Assim, segue da Proposição 1.1.27 que $\mathfrak{p}$ é totalmente decomposto em $\mathbb{L}_1\mathbb{L}_2$, isto é,

$$p_1\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2} = (\mathfrak{P}_1 \dots \mathfrak{P}_p)^p,$$

onde $\mathfrak{P}_i$ é um ideal primo de $\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2}$, com $i = 1, \dots, p$. Suponha agora que $\mathrm{ord}_{m_2} p_1 = \phi(m_2)$. Nesse caso, p_1 é inerte em $\mathbb{L}_2$, ou seja, $\mathfrak{p}$ é inerte em $\mathbb{L}_1\mathbb{L}_2$. Logo,

$$p_1\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2} = \mathfrak{P}^p,$$

onde $\mathfrak{P}$ é um ideal primo de $\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2}$. Assim sendo, é parte das investigações futuras descrever explicitamente os ideais $\mathfrak{P}$ e $\mathfrak{P}_1, \dots, \mathfrak{P}_p$ de $\mathfrak{O}_{\mathbb{L}_1\mathbb{L}_2}$ que estão acima de p_1 (sob as respectivas condições de decomposição) e minimizar a forma traço integral de $\mathbb{L}_1\mathbb{L}_2$, obtida no Corolário 3.2.4, restrita a esses ideais, de modo a estimar a densidade de centro dos reticulados p^2-dimensionais $\sigma_{\mathbb{L}_1\mathbb{L}_2}(\mathfrak{P})$ e $\sigma_{\mathbb{L}_1\mathbb{L}_2}(\mathfrak{P}_i)$, com $i = 1, \dots, p$.

Referências Bibliográficas

[1] Conner, P. E., Perlis, R.: *A Survey of Trace Forms of Algebraic Number Fields*, World Scientific Publishing Co Pte Ltd., Singapore, 1984.

[2] Conway, J. H., Sloane, N. J. A.: *Sphere Packings, Lattices and Groups*, 3rd Edition, Springer Verlag, New York, 1999.

[3] Endler, O.: *Teoria dos Números Algébricos*, Projeto Euclides, IMPA, Rio de Janeiro, 1986.

[4] Epkenhans, M.: *On Trace Forms of Algebraic Number Fields*, Arch. Math. 60 (1993), 527-529.

[5] Golod, E. S., Shafarevich, I. R.: *On Class Field Towers*, IANS 28 (1964), 261-272.

[6] Lang S.: *Algebraic Number Theory*, Addison-Wesley, New York, 1970.

[7] Marcus, D. A.: *Number Fields*, Springer-Verlag, New-York, 1977.

[8] Martinet, J.: *Tours de corps de classes et estimations de discriminants*, Invent. Math. 44 (1978), 65-73 [1,8].

[9] Milies, F. C. P.: *Anéis de Grupos*, SBM, São Paulo, 1976.

[10] Milies, F. C. P.: *Anéis e Módulos*, L.P.M., São Paulo, 1972.

[11] Narkiewicz, W.: *Elementary and Analytic Theory of Algebraic Numbers*, 3rd Edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[12] Nóbrega Neto, T. P., Lopes, J. O. D., Interlando, J. C.: *The Discriminant of Abelian Number Fields*, Journal of Algebra and its Applications 05 (2006), 35-41.

[13] Ribenboim, P.: *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[14] Roquette, P.: *On Class Field Towers*, Thompson Book Co., 231-249, Washington, 1967.

[15] Samuel P.: *Algebraic Theory of Numbers*, Hermann, Paris, 1970.

[16] Scharlau, W.: *On Trace Forms of Algebraic Number Fields*, Math. Z. 196 (1987), 125-127.

[17] Stewart, I. N.: *Galois Theory*, Chapman and Hall, London, 2003.

[18] Washington, L. C.: *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

[19] Xianke, Z.: *A Simple Construction of Genus Fields of Abelian Number Fields*, AMS 94 (1985), 393-395.

Índice Remissivo