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

Daniel Kenny Máximo Alves

Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas

São José do Rio Preto
2021

Daniel Kenny Máximo Alves

Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas

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

Financiadora: CAPES

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

São José do Rio Preto
2021

A474f

Alves, Daniel Kenny Máximo

Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas / Daniel Kenny Máximo Alves. -- São José do Rio Preto, 2020

115 p. : il.

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto

Orientador: Trajano Pires da Nobrega Neto

1. Corpos de Números. 2. Reticulados Algébricos. 3. Forma Traço Integral. 4. Corpo de Gênero. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Daniel Kenny Máximo Alves

Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas

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

Financiadora: CAPES

Comissão Examinadora

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

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

Prof. Dr. José Carmelo Interlando
San Diego State University

Prof. Dr. Everton Luiz de Oliveira
Universidade Federal de Mato Grosso do Sul

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

São José do Rio Preto
24 de novembro de 2020

A minha esposa Thaís,
a minha mãe Irani e aos meus
irmãos Kesley e Tatiane,
dedico

AGRADECIMENTOS

Ao concluir este trabalho, agradeço:

Primeiramente à Deus, por ter me dado a oportunidade de alcançar esse sonho.

À minha família, por entender minhas decisões, principalmente à minha esposa que eu tanto amo e que sempre permaneceu ao meu lado, me dando forças e ânimo para continuar em frente.

Ao professor Dr. Trajano Pires da Nóbrega Neto pela orientação nesses anos de doutorado, pela confiança, conselhos e incentivos para a realização deste trabalho.

Ao grande amigo Eliton pela troca de experiências e encontros semanais que muito contribuíram para o direcionamento das ideías aqui expostas.

Ao Corpo Docente e colegas do Departamento de Matemática do IBILCE, em especial aos professores Dr. Antonio e Dr. Ali por terem contribuído com valiosas lições na área de álgebra.

Deixo aqui um agradecimento especial ao professor Dr. Everton Luiz de Oliveira que mesmo não o conhecendo pessoalmente muito contribuiu para este trabalho, pois foi através de sua tese de doutorado que me inspirei para escrever este texto.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

Sejam $\mathbb{K}$ e $\mathbb{L}$ *p*-extensões abelianas não ramificadas de condutores livres de quadrados *m* e *n*, respectivamente, com *p* um primo ímpar. O objetivo principal deste trabalho é o de apresentar a Forma Traço Integral $Tr_{\mathbb{KL}/\mathbb{Q}}(x^2)$, com x um inteiro de $\mathbb{KL}$, nos casos em que *m* e *n* são relativamente primos e nos casos em que o mdc(*m*,*n*) é um inteiro primo. Se $m = p_1 p_2 \ldots p_s$ é a decomposição prima de *m* e $\mathbb{K}^*$ é o Corpo de Gênero de $\mathbb{K}$, também foi explicitada uma cadeia crescente de extensões de corpos $\mathbb{Q} \subset \mathbb{K}_1 = \mathbb{K} \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_s = \mathbb{K}^* \subseteq \mathbb{Q}(\xi_m)$, de forma que para cada i=1,2,...,s-1, a extensão $\mathbb{K}_{i+1}/\mathbb{K}_i$ é de grau *p*, não ramificada e é conhecido a expressão da Forma Traço Integral $Tr_{\mathbb{K}_i/\mathbb{Q}}(x^2)$, com x um inteiro de $\mathbb{K}_i$.

Palavras–chave: Corpos de Números. Reticulados Algébricos. Forma Traço Integral. Corpo de Gênero.

ABSTRACT/ RESUMEN/ RÉSUMÉ

Let $\mathbb{K}$ and $\mathbb{L}$ be unramified abelian *p*-extensions of square-free conductors *m* and *n*, respectively. The principal objective of this work is to present the integral trace form $Tr_{\mathbb{KL}/\mathbb{Q}}(x^2)$, with x a integer in $\mathbb{KL}$, in cases where *m* and *n* are relatively prime and in cases where the mdc(*m*,*n*) is a positive prime integer. If $m = p_1 p_2 \ldots p_s$ is the prime decomposition of *m* and $\mathbb{K}^*$ is the genus field of $\mathbb{K}$, also explained a ascending chain of fields extesions $\mathbb{Q} \subset \mathbb{K}_1 = \mathbb{K} \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_s = \mathbb{K}^* \subseteq \mathbb{Q}(\xi_m)$, so that for each i=1,2,…, s-1, $\mathbb{K}_{i+1}/\mathbb{K}_i$ is a unramified extesion of degree *p* and the expression of the integral trace form $Tr_{\mathbb{K}_i/\mathbb{Q}}(x^2)$, with x a integer in $\mathbb{K}_i$, is known.

Keywords/ Palabras-claves / Mots-clés: Number Fields. Algebraic Lattices. Integral Trace Form. Genus Field.

Sumário

1 Introducao

Os reticulados (subgrupos aditivos discretos) no $\mathbb{R}^n$ têm sido bastante estudados nos últimos tempos, neste tema um assunto que tem se sobressaído em pesquisas é o de quão denso é um empacotamento reticulado, ou seja, o estudo da proporção do espaço $\mathbb{R}^n$ recoberto por um empacotamento de esferas de mesmo raio.

Seja $\mathbb{K}/\mathbb{Q}$ uma extensão abeliana de grau n. Se $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n, então $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado algébrico de posto n, sendo $\sigma_{\mathbb{K}}$ o homomorfismo canônico. Além disso, conforme Corolário 2.3.14, a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{M})$ é dado por

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

onde

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

e

$$|\sigma_{\mathbb{K}}(x)|^2 = \begin{cases} Tr_{\mathbb{K}/\mathbb{Q}}(x^2) & \text{se} \quad \mathbb{K} \text{ é totalmente real;} \\ \dfrac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) & \text{se} \quad \mathbb{K} \text{ é totalmente imaginário,} \end{cases}$$

sendo $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$ uma forma quadrática, com x um inteiro algébrico de $\mathbb{K}$ sobre $\mathbb{Q}$, chamada de Forma Traço Integral de $\mathbb{K}$. Se $\{w_1, w_2, \ldots, w_n\}$ é uma base integral de $\mathbb{K}$, com $\mathbb{K}$ um corpo totalmente real, essa forma quadrática é dada por

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

onde $x = a_1w_1 + a_2w_2 + \cdots + a_nw_n \in \mathcal{O}_{\mathbb{K}}$.

Dessa forma, é possível estudar reticulados através de objetos algébricos, isto é, se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana de grau n e $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n, podemos determinar um reticulado de posto n. Além disso, para conhecermos sua densidade de centro, basta conhecermos o discriminante do corpo $\mathbb{K}$ ($\mathrm{Disc}(\mathbb{K})$), o índice do $\mathbb{Z}$-módulo $\mathcal{M}$ em $\mathcal{O}_{\mathbb{K}}$ ($[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$) e no caso de $\mathbb{K}$ ser um corpo totalmente real, o mínimo da Forma Traço Integral restrita ao $\mathbb{Z}$-módulo $\mathcal{M}$. Sendo que destes três objetos, geralmente o mais complexo de se obter é a Forma Traço Integral e sua minimização.

A motivação deste trabalho é contribuir com um acréscimo ao realizado por Oliveira, E. L. em sua tese de doutorado, referência [7], na qual ele exibiu a Forma Traço Integral de uma p-extensão abeliana não ramificada e também a Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas de condutores relativamente primos e linearmente disjuntos. Nos propomos estudar a Forma Traço Integral de um

compósito, de grau p^2, de p-extensões abelianas não ramificadas de condutor cheio, exigindo a existência de dois subcorpos de grau p e condutores coprimos. Também estudamos a Forma Traço Integral de um compósito, de grau p^2, de p-extensões abelianas não ramificadas de condutores m_1 e m_2, respectivamente, com $\mathrm{mdc}(m_1, m_2) = p_k$, sendo p_k um número primo.

Outras teses de doutorado também contribuíram com o estudo da Forma Traço Integral e vale ser ressaltado aqui: Em [3], Chagas, A. C., descreveu a Forma Traço Integral de uma p-extensão abeliana ramificada de condutor $n = p^2q$, onde $q \equiv 1(\mathrm{mod}\ p)$ e q é primo. Já em [1], Araujo, R. R., estendeu esse feito, obtendo a expressão da Forma Traço Integral de p-extensões abelianas ramificadas de condutores $n = p^2p_1p_2 \dots p_s$, sendo $p_i \equiv 1(\mathrm{mod}\ p)$ e $p_1, p_2, \dots, p_s$ primos distintos. Por fim, Moro, E. M., propôs em [6] a obtenção da Forma Traço Integral para compósitos $\mathbb{KL}$ de grau pq, com $\mathbb{K}$ e $\mathbb{L}$ p e q-extensões abelianas não ramificadas, respectivamente, com $p \neq q$.

O primeiro capítulo deste trabalho está reservado para os conceitos necessários para o amplo entendimento dos resultados aqui expostos. Ele é basicamente composto de resultados mais elementares conhecidos da Teoria de Galois, da Teoria Algébrica dos Números e também de Reticulados Algébricos.

No Capítulo 3 detalhamos resultados já obtidos em outros trabalhos (teses de doutorado) sobre o tema: Forma Traço Integral de p-extensões abelianas (ramificadas e não ramificadas) e o compósito de p e q extensões abelianas não ramificadas. Uma contribuição nossa para este capítulo, foi desenvolver uma maneira "adequada" e natural de obter a Forma Traço Integral do Corpo de Gênero $\mathbb{K}^*$ de uma p-extensão abeliana não ramificada $\mathbb{K}$ de condutor $n = p_1p_2 \dots p_s$, livre de quadrados. Para isso foi apresentado um algoritmo para expressar o compósito $\mathbb{K}\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_u$ na forma de um compósito do tipo $\mathbb{M}\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_u$, sendo $\mathbb{M}$ uma p-extensão abeliana não ramificada com $m, p_1, p_2, \dots, p_u$ coprimos entre em si, onde $m = \mathrm{cond}(\mathbb{M})$ e $p_i = \mathrm{cond}(\mathbb{K}_i)$, para $1 \leqslant i \leqslant u$. Em [7] foi apresentado uma expressão para a Forma Traço Integral para um compósito do tipo $\mathbb{M}\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_u$.

Em [7], Oliveira, E. L. determinou a Forma Traço Integral de um compósito de p-extensões abelianas não ramificadas de condutores coprimos na respectiva base normal integral. Em particular, para o caso de duas p-extensões abelianas não ramificadas $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ de condutores coprimos e livre de quadrados m_1 e m_2, respectivamente, tomando $n = m_1m_2$, temos que o compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ possui $p-1$ subcorpos de grau p e condutor n, conforme 3.1.5. O Capítulo 4 deste trabalho está dividido em quatro seções, onde nas duas primeiras é proposto o estudo da Forma Traço Integral dos compósitos de p-extensões abelianas não ramificadas $\mathbb{L}_1\mathbb{L}_2$, com $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$ ambos de condutor n, na respectiva base normal integral enquanto que nas duas últimas seções, buscamos contribuir com o estudo da Forma Traço Integral de um compósito de duas p-extensões abelianas não ramificadas, mas agora considerando o caso em que os condutores não sejam coprimos. Mais especificamente, sendo $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores m_1 e m_2, respectivamente, com $\mathrm{mdc}(m_1, m_2) = p_k$, sendo p_k um número primo diferente de m_1 e m_2. Os resultados mais relevantes das duas primeiras seções são: a Proposição 4.1.5, que relaciona geradores dos grupos $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q})$ e $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$ a uma potência $\tilde{t}$ e o Teorema 4.2.4 o qual expressa a forma traço integral canônica. Já nas seções finais, tem ênfase o Teorema 4.4.4, o qual expõe a expressão da Forma Traço Integral do compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$. A fim de deixar este capítulo mais leve, alguns resultados foram colocadas no Apêndice **??**, o qual será necessário apenas para a total compressão e veracidade dos resultados.

Por fim, no Capítulo 5 é apresentado algumas perspectivas de estudos a serem realizadas a partir dos resultados obtidos neste trabalho.

2 Conceitos Preliminares

Neste capítulo trataremos de tópicos fundamentais para a compreensão deste trabalho, tais tópicos serão divididos em 3 grandes vertentes, sendo elas: Teoria de Galois, Teoria Algébrica dos Números e conceitos de reticulados.

A primeira seção, que aborda assuntos da Teoria de Galois, tem seu foco principal no Teorema da Correspondência de Galois, Teorema 2.1.9.

Na sequência, dividimos a seção de Teoria Algébrica dos Números em três subseções, onde o primeiro refere-se a módulos e elementos inteiros algébricos, o segundo trás os conceitos de norma, traço e discriminante de Corpos de Números e alguns resultados relacionados e por fim, a última subseção é reservada para tratar sobre a decomposição de ideais.

Na última seção deste capítulo é abordado o conceito de reticulados e alguns resultados. A motivação central dessa seção é fazermos uma identificação dos $\mathbb{Z}$-módulos livres de posto finito n em um Corpo de Números $\mathbb{K}$ com reticulados em $\mathbb{R}^n$, através do mergulho de Minkowski.

A prova dos resultados deste capítulo serão omitidas, contudo, inserimos as referências utilizadas.

2.1 Teoria de Galois

Esta seção estará voltada para uma abordagem simples e direta sobre a Teoria de Galois que será útil no decorrer do trabalho. As referências principais utilizadas são os livros: Galois Theory de Ian Stewart, [15] e Classical Theory of Algebraic Numbers, [13]. Estaremos sempre considerando subcorpos de $\mathbb{C}$.

Definição 2.1.1. *Dizemos que um corpo $\mathbb{L}$ é uma* ***extensão de um corpo*** *$\mathbb{K}$ se $\mathbb{K} \subseteq \mathbb{L}$. Naturalmente, $\mathbb{L}$ pode ser identificado como um $\mathbb{K}$-espaço vetorial e a dimensão $dim_{\mathbb{K}}\mathbb{L} = [\mathbb{L} : \mathbb{K}]$ é chamada de* ***grau da extensão*** *de $\mathbb{L}$ sobre $\mathbb{K}$. Denotamos tal extensão por $\mathbb{L}/\mathbb{K}$.*

Qualquer extensão de corpos finita de $\mathbb{Q}$ é chamada de **corpo de números algébricos**, ou simplesmente, **corpo de números**. Além disso, dado um número primo p, chamaremos qualquer extensão $\mathbb{L}/\mathbb{Q}$ de grau p de ***p*-extensão**.

Exemplo 2.1.2. Dado $\alpha = \sqrt{3}$, temos que o polinômio minimal de α sobre $\mathbb{Q}$ é $p_\alpha(x) = x^2 - 3$, logo $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = \partial(p_\alpha(x)) = 2$ e portanto, $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3};\ a, b \in \mathbb{Q}\}$ é uma 2-extensão.

Exemplo 2.1.3. Considerando $\beta = \sqrt[3]{2}$, segue que $p_\beta(x) = x^3 - 2$ é o polinômio minimal de β sobre $\mathbb{Q}$ e assim $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4};\ a, b, c \in \mathbb{Q}\}$ é uma 3-extensão.

O teorema a seguir é conhecido como o Teorema da Multiplicidade dos Graus, ou ainda, como a lei das torres.

Teorema 2.1.4. (*[15], pág.68*) (*A Lei das Torres*) *Sejam* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ *corpos. Então a extensão* $\mathbb{L}/\mathbb{K}$ *é finita se, e somente se, as extensões* $\mathbb{L}/\mathbb{M}$ *e* $\mathbb{M}/\mathbb{K}$ *são finitas. Neste caso,* $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}].[\mathbb{M} : \mathbb{K}]$.

Sejam $\mathbb{L}/\mathbb{K}$ uma extensão e $\mathrm{Aut}(\mathbb{L}) = \{\sigma : \mathbb{L} \longrightarrow \mathbb{L};\ \sigma \text{ é isomorfismo de anéis}\}$ 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 $\mathrm{Aut}(L)$, chamado de **grupo de Galois de** $\mathbb{L}$ **sobre** $\mathbb{K}$.

Proposição 2.1.5 ([15] pág 128)**.** *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* $\mathbb{F}$.

Estabelecido o conceito de grupo de Galois de uma extensão de corpos $\mathbb{L}/\mathbb{K}$, podemos definir o que é uma extensão galoisiana, como segue:

Definição 2.1.6. *Uma extensão finita de corpos* $\mathbb{L}/\mathbb{K}$ *é dita ser de* ***Galois*** *ou* ***galoisiana*** *se* $[\mathbb{L} : \mathbb{K}] = \circ(Gal(\mathbb{L}/\mathbb{K}))$*. Nesse caso, se* $Gal(\mathbb{L}/\mathbb{K})$ *é abeliano* (*cíclico*) *dizemos que* $\mathbb{L}/\mathbb{K}$ *é uma extensão* ***abeliana*** (***cíclica***).

Um Corpo de Números $\mathbb{K}$ de grau finito n com grupo de Galois $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ abeliano é dito ser **uma extensão abeliana absoluta**, vide [18] página 316. Dessa forma, sempre que considerarmos p-extensões abelianas, estaremos tratando de extensões abelianas absolutas.

Exemplo 2.1.7. Dado um primo q, temos que $\mathbb{Q}[\sqrt{q}]$ é uma 2-extensão abeliana.

De fato, note que $[\mathbb{Q}[\sqrt{q}] : \mathbb{Q}] = 2$, uma vez que o polinômio minimal de $\sqrt{q}$ sobre $\mathbb{Q}$ é $p_{\sqrt{q}}(x) = x^2 - q$. Se $\sigma \in \mathrm{Gal}(\mathbb{Q}[\sqrt{q}]/\mathbb{Q})$, dado $x = a + b\sqrt{q} \in \mathbb{Q}[\sqrt{q}]$, temos que $\sigma(x) = \sigma(a) + \sigma(b)\sigma(\sqrt{q}) = a + b\sigma(\sqrt{q})$. Além disso, $\sigma(\sqrt{q})^2 = \sigma(\sqrt{q}^2) = \sigma(q) = q$, ou seja, $\sigma(\sqrt{q}) = \pm\sqrt{q}$. Dessa forma, $\mathrm{Gal}(\mathbb{Q}[\sqrt{q}]/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$, onde σ_1 é a aplicação identidade $(\sigma_1 : \sqrt{q} \longrightarrow \sqrt{q})$ e $\sigma_2 : \sqrt{q} \longrightarrow -\sqrt{q}$ é a aplicação conjugação. Portanto, $\mathbb{Q}[\sqrt{q}]$ é uma 2-extensão abeliana.

Exemplo 2.1.8. $\mathbb{Q}[\sqrt[3]{2}]$ é uma 3-extensão, porém não é uma extensão de Galois. Basta observar que dado $\sigma \in \mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$, temos que $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega^k$ para $k = 0, 1, 2$, onde $w = e^{\frac{2\pi i}{3}}$. Além disso, $\sigma \in \mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}])$, logo $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, ou seja, $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$ é o grupo trivial.

O próximo resultado é o mais importante dessa seção.

Teorema 2.1.9 ([15], pág.133) (Teorema da Correspondência de Galois)**.** *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão galoisiana.*

(i) Se H *é um subgrupo de* $G = Gal(\mathbb{L}/\mathbb{K})$*, então existe um único corpo* $\mathbb{M}$ *tal que* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ *e* $H = Gal(\mathbb{L}/\mathbb{M})$*. 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* $Gal(\mathbb{L}/\mathbb{M})$ *é o único subgrupo de* $Gal(\mathbb{L}/\mathbb{K})$ *que satisfaz*

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

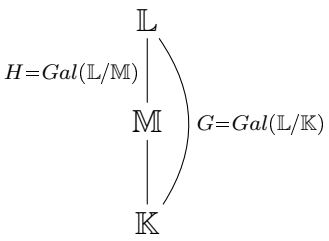

Figura 2.1: Correspondência de Galois.
Fonte: Próprio autor.

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

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

Observação 2.1.10. O teorema anterior foi reescrito de uma forma mais adequada para a utilização neste trabalho.

Sejam $\tilde{\mathbb{K}}$ uma extensão de $\mathbb{K}$, com $\mathbb{L}$ e $\mathbb{L}'$ subcorpos de $\tilde{\mathbb{K}}$ contendo $\mathbb{K}$. O **compósito de** $\mathbb{L}$ **e** $\mathbb{L}'$ **em** $\tilde{\mathbb{K}}$ é o menor subcorpo de $\tilde{\mathbb{K}}$ contendo $\mathbb{L}$ e $\mathbb{L}'$. Denotamos tal corpo por $\mathbb{L}\mathbb{L}'$.

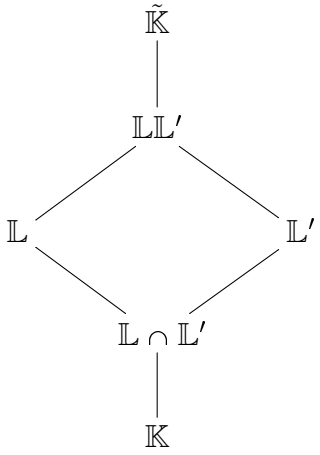

Figura 2.2: Compósito de dois corpos.
Fonte: Próprio autor.

O próximo resultado nos fornecerá uma forma de verificar se um compósito de corpos é galoisiano.

Proposição 2.1.11. (*[13], pág.17*) *Sejam* $\mathbb{L}/\mathbb{K}$ *e* $\mathbb{L}'/\mathbb{K}$ *extensões finitas de corpos, com* $\mathbb{L}/\mathbb{K}$ *uma extensão de Galois. Então o compósito* $\mathbb{L}\mathbb{L}'$ *é uma extensão de Galois sobre* $\mathbb{L}'$ *e* $Gal(\mathbb{L}\mathbb{L}'/\mathbb{L}') \cong Gal(\mathbb{L}/\mathbb{L}\cap\mathbb{L}')$*. Em particular, se* $\mathbb{L}/\mathbb{L}\cap\mathbb{L}'$ *e* $\mathbb{L}'/\mathbb{L}\cap\mathbb{L}'$ *são extensões de Galois, então* $\mathbb{L}\mathbb{L}'/\mathbb{L} \cap \mathbb{L}'$ *é uma extensão de Galois, com*

$$Gal(\mathbb{L}\mathbb{L}'/\mathbb{L} \cap \mathbb{L}') \cong Gal(\mathbb{L}/\mathbb{L} \cap \mathbb{L}') \times Gal(\mathbb{L}'/\mathbb{L} \cap \mathbb{L}').$$

Exemplo 2.1.12. Pelo exemplo 2.1.7, temos que $\mathbb{L} = \mathbb{Q}[\sqrt{2}]$ e $\mathbb{L}' = \mathbb{Q}[\sqrt{3}]$ são 2-extensões abelianas. Uma vez que x^2-3 é irredutível sobre $\mathbb{L}$, segue que $[\mathbb{L}[\sqrt{3}] : \mathbb{L}] = 2$

e pelo Teorema 2.1.4, temos que $\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}] = [\mathbb{L}[\sqrt{3}]:\mathbb{L}][\mathbb{L}:\mathbb{Q}] = 2.2 = 4$. Por outro lado, $\mathbb{L} \neq \mathbb{L}'$, assim $[\mathbb{L}\mathbb{L}':\mathbb{L}] \geqslant 2$, ou ainda, $[\mathbb{L}\mathbb{L}':\mathbb{Q}] \geqslant 4$. Além disso, como $\mathbb{L}\mathbb{L}' \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}]$, segue que $\mathbb{L}\mathbb{L}' = \mathbb{Q}[\sqrt{2},\sqrt{3}]$. Logo, $\mathbb{Q}[\sqrt{2},\sqrt{3}]/(\mathbb{L}\cap\mathbb{L}') = \mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$ é de Galois com

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}[\sqrt{3}]/\mathbb{Q}).$$

Seja n um inteiro positivo, o corpo $\mathbb{Q}(\zeta_n)$, onde $\zeta_n = e^{\frac{2\pi i}{n}}$, é chamado de n-ésimo corpo ciclotômico. Conforme [16], página 11, o grau da extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é dada pela função de Euler $\phi(n)$, isto é, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n) = \#\{t \in \{1,2,\ldots,n\}\,;\, mdc(t,n)=1\}$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_n/\mathbb{Q})) \simeq \mathbb{Z}_n^*$. É fácil ver que, se p é um número primo, então $\phi(p^r) = (p-1)p^{r-1}$, e se $\mathrm{mdc}(a,b)=1$, então $\phi(ab) = \phi(a)\phi(b)$.

O conjunto $\{1,\zeta_n,\zeta_n^2,\ldots,\zeta_n^{\phi(n)-1}\}$ é uma base de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$. Os elementos ζ_n^j tais que $1 \leqslant j \leqslant n$ e $mdc(j,n) = 1$ são chamados de raízes n-ésimas primitivas da unidade, e vale $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^j)$.

O polinômio minimal de ζ_n sobre $\mathbb{Q}$ será denotado por $\phi_n(x)$. Para um inteiro primo p, tem-se que

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

De modo geral, vale

$$\phi_n(x) = \prod_{d|n} \phi_d(x) = \prod_{\substack{1\leqslant j\leqslant n \\ mdc(j,n)=1}} (x-\zeta_n^j).$$

Estes resultados também podem ser encontrados em [8], a partir da página 12.

Por fim, enunciaremos o Teorema de Kronecker-Weber, um teorema clássico na teoria de extensões de corpos.

Teorema 2.1.13. (*[13], pág. 273*) (*Teorema de Kronecker-Weber*) *Se $\mathbb{K}$ é um Corpo de Números abeliano, então existe um inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$.*

O menor inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, é definido como o **condutor** de $\mathbb{K}$ e denotado por $\mathrm{cond}(\mathbb{K})$.

Exemplo 2.1.14. Note que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$ e $\mathbb{Q}(\sqrt{2}) \nsubseteq \mathbb{Q}(\zeta_4)$, logo $\mathrm{cond}(\mathbb{Q}(\sqrt{2})) = 8 = 2^3$.

2.2 Teoria Algébrica dos Números

Colocaremos nessa seção algumas definições e resultados da Teoria Algébrica dos Números os quais acreditamos serem importantes no intuito de inserir o leitor no conteúdo estudado nos capítulos centrais deste trabalho. As principais referências utilizadas nesta seção são [8] e [13].

2.2.1 Módulos e Elementos Inteiros Algébricos

Nesta parte apresentaremos os conceitos de módulos e submódulos, além de algumas propriedades e resultados relacionados. Consideraremos sempre $\mathcal{A}$ como um anel comutativo com unidade.

Definição 2.2.1. *Um* $\mathcal{A}$***-módulo*** $\mathcal{M}$ *é um grupo abeliano aditivo* $\mathcal{M}$*, munido de uma aplicação* $\mathcal{A} \times \mathcal{M} \to \mathcal{M}$*, definida por* $(a, m) \to am$*, tal que para quaisquer* $a, b \in \mathcal{A}$ *e* $x, y \in \mathcal{M}$*, tem-se:*

1. $a(x + y) = ax + ay$;
2. $(a + b)x = ax + bx$;
3. $(ab)x = a(bx)$;
4. $1x = x$.

Observe que um anel $\mathcal{A}$ por ser visto como um $\mathcal{A}$-módulo e todo espaço vetorial V sobre um corpo $\mathbb{K}$ é um K-módulo.

Definição 2.2.2. *Seja* $\mathcal{M}$ *um* $\mathcal{A}$*-módulo. Um subconjunto não vazio* $\mathcal{N} \subseteq \mathcal{M}$ *é um* $\mathcal{A}$***-submódulo de*** $\mathcal{M}$ *se* $\mathcal{N}$ *é um subgrupo de* $(\mathcal{M}, +)$ *e* $an \in \mathcal{N}$ *para todo* $a \in \mathcal{A}$ *e* $n \in \mathcal{N}$*.*

Em particular, $\mathcal{N}$ é por si só um $\mathcal{A}$-módulo.

Definição 2.2.3. *Sejam* $\mathcal{M}$ *um* $\mathcal{A}$*-módulo e* $\{x_1, x_2, \ldots, x_n\} \subseteq \mathcal{M}$*.*

i) Dizemos que $\{x_1, x_2, \ldots, x_n\}$ *é um* ***conjunto gerador de*** $\mathcal{M}$ *se todo elemento* $x \in \mathcal{M}$ *pode ser expresso na forma* $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$*, com* $a_i \in \mathcal{A}$*, para* $i = 1, 2, \ldots, n$*.*

ii) O conjunto $\{x_1, x_2, \ldots, x_n\}$ *é dito ser* ***linearmente independente*** *se a única solução da equação* $0 = a_1x_1 + a_2x_2 + \cdots + a_nx_n$*, com* $a_i \in \mathcal{A}$*, para* $i = 1, 2, \ldots, n$*, for a solução nula, isto é,* $a_1 = a_2 = \cdots = a_n = 0$*.*

Se $\{x_1, x_2, \ldots, x_n\}$ *é um conjunto gerador de* $\mathcal{M}$*, então* $\mathcal{M}$ *é dito ser* ***finitamente gerado****. Se além disso* $\{x_1, x_2, \ldots, x_n\}$ *for um conjunto linearmente independente, dizemos que* $\{x_1, x_2, \ldots, x_n\}$ *é uma* ***base*** *de* $\mathcal{M}$ *e que* $\mathcal{M}$ *é um* $\mathcal{A}$***-módulo livre****. Neste caso, a cardinalidade do conjunto* $\{x_1, x_2, \ldots, x_n\}$ *é chamada de* ***posto*** *do* $\mathcal{A}$*-módulo* $\mathcal{M}$*.*

O próximo resultado relaciona o posto de um $\mathcal{A}$-módulo $\mathcal{M}$ com o posto de seus $\mathcal{A}$-submódulos.

Teorema 2.2.4 ([13], pág 113 e 115)**.** *Sejam* $\mathcal{A}$ *um anel principal,* $\mathcal{M}$ *um* $\mathcal{A}$*-módulo livre de posto* n *e* $\mathcal{N}$ *um* $\mathcal{A}$*-submódulo de* $\mathcal{M}$*. Então,*

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

ii) Se $\mathcal{N} \neq \{0\}$*, existe uma base* $\{e_1, e_2, \ldots, e_n\}$ *de* $\mathcal{M}$ *e elementos não nulos* $a_1, a_2, \ldots, a_q$ *em* $\mathcal{A}$*, tais que* $\{a_1e_1, a_2e_2, \ldots, a_qe_q\}$ *é uma base de* $\mathcal{N}$*, de modo que* a_i *divide* a_{i+1}*, para* $1 \leqslant i \leqslant q - 1$*.*

Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis. Um elemento $\alpha \in \mathcal{B}$ é dito ser um **elemento inteiro algébrico** (ou simplesmente um elemento inteiro) sobre $\mathcal{A}$ se existir algum polinômio mônico não nulo $f(x) \in \mathcal{A}[x]$, tal que $f(\alpha) = 0$, ou seja, se existirem $a_0, a_1, \ldots, a_{n-1} \in \mathcal{A}$ tais que,

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

Exemplo 2.2.5. O elemento $1 - i \in \mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$ é inteiro sobre $\mathbb{Z}$, pois é raiz do polinômio $f(x) = x^2 - 2x + 2 \in \mathbb{Z}[x]$.

Definição 2.2.6. *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis. O conjunto*

$$\mathcal{O}_{\mathcal{B}}(\mathcal{A}) = \{\alpha \in \mathcal{B};\ \alpha \text{ é um inteiro algébrico sobre } \mathcal{A}\}$$

é chamado de ***fecho integral de $\mathcal{A}$ em $\mathcal{B}$****. Se $\mathcal{A}$ é um domínio de integração e $\mathcal{B}$ é o seu corpo de frações, o conjunto $\mathcal{O}_{\mathcal{B}}(\mathcal{A})$ é chamado de* ***fecho integral de $\mathcal{A}$****.*

Exemplo 2.2.7. O elemento $1/2$ não é inteiro sobre $\mathbb{Z}$, logo $\mathbb{Z}[1/2]$ não é inteiro sobre $\mathbb{Z}$.

Se $\mathbb{K}$ é um Corpo de Números, o conjunto $\mathcal{O}_{\mathbb{K}}(\mathbb{Z})$ é chamado de **anel de inteiros** e será denotado simplesmente por $\mathcal{O}_{\mathbb{K}}$.

A referência [13] traz uma seção inteira abordando resultados para os corpos (de números) quadráticos e seus respectivos anéis de inteiro, em especial temos que:

Teorema 2.2.8 ([13], pág. 98)**.** *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados.*

1. *Se $d \equiv 2\ (mod\ 4)$ ou $d \equiv 3\ (mod\ 4)$, então $\{1, \sqrt{d}\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*
2. *Se $d \equiv 1\ (mod\ 4)$, então $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*

Exemplo 2.2.9. Temos que $\mathcal{O}_{\mathbb{Q}[\sqrt{2}]} = \mathbb{Z}[\sqrt{2}]$ e $\mathcal{O}_{\mathbb{Q}[\sqrt{3}]} = \mathbb{Z}[\sqrt{3}]$.

Teorema 2.2.10 ([13], pág 115)**.** *Sejam $\mathcal{A}$ um anel principal, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$. Nessas condições,*

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

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

Se $\mathbb{K}$ é um Corpo de Números de grau n, segue pelo teorema anterior que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Nesse caso, uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é dita ser uma **base integral** de $\mathbb{K}$.

Teorema 2.2.11 ([16], pág 11)**.** *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 $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.*

Uma família bastante estudada em Teoria Algébrica dos Números é a coleção dos n distintos $\mathbb{K}$-monomorfismos de $\mathbb{L}$ sobre um fecho algébrico, onde $\mathbb{L}/\mathbb{K}$ é uma extensão finita de corpos de grau n. Para este estudo iniciamos com o Lema de Dedekind.

Teorema 2.2.12 ([13], pág 20) (Lema de Dedekind)**.** *Sejam $\mathbb{L}/\mathbb{K}$ uma extensão de corpos finita de grau n e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ sobre um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$. Então, $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ é linearmente independente sobre $\mathbb{F}$.*

Definição 2.2.13. *Seja $\mathbb{K}/\mathbb{Q}$ uma extensão galoisiana finita, com*

$$Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}.$$

Se existir $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$ é uma base integral de $\mathbb{K}$, então ela é dita ser uma ***base normal integral*** *de $\mathbb{K}$. O elemento α é chamado de* ***gerador*** *dessa base.*

Na próxima subseção iremos exibir uma base normal integral associadas a Corpo de Números de condutores ímpares livres de quadrados.

2.2.2 Traço, Norma e Discriminante

Nesta parte introduziremos os conceitos de traço e norma de um elemento e de discriminante de um conjunto de uma extensão finita $\mathbb{L}/\mathbb{K}$ de grau n, além de alguns resultados relacionados.

Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita de grau n e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$.

Definição 2.2.14. *Seja $\alpha \in \mathbb{L}$. Definimos o* ***traço*** *e a* ***norma*** *de α na extensão $\mathbb{L}/\mathbb{K}$, como sendo respectivamente*

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

Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos, $a \in \mathbb{K}$ e $\alpha, \beta \in \mathbb{L}$, conforme [14] página 36, valem as seguintes propriedades:

- $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\beta)$;
- $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a\alpha) = a.\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$;
- $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}].a$;
- $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha).\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\beta)$;
- $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$.

Além disso, se $\mathbb{M}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ e $\gamma \in \mathbb{M}$, então:

- $\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\gamma) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{M}/\mathbb{L}}(\gamma))$;
- $\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\alpha) = [\mathbb{M} : \mathbb{L}].\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$;
- $\mathrm{N}_{\mathbb{M}/\mathbb{K}}(\gamma) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathrm{N}_{\mathbb{M}/\mathbb{L}}(\gamma))$;
- $\mathrm{N}_{\mathbb{M}/\mathbb{K}}(\alpha) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\alpha)^{[\mathbb{M}:\mathbb{L}]}$.

Proposição 2.2.15 ([14], pág 36)**.** *Se $\mathbb{K}$ é um Corpo de Números, $\mathbb{L}$ uma extensão finita de grau n de $\mathbb{K}$, $\alpha \in \mathbb{L}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$ as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}[\alpha]]$ vezes, então $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$.*

Exemplo 2.2.16. Considere o corpo $\mathbb{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Logo $[\mathbb{K} : \mathbb{Q}[\sqrt{6}]] = 2$ e $\min_{\mathbb{Q}}(\sqrt{6}) = (x - \sqrt{6})(x + \sqrt{6})$, assim pela Proposição 2.2.15, segue que $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\sqrt{6}) = \sqrt{6} + \sqrt{6} + (-\sqrt{6}) + (-\sqrt{6}) = 0$ e $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\sqrt{6}) = \sqrt{6}\sqrt{6}(-\sqrt{6})(-\sqrt{6}) = 36$.

A proposição a seguir nos fornece a informação de que a norma e o traço de um elemento inteiro é ainda inteiro com relação a qualquer subcorpo.

Proposição 2.2.17 ([14], pág 38)**.** *Se $\mathbb{K}$ é um Corpo de Números, $\mathbb{L}$ uma extensão finita de grau n de $\mathbb{K}$, $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de $\mathcal{O}_{\mathbb{K}}$.*

Se $\mathbb{L}$ e $\mathbb{M}$ são extensões galoisianas de um corpo $\mathbb{K}$ e $\alpha \in \mathbb{L}$, pela Proposição 2.1.11, temos que $\mathrm{Tr}_{\mathbb{LM}/\mathbb{M}}(\alpha) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$, com isso podemos enunciar o seguinte lema:

Lema 2.2.18. *Sejam a e b inteiros com $mdc(a,b)=1$. Se $n=a.b$, então*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a).Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b).$$

Demonstração. Desde que $\mathrm{mdc}(a,b)=1$, existem $r,s\in\mathbb{Z}$ tais que $ar+bs=1$. Assim,

$$\zeta_n = \zeta_{ab}^{ar+bs} = \zeta_{ab}^{ar}.\zeta_{ab}^{bs} = \zeta_b^r.\zeta_a^s.$$

Além disso, $\mathrm{mdc}(a,s)=\mathrm{mdc}(b,r)=1$, logo ζ_a^s e ζ_a são conjugados e dessa forma possuem o mesmo traço. Da mesma forma, ζ_b^r e ζ_b são conjugados, logo $Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^r) = Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b)$. Assim,

$$\begin{aligned}
Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) &= Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)}(\zeta_n)) \\
&= Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_a)}(\zeta_a^s.\zeta_b^r)) \\
&= Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^s).Tr_{\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b)/\mathbb{Q}(\zeta_a)}(\zeta_b^r) \\
&= Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^s).Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^r) \\
&= Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a).Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b).
\end{aligned}$$

□

O próximo teorema estabelece uma base normal integral para uma p-extensão abeliana não ramificada a qual usaremos para expressar os resultados deste trabalho, sua demonstração pode ser encontrada em [7] (Teorema 1.3.4, pág. 30).

Teorema 2.2.19. *Seja n um inteiro positivo ímpar livre de quadrados, $\mathbb{K}\subset\mathbb{Q}(\zeta_n)$ um Corpo de Números de grau r e $Gal(\mathbb{K}/\mathbb{Q})=\{\theta_1,\theta_2,\ldots,\theta_r\}$, então*

$$\{\theta_1(t),\theta_2(t),\ldots,\theta_r(t)\}$$

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

Além disso, temos que:

Proposição 2.2.20 ([7], pág 29)**.** *Seja n um inteiro positivo ímpar livre de quadrados, $\mathbb{K}\subset\mathbb{Q}(\zeta_n)$ um Corpo de Números e $t=Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então $\mathbb{K}=\mathbb{Q}(t)$.*

Iremos agora introduzir o conceito de discriminante de uma extensão de corpos finita. Dada uma n-upla $(\alpha_1,\alpha_2,\ldots,\alpha_n)$ de elementos de $\mathbb{L}$, definimos o **discriminante** em $\mathbb{L}/\mathbb{K}$ dessa n-upla por

$$\mathrm{Disc}_{\mathbb{L}/\mathbb{K}}(\alpha_1,\alpha_2,\ldots,\alpha_n) = \det(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)).$$

Proposição 2.2.21 ([14], pág 39)**.** *Se $\sigma_1,\sigma_2,\ldots,\sigma_n$ são os $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$, então*

$$Disc_{\mathbb{L}/\mathbb{K}}(\alpha_1,\alpha_2,\ldots,\alpha_n) = \big[det(\sigma_i(\alpha_j))\big]^2.$$

Proposição 2.2.22 ([14], pág 38)**.** *Seja $(\beta_1,\beta_2,\ldots,\beta_n)$ 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 $j=1,2,\ldots,n$. Então*

$$Disc_{\mathbb{L}/\mathbb{K}}(\beta_1,\beta_2,\ldots,\beta_n) = \big[det(a_{ij})\big]^2 Disc_{\mathbb{L}/\mathbb{K}}(\alpha_1,\alpha_2,\ldots,\alpha_n).$$

Pelas Proposições 2.2.22 e 2.2.17, se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base integral de um corpo de números $\mathbb{K}$ de grau n, então $\{\beta_1, \beta_2, \ldots, \beta_n\}$ também será uma base integral de $\mathbb{K}$ se, e somente se,

$$\mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathrm{Disc}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n).$$

Com isso, podemos enunciar:

Definição 2.2.23. *Seja $\mathbb{K}$ um corpo de números. O discriminante na extensão $\mathbb{K}/\mathbb{Q}$, de qualquer base integral de $\mathbb{K}$, é chamado de* ***discrimante do corpo*** *$\mathbb{K}$, e denotado por $Disc(\mathbb{K})$.*

Podemos determinar a norma do discriminante de um corpo de números $\mathbb{K}$ conhecendo apenas o seu condutor e o seu grau, conforme o teorema a seguir:

Teorema 2.2.24 ([10], pág 38)**.** *Seja $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ e $\mathbb{K}$ um corpo de números abeliano de condutor m. Então,*

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

Como consequência obtemos:

Proposição 2.2.25. *Seja $\mathbb{K}$ um corpo de números abeliano de grau primo p e condutor m. Então,*

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

Exemplo 2.2.26. Dados números primos p e q, de forma que $q \equiv 1(\bmod p)$, é visto em [5] que exite um único subcorpo $\mathbb{L}_q \subseteq \mathbb{Q}(\zeta_q)$, com $[\mathbb{L}_q : \mathbb{Q}] = p$. Dessa forma,

$$|\mathrm{Disc}(\mathbb{L}_q)| = q^{p-1}.$$

Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números de grau n e m, respectivamente. Dizemos que $\mathbb{K}$ e $\mathbb{L}$ são **disjuntos** quando $[\mathbb{KL} : \mathbb{Q}] = nm$. Quando $\mathbb{K}$ e $\mathbb{L}$ são disjuntos e seus discriminantes relativamente primos, eles são ditos ser **linearmente disjuntos**. Se $\mathbb{K}/\mathbb{Q}$ e $\mathbb{L}/\mathbb{Q}$ são extensões galoisianas, segue pelo Teorema 2.1.9 que $\mathbb{K}$ e $\mathbb{L}$ são disjuntos se, e somente se, $\mathbb{K} \cap \mathbb{L} = \mathbb{Q}$.

Proposição 2.2.27 ([9], pág 68)**.** *Se $\mathbb{K}$ e $\mathbb{L}$ são corpos de números linearmente disjuntos, de graus n e m, respectivamente, então*

i) $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$.

ii) $Disc(\mathbb{KL}) = Disc(\mathbb{K})^m Disc(\mathbb{L})^n$.

Se $\mathbb{K}$ é um corpo de números de grau n e $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto também n, chamamos de **norma de** $\mathcal{M}$ a cardinalidade do quociente $\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{M}}$, a qual será denotada por $[\mathcal{O}_{\mathbb{K}} : \mathcal{M}]$. Se $\mathfrak{a}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, denotaremos tal norma por $N(\mathfrak{a}) = [\mathcal{O}_{\mathbb{K}} : \mathfrak{a}]$.

2.2.3 A Decomposição de Ideais Primos

Seja $\mathbb{K}$ um Corpo de Números e $\mathbb{L}$ uma extensão finita de grau n de $\mathbb{K}$. Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, então o ideal $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$, gerado por $\mathfrak{p}$ em $\mathcal{O}_{\mathbb{L}}$, não é em geral um ideal primo em $\mathcal{O}_{\mathbb{L}}$, contudo veremos nesta parte algumas informações interessantes a seu respeito. As referências utilizadas aqui são: [8], [13] e [14]. Alguns enunciados aqui descritos estão readequados de forma a abordar os casos estudados neste trabalho.

Teorema 2.2.28 ([14], pág. 71)**.** *O ideal $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ é expresso de maneira única na forma*

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\ldots\mathfrak{B}_q^{e_q},$$

onde $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_q$ são os ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$ satisfazendo $\mathfrak{B}_{\mathfrak{i}} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$, para cada $i = 1, 2, \ldots, q$.

Dizemos que um ideal primo $\mathfrak{B}$ de $\mathcal{O}_{\mathbb{L}}$ está **acima** de $\mathfrak{p}$ se $\mathfrak{B}_{\mathfrak{i}} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$. Sendo assim, os ideias $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_q$ do teorema anterior são justamente os ideias de $\mathcal{O}_{\mathbb{L}}$ que estão acima de $\mathfrak{p}$. Os inteiros $e_1 = e(\mathfrak{B}_1/\mathfrak{p}), e_2 = e(\mathfrak{B}_2/\mathfrak{p}), \ldots, e_q = e(\mathfrak{B}_q/\mathfrak{p})$ são chamados de **índice de ramificação** de $\mathfrak{B}_{\mathfrak{1}}, \mathfrak{B}_{\mathfrak{2}}, \ldots, \mathfrak{B}_{\mathfrak{q}}$, respectivamente. Quando ao menos um dos índices de ramificação e_i é maior que 1, dizemos que $\mathfrak{p}$ se **ramifica**, ou é **ramificado** em $\mathbb{L}$ (ou em $\mathcal{O}_{\mathbb{L}}$). Se $\mathfrak{p}$ é o ideal de $\mathcal{O}_{\mathbb{K}}$ gerado pelo número primo p, diremos que p se **ramifica** em $\mathbb{L}$ sempre que $\mathfrak{p}$ for ramificado em $\mathbb{L}$.

Além disso, conforme [8] página 64, se $\mathfrak{B}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$, então $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{B}}$ é uma extensão de corpos de $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}$ e seu grau, $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{B}} : \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}\right] \leqslant n$, é chamado **grau de ínercia** de $\mathfrak{B}$, o qual será denotado por $f = f(\mathfrak{B}/\mathfrak{p})$.

Dizemos que $\mathbb{L}/\mathbb{K}$ é uma **extensão de corpos não ramificada** quando todos os ideais primos de $\mathcal{O}_{\mathbb{K}}$ são não ramificados em $\mathbb{L}$. A extensão abeliana maximal sobre $\mathbb{K}$ ($\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ é um grupo abeliano) é chamada de **Corpo de Classes de Hilbert de** $\mathbb{K}$, o qual será denotamos por $H(\mathbb{K})$, conforme referência [8], página 232.

Teorema 2.2.29 ([14], pág. 71)**.** *(Igualdade Fundamental) Seja $\mathbb{K}$ um corpo de números, $\mathbb{L}/\mathbb{K}$ uma extensão finita de grau n, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_q$ os ideias de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$. Então,*

$$\sum_{i=1}^{q} e_i f_i = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} : \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}\right] = n.$$

No caso de extensões galoisianas, podemos ainda destacar o seguinte teorema:

Teorema 2.2.30 ([8], pág. 71)**.** *Se $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão galoisiana de grau n de corpos de números e $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, então $e_1 = e_2 = \ldots = e_q$ e $f_1 = f_2 = \ldots = f_q$, sendo $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_q$ os ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$ satisfazendo $\mathfrak{B}_{\mathfrak{i}} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$, para $i = 1, 2 \ldots, q$.*

Dessa forma, se $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão galoisiana de grau n de corpos de números, denotando $e = e_1$ e $f = f_1$, segue que a igualdade fundamental é dada por

$$efq = n.$$

2.3 Reticulados

Nesta seção iremos definir reticulado n-dimensional e desenvolver alguns de seus conceitos, relacionando posteriormente $\mathbb{Z}$-módulos livres de posto finito contidos em corpos de números com reticulados no $\mathbb{R}^n$. Essa identificação nos permite descrever algumas propriedades do reticulado obtido, através das propriedades do corpo de números que contém o respectivo $\mathbb{Z}$-módulo. As principais referências utilizadas nesta seção serão [14] e [17].

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

Sejam $\Lambda \subset \mathbb{R}^n$ um subgrupo. Dizemos que Λ é um **subgrupo discreto** do $\mathbb{R}^n$ se para qualquer subconjunto compacto $K \subset \mathbb{R}^n$, a interseção $K \cap \Lambda$ é finita. Um exemplo típico de subgrupo discreto de $\mathbb{R}^n$ é o $(\mathbb{Z}^n, +)$.

Teorema 2.3.1 ([14], pág. 53)**.** *Se $\Lambda \subset \mathbb{R}^n$ é um subgrupo discreto, então Λ é um $\mathbb{Z}$-módulo livre, gerado por m vetores linearmente independentes sobre $\mathbb{R}$, com $m \leqslant n$.*

Definição 2.3.2. *Um $\mathbb{Z}$-módulo livre contido em $\mathbb{R}^n$ é chamado de **reticulado em** $\mathbb{R}^n$. Se $\{w_i\}_{i=1}^m$ é um conjunto gerador de Λ, linearmente independente sobre $\mathbb{R}$, então dizemos que Λ é um **reticulado m dimensional** com base $\{w_i\}_{i=1}^m$, ou seja,*

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

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

Se $B = \{w_i\}_{i=1}^n$ é uma base de um reticulado n-dimensional $\Lambda \subset \mathbb{R}^n$, então a matriz $M = (v_{ij})$, onde para cada $i = 1, 2, \ldots, n$, $w_i = (w_{i1}, w_{i2}, \ldots, w_{in}) \in \mathbb{R}^n$, é chamada de **matriz geradora do reticulado** Λ. Assim, $\Lambda = \{aM;\ a \in \mathbb{Z}^n\}$. O conjunto

$$\mathcal{P}_B = \left\{ \sum_{i=1}^{n} \lambda_i w_i;\ 0 \leqslant \lambda_i < 1 \right\}$$

é denominado **região fundamental** de Λ com relação a base B. O **volume da região fundamental** $\mathcal{P}_B$ é dado por

$$vol(\mathcal{P}_B) = |\det(M)|.$$

Proposição 2.3.3. *Sejam $B = \{w_i\}_{i=1}^n$ uma base de Λ e $\{v_i\}_{i=1}^n \subset \Lambda$ um conjunto de vetores linearmente independente sobre $\mathbb{R}$, tais que $v_j = \sum_{i=1}^n a_{ij} w_j$, com $a_{ij} \in \mathbb{Z}$. Então, $\{v_i\}_{i=1}^n$ é uma base de Λ se, e somente se, $det(a_{ij}) = \pm 1$.*

Demonstração. Basta ver que $A = (a_{ij})$ é uma matriz mudança de base se, e somente se, A é invertível, ou seja, $\det A = \pm 1$. □

A partir da Proposição 2.3.3, se B e C são duas bases de um reticulado Λ, com matrizes geradoras associadas M e N, respectivamente, então $|\det(M)| = |\det(N)|$ e $\det(MM^t) = \det(NN^t)$, logo ficam bem estabelecidas as seguintes definições:

Definição 2.3.4. *Seja B uma base de Λ, o* ***volume do reticulado*** Λ *é o volume da região fundamental $\mathcal{P}_B$ e é denotado por $vol(\Lambda)$, isto é,*

$$vol(\Lambda) = vol(\mathcal{P}_B).$$

Se M é a matriz geradora de um reticulado Λ associada a uma base $B = \{w_i\}_{i=1}^{n}$, definimos a **matriz de Gram** de Λ, associada a M, como sendo a matriz

$$G = MM^t.$$

Definição 2.3.5. *Seja G uma matriz de Gram do reticulado Λ. Definimos o* ***determinante do reticulado*** Λ *como sendo o determinante de G, e o denotamos por $det(\Lambda)$. Desta forma, $det(\Lambda) = det(M)^2$.*

Exemplo 2.3.6. Considere o reticulado hexagonal no plano conforme figura abaixo.

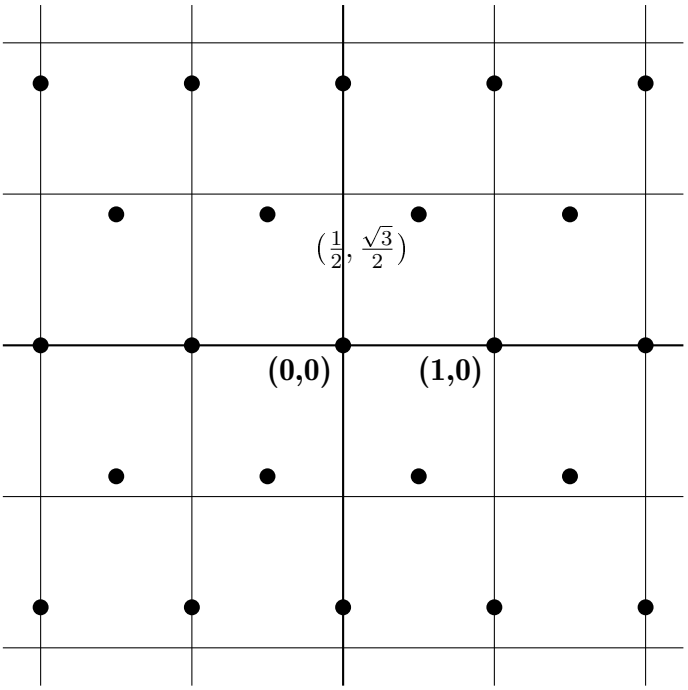

Figura 2.3: Reticulado hexagonal.
Fonte: Próprio autor.

Uma matriz geradora pode ser dada por

$$M = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix},$$

obtendo a matriz de Gram

$$G = MM^t = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix},$$

e $\det \Lambda = \det G = \frac{3}{4}$.

Um **empacotamento esférico** em $\mathbb{R}^n$ é uma coleção de esferas de mesmo raio no $\mathbb{R}^n$, distribuídas de maneira que a interseção de quaisquer duas esferas tenham no máximo um ponto. Se a coleção dos centros dessas esferas formam um reticulado $\Lambda \subset \mathbb{R}^n$, dizemos que este empacotamento é um **empacotamento reticulado**. O maior raio para o qual é possível definir um empacotamento de Λ é obtido pelo número

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

o qual é chamado de **raio de empacotamento de** Λ.

Dado um reticulado Λ no $\mathbb{R}^n$, um assunto bastante estudado atualmente é o de quão denso é o empacotamento reticulado, ou seja, o estudo da proporção do espaço $\mathbb{R}^n$ recoberto pelo empacotamento de esferas de raio ρ. Assim, se B é uma base de Λ e $B(\rho)$ é a esfera de centro na origem e raio ρ, então:

Definição 2.3.7. *A* ***densidade de empacotamento de*** Λ *é definido por*

$$\Delta(\Lambda) = \frac{vol(B(\rho))}{vol(\mathcal{P}_B)} = \frac{vol(B(1))\rho^n}{vol(\Lambda)}.$$

Definição 2.3.8. *Definimos a* ***densidade de centro*** $\delta(\Lambda)$ *do reticulado* Λ *como sendo*

$$\delta(\Lambda) = \frac{\rho^n}{vol(\Lambda)}.$$

Exemplo 2.3.9. Considerando o reticulado Λ apresentado no Exemplo 2.3.6, temos que $\rho = \frac{\min\{|\lambda|;\ \lambda\in\Lambda,\ \lambda\neq 0\}}{2} = \frac{1}{2}$ e $vol(\Lambda) = \sqrt{3}/2$. Portanto,

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

e

$$\delta(\Lambda) = \frac{1}{\sqrt{12}} \simeq 0,288675.$$

2.3.2 O Mergulho Canônico de um Corpo de Números

Nosso próximo passo é abordar o conceito de mergulho de Minkowski, também conhecido como homomorfismo canônico. Para isso, faremos uso dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$.

Definição 2.3.10. *Sejam* $\mathbb{K}$ *um Corpo de Números de grau* n *e* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *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 todo monomorfismo σ_i *é um monomorfismo real, dizemos que* $\mathbb{K}$ *é um* ***corpo totalmente real****. Se todo monomorfismo* σ_i *é um monomorfismo complexo, dizemos que* $\mathbb{K}$ *é um* ***corpo totalmente complexo****.*

Observação 2.3.11. Se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana de grau n, então $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Dessa forma, $\mathbb{K}$ será um corpo totalmente real ou totalmente complexo, uma vez que $\sigma_i(\mathbb{K}) = \mathbb{K}$, para todo $i = 1, 2, \ldots, n$. Em particular, como para cada $\mathbb{Q}$-monomorfismo, seu conjugado também é um $\mathbb{Q}$-monomorfismo, segue que se n é

ímpar então $\mathbb{K}$ será um corpo totalmente real. Logo, a quantidade de monomorfismos complexos é par. Denotemos por r_1 o número de monomorfismos reais, por $2r_2$ o números de monomorfismos complexos e os ordenaremos de maneira que $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ sejam reais e $\sigma_{r_1+1}, \sigma_{r_1+2}, \ldots, \sigma_{r_1+2r_2}$ sejam complexos, com $n = r_1 + 2r_2$ e $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$, para $i = 1, 2, \ldots, r_2$.

Definição 2.3.12. *Chamamos de* ***homomorfismo canônico*** *(ou homomorfismo de Minkowski) de $\mathbb{K}$ em $\mathbb{R}^n$ a aplicação*

$$\begin{array}{rccl} \sigma_{\mathbb{K}}: & \mathbb{K} & \to & \mathbb{R}^n \\ & x & \mapsto & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \ldots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))), \end{array}$$

onde $\Re(y)$ e a parte real de y em $\mathbb{C}$ e $\Im(y)$ e a parte imaginária de y em $\mathbb{C}$.

Teorema 2.3.13 ([14], pág. 56)**.** *Seja $\mathbb{K}$ um corpo de números de grau n, $\mathcal{M}$ um submódulo $\mathcal{O}_{\mathbb{K}}$ de posto n e $\{u_1, u_2, \ldots, u_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, então $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado em $\mathbb{R}^n$, cujo volume é dado por*

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

Corolário 2.3.14 ([14], pág. 57)**.** *Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$ e $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathcal{M})$ são reticulados em $\mathbb{R}^n$, cujos volumes são, respectivamente,*

$$vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|Disc(\mathbb{K})|^{1/2} \text{ e } vol(\sigma_{\mathbb{K}}(\mathcal{M})) = vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))[\mathcal{O}_{\mathbb{K}} : \mathcal{M}].$$

Seja $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. Pelo Corolário 2.3.14 segue que a densidade de centro do Reticulado Algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é dada por

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

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

$$|\sigma_{\mathbb{K}}(x)|^2 = \begin{cases} Tr_{\mathbb{K}/\mathbb{Q}}(x^2) & \text{se } \mathbb{K} \text{ é totalmente real;} \\ \dfrac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) & \text{se } \mathbb{K} \text{ é totalmente imaginário.} \end{cases}$$

Conforme [17] pág 225. Nos casos em que n é ímpar segue que $\mathbb{K}$ é totalmente real.

Nos próximos capítulos focaremos o estudo nas p-extensões, assim, pela observação anterior trabalharemos com corpos de números totalmente reais.

3 Extensões abelianas de grau primo

Neste capítulo abordaremos alguns resultados sobre a forma traço integral de p-extensões abelianas, onde p é um número primo ímpar, além de alguns algoritmos utilizados na minimização de tal forma. Em geral, o método para isso consiste em considerar alguns $\mathbb{Z}$-módulos "interessantes" contidos em seus anéis de inteiros envolvendo congruências módulo m, para algum natural m. Uma vez que p é ímpar, segue que as p-extensões galoisianas aqui estudadas serão sempre totalmente reais.

3.1 Caracterização das p-Extensões Via Condutor

Seja p um inteiro primo ímpar e $\mathbb{K}$ uma p-extensão abeliana. Dizemos que $\mathbb{K}$ é uma **p-extensão ramificada** se o primo p se ramifica em $\mathbb{K}$, caso contrário, o corpo $\mathbb{K}$ é denominado ser uma **p-extensão abeliana não ramificada**.

O resultado a seguir estabelece uma conexão entre as p-extensões galoisianas que se ramificam (e as que não se ramificam) com o seu condutor.

Proposição 3.1.1 ([7], pág. 33)**.** *Seja $\mathbb{K}$ uma p-extensão abeliana de condutor n. Então,*

i. p se ramifica em $\mathbb{K}$ se, e somente se, o condutor $n = p^2 p_1 p_2 \dots p_s$;

ii. p não se ramifica em $\mathbb{K}$ se, e somente se, o condutor $n = p_1 p_2 \dots p_s$,

onde $p_1, p_2, \dots, p_s$ são números primos ímpares distintos, tais que $p_i \equiv 1 (mod\ p)$, para cada $i = 1, 2, \dots, s$.

A partir dessa Proposição, podemos dividir o estudo da Forma Traço Integral de uma p-extensão abeliana em dois casos. O primeiro caso é quando o primo p se ramifica em $\mathbb{K}$ e o segundo é quando o primo p não se ramifica em $\mathbb{K}$. Esses dois casos foram estudados em teses de doutorados aos quais exibiremos seus principais resultados nas seções 3.2 e 3.3.

Naturalmente, o próximo passo a seguir é nos perguntarmos sobre o comportamento da Forma Traço Integral de uma extensão galoisiana de grau ímpar qualquer. Parte desta pergunta foi respondida na tese de doutorado de Moro, E. M., [6], ao qual descreveu a foma traço integral de um o compósito finito $\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_s$, onde cada Corpo de Números $\mathbb{K}_i$ é uma p_i-extensão abeliana não ramificada, com os primos $p_1, p_2, \dots, p_s$ distintos (note que $\mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_s$ tem grau $p_1 p_2 \dots p_s$). Este caso será visto na seção 3.4.

O objetivo deste trabalho é o de contribuir respondendo um pouco mais a questão acima, descrevendo a Forma Traço Integral do compósito $\mathbb{K}_1\mathbb{K}_2$, onde $\mathbb{K}_1$ e $\mathbb{K}_2$ são ambos p-extensões abelianas não ramificadas distintas. Note que neste caso, $\mathbb{K}_1\mathbb{K}_2$ é um corpo de números de grau p^2. Essa exploração será exposta no Capítulo 4,

sendo está dividade em duas partes, a primeira estudará o caso de condutores coprimos enquanto que a segunda parte analisa o caso em que os condutores de $\mathbb{K}_1$ e $\mathbb{K}_2$ possuem exatamente um primo em comum, na suas respectivas fatorações dos seus condutores.

Prosseguindo nesta seção, iremos destacar alguns resultados sobre contagem das p-extensões. O primeiro destes resultados estabelece a quantidade de p-extensões abelianas que há no corpo ciclotômico $\mathbb{Q}(\zeta_m)$, com m um inteiro positivo, enquanto que o segundo expressa a quantidade de p-extensões abelianas não ramificadas em corpos ciclotômicos $\mathbb{Q}(\zeta_n)$, com n um inteiro livre de quadrados, de condutor cheio, isto é, a quantidade de p-extensões abelianas não ramificadas de condutor n.

Proposição 3.1.2 ([7], pág. 33)**.** *Sejam $m = p_1^{a_1}p_2^{a_2}\dots p_u^{a_u}$ um inteiro positivo e*

$$s = \#\{p_i \ ; \ p \mid \phi(p_i^{a_i}), \ i = 1, 2, \dots, u\}.$$

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

Proposição 3.1.3 ([7], pág. 34)**.** *Se $n = p_1p_2\dots p_s$, com $p_i \equiv 1(mod\ p)$ para $i = 1, 2, \dots, s$, então o corpo ciclotômico $\mathbb{Q}(\zeta_n)$ contém $(p-1)^{s-1}$ p-extensões abelianas não ramificadas de condutor n.*

Os dois últimos resultados sobre a contagem de p-extensões abelianas em corpos ciclotômicos podem ser estendidos em dois teoremas sobre a contagem de subcorpos de grau p (sobre $\mathbb{Q}$) de compósitos de p-extensões, como segue:

Teorema 3.1.4 ([7], pág 50)**.** *Se $\mathbb{L}_1, \mathbb{L}_2, \dots, \mathbb{L}_u$ são p-extensões abelianas tais que $\mathbb{L}_1\mathbb{L}_2\dots\mathbb{L}_{k-1} \cap \mathbb{L}_k = \mathbb{Q}$, para todo $k = 2, 3, \dots, u$, então o compósito $\mathbb{L}_1\mathbb{L}_2\dots\mathbb{L}_u$ tem grau p^u e contém $(p^u - 1)/(p - 1)$ p-extensões abelianas.*

Teorema 3.1.5 ([7], pág 52)**.** *Sejam $\mathbb{L}_1, \mathbb{L}_2, \dots, \mathbb{L}_u$ p-extensões abelianas e $m_i = cond(\mathbb{L}_i)$, $i = 1, 2, \dots, u$. Se $m_1, m_2, \dots, m_u$ são coprimos entre si e $n = \prod_{i=1}^{u} m_i$, então o compósito $\mathbb{L}_1\mathbb{L}_2\dots\mathbb{L}_u$ contém $(p-1)^{u-1}$ p-extensões abelianas de condutor n.*

Mais adiante faremos uso do Lema 3.1.6 e da Proposição 3.1.7, a seguir, a fim de expressar a Forma Traço Integral do compósito $\mathbb{L}_1\mathbb{L}_2$, onde $\mathbb{L}_1$ e $\mathbb{L}_2$ são p-extensões abelianas não ramificadas.

Lema 3.1.6 ([7], pág 51)**.** *Sejam $\mathbb{L}_1\mathbb{L}_2\cdots\mathbb{L}_u$ um compósito de p-extensões abelianas de grau p^u e $\mathbb{K} \nsubseteq \mathbb{L}_1\mathbb{L}_2\cdots\mathbb{L}_u$ uma p-extensão abeliana. Então, toda p-extensão abeliana contida em $\mathbb{K}\mathbb{L}_1\mathbb{L}_2\cdots\mathbb{L}_u$ é também um subcorpo de $\mathbb{K}\mathbb{L}_i$, para algum $i = 1, \cdots, \alpha_u$, onde os $\mathbb{L}_i's$ são as p-extensões abelianas contidas em $\mathbb{L}_1\mathbb{L}_2\cdots\mathbb{L}_u$ e $\alpha_u = (p^u - 1)/(p - 1)$.*

Proposição 3.1.7 ([7], pág 50)**.** *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões distintas, tal que $\mathbb{L}_1\mathbb{L}_2$ possui condutor n e $\mathbb{M} \subseteq \mathbb{L}_1\mathbb{L}_2$ uma p-extensão de condutor $m < n$. Então,*

$$\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cap \mathbb{Q}(\zeta_m)$$

e é a única p-extensão de condutor m contida em $\mathbb{L}_1\mathbb{L}_2$.

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

3.2 p-Extensões Ramificadas

Nessa seção iremos expor alguns resultados para o caso de corpos de números $\mathbb{K}$ de grau p, sendo p um número primo ramificando em $\mathbb{K}$. As referência serão as Teses de Doutorado de Chagas, A. C. e de Araujo, R. R., [3] e [1], respectivamente.

Para esta seção, consideremos sempre $\mathbb{K}$ como uma p-extensão abeliana ramificada e $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$. Assim,

Proposição 3.2.1 ([3], pág 37)**.** *Supondo que cond*$(\mathbb{K}) = n$*, então:*

1. $\mathbb{K} = \mathbb{Q}(t)$*, onde* $t = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_n)$.
2. $\{1, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$*, é uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}}$*, onde* $\langle\theta\rangle = Gal(\mathbb{K}/\mathbb{Q})$.

Além disso, em [3], Chagas obteve a expressão da forma traço para os casos em que $\text{cond}(\mathbb{K}) = p^2$ ou p^2q, com $q \equiv 1(\bmod p)$ um primo. Nesses casos observou-se que:

Proposição 3.2.2 ([3], pág 38 e 46)**.** *Seja* $\mathbb{K}$ *um corpo de números abeliano de grau primo* p *e condutor* n*,* $p^2 \mid n$*,* $\{1, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$ *uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}}$*, com* θ *um gerador de* $Gal(\mathbb{K}/\mathbb{Q})$ *e* $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$*. Dado* $x = a_0 + \sum_{i=1}^{p-1} \theta^i(t) \in \mathcal{O}_{\mathbb{K}}$*:*

1. *Se* $n = p^2$*, então*

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

2. *Se* $n = p^2q$*, com* $q \equiv 1(\ mod\ p)$ *um número primo, então*

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

Em sua tese de doutorado, [1], Araújo estendeu a Proposição anterior, como segue:

Proposição 3.2.3 ([1], pág 66)**.** *Seja* $\mathbb{K}$ *um corpo de números abeliano de grau primo* p *e condutor* $n = p^2p_1p_2\cdots p_r$*, com* $p_i \equiv 1(\ mod\ p)$ *primo, para cada* $i = 1, 2, \ldots, r$ *e* $p_i \neq p_j$*,* $\{1, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$ *uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}}$*, com* θ *um gerador de* $Gal(\mathbb{K}/\mathbb{Q})$ *e* $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$*. Dado* $x = a_0 + \sum_{i=1}^{p-1} \theta^i(t) \in \mathcal{O}_{\mathbb{K}}$*, então:*

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x^2) &= p\left(a_0^2 + p_1p_2\cdots p_r(p-1)\sum_{i=1}^{p-1} a_i^2 - 2p_1p_2\cdots p_r\sum_{1\leqslant i<j\leqslant p-1} a_i a_j\right) \\ &= pa_0^2 + pp_1p_2\cdots p_r\left((p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leqslant i<j\leqslant p-1} a_i a_j\right) \\ &= p\left(a_0^2 + \frac{n}{p^2}Q_{p-1}(a_1, a_2, \ldots, a_r)\right), \end{aligned}$$

onde $Q_{p-1}(a_1, a_2, \ldots, a_r)$ *é a forma quadrática* $\sum_{i=1}^{p-1} a_i^2 + \sum_{1\leqslant i<j\leqslant p-1} (a_i - a_j)^2$.

Se $\mathbb{K}$ é uma p-extensão abeliana ramificada, $n = p^2p_1p_2\cdots p_r$ é o condutor de $\mathbb{K}$ com $r \geqslant 1$ e $\mathfrak{B}_i$ são os únicos ideais primos de $\mathcal{O}_\mathbb{K}$ acima de p_i para $i = 1, 2, \ldots, r$, respectivamente. Em [3], página 48, é visto que cada ideal $\mathfrak{B}_i$ pode ser descrito como:

$$\mathfrak{B}_i = \left\{ a_0 + \sum_{k=1}^{p-1} a_i\theta^k(t);\ a_0 \equiv 0(\text{mod } p_i) \right\},$$

sendo θ e t como na proposição anterior. A densidade de centro de cada um desses reticulados algébricos $\sigma_\mathbb{K}(\mathfrak{B}_i)$ é dado por:

Proposição 3.2.4 ([1], pág 75)**.** *Sejam $\mathbb{K}$ uma p-extensão abeliana ramificada de condutor $n = p^2p_1p_2\cdots p_r$, $r \geqslant 1$, com $p_i \equiv 1(mod\ p)$ para $i = 1, 2, \ldots, s$ e $\mathfrak{B}_i$ o ideal primo de $\mathcal{O}_\mathbb{K}$ acima de p_i. Então a densidade de centro do reticulados algébricos de posto completo $\sigma_\mathbb{K}(\mathfrak{B}_i) \subseteq \mathbb{R}^p$ é*

$$\delta(\sigma_\mathbb{K}(\mathfrak{B}_i)) = \frac{\lambda_i^{p/2}}{2^p p_i n^{(p-1)/2}},$$

onde

$$\lambda_i = \min\{pp_i^2, n(p-1)/p\}.$$

Exemplo 3.2.5 ([1], pág. 75)**.** Para $p = 3$, $n = 819 = 3^2 \times 7 \times 13$ (note que $p_1 = 7$ e $p_2 = 13$).

1. Sendo $\mathfrak{B}_1$ o ideal de $\mathcal{O}_\mathbb{K}$ acima de $p_1 = 7$, então $\delta(\sigma_\mathbb{K}(\mathfrak{B}_1)) \simeq 0,03886$.
2. Sendo $\mathfrak{B}_2$ o ideal de $\mathcal{O}_\mathbb{K}$ acima de $p_2 = 13$, então $\delta(\sigma_\mathbb{K}(\mathfrak{B}_2)) \simeq 0,13403$.

A maior densidade de centro de um reticulado na dimensão 3 é obtida pelo reticulado A_3, sendo $\delta(A_3) \simeq 0,17678$.

3.3 p-Extensões Não Ramificadas

Nessa seção iremos expor resultados importantes obtidos para os corpos de números $\mathbb{K}$ de grau primo p, com p não ramificando em $\mathbb{K}$. A referência será a Tese de Doutorado de Oliveira, E. L., [7].

Seja $\mathbb{K}$ uma p-extensão abeliana de condutor $n = p_1p_2\ldots p_s$, com p não ramificando em $\mathbb{K}$, $p_i \equiv 1(\text{ mod } p)$, para $i = 1, 2, \ldots, s$ e $p_i \neq p_j$, se $i \neq j$. Se θ é um gerador de $\text{Gal}(\mathbb{K}/\mathbb{Q})$, então o conjunto

$$\{t, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$$

é uma base normal integral de $\mathbb{K}$, gerada pelo elemento $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$.

Dado $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_\mathbb{K}$, temos que $x^2 = \sum_{i,j=0}^{p-1} a_ia_j\theta^i(t)\theta^j(t)$. Além disso,

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

com $i, j = 0, 1, \ldots, p-1$. Dessa forma,

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

A partir disso, obtemos:

Teorema 3.3.1 ([7], pág. 35)**.** *Se θ é um gerador de $Gal(\mathbb{K}/\mathbb{Q})$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(t\theta^k(t)) = \begin{cases} n - \left(\dfrac{n-1}{p}\right) & se \quad k = 0 \\ -\left(\dfrac{n-1}{p}\right) & se \quad k \neq 0 \end{cases}, \tag{3.1}$$

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

Com isso, podemos enunciar o resultado que descreve a Forma Traço Integral das p-extensões abelianas não ramificadas, como segue:

Corolário 3.3.2 ([7], pág. 42)**.** *Se $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$, então*

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = n\left(\sum_{i=0}^{p-1} a_i^2\right) - \frac{n-1}{p}\left(\sum_{i=0}^{p-1} a_i\right)^2. \tag{3.2}$$

Em sua tese, Oliveira desenvolveu um algoritmo para determinar o mínimo da Forma Traço Integral $Tr_{\mathbb{K}/\mathbb{Q}}(x^2)$, restrita ao $\mathbb{Z}$-módulo livre

$$\mathcal{M}_m := \left\{ \sum_{k=0}^{p-1} a_k\theta^k(t) \in \mathcal{O}_{\mathbb{K}};\ \sum_{k=0}^{p-1} a_k \equiv 0 \ (\bmod\ m) \right\}, \tag{3.3}$$

onde m é um inteiro positivo, obtendo o seguinte resultado:

Teorema 3.3.3 ([7], pág. 45)**.** *Sejam m um inteiro positivo e*

$$M^* = \min_{\substack{x \in \mathcal{M}_m \\ x \neq 0}} Tr_{\mathbb{K}/\mathbb{Q}}(x^2).$$

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

ii. Se p não divide m, então $M^* = \min\{2n, M(m), M(2m), \ldots, M(pm)\}$, onde

$$M(S) = pq_S^2 + 2q_S r_S + nr_S - \frac{n-1}{p} r_S^2,$$

sendo q_S e r_S o quociente e resto, respectivamente, da divisão de S por p.

Exemplo 3.3.4 ([7], pág. 46)**.**

1. Para $p = 3$, $n = 1123$ e $m = 67$, temos que $M^* = 2245$. Assim o reticulado $\sigma_{\mathbb{K}}(\mathcal{M}_{67})$, de dimensão 3, tem densidade de centro igual a $\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{67})) \simeq 0,17672$.

2. Para $p = 5$, $n = 92111$ e $m = 607$, a densidade de centro do reticulado 5-dimensional $\sigma_{\mathbb{K}}(\mathcal{M}_{607})$ é dada por $\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{607})) \simeq 0,08839$.

3. Para $p = 7$, $n = 600601$ e $m = 1096$, a densidade de centro do reticulado 7-dimensional $\sigma_{\mathbb{K}}(\mathcal{M}_{1096})$ é dada por $\delta(\sigma_{\mathbb{K}}(\mathcal{M}_{1096})) \simeq 0,0625$.

Observação 3.3.5. A maior densidade de centro de um reticulado na dimensão 3 é obtido pelo reticulado A_3, sendo $\delta(A_3) \simeq 0,17678$. Já de posto 5, a maior densidade de centro é obtida pelo reticulado D_5, tendo $\delta(D_5) \simeq 0,08839$. Por fim, o reticulado E_7 possui a maior densidade de centro entre os reticulado 7-dimensional, obtendo $\delta(E_7) \simeq 0,0625$.

3.4 Compósitos $\mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_s$ de grau $p_1p_2\ldots p_s$ livre de quadrados

Nessa seção iremos expor resultados obtidos na Tese de Doutorado de Moro, E. M., [6], o qual estudou a Forma Traço Integral para compósitos na forma $\mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_s$ de grau $p_1p_2\ldots p_s$ livre de quadrados, sendo cada $\mathbb{K}_i$ uma p_i-extensão abeliana não ramificada, com $p_1, p_2, \ldots, p_s$, primos. Para esta seção, estaremos sempre considerando $\mathbb{K}$ uma p-extensão abeliana não ramificada de condutor n_1 e $\mathbb{L}$ uma q-extensão abeliana não ramificada de condutor n_2, com $p \neq q$ primos. Com isso, temos:

Lema 3.4.1 ([6], pág. 38)**.** *Se $mdc(n_1, n_2) = d$, então $cond(\mathbb{KL}) = \frac{n_1 n_2}{d}$.*

Para o próximo teorema, considere o compósito $\mathbb{M} = \mathbb{KL}$, $n = \text{cond}(\mathbb{M})$ e o grupo de Galois $\text{Gal}(\mathbb{M}/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i=0,1,\ldots,p-1}^{j=0,1,\ldots,q-1}$, onde $\theta_1|_{\mathbb{K}}$ é um gerador de $\text{Gal}(\mathbb{K}/\mathbb{Q})$, com $\theta_1|_{\mathbb{L}} = Id_{\mathbb{L}}$, $\theta_2|_{\mathbb{L}}$ é um gerador de $\text{Gal}(\mathbb{L}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}} = Id_{\mathbb{K}}$. Se $t = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)$, segue que:

Teorema 3.4.2 ([6], pág. 41)**.** *Se $x \in \mathcal{O}_{\mathbb{M}}$, com $x = \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\left(\theta_1^i \circ \theta_2^j\right)(t)$, então*

$$\begin{aligned} Tr_{\mathbb{M}/\mathbb{Q}}(x^2) &= n\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}^2 - \frac{n-n_1}{q}\sum_{i=0}^{p-1}\left(\sum_{j=0}^{q-1} a_{ij}\right)^2 \\ &\quad -\frac{n-n_2}{p}\sum_{j=0}^{q-1}\left(\sum_{i=0}^{p-1} a_{ij}\right)^2 + \frac{n-n_1-n_2+1}{pq}\left(\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\right)^2. \end{aligned}$$

Vejamos uma generalização desse teorema. Para cada $i = 1, 2, \ldots, s$, sejam $\mathbb{K}_i$ uma p_i-extensão abeliana não ramificada de condutor n_i, com $p_i \neq p_j$, se $i \neq j$ e $\mathbb{M} = \mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_s$. Considere $n_{i_1,i_2,\ldots,i_r} = \text{cond}(\mathbb{K}_{i_1}\mathbb{K}_{i_2}\ldots\mathbb{K}_{i_r})$, $n = \text{cond}(\mathbb{M})$, $\text{Gal}(\mathbb{M}/\mathbb{Q}) = \{\theta_1^{j_1} \circ \theta_2^{j_2} \circ \cdots \circ \theta_s^{j_s}\}_{j_i=0,1,\ldots,p_i-1}$, onde $\theta_i|_{\mathbb{K}_i}$ é um gerador de $\text{Gal}(\mathbb{K}_i/\mathbb{Q})$, com $\theta_i|_{\mathbb{K}_j} = Id_{\mathbb{K}_j}$, se $i \neq j$ e $t = \text{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)$. Com essas notações obtemos:

Teorema 3.4.3 ([6], pág. 47)**.** *Se $x \in \mathcal{O}_{\mathbb{M}}$, com $x = \sum_{i=1}^{s}\sum_{j_i=0}^{p_i-1} a_{j_1,j_2,\ldots,j_s}(\theta_1^{j_1} \circ \theta_2^{j_2} \circ \cdots \circ \theta_s^{j_s}(t))$, então*

$$\begin{aligned} Tr_{\mathbb{M}/\mathbb{Q}}(x^2) &= n\sum_{i=0}^{s}\sum_{j_i=0}^{p_i-1} a_{j_1,j_2,\ldots,j_s}^2 + \sum_{i=1}^{s} T_{p_i}\sum_{\substack{k=0\\k\neq i}}^{s}\sum_{j_k=0}^{p_k-1}\left(\sum_{j_i=0}^{p_i-1} a_{j_1,j_2,\ldots,j_s}\right)^2 \\ &\quad + \sum_{i_1<i_2} T_{p_{i_1}}T_{p_{i_2}}\sum_{\substack{k=0\\k\neq i_1,i_2}}^{s}\sum_{j_k=0}^{p_k-1}\left(\sum_{j_{i_1}=0}^{p_{j_{i_1}}-1}\sum_{j_{i_2}=0}^{p_{j_{i_2}}-1} a_{j_1,j_2,\ldots,j_s}\right)^2 \\ &\quad + \cdots + T_{p_1p_2\cdots p_s}\left(\sum_{i=1}^{s}\sum_{j_i=0}^{p_{j_i}-1} a_{j_1,j_2,\ldots,j_s}\right)^2, \end{aligned}$$

onde

$$T_{p_{i_1}p_{i_2}\cdots p_{i_r}} = \frac{h}{p_{i_1}p_{i_2}\cdots p_{i_r}}\left((-1)^r n + (-1)^{r-1}\sum_{k=1}^{r} n_{\hat{i}_k} + (-1)^{r-2}\sum_{k_1<k_2} n_{\hat{i}_{k_1},\hat{i}_{k_2}} + n_{\hat{j}_{i_1},\hat{j}_{i_2},\ldots,\hat{j}_{i_r}}\right),$$

sendo $h = \frac{\phi(n)}{p_1p_2\cdots p_s}$, $n_{\hat{i},\hat{k}} = n_{1,2,\ldots,i-1,i+1,\ldots,k-1,k+1,\ldots,s}$ e $n_{\hat{1},\hat{2},\ldots,\hat{s}} = 1$.

Em sua Tese, Moro observou que é possível simplificar a expressão da Forma Traço Integral do Teorema 3.4.2 tomando $n_1 = n_2 = n$, obtendo assim a equação:

$$\mathrm{Tr}_{\mathbb{M}/\mathbb{Q}}(x^2) \;=\; n\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}^2 - \frac{n-1}{pq}\left(\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\right)^2.$$

Além disso, ele obteve o mínimo da Forma Traço Integral para os $\mathbb{Z}$-módulos livres da forma

$$\mathcal{M}_m = \left\{ \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}(\theta_1^i \circ \theta_2^j(t));\ \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij} \equiv 0 \pmod{m} \right\},$$

como segue:

Teorema 3.4.4 ([6], pág. 58)**.** *Se m é um inteiro positivo, então*

$$M^* = \min_{x\in\mathcal{M}_m\setminus\{0\}} Tr_{\mathbb{M}/\mathbb{Q}}(x^2) = \min\left\{2n, F(m), F(2m), \ldots, F\left(\frac{pq}{d}m\right)\right\},$$

onde $d = mdc(pq, m)$, $F(km) = pqs_k^2 + 2s_kr_k + nr_k - \frac{n-1}{pq}r_k^2$, para k inteiro positivo, sendo s_k e r_k o quociente e resto da divisão de km por pq, respectivamente.

Exemplo 3.4.5 ([6], pág. 59)**.** Para $p_1 = 3$, $p_2 = 5$ $n_1 = n_2 = n = 2371$ e $m = 49$, a densidade de centro do reticulado 15-dimensional $\sigma_{\mathbb{M}}(\mathcal{M}_{49})$ é dada por $\delta(\sigma_{\mathbb{M}}(\mathcal{M}_{49})) \simeq 0,0055$. A melhor densidade de centro conhecida na dimensão 15 é $1/(16\sqrt{2}) \simeq 0,04419$.

3.5 Torre de p-Extensões Abelianas

Nesta seção iremos estudar alguns aspectos de corpos da forma $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_u$ (compósitos) de grau p^u, para $u \in \mathbb{N}$, com $\mathbb{L}_1, \mathbb{L}_2, \ldots, \mathbb{L}_u$ p-extensões abelianas não ramificadas e linearmente disjuntas, isto é, sendo $m_1, m_2, \ldots, m_u$ os condutores de $\mathbb{L}_1, \mathbb{L}_2, \ldots, \mathbb{L}_u$, respectivamente, então m_i e m_j são coprimos, ou equivalentemente, $\mathrm{cond}(\mathbb{M}) = n = \prod_{i=1}^{u} m_i$.

Note que neste caso obtemos a torre de compósitos em $\mathbb{Q}(\zeta_n)$ dada pela Figura 3.1, onde cada extensão de corpos $\mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_k/\mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_{k-1}$ é uma extensão ramificada de grau p, para $2 \leqslant k \leqslant u$. Mais especificamente, sendo $m_k = p_{k_1}p_{k_2}\ldots p_{k_s}$ a fatoração prima de m_k, então os ideais primos de $\mathcal{O}_{\mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_{k-1}} = \mathcal{O}_{\mathbb{L}_1}\mathcal{O}_{\mathbb{L}_2}\ldots\mathcal{O}_{\mathbb{L}_{k-1}}$, acima de p_{k_i}, para algum $1 \leqslant i \leqslant s$, são os ideais primos que se ramificam em $\mathcal{O}_{\mathbb{L}_1\mathbb{L}_2\ldots\mathbb{L}_k}$.

Vamos iniciar definindo Corpo de Gênero de um Corpo de Números e alguns resultados sobre ele com o objetivo final de associar o Corpo de Gênero de uma p-extensão abeliana não ramificada com o topo de qualquer torre como na Figura 3.1, para $u = s$ e $n = p_1p_2\ldots p_s$ livre de quadrados.

Definição 3.5.1. *Seja $\mathbb{K}$ um Corpo de Números algébricos. O* ***Corpo de Gênero*** *$\mathbb{K}^*$ de $\mathbb{K}$ é a extensão abeliana maximal de $\mathbb{K}$ de forma que $\mathbb{K}^* = \mathbb{K}\mathbb{L}$, onde $\mathbb{L}$ é um Corpo de Números abeliano absoluto, e $\mathbb{K}^*$ é não ramificado sobre $\mathbb{K}$. O grau $g_{\mathbb{K}} = [\mathbb{K}^* : \mathbb{K}]$ é denominado o* ***número de gênero*** *de $\mathbb{K}$ e o grupo de Galois $G = Gal(\mathbb{K}^*/\mathbb{K})$ é chamado de* ***grupo de gênero*** *de $\mathbb{K}$.*

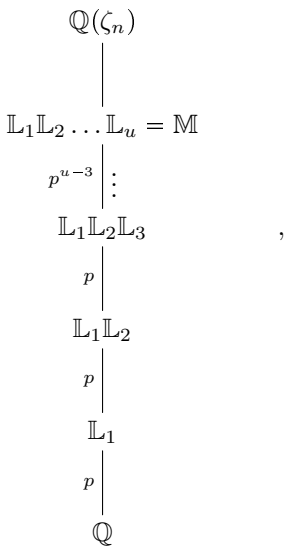

Figura 3.1: Torre ramificada de p-extensões abelianas.
Fonte: Próprio autor.

A definição acima pode ser encontrada na referência [12], página 1. A partir do Teorema de Kronecker-Weber (Teorema 2.1.13), essa definição pode ser representada através do seguinte diagrama:
onde $\mathbb{K}_0$ é o maior subcorpo abeliano de $\mathbb{K}$ e $\text{cond}(\mathbb{L}) = n$.

Se $\mathbb{K}$ é um corpo de números abeliano de condutor $n = p_1p_2\ldots p_s$ livre de quadrados, então o Corpo de Gênero pode ser visto como a parte abeliana do Corpo de Classes de Hilbert, $H(\mathbb{K})$, de $\mathbb{K}$, isto é, $\mathbb{K}^* = H(\mathbb{K}) \cap \mathbb{Q}(\zeta_n)$. Sendo assim, $\mathbb{K} = \mathbb{K}_0$, $\mathbb{K}^* = \mathbb{L}$ e o diagrama acima se reduz na Figura 3.3.

Quando o Corpo de Classes de Hilbert de $\mathbb{K}$ é uma extensão abeliana (sobre $\mathbb{Q}$), então o Corpo de Classes de Hilbert de $\mathbb{K}$ é o Corpo de Gênero $\mathbb{K}^*$ de $\mathbb{K}$.

Destacamos alguns resultados sobre Corpo de Gênero.

Proposição 3.5.2 ([12], pág 46)**.** *Seja $\mathbb{K}$ um Corpo de Números algébricos de grau $n = n_1n_2$, com $mdc(n_1, n_2) = 1$. Suponha que $\mathbb{K}$ é o compósito de dois subcorpos $\mathbb{L}_1$ e $\mathbb{L}_2$ de forma que $[\mathbb{L}_1 : \mathbb{Q}] = n_1$ e $[\mathbb{L}_2 : \mathbb{Q}] = n_2$ e seja $\mathbb{L}_i^*$ o Corpo de Gênero de $\mathbb{L}_i$ $(i = 1, 2)$. Então, o Corpo de Gênero de $\mathbb{K}$ é $\mathbb{K}^* = \mathbb{L}\mathbb{K}$, sendo $\mathbb{L} = \mathbb{L}_1'\mathbb{L}_2'$ e $\mathbb{L}_i'$ o subcorpo abeliano maximal de $\mathbb{K}_i^*$, isto é, $\mathbb{K}^* = \mathbb{L}_1^*\mathbb{L}_2^*$.*

Teorema 3.5.3 ([12], pág 48)**.** *Seja $\mathbb{K}$ um Corpo de Números abeliano de grau $n = q_1^{s_1}q_2^{s_2}\ldots q_t^{s_t}$, com $q_1, q_2\ldots q_t$ números primos distintos e $s_i > 0$, para $i = 1, 2, \cdots, t$. Então $\mathbb{K}$ é um compósito de corpos de números abelianos absolutos $\mathbb{L}_1, \mathbb{L}_2, \cdots, \mathbb{L}_t$, com $[\mathbb{L}_i : \mathbb{Q}] = q_i^{s_i}$. Além disso, $\mathbb{K}^* = \mathbb{L}_1^*\mathbb{L}_2^*\ldots\mathbb{L}_t^*$.*

Teorema 3.5.4 ([5], pág. 393)**.** *Sejam $\mathbb{K}$ um corpo de números abeliano absoluto de grau p^s, p primo, $s \geqslant 1$, S o conjunto de todos os primos $q \in \mathbb{Z}$ ramificados em $\mathbb{K}$ e $e(q)$ o índice de ramificação de q em $\mathbb{K}/\mathbb{Q}$. Então o Corpo de Gênero de $\mathbb{K}$ é*

$$\mathbb{K}^* = \mathbb{K}\prod_{q\in S\setminus\{p\}}\mathbb{K}_q = \prod_{q\in S}\mathbb{K}_q \quad \textit{(compósito)},$$

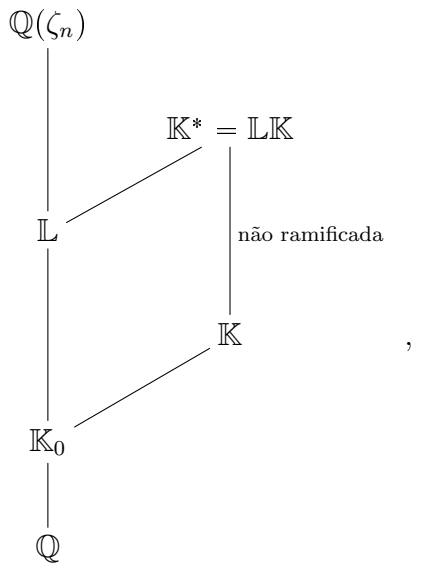

Figura 3.2: Diagrama do Corpo de Gênero.
Fonte: Próprio autor.

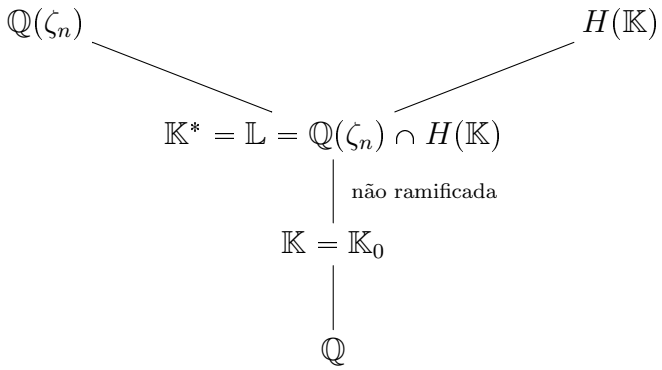

Figura 3.3: Diagrama do Corpo de Gênero no caso $\mathbb{K}$ abeliano.
Fonte: Próprio autor.

onde, $\mathbb{K}_q$ é o único subcorpo de grau $e(q)$ de de $\mathbb{Q}(\zeta_q)$ $(q \neq p)$, $\mathbb{K}_p$ é o único subcorpo de grau $e(p)$ de $\mathbb{Q}(\zeta_{p^t})$, para algum t.

Seja $\mathbb{K}$ um Corpo de Números de grau primo ímpar p não ramificado de condutor $n = p_1 \cdots p_s$, com $p_i \equiv 1 \pmod{p}$, e $p_i \neq p_j$. Tome $\mathbb{K}_i$ o único Corpo de Números (abeliano absoluto) de grau p e condutor p_i. Logo, o compósito $\mathbb{K}\mathbb{K}_i$ é um Corpo de Números de grau p^2 e podemos enunciar o seguinte resultado:

Proposição 3.5.5. *Sejam $\mathbb{K}$ uma p-extensão abeliana não ramificada de condutor $n = p_1 p_2 \cdots p_s$ livre de quadrados e $\mathbb{K}_1$ a única p-extensão (abeliana não ramificada) contida em $\mathbb{Q}(\zeta_{p_1})$, então existe um único Corpo de Números $\mathbb{M}$ de grau p com cond$(\mathbb{M}) = n/p_1 = p_2 \cdots p_s$, tal que $\mathbb{K}\mathbb{K}_1 = \mathbb{K}\mathbb{M} = \mathbb{K}_1\mathbb{M}$.*

Demonstração. Seja $\mathbb{K}_i$ a única p-extensão abeliana não ramificada de condutor p_i, para $i = 1, 2, \cdots, s$. Conforme o Teorema 3.5.4, o Corpo de Gênero de $\mathbb{K}$ é $\mathbb{K}^* = \mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_s$ e assim, $\mathbb{K}\mathbb{K}_2 \cdots \mathbb{K}_s \subseteq \mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_s$ e pelo Teorema 3.1.4 ambos os compósitos possuem o mesmo grau sobre $\mathbb{Q}$, a saber p^s, com isso $\mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_s = \mathbb{K}\mathbb{K}_2 \cdots \mathbb{K}_s$. Logo, $\mathbb{K}_1 \subset \mathbb{K}\mathbb{K}_2 \cdots \mathbb{K}_s$ e pelo Lema 3.1.6 existe uma p-extensão $\mathbb{M}$ contida em $\mathbb{K}_2 \cdots \mathbb{K}_s$ de forma

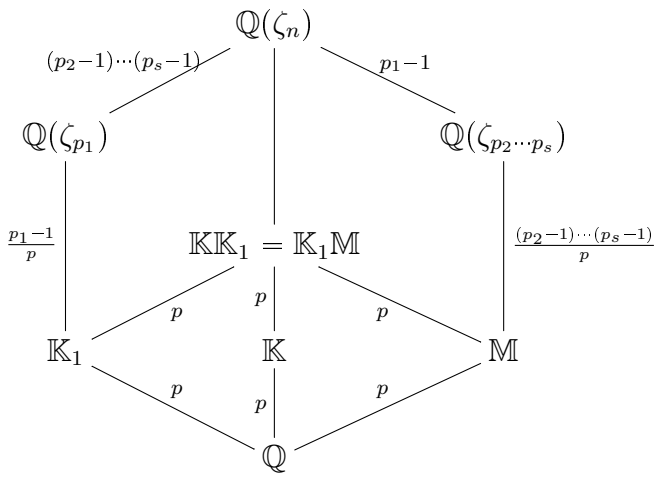

Figura 3.4: Existência da p-extensão $\mathbb{M}$ de condutor n/p_1.
Fonte: Próprio autor.

que $\mathbb{K}_1 \subset \mathbb{K}\mathbb{M}$. Note que, $\text{cond}(\mathbb{M}) = m$ divide $p_2 \cdots p_s$, uma vez que $\mathbb{M} \subset \mathbb{K}_2 \cdots \mathbb{K}_s$ e $\text{cond}(\mathbb{K}_2 \cdots \mathbb{K}_s) = p_2 \cdots p_s$. Além disso, $\mathbb{K}_1, \mathbb{M} \subseteq \mathbb{K}\mathbb{M}$ e $\mathbb{K}_1 \cap \mathbb{M} = \mathbb{Q}$, assim $\mathbb{K}_1\mathbb{M}$ é um subcorpo de $\mathbb{K}\mathbb{M}$ de grau p^2, ou seja, $\mathbb{K}_1\mathbb{M} = \mathbb{K}\mathbb{M}$. Como $\text{cond}(\mathbb{K}_1) = p_1$ é coprimo com $\text{cond}(\mathbb{M})$ e $\text{cond}(\mathbb{K}_1\mathbb{M}) = \text{cond}(\mathbb{K}\mathbb{M}) = \text{cond}(\mathbb{K}) = n = p_1p_2 \cdots p_s$, temos que $\text{cond}(\mathbb{M}) = p_2 \cdots p_s$. Por outro lado, $\mathbb{K}_1$ e $\mathbb{K}$ são p-extensões distintas contidas em $\mathbb{K}\mathbb{M}$, logo $\mathbb{K}\mathbb{K}_1 = \mathbb{K}\mathbb{M} = \mathbb{K}_1\mathbb{M}$.

Por fim, a unicidade do Corpo de Números $\mathbb{M}$ segue da Proposição 3.1.7, pois $\mathbb{M} \subseteq \mathbb{K}\mathbb{K}_1$ e $\text{cond}(\mathbb{M}) = p_2 \cdots p_s < n$, logo, $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$ é a única p-extensão de condutor $p_2 \cdots p_s$ contida no compósito $\mathbb{K}\mathbb{K}_1$. □

Pela Proposição 3.5.5 temos a unicidade do corpo $\mathbb{M}$ de $\text{cond}(\mathbb{M}) = p_2p_3 \cdots p_s$, porém a recíproca dessa afirmação não é em geral verdadeira, isto é, se $\mathbb{K}$ e $\mathbb{K}'$ são p-extensões abelianas não ramificadas tais que $\mathbb{M} = \mathbb{M}'$, onde $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$ e $\mathbb{M}' = \mathbb{K}'\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$, não temos a garantia de $\mathbb{K} = \mathbb{K}'$, contudo podemos reduzir essa afirmação, conforme segue:

Proposição 3.5.6. *Sejam $\mathbb{K}$ e $\mathbb{K}'$ p-extensões abelianas não ramificadas de condutor $n = p_1p_2 \ldots p_s$, $\mathbb{K}_1$ a única p-extensão com cond$(\mathbb{K}_1) = p_1$, $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$ e $\mathbb{M}' = \mathbb{K}'\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$. Então, $\mathbb{M} = \mathbb{M}'$ se, e somente se, $\mathbb{K}\mathbb{K}_1 = \mathbb{K}'\mathbb{K}_1$.*

Demonstração. Suponha que $\mathbb{M} = \mathbb{M}'$. Se $\mathbb{K} = \mathbb{K}'$, então $\mathbb{K}\mathbb{K}_1 = \mathbb{K}'\mathbb{K}_1$, caso contrário $[\mathbb{K}\mathbb{K}' : \mathbb{Q}] = p^2$. Note que neste caso, pela Proposição 3.5.5

$$\mathbb{K}\mathbb{K}'\mathbb{K}_1 = \mathbb{K}\mathbb{K}_1\mathbb{M}' = \mathbb{K}_1\mathbb{M}\mathbb{M}' = \mathbb{K}_1\mathbb{M},$$

assim $[\mathbb{K}\mathbb{K}'\mathbb{K}_1 : \mathbb{Q}] = [\mathbb{K}_1\mathbb{M} : \mathbb{Q}] = p^2$, ou seja, $\mathbb{K}_1 \subset \mathbb{K}\mathbb{K}'$ dessa forma, $\mathbb{K}_1\mathbb{K}, \mathbb{K}'\mathbb{K}_1 \subseteq \mathbb{K}\mathbb{K}'$ como ambos os compósitos são corpos de números de grau p^2, segue que $\mathbb{K}\mathbb{K}_1 = \mathbb{K}\mathbb{K}' = \mathbb{K}'\mathbb{K}_1$.

Reciprocamente, supondo a igualdade dos compósitos $\mathbb{K}\mathbb{K}_1$ e $\mathbb{K}'\mathbb{K}_1$, obtemos que $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s}) = \mathbb{K}'\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s}) = \mathbb{M}'$. □

Segue diretamente dessa proposição que:

Corolário 3.5.7. *Dados $\mathbb{K}$ e $\mathbb{K}'$ p-extensões abelianas não ramificadas distintas de condutor $n = \prod_{i=1}^{s} p_i$, $\mathbb{K}_1$ a única p-extensão com cond$(\mathbb{K}_1) = p_1$, $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$ e $\mathbb{M}' = \mathbb{K}'\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2\cdots p_s})$. Então, são equivalentes:*

1. $\mathbb{M} = \mathbb{M}'$.

2. $\mathbb{K}_1 \subseteq \mathbb{K}\mathbb{K}'$.

3. $\mathbb{K}\mathbb{K}' = \mathbb{K}_1\mathbb{M}$.

Novamente, consideremos $\mathbb{L}_1, \mathbb{L}_2, \ldots, \mathbb{L}_u \subseteq \mathbb{Q}(\zeta_n)$ p-extensões abelianas não ramificadas linearmente disjuntas de condutores $m_1, m_2, \ldots, m_u$, respectivamente, $n = p_1p_2 \ldots p_s$ livre de quadrados e $\mathbb{L} = \mathbb{L}_1\mathbb{L}_2 \ldots \mathbb{L}_u$. Logo, cada uma das extensões de corpos $\mathbb{L}_1\mathbb{L}_2 \ldots \mathbb{L}_k/\mathbb{L}_1\mathbb{L}_2 \ldots \mathbb{L}_{k-1}$ de grau p é ramificada, para $k = 1, 2, \ldots, u$.

Se $\mathbb{K}_i$ é a única p-extensão abeliana não ramificada de condutor p_i, para $1 \leqslant i \leqslant s$, então $\mathbb{K}_1\mathbb{K}_2 \ldots \mathbb{K}_s$ é o Corpo de Gênero de qualquer p-extensão abeliana não ramificada $\mathbb{K}$ de condutor n, com $[\mathbb{K}^* : \mathbb{Q}] = p^s$, assim a Figura 3.1 pode ser vista como na Figura 3.5, observando os condutores de cada um dos compósitos.

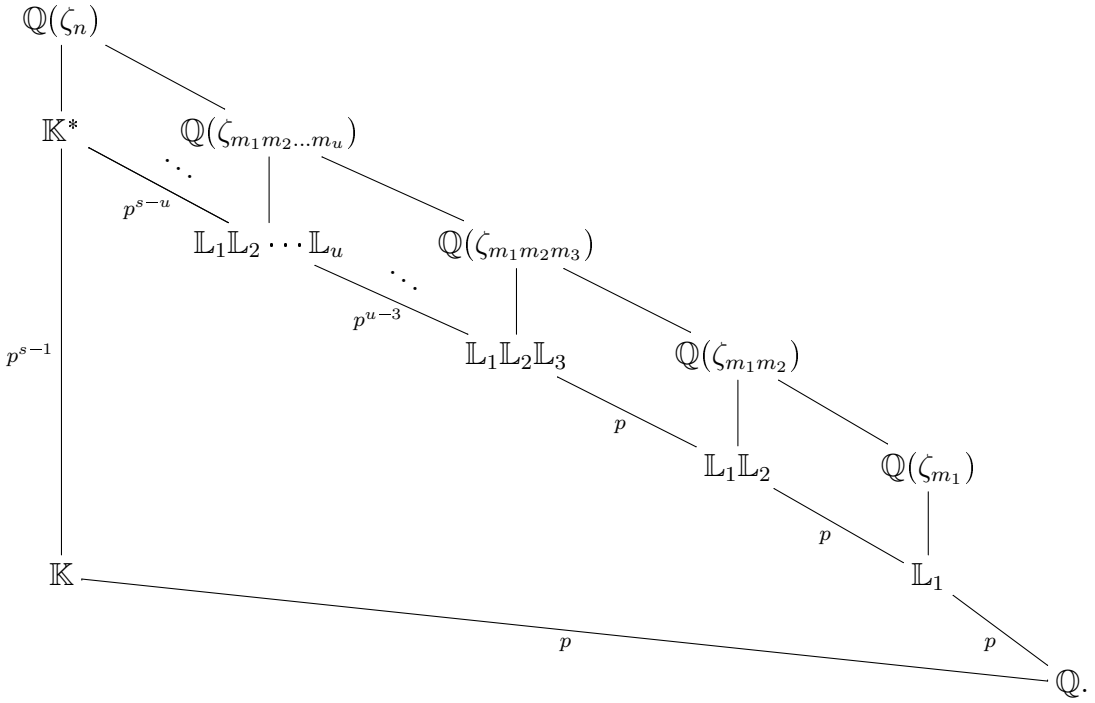

Figura 3.5: Condutores de cada compósito de p-extensões linearmente disjuntos.
Fonte: Próprio autor

Se $m = m_1m_2 \ldots m_u$, $\theta_i|_{\mathbb{L}_i}$ é um gerador de $\mathrm{Gal}(\mathbb{L}_i/\mathbb{Q})$, com $\theta_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, então

$$\left\{(\theta_1^{k_1} \circ \theta_2^{k_2} \circ \cdots \circ \theta_u^{k_u})(t) \ ; \ k_i = 0, 1, \ldots, p-1, \ i = 1, 2 \ldots, u\right\}$$

é uma base normal integral de $\mathbb{L} = \mathbb{L}_1\mathbb{L}_2 \ldots \mathbb{L}_u$, onde $t = Tr_{\mathbb{Q}(\zeta_m)/\mathbb{L}}(\zeta_m)$. Assim, conforme [7] página 58, se $t_i = Tr_{\mathbb{Q}(\zeta_{m_i})/\mathbb{L}_i}(\zeta_{m_i})$, então

$$Tr_{\mathbb{L}/\mathbb{Q}}(t(\theta_1^{k_1} \circ \theta_2^{k_2} \circ \cdots \circ \theta_u^{k_u})(t)) = \prod_{i=1}^{u} Tr_{\mathbb{L}_i/\mathbb{Q}}(t_i\theta_i^{k_i}(t_i)),$$

onde para cada $k_i = 0, 1, \ldots, p-1$, com $i = 1, 2, \ldots, u$, temos que

$$Tr_{\mathbb{L}_i/\mathbb{Q}}(t_i\theta_i^{k_i}(t_i)) = \begin{cases} m_i - \dfrac{m_i - 1}{p}, & \text{se} \quad k_i = 0 \\ -\dfrac{m_i - 1}{p}, & \text{se} \quad k_i \neq 0 \end{cases}.$$

Em particular, obtemos que

Proposição 3.5.8 ([7], pág 57)**.** *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* $\mathcal{O}_{\mathbb{L}_1\mathbb{L}_2}$*, então*

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

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

Dado uma p-extensão abeliana não ramificada $\mathbb{K}$ de condutor $n = p_1p_2\ldots p_s$ livre de quadrados, podemos utilizar as proposições desta seção para descrever uma maneira adequada para "subir" até o Corpo de Gênero $\mathbb{K}^*$ de $\mathbb{K}$, de forma que em cada subida (próximo compósito) obtemos um compósito de p-extensões abelianas não ramificadas linearmente disjunta.

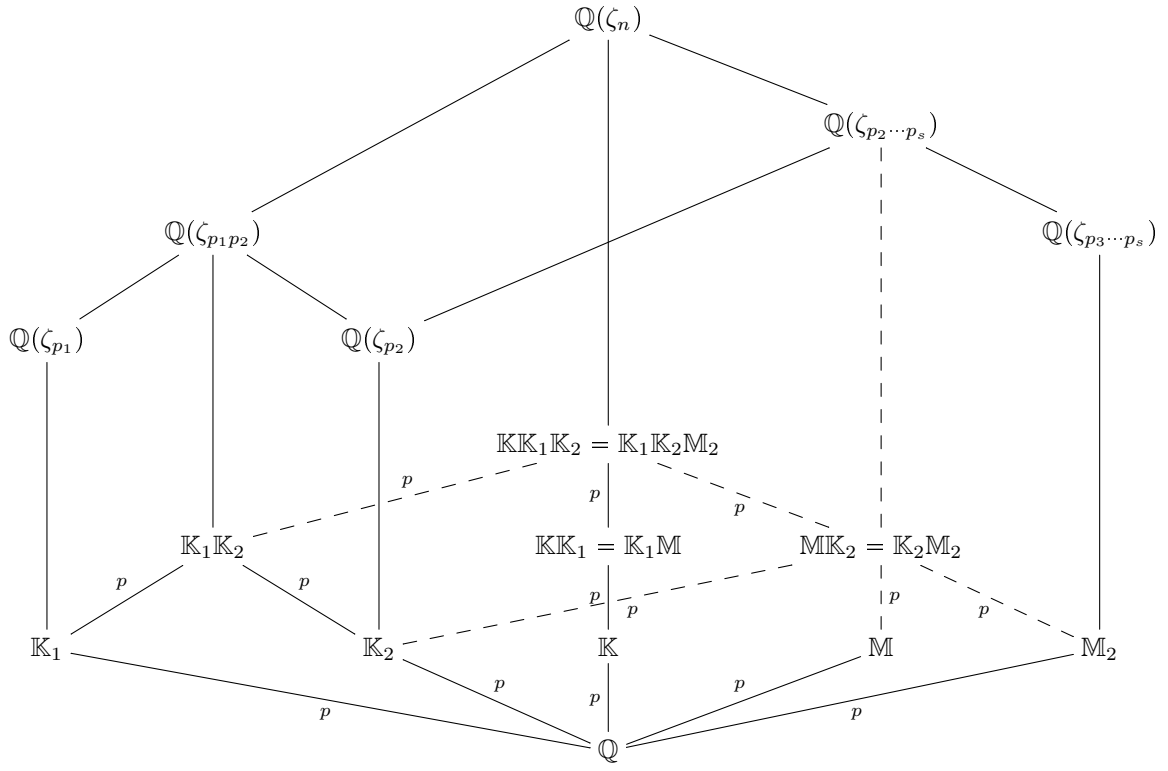

Figura 3.6: Construção de compósito de p-extensões de condutores coprimos.
Fonte: Próprio autor.

Considere $\mathbb{K}_i$ a única p-extensão de condutor p_i, para cada $i = 1, 2, \cdots, s$. Dessa forma o Corpo de Gênero $\mathbb{K}^*$ de $\mathbb{K}$ pode ser visto como o compósito $\mathbb{K}\mathbb{K}_1\mathbb{K}_2\cdots\mathbb{K}_{s-1}$. Pela Proposição 3.5.5, temos que $\mathbb{K}\mathbb{K}_1 = \mathbb{K}_1\mathbb{M}$, onde $\mathbb{M} = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2p_3\cdots p_s})$ é a única p-extensão abeliana não ramificada de condutor $p_2p_3\cdots p_s$ contida no compósito

$\mathbb{K}\mathbb{K}_1$. Assim, $\mathbb{K}\mathbb{K}_1\mathbb{K}_2 = \mathbb{K}_1\mathbb{M}\mathbb{K}_2$. Podemos utilizar novamente a Proposição 3.5.5, substituindo $\mathbb{K}$ por $\mathbb{M}$ e $\mathbb{K}_1$ por $\mathbb{K}_2$, isto é, $\mathbb{M}\mathbb{K}_2 = \mathbb{K}_2\mathbb{M}_2$, onde $\mathbb{M}_2 = \mathbb{M}\mathbb{K}_2 \cap \mathbb{Q}(\zeta_{p_3p_4\cdots p_s})$ é a única p-extensão abeliana não ramificada de condutor $p_3p_4 \ldots p_s$ contida em $\mathbb{M}\mathbb{K}_2$. Logo,

$$\mathbb{K}\mathbb{K}_1\mathbb{K}_2 = \mathbb{K}_1\mathbb{M}\mathbb{K}_2 = \mathbb{K}_1\mathbb{K}_2\mathbb{M}_2,$$

conforme a Figura 3.6.

Continuando o processo, de forma iterativa obtemos que

$$\mathbb{K}\mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_i = \mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_i\mathbb{M}_i,$$

sendo $\mathbb{M}_i = \mathbb{M}_{i-1}\mathbb{K}_i \cap \mathbb{Q}(\zeta_{p_{i+1}p_{i+2}\cdots p_s})$ a única p-extensão abeliana não ramificada de condutor $p_{i+1}p_{i+2}\cdots p_s$ contida em $\mathbb{M}_{i-1}\mathbb{K}_i$, para $i = 2, 3, \ldots, s-2$.

Note que na $(s-1)$-ésima iteração obtemos o Corpo de Gênero $\mathbb{K}^*$ de $\mathbb{K}$, onde $\mathbb{K}^* = \mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_{s-1}\mathbb{M}_{s-1}$, além disso $\mathbb{M}_{s-1} = \mathbb{M}_{s-2}\mathbb{K}_{s-1} \cap \mathbb{Q}(\zeta_{p_s}) = \mathbb{K}_s$.

4 Compósitos de grau p^2

Em [7], Oliveira obteve a expressão da forma traço integral de um compósito $\mathbb{KL}$, sendo $\mathbb{K}$ e $\mathbb{L}$ p-extensões abelianas não ramificadas de condutores coprimos m_1 e m_2, respectivamente. Neste contexto, as extensões $\mathbb{LK}/\mathbb{K}$ e $\mathbb{LK}/\mathbb{L}$ são ramificadas. Como uma das proposta em [7] foi a de descrever a forma traço integral com relação ao corpo de Gênero, o qual tem a propriedade que $\mathbb{K}^*/\mathbb{K}$ é não ramificada, podemos pensar em obter a forma traço integral de um compósito $\mathbb{L}_1\mathbb{L}_2$, com $\mathbb{L}_1$ e $\mathbb{L}_2$ sendo p-extensões abelianas não ramificadas, de forma que $\mathbb{L}_1\mathbb{L}_2/\mathbb{L}_1$ é não ramificado. Este é o primeiro desafio atribuído para este capítulo, o qual está situado nas seções 4.1 e 4.2 e tem como principal resultado a expressão da forma traço integral dado no Teorema 4.2.4.

As Seções 4.3 e 4.4 tem o propósito de fornecer a expressão da forma traço integral sobre uma nova perspectiva: Sejam $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2 \dots p_k$ e $m_2 = p_kp_{k+1} \dots p_s$, respectivamente, com $\mathrm{mdc}(m_1, m_2) = p_k$ de forma que exista uma p-extensão abeliana não ramificada $\mathbb{P} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$ de condutor m_1m_2/p_k. A forma traço integral para essa configuração esta descrita no Teorema 4.4.4, o qual é o principal resultado desta parte.

A fim de não sobrecarregador este capítulo com resultados extensos, recorreremos ao auxilio das Seções 5 e 5 do Apêndice **??**.

4.1 Construção de uma base normal integral para $\mathbb{L}_1\mathbb{L}_2$

Sejam $\mathbb{L}_1, \mathbb{L}_2, \dots, \mathbb{L}_u$ p-extensões abelianas não ramificadas de condutor cheio (isto é, $\mathrm{cond}(\mathbb{L}_i) = n$, para todo $1 \leqslant i \leqslant u$), tal que $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_{k-1} \cap \mathbb{L}_k = \mathbb{Q}$ para todo $2 \leqslant k \leqslant u$ e $\mathbb{K}, \mathbb{L}$ p-extensões abelianas não ramificadas de condutores coprimos m_1 e m_2, respectivamente. Note que cada extensão $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_k/\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_{k-1}$ é de grau p e não ramificada, pois $\mathbb{L}_1\mathbb{L}_2 \dots \mathbb{L}_k \subseteq \mathbb{L}_1^* = \mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_s$ e $\mathbb{L}_1^*/\mathbb{L}_1$ é não ramificada, sendo $\mathbb{K}_i$ a única p-extensão abeliana não ramificada de condutor p_i, conforme a Figura 4.1.

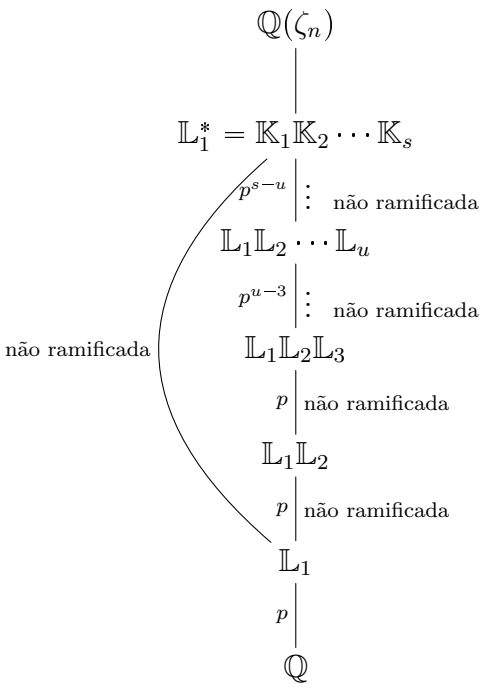

Figura 4.1: Torre não ramificada de p-extensões abelianas não ramificadas
Fonte: Próprio autor.

Pelo Teorema 3.1.4 temos que $\mathbb{KL}$ contém $(p^2-1)/(p-1) = p+1$ p-extensões abelianas não ramificadas, sendo que $(p-1)^{2-1} = p-1$ destas p-extensões possuem condutor n, conforme o Teorema 3.1.5. Uma vez que $p \geqslant 3$, existem ao menos duas p-extensões abelianas não ramificadas, $\mathbb{L}_1$ e $\mathbb{L}_2$, contidas em $\mathbb{KL}$ de condutor cheio, isto é, $\text{cond}(\mathbb{L}_1) = \text{cond}(\mathbb{L}_2) = n$. Além disso, $\mathbb{K}$ e $\mathbb{L}$ são as únicas duas p-extensões em $\mathbb{KL}$ de condutor menor que n.

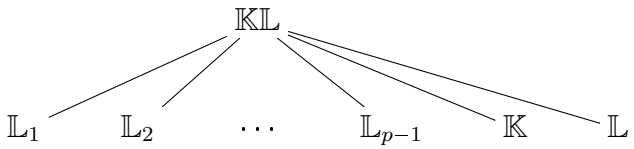

Figura 4.2: Subcorpos de grau p contidos em $\mathbb{KL}$.
Fonte: Próprio autor

Com isso, $\mathbb{KL} = \mathbb{L}_1\mathbb{L}_2$, onde $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{KL} = \mathbb{L}_1\mathbb{L}_2$ é uma cadeia de corpos ramificada e $\mathbb{Q} \subseteq \mathbb{L}_1 \subseteq \mathbb{KL} = \mathbb{L}_1\mathbb{L}_2$ é uma cadeia de corpos com $\mathbb{L}_1\mathbb{L}_2/\mathbb{L}_1$ não ramificada.

Logo, uma pergunta pertinente a se fazer é: Como se comporta a Forma Traço Integral $\text{Tr}_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2)$, com $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$, onde $\theta_1, \theta_2 \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\theta_1|_{\mathbb{L}_1}$ é um gerador de $\text{Gal}(\mathbb{L}_1/\mathbb{Q})$, $\theta_1|_{\mathbb{L}_2} = Id_{\mathbb{L}_2}$, $\theta_2|_{\mathbb{L}_2}$ é um gerador de $\text{Gal}(\mathbb{L}_2/\mathbb{Q})$ e $\theta_2|_{\mathbb{L}_1} = Id_{\mathbb{L}_1}$.

Responder a esta pergunta é a proposta desta e da próxima seção deste capítulo. Para isso, considere p-extensões abelianas não ramificadas $\mathbb{L}_1$ e $\mathbb{L}_2$, de mesmo condutor $n = p_1p_2\ldots p_s$, e p-extensões abelianas não ramificadas $\mathbb{K}, \mathbb{L} \subset \mathbb{L}_1\mathbb{L}_2$, de forma que $n = m_1m_2$, onde $m_1 = p_1p_2\ldots p_{s_1} = \text{cond}(\mathbb{K})$, $m_2 = p'_1p'_2\ldots p'_{s_2} = \text{cond}(\mathbb{L})$, $s_1 + s_2 = s$ e $\text{mdc}(m_1, m_2) = 1$, ou seja, $\mathbb{K}$ e $\mathbb{L}$ são p-extensões abelianas não ramificadas e linearmente disjuntas contidas no compósito $\mathbb{L}_1\mathbb{L}_2$.

Seja H o subgrupo de $\mathbb{Z}_n^* = Z_{p_1}^* \times Z_{p_2}^* \times \ldots \times Z_{p_s}^* \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{L}_1\mathbb{L}_2$. Assim, obtemos a correspondência de Galois conforme a Figura 4.3:

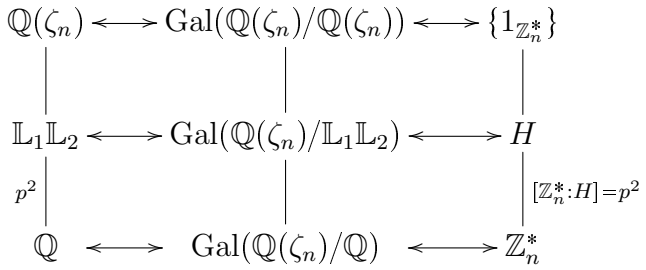

Figura 4.3: Correspondência de Galois.
Fonte: Próprio autor.

Se $\mathrm{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$, onde $\theta_1|_{\mathbb{L}_1}$ é um gerador de $\mathrm{Gal}(\mathbb{L}_1/\mathbb{Q})$ e $\theta_2|_{\mathbb{L}_2}$ é um gerador de $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$, $\sigma_{r_1}, \sigma_{r_2} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}))$ tal que $\sigma_{r_i}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_i$, com $\sigma_{r_i}(\zeta_n) = \zeta_n^{r_i}$, para $i = 1, 2$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$, então

$$t\left(\theta_1^i \circ \theta_2^j\right)(t) = \sum_{\alpha\in H} \zeta_n^{\alpha}\left(\theta_1^i \circ \theta_2^j\right)\left(\sum_{\beta\in H}\zeta_n^{\beta}\right) = \sum_{\alpha\in H}\zeta_n^{\alpha}\left(\sum_{\beta\in H}\zeta_n^{\beta r_1^i r_2^j}\right) = \sum_{\alpha,\beta\in H}\zeta_n^{\alpha+\beta r_1^i r_2^j}.$$

Seja $d = \frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_s}$, assim $\mathrm{mdc}(n, d) = 1$ e $\zeta_n^d = \zeta_{p_1}\zeta_{p_2}\ldots\zeta_{p_s}$, desta forma $\zeta_n^{\alpha+\beta r_1^i r_2^j}$ é uma raiz primitiva da unidade se, e somente se,

$$\zeta_n^{d\left(\alpha+\beta r_1^i r_2^j\right)} = \zeta_{p_1}^{\alpha+\beta r_1^i r_2^j}\zeta_{p_2}^{\alpha+\beta r_1^i r_2^j}\ldots\zeta_{p_s}^{\alpha+\beta r_1^i r_2^j}$$

também é uma raiz primitiva da unidade.

Denotando $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_s) \in H$ e $r_1 = (r_{1_1}, r_{1_2}, \ldots, r_{1_s})$, $r_2 = (r_{2_1}, r_{2_2}, \ldots, r_{2_s}) \in \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \ldots \times \mathbb{Z}_{p_s}^*$, temos que:

$$\alpha + \beta r_1^i r_2^j \pmod{p_k} \equiv \alpha_k + \beta_k r_{1_k}^i r_{2_k}^j,$$

para todo $k = 1, 2, \ldots, s$. Assim,

$$\begin{aligned}
Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(t(\theta_1^i \circ \theta_2^j)(t)\right) &= Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\sum_{\alpha,\beta\in H}\zeta_n^{\alpha+\beta r_1^i r_2^j}\right) \\
&= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\zeta_n^{\alpha+\beta r_1^i r_2^j}\right) \\
&= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\prod_{k=1}^{s}\zeta_{p_k}^{\alpha+\beta r_1^i r_2^j}\right) \\
&= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\prod_{k=1}^{s}\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right).
\end{aligned}$$

Além disso, para todo $y \in \mathbb{Q}(\zeta_n)$ e todo $l = 1, 2, \ldots, s$,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(y) = Tr_{\mathbb{Q}\left(\zeta_{\frac{n}{p_l}}\right)/\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}\left(\zeta_{\frac{n}{p_l}}\right)}(y)\right),$$

em que,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}\left(\zeta_{\frac{n}{p_l}}\right)}\left(\prod_{k=1}^{s}\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right) = \left(\prod_{k=1,k\neq l}^{s}\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right) Tr_{\mathbb{Q}(\zeta_{p_l})/\mathbb{Q}}\left(\zeta_{p_l}^{\alpha_l+\beta_l r_{1_l}^i r_{2_l}^j}\right).$$

Logo, o traço canônico parcial $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(t(\theta_1^i \circ \theta_2^j)(t)\right)$ é dado por:

$$\begin{aligned} &\sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_{1_1}^i r_{2_1}^j}) Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}\left(\zeta_{\frac{n}{p_1}}\right)}\left(\prod_{k=2}^{s}\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right) \\ = &\sum_{\alpha,\beta\in H}\prod_{k=1}^{s}\left(Tr_{\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}}\left(\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right)\right), \end{aligned} \tag{4.1}$$

onde

$$Tr_{\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}}\left(\zeta_{p_k}^{\alpha_k+\beta_k r_{1_k}^i r_{2_k}^j}\right) = \begin{cases} p_k - 1, & \text{se} \quad \alpha_k + \beta_k r_{1_k}^i = 0 \\ -1, & \text{se} \quad \alpha_k + \beta_k r_{1_k}^i \neq 0 \end{cases},$$

para $k = 1, 2, \ldots, s$.

Utilizando as notações dessa seção enunciaremos o próximo lema. De forma a facilitar as equações faremos uso da conversão $q_k = p_k - 1$, para cada $1 \leqslant k \leqslant s$.

Lema 4.1.1. *Sejam $P = \{1, 2, \ldots, s_1\}$, $P' = \{1, 2, \ldots, s_2\}$, $Y = \{y_i\}_{i=1}^{u} \subset P$ e $Y' = \{y'_{i'}\}_{i'=1}^{u'} \subset P'$, com $1 \leqslant y_1 < y_2 < \ldots < y_u \leqslant s_1$ e $1 \leqslant y'_1 < y'_2 < \ldots < y'_{u'} \leqslant s_2$ e considere as projeções canônicas $\Pi_{Y\times Y'} : H \to Z_{Y\times Y'}$, dadas por:*

$$\Pi_{Y\times Y'}(\alpha_1, \alpha_2, \ldots, \alpha_s) = (\alpha_{y_1}, \alpha_{y_2}, \ldots, \alpha_{y_u}, \alpha_{s_1+y'_1}, \alpha_{s_1+y'_2}, \ldots, \alpha_{s_1+y'_{u'}}),$$

onde $Z_{Y\times Y'} = Z_Y \times Z_{Y'}$, com $Z_Y = \mathbb{Z}_{p_{y_1}}^* \times \mathbb{Z}_{p_{y_2}}^* \times \cdots \times \mathbb{Z}_{p_{y_u}}^*$, $Z_{Y'} = \mathbb{Z}_{p'_{y'_1}}^* \times \mathbb{Z}_{p'_{y'_2}}^* \times \cdots \times \mathbb{Z}_{p'_{y'_{u'}}}^*$. Então $\Pi_Y(H) = Z_Y$, se $Y \subsetneq P$, $\Pi_{Y'}(H) = Z_{Y'}$, se $Y' \subsetneq P'$, $\Pi_P(H)$ e $\Pi_{P'}(H)$ são subgrupos próprios de índice p de $Z_P = \mathbb{Z}_{m_1}^*$ e $Z_{P'} = \mathbb{Z}_{m_2}^*$, respectivamente. Além disso, $\Pi_{Y\times Y'}(H) = \Pi_Y(H) \times \Pi_{Y'}(H)$. Em particular, $H = \Pi_P(H) \times \Pi_{P'}(H)$.

Demonstração. Para cada $j = 1, 2, \ldots, s_1$ e $j' = 1, 2, \ldots, s_2$, temos que $\Pi_j(H) \leqslant \mathbb{Z}_{p_j}^*$ e $\Pi_{j'}(H) \leqslant \mathbb{Z}_{p'_{j'}}^*$, logo

$$|\Pi_j(H)| = \frac{\left|\mathbb{Z}_{p_j}^*\right|}{r_j} = \frac{q_j}{r_j} \text{ e } |\Pi_{j'}(H)| = \frac{\left|\mathbb{Z}_{p'_{j'}}^*\right|}{r_{j'}} = \frac{q'_{j'}}{r_{j'}},$$

onde r_j e $r_{j'}$ são números naturais não nulos. Tome

$$\tilde{H} = \Pi_1(H) \times \Pi_2(H) \times \ldots \times \Pi_{s_1}(H) \times \Pi_{s_1+1}(H) \times \Pi_{s_1+2}(H) \times \ldots \times \Pi_s(H),$$

assim $H \leqslant H' \leqslant \mathbb{Z}_n^*$ e daí, $\frac{q_1 q_2 \ldots q_{s_1} q'_1 q'_2 \ldots q'_{s_2}}{p^2}$ divide $\frac{q_1 q_2 \ldots q_{s_1} q'_1 q'_2 \ldots q'_{s_2}}{r_1 r_2 \ldots r_{s_1} r'_1 r'_2 \ldots r'_{s_2}}$, dessa forma $r = r_1 r_2 \ldots r_{s_1} r'_1 r'_2 \ldots r'_{s_2}/p^2$, ou seja, $r = 1, p$ ou p^2.

Além disso,

$$|\Pi_P(H)| = \frac{\left|\mathbb{Z}^*_{m_1}\right|}{t_1} = \frac{q_1 q_2 \dots q_{s_1}}{t_1} \text{ e } |\Pi_{P'}(H)| = \frac{\left|\mathbb{Z}^*_{m_2}\right|}{t_2} = \frac{q'_1 q'_2 \dots q'_{s_2}}{t_2},$$

onde t_1 e t_2 são números naturais não nulos. Considere os grupos $J_{\mathbb{K}} = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$, $J_{\mathbb{L}} = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L})$ e as projeções canônicas $\Pi'_P : \mathbb{Z}^*_n \to Z_P$ e $\Pi'_{P'} : \mathbb{Z}^*_n \to Z_{P'}$. Note que $\Pi'_P(J_{\mathbb{K}}) = \text{Gal}(\mathbb{Q}(\zeta_{m_1})/\mathbb{K})$ e $\Pi'_{P'}(J_{\mathbb{L}}) = \text{Gal}(\mathbb{Q}(\zeta_{m_2})/\mathbb{L})$ e como $H \leqslant J_{\mathbb{K}} \cap J_{\mathbb{L}}$, segue que:

$$\Pi_P(H) = \Pi'_P(H) \leqslant \Pi'_P(J_1) \neq \mathbb{Z}^*_{m_1} \text{ e } \Pi_{P'}(H) = \Pi'_{P'}(H) \leqslant \Pi'_{P'}(J_2) \neq \mathbb{Z}^*_{m_2},$$

assim $t_1 = t_2 = p$ ($\Pi_P(H) = \text{Gal}(\mathbb{Q}(\zeta_{m_1})/\mathbb{K})$ e $\Pi_{P'}(H) = \text{Gal}(\mathbb{Q}(\zeta_{m_2})/\mathbb{L})$). Mas, $H \leqslant \Pi_P(H) \times \Pi_{P'}(H)$ e ambos possui ordem $\frac{q_1 q_2 \dots q_s}{p^2}$, dessa forma $H = \Pi_P(H) \times \Pi_{P'}(H)$.

Considere os subgrupos de $\mathbb{Z}^*_{m_1}$ e $\mathbb{Z}^*_{m_2}$,

$$\tilde{H}_P = \Pi_1(H) \times \Pi_2(H) \times \dots \times \Pi_{s_1}(H) \text{ e } \tilde{H}_{P'} = \Pi_{s_1+1}(H) \times \Pi_{s_1+2}(H) \times \dots \times \Pi_s(H),$$

respectivamente. Logo, obtemos as correspondências de Galois dadas na Figura 4.4.

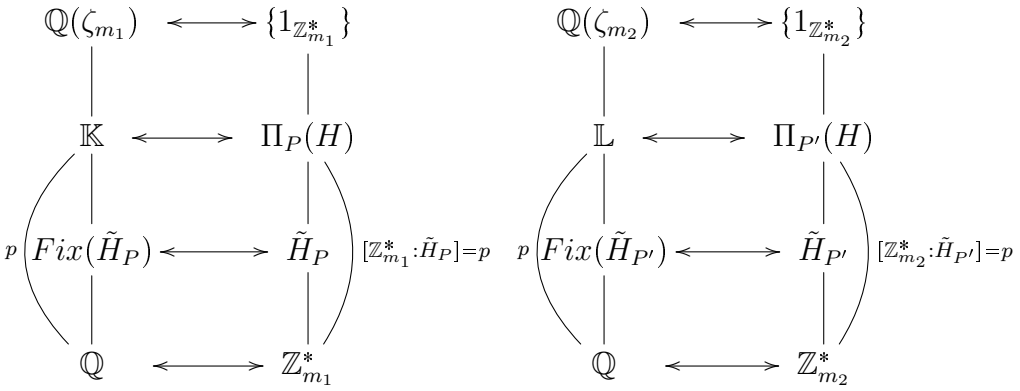

Figura 4.4: Correspondência de Galois dos corpos fixos de $\tilde{H}_P$ e $\tilde{H}_{P'}$.
Fonte: Próprio autor.

onde $\text{Fix}(\tilde{H}_P)$ e $\text{Fix}(\tilde{H}_{P'})$ são os corpos fixos por $\tilde{H}_P$ e $\tilde{H}_{P'}$, respectivamente.

Assim, $r_1 r_2 \dots r_{s_1}/t_1 = p$ e $r'_1 r'_2 \dots r'_{s_2}/t_2 = p$. Suponha que $r_1 r_2 \dots r_{s_1} = p$, então existe $1 \leqslant j \leqslant s_1$ de forma que $r_j = p$ e $r_k = 1$, para todo $k \in P \backslash \{i\}$. Então $\text{Fix}(\tilde{H}_P) = \mathbb{K}$ e $\text{cond}(\mathbb{K}) = p_j$, o que é um absurdo. Da mesma forma, $r'_1 = r'_2 = \dots = r'_{s_1} = 1$.

Se $Y \neq P$ e $Y' \neq P'$, considere os subgrupos

$$\tilde{H}_Y = \Pi_Y(H) \times \left(\prod_{l \in P \backslash Y} \Pi_l(H) \right) \text{ e } \tilde{H}_{Y'} = \Pi_{Y'}(H) \times \left(\prod_{l \in P' \backslash Y'} \Pi_l(H) \right),$$

de $\mathbb{Z}^*_{m_1}$ e $\mathbb{Z}^*_{m_2}$, respectivamente. Um argumento similar ao feito acima mostra que $\Pi_P(H)$ é um subgrupo próprio de $\tilde{H}_Y$ e $\Pi_{P'}(H)$ é um subgrupo próprio de $\tilde{H}'_Y$, ou seja, $\Pi_Y(H) = Z_Y$ e $\Pi_{Y'}(H) = Z_{Y'}$.

Resta mostrarmos que $\Pi_{Y \times Y'}(H) = \Pi_Y(H) \times \Pi_{Y'}(H)$. Note que,

$$\Pi_{Y \times Y'}(H) \subseteq \Pi_Y(H) \times \Pi_{Y'}(H).$$

Por outro lado, dado

$$\overline{\alpha} = (\alpha_{y_1}, \alpha_{y_2}, \ldots, \alpha_{y_u}, \alpha_{s_1+y'_1}, \alpha_{s_1+y'_2}, \ldots, \alpha_{s_1+y'_{u'}}) \in \Pi_Y(H) \times \Pi_{Y'}(H),$$

existem elementos

$$\tilde{\alpha} = (\alpha_1, \alpha_2 \ldots, \alpha_{s_1}, \tilde{\alpha}_{s_1+1}, \tilde{\alpha}_{s_1+2}, \ldots, \tilde{\alpha}_s) \in H$$

e

$$\alpha' = (\alpha'_1, \alpha'_2, \ldots, \alpha'_{s_1}, \alpha_{s_1+1}, \alpha_{s_1+2}, \ldots, \alpha_s) \in H,$$

assim $\overline{\alpha} = \Pi_Y(\tilde{\alpha}) \times \Pi_{Y'}(\alpha')$. Como $H = \Pi_P(H) \times \Pi_{P'}(H)$, então

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s) = \Pi_P(\tilde{\alpha}) \times \Pi_{P'}(\alpha') \in H \text{ e } \overline{\alpha} = \Pi_{Y\times Y'}(\alpha) \in \Pi_{Y\times Y'}(H).$$

Logo, $\Pi_{Y\times Y'}(H) = \Pi_Y(H) \times \Pi_{Y'}(H)$. □

Com as mesma notações do lema anterior temos que:

Corolário 4.1.2. *Se* $1 \leqslant l_1 < l_2 < \ldots < l_{s_1-u} \leqslant s_1$ *são os elementos distintos de* $y_1, y_2, \ldots, y_u$ *e* $1 \leqslant l'_1 < l'_2 < \ldots < l'_{s_2-u'} \leqslant s_2$ *são os elementos distintos de* $y'_1, y'_2, \ldots, y'_{u'}$, *denotando* $L = \{l_i\}_{i=1}^{s_1-u}$ *e* $L' = \{l'_{i'}\}_{i'=1}^{s_2-u'}$, *então*

$$A_L = |\ker \Pi_Y| = \begin{cases} 1 & , se \quad u = s_1 \ (L = \varnothing \Longleftrightarrow Y = P) \\ \dfrac{\prod_{i=1}^{s_1-u} q_{l_i}}{p} & , se \quad u < s_1 \ (L \neq \varnothing \Longleftrightarrow Y \neq P) \end{cases},$$

$$A_{L'} = |\ker \Pi_{Y'}| = \begin{cases} 1 & , se \quad u' = s_2 \ (L' = \varnothing \Longleftrightarrow Y' = P') \\ \dfrac{\prod_{i'=1}^{s_2-u'} q'_{l_{i'}}}{p} & , se \quad u' < s_2 \ (L' \neq \varnothing \Longleftrightarrow Y' \neq P') \end{cases}.$$

E,

$$A_{L\times L'} = |\ker \Pi_{Y\times Y'}| = \begin{cases} 1 & , se \quad u = s_1 \ e \ u' = s_2 \ (Y = P \ e \ Y' = P') \\ \dfrac{\prod_{i=1}^{s_1-u} q_{l_i}}{p} & , se \quad u < s_1 \ e \ u' = s_2 \ (Y \neq P \ e \ Y' = P') \\ \dfrac{\prod_{i'=1}^{s_2-u'} q'_{l_{i'}}}{p} & , se \quad u = s_1 \ e \ u' < s_2 \ (Y = P \ e \ Y' \neq P') \\ \dfrac{\prod_{i=1}^{s_1-u} q_{l_i} \prod_{i'=1}^{s_2-u'} q'_{l_{i'}}}{p^2} & , se \quad u < s_1 \ e \ u' < s_2 \ (Y \neq P \ e \ Y' \neq P') \end{cases}.$$

Demonstração. De fato, basta notar que

$$A_L = |\ker \Pi_Y| = \frac{|H|}{|\Pi_Y(H)|},$$

$$A_{L'} = |\ker \Pi_{Y'}| = \frac{|H|}{|\Pi_{Y'}(H)|}$$

e,

$$A_{L\times L'} = |\ker \Pi_{Y\times Y'}| = \frac{|H|}{|\Pi_{Y\times Y'}(H)|} = \frac{|H|}{|\Pi_Y(H)||\Pi_{Y'}(H)|}.$$

□

Corolário 4.1.3. *Dado $z \in \Pi_{Y\times Y'}(H)$, então $|\Pi^{-1}_{Y\times Y'}(z)| = |Ker\Pi_{Y\times Y'}| = A_{L\times L'}$.*

Demonstração. Basta notar que dado $\alpha \in \Pi^{-1}_{Y\times Y'}(z)$, obtemos que $\Pi^{-1}_{Y\times Y'}(z) = \alpha + Ker\Pi_{Y\times Y'}$. □

Com isso, para cada $\alpha \in H$, a quantidade de elementos em H que coincidem com α em todas as coordenadas de $Y \times Y'$ é exatamente $A_{L\times L'}$.

Observação 4.1.4. Usaremos também a notação $A_{l_1,l_2,l_{s_1-u},l'_1,l'_2,l'_{s_2-u'}}$ para $A_{L\times L'}$.

A proposição a seguir nos fornecerá uma base normal integral, a qual utilizaremos a fim de obter a Forma Traço Integral da extensão $\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}$.

Proposição 4.1.5. *Seja $\varphi_1 \in Gal(\mathbb{L}_1/\mathbb{Q})$, com $\varphi_1 \neq Id_{\mathbb{L}_1}$. Então existe $1 \leqslant \tilde{t} \leqslant p-1$ e elementos σ_{r_1} e σ_{r_2} em $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, de forma que $G = Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$, onde $\theta_1 = \sigma_{r_1}|_{\mathbb{L}_1\mathbb{L}_2}$, $\sigma_{r_1}|_{\mathbb{L}_1} = \varphi_1$, $\theta_2 = \sigma_{r_2}|_{\mathbb{L}_1\mathbb{L}_2}$, $\theta_2|_{\mathbb{L}_2}$ é um gerador de $Gal(\mathbb{L}_2/\mathbb{Q})$ e ao identificarmos σ_{r_1} e σ_{r_2} em $\mathbb{Z}_n^* \simeq Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, obtemos:*

$$r_1 = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}, r_{1_{s_1+2}}, \ldots, r_{1_s})$$

e,

$$r_2 = (r_{2_1}, r_{2_2}, \ldots, r_{2_{s_1}}, r_{2_{s_1+1}}, r_{2_{s_1+2}}, \ldots, r_{2_s}) = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r^{\tilde{t}}_{1_{s_1+1}}, r^{\tilde{t}}_{1_{s_1+2}}, \ldots, r^{\tilde{t}}_{1_s}),$$

respectivamente.

Demonstração. Dado um gerador φ_1 de Gal$(\mathbb{L}_1/\mathbb{Q})$, considere a extensão $\theta_1 \in$ G de φ_1 pelo homomorfismo $Id_{\mathbb{L}_2}$, logo $\theta_1|_{\mathbb{L}_1} = \varphi_1 \neq Id_{\mathbb{L}_1}$ e $\theta_1|_{\mathbb{L}_2} = Id_{\mathbb{L}_2}$.

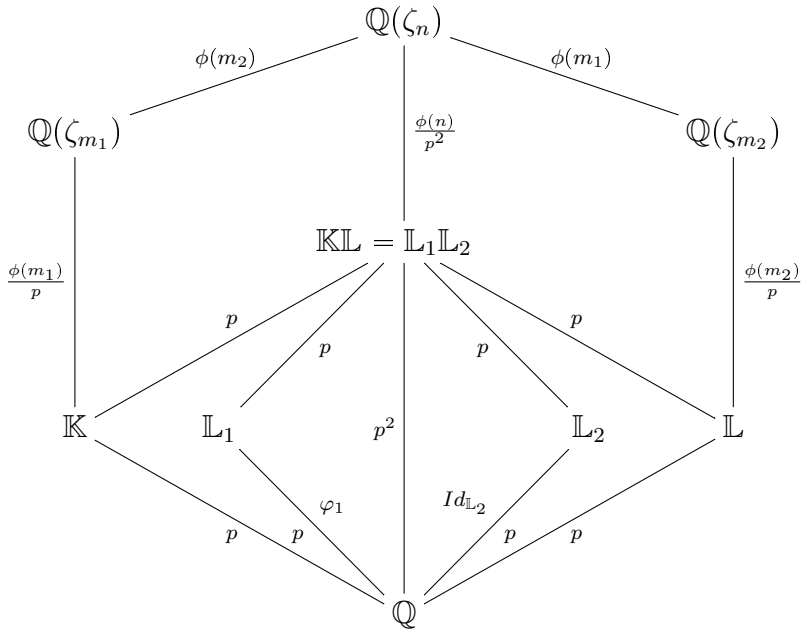

Figura 4.5: Obtenção de θ_1.
Fonte: Próprio autor.

Tome $\sigma_{r_1} \in$ Gal$(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, tal que $\sigma_{r_1}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_1$, isto é, qualquer extensão de θ_1 em Gal$(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e

$$r_1 = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}, r_{1_{s_1+2}}, \ldots, r_{1_s})$$

a identificação de σ_{r_1} em

$$\mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \ldots \times \mathbb{Z}_{p_{s_1}}^* \times \mathbb{Z}_{p_{s_1+1}}^* \times \mathbb{Z}_{p_{s_1+2}}^* \times \ldots \times \mathbb{Z}_{p_s}^*.$$

Note que, $\sigma_{r_1} \notin \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}\mathbb{L})$, ou seja, $r_1 \notin H$, em particular $\sigma_{r_1} \notin \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$ e $\sigma_{r_1} \notin \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L})$. Além disso, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L})$ são subgrupos normais de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, com

$$\left|\frac{\mathrm{Gal}\ (\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\mathrm{Gal}\ (\mathbb{Q}(\zeta_n)/\mathbb{K})}\right| = \left|\frac{\mathrm{Gal}\ (\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\mathrm{Gal}\ (\mathbb{Q}(\zeta_n)/\mathbb{L})}\right| = p.$$

Logo, $\sigma_{r_1}^p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K})$ e $\sigma_{r_1}^p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L})$, ou seja,

$$(r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}})^k = (r_{1_1}^k, r_{1_2}^k, \ldots, r_{1_{s_1}}^k) \in J_{\mathbb{K}} \Longleftrightarrow k \equiv 0 \pmod{p},$$

onde $J_{\mathbb{K}}$ é o subgrupo de $\mathbb{Z}_{m_1}^*$ que fixa $\mathbb{K}$ e

$$(r_{1_{s_1+1}}, r_{1_{s_1+2}}, \ldots, r_{1_s})^p = (r_{1_{s_1+1}}^p, r_{1_{s_1+2}}^p, \ldots, r_{1_s}^p) \in J_{\mathbb{L}} \Longleftrightarrow k \equiv 0 \pmod{p},$$

onde $J_{\mathbb{L}}$ é o subgrupo de $\mathbb{Z}_{m_2}^*$ que fixa $\mathbb{L}$.

Dado $\tilde{t} \in \{1, 2 \ldots, p-1\}$, denotemos $\tilde{\sigma}_{\tilde{t}}$ o elemento de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que na identificação $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$ obtemos

$$(r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \ldots, r_{1_s}^{\tilde{t}}).$$

Claramente, temos que

$$\tilde{\sigma}_{\tilde{t}} \notin \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}),\ \tilde{\sigma}_{\tilde{t}} \notin \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}),\ \tilde{\sigma}_{\tilde{t}}^p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}) \text{ e } \tilde{\sigma}_{\tilde{t}}^p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{L}),$$

com isso $\left|\tilde{\sigma}_{\tilde{t}}|_{\mathbb{L}_1\mathbb{L}_2}\right| = p$. Seja $\mathbb{P}_{\tilde{t}}$ o subcorpo de $\mathbb{L}_1\mathbb{L}_2$ fixo por $\tilde{\sigma}_{\tilde{t}}|_{\mathbb{L}_1\mathbb{L}_2}$. Note que,

$$\left[\mathbb{P}_{\tilde{t}} : \mathbb{Q}\right] = p = \left[\mathbb{L}_1\mathbb{L}_2 : \mathbb{P}_{\tilde{t}}\right],\ \mathbb{P}_{\tilde{t}} \neq \mathbb{K} \text{ e } \mathbb{P}_{\tilde{t}} \neq \mathbb{L}.$$

Sejam $1 \leqslant t_1, t_2 \leqslant p-1$, com $\mathbb{P}_{t_1} = \mathbb{P}_{t_2}$, logo

$$(r_{1_1}^p, r_{1_2}^p, \ldots, r_{1_{s_1}}^p, r_{1_{s_1+1}}^{pt_1+(t_2-t_1)}, r_{1_{s_1+2}}^{pt_1+(t_2-t_1)}, \ldots, r_{1_s}^{pt_1+(t_2-t_1)}) = \tilde{\sigma}_{t_1}^{p-1}\tilde{\sigma}_{t_2}$$

fixa $\mathbb{P}_{t_1}$ e também fixa $\mathbb{K} \neq \mathbb{P}_{t_1}$. Dessa forma, $\mathbb{P}_{t_1}\mathbb{K} = \mathbb{K}\mathbb{L}$, em particular fixa $\mathbb{L}$, portanto $t_2 = t_1$. Como a quantidade de p-extensões contidas em $\mathbb{L}_1\mathbb{L}_2$, distintas de $\mathbb{K}$ e $\mathbb{L}$, é $p-1$, segue que existe $1 \leqslant \tilde{t} \leqslant p-1$, tal que $\tilde{\sigma}_{\tilde{t}}|_{\mathbb{L}_2}$ gera $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$. Tomando $\sigma_{r_2} = \tilde{\sigma}_{\tilde{t}}$, obtemos que

$$r_2 = (r_{2_1}, r_{2_2}, \ldots, r_{2_{s_1}}, r_{2_{s_1+1}}, r_{2_{s_1+2}}, \ldots, r_{2_s}) = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \ldots, r_{1_s}^{\tilde{t}}),$$

$\sigma_{r_2}|_{\mathbb{L}_2}$ gera $\mathrm{Gal}(\mathbb{L}_2/\mathbb{Q})$ e $\mathrm{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$, onde $\theta_2 = \sigma_{r_2}|_{\mathbb{L}_1\mathbb{L}_2}$. □

Segue diretamente dessa proposição que:

Corolário 4.1.6. *Se* $0 \leqslant i, j \leqslant p-1$ *e* $1 \leqslant \tilde{t} \leqslant p-1$, *então:*

1) $(r_{1_1}^{i+j}, r_{1_2}^{i+j}, \ldots, r_{1_{s_1}}^{i+j}, 1, 1, \ldots, 1) \in H$ *se, e somente se,* $i + j \equiv 0$ *(mod* p*).*

2) $(1, 1, \ldots, 1, r_{1_{s_1+1}}^{i+\tilde{t}j}, r_{1_{s_1+2}}^{i+\tilde{t}j}, \ldots, r_{1_s}^{i+\tilde{t}j}) \in H$ *se, e somente se,* $i + \tilde{t}j \equiv 0$ *(mod* p*).*

4.2 Forma Traço Integral no caso linearmente disjunto

Com os resultados obtidos na Seção 5 podemos enunciar o Teorema 4.2.4, principal resultado deste capítulo. Para facilitar a sua prova, faremos uso de três lemas auxiliares (Lemas 5.0.4, 5.0.5 e 5.0.6) como segue:

Lema 4.2.1. *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões abelianas não ramificadas de condutor $n = p_1p_2\dots p_s$, com $p_1, p_2, \dots, p_s$ números primos distintos, $\mathbb{K}$ e $\mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$ p-extensões de condutores m_1 e m_2, respectivamente, com $n = m_1m_2$ $(mdc(m_1, m_2 = 1))$ e $Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\dots p-1}$, onde $\theta_1|_{\mathbb{L}_1}$ é um gerador de $Gal(\mathbb{L}_1/\mathbb{Q})$ e $\theta_2|_{\mathbb{L}_2}$ é um gerador de $Gal(\mathbb{L}_2/\mathbb{Q})$, $\sigma_{r_i}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_i$, para $i = 1, 2$ satisfazendo*

$$r_2 = (r_{1_1}, r_{1_2}, \dots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \dots, r_{1_s}^{\tilde{t}}),$$

para algum $2 \leqslant \tilde{t} \leqslant p-1$. Então, dado $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$ e escrevendo $x \in \mathcal{O}_{\mathbb{L}_1\mathbb{L}_2}$ como $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$, temos que

$$\begin{aligned} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2) &= \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) \\ &= \frac{(m_1-1)(m_2-1)}{p^2} - \frac{m_1(m_2-1)+(m_1-1)m_2}{p} + n. \end{aligned}$$

Demonstração. A prova deste resultado encontra-se no Apêndice **??**, Lema 5.0.4. □

Lema 4.2.2. *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões abelianas não ramificadas de condutor $n = p_1p_2\dots p_s$, com $p_1, p_2, \dots, p_s$ números primos distintos, $\mathbb{K}$ e $\mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$ p-extensões de condutores m_1 e m_2, respectivamente, com $n = m_1m_2$ $(mdc(m_1, m_2 = 1))$ e $Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\dots p-1}$, onde $\theta_1|_{\mathbb{L}_1}$ é um gerador de $Gal(\mathbb{L}_1/\mathbb{Q})$ e $\theta_2|_{\mathbb{L}_2}$ é um gerador de $Gal(\mathbb{L}_2/\mathbb{Q})$, $\sigma_{r_i}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_i$, para $i = 1, 2$ satisfazendo*

$$r_2 = (r_{1_1}, r_{1_2}, \dots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \dots, r_{1_s}^{\tilde{t}}),$$

para algum $2 \leqslant \tilde{t} \leqslant p-1$. Então, dado $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$ e escrevendo $x \in \mathcal{O}_{\mathbb{L}_1\mathbb{L}_2}$ como $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$, temos que

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i)(t)) = \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i)(t)) = \frac{(m_1-1)(m_2-1)}{p^2},$$

e

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_2^j)(t)) = \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_2^j)(t)) = \frac{(m_1-1)(m_2-1)}{p^2}.$$

Demonstração. A prova deste resultado encontra-se no Apêndice **??**, Lema 5.0.5. □

Lema 4.2.3. *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões abelianas não ramificadas de condutor $n = p_1p_2\dots p_s$, com $p_1, p_2, \dots, p_s$ números primos distintos, $\mathbb{K}$ e $\mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$ p-extensões de condutores m_1 e m_2, respectivamente, com $n = m_1m_2$ $(mdc(m_1, m_2 = 1))$ e $Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) =$*

$\{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$, *onde* $\theta_1|_{\mathbb{L}_1}$ *é um gerador de* $Gal(\mathbb{L}_1/\mathbb{Q})$ *e* $\theta_2|_{\mathbb{L}_2}$ *é um gerador de* $Gal(\mathbb{L}_2/\mathbb{Q})$, $\sigma_{r_i}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_i$, *para* $i = 1, 2$ *satisfazendo*

$$r_2 = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \ldots, r_{1_s}^{\tilde{t}}),$$

para algum $2 \leqslant \tilde{t} \leqslant p-1$. *Então, dado* $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$ *e escrevendo* $x \in \mathcal{O}_{\mathbb{L}_1\mathbb{L}_2}$ *como* $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$, *temos que*

1. *Se* $i \not\equiv -j \pmod p$ *e* $i \not\equiv -\tilde{t}j \pmod p$, *então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{1}{h} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{(m_1-1)(m_2-1)}{p^2}.$$

2. *Se* $i \equiv -j \pmod p$, *então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{1}{h} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{(m_1-1)(m_2-1)}{p^2} - \frac{m_1(m_2-1)}{p}.$$

3. *Se* $i \equiv -\tilde{t}j \pmod p$, *então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{1}{h} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{(m_1-1)(m_2-1)}{p^2} - \frac{(m_1-1)m_2}{p}.$$

Demonstração. A prova deste resultado encontra-se no Apêndice **??**, Lema 5.0.6. □

Juntando estes três Lemas, destacamos o próximo resultado que nos fornece a forma traço integral.

Teorema 4.2.4. *Sejam* $\mathbb{L}_1$ *e* $\mathbb{L}_2$ *p-extensões abelianas não ramificadas de condutor* $n = p_1p_2\ldots p_s$, *com* $p_1, p_2, \ldots, p_s$ *números primos distintos,* $\mathbb{K}$ *e* $\mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$ *p-extensões de condutores* m_1 *e* m_2, *respectivamente, com* $n = m_1m_2$ $(mdc(m_1, m_2 = 1))$ *e* $Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$, *onde* $\theta_1|_{\mathbb{L}_1}$ *é um gerador de* $Gal(\mathbb{L}_1/\mathbb{Q})$ *e* $\theta_2|_{\mathbb{L}_2}$ *é um gerador de* $Gal(\mathbb{L}_2/\mathbb{Q})$, $\sigma_{r_i}|_{\mathbb{L}_1\mathbb{L}_2} = \theta_i$, *para* $i = 1, 2$ *satisfazendo*

$$r_2 = (r_{1_1}, r_{1_2}, \ldots, r_{1_{s_1}}, r_{1_{s_1+1}}^{\tilde{t}}, r_{1_{s_1+2}}^{\tilde{t}}, \ldots, r_{1_s}^{\tilde{t}}),$$

para algum $2 \leqslant \tilde{t} \leqslant p-1$. *Então, dado* $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{L}_1\mathbb{L}_2}(\zeta_n)$ *e escrevendo* $x \in \mathcal{O}_{\mathbb{L}_1\mathbb{L}_2}$ *como* $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$, *temos que*

$$\begin{aligned} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2 \\ &- \frac{m_1(m_2-1)}{p}\sum_{j=0}^{p-1} A_j^2 - \frac{(m_1-1)m_2}{p}\sum_{j=0}^{p-1} B_j^2, \end{aligned} \tag{4.2}$$

onde $A_j = a_{0j} + \sum_{\substack{u=1,v=0 \\ u\equiv(j-v) \pmod p}}^{p-1} a_{uv}$ *e* $B_j = a_{0j} + \sum_{\substack{u=1,v=0 \\ u\equiv\tilde{t}(j-v) \pmod p}}^{p-1} a_{uv}$.

Demonstração. Dado

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

temos que

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

Assim,

$$\begin{aligned} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}\left(\sum_{i,j=0}^{p-1} \sum_{u,v=0}^{p-1} a_{ij}a_{uv}(\theta_1^i \circ \theta_2^j)(t)(\theta_1^u \circ \theta_2^v)(t)\right) \\ &= \sum_{i,j=0}^{p-1} \sum_{u,v=0}^{p-1} a_{ij}a_{uv} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}\left((\theta_1^i \circ \theta_2^j)(t)(\theta_1^u \circ \theta_2^v)(t)\right) \\ &= \sum_{i,j=0}^{p-1} \sum_{u,v=0}^{p-1} a_{ij}a_{uv} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}\left(t(\theta_1^{i-u} \circ \theta_2^{j-v})(t)\right). \end{aligned}$$

Logo, utilizando os Lemas 5.0.4, 5.0.5 e 5.0.6, temos que o valor de $Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2)$ é:

$$\begin{aligned} & \sum_{i,j=0}^{p-1} a_{ij}^2 Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2) + \sum_{i=0}^{p-1} \sum_{\substack{j,v=0 \\ j\neq v}}^{p-1} a_{ij}a_{iv} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_2^{j-v})(t)) \\ + & \sum_{\substack{i,u=0 \\ i\neq u}}^{p-1} \sum_{j=0}^{p-1} a_{ij}a_{uj} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^{i-u})(t)) + \sum_{\substack{i,u=0 \\ i\neq u}}^{p-1} \sum_{\substack{j,v=0 \\ j\neq v}}^{p-1} a_{ij}a_{uv} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^{i-u} \circ \theta_2^{j-v})(t)) \\ = & \sum_{i,j=0}^{p-1} a_{ij}^2 \left[\frac{(m_1-1)(m_2-1)}{p^2} - \frac{m_1(m_2-1)+(m_1-1)m_2}{p} + n\right] \\ + & \sum_{i=0}^{p-1} \sum_{\substack{j,v=0 \\ j\neq v}}^{p-1} a_{ij}a_{iv}\left[\frac{(m_1-1)(m_2-1)}{p^2}\right] + \sum_{\substack{i,u=0 \\ i\neq u}}^{p-1} \sum_{j=0}^{p-1} a_{ij}a_{uj}\left[\frac{(m_1-1)(m_2-1)}{p^2}\right] \\ + & \sum_{\substack{i,u=0 \\ i\neq u}}^{p-1} \sum_{\substack{j,v=0 \\ j\neq v}}^{p-1} a_{ij}a_{uv}\left[\frac{(m_1-1)(m_2-1)}{p^2}\right] \\ + & \left[\sum_{j=0}^{p-1}\left(a_{0j} + \sum_{\substack{u=1,v=0 \\ u\equiv(j-v) \pmod p}}^{p-1} a_{uv}\right)^2 - \sum_{i,j=0}^{p-1} a_{ij}^2\right]\left[-\frac{m_1(m_2-1)}{p}\right] \end{aligned}$$

$$
\begin{aligned}
&+ \left[\sum_{j=0}^{p-1}\left(a_{0j}+\sum_{\substack{u=1,v=0\\ u\equiv\tilde{t}(j-v)\ (mod\ p)}}^{p-1} a_{uv}\right)^2-\sum_{i,j=0}^{p-1}a_{ij}^2\right]\left[-\frac{(m_1-1)m_2}{p}\right]\\
&= n\sum_{i,j=0}^{p-1}a_{ij}^2-\frac{m_1(m_2-1)}{p}\sum_{j=0}^{p-1}\left(a_{0j}+\sum_{\substack{u=1,v=0\\ u\equiv(j-v)\ (mod\ p)}}^{p-1} a_{uv}\right)^2\\
&- \frac{(m_1-1)m_2}{p}\sum_{j=0}^{p-1}\left(a_{0j}+\sum_{\substack{u=1,v=0\\ u\equiv\tilde{t}(j-v)\ (mod\ p)}}^{p-1} a_{uv}\right)^2+\frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1}a_{ij}\right)^2.
\end{aligned}
$$

Portanto,

$$
\begin{aligned}
Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= n\sum_{i,j=0}^{p-1}a_{ij}^2+\frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1}a_{ij}\right)^2\\
&- \frac{m_1(m_2-1)}{p}\sum_{j=0}^{p-1}A_j^2-\frac{(m_1-1)m_2}{p}\sum_{j=0}^{p-1}B_j^2,
\end{aligned}
$$

onde $A_j = a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv(j-v)\ (mod\ p)}}^{p-1} a_{uv}$ e $B_j = a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv\tilde{t}(j-v)\ (mod\ p)}}^{p-1} a_{uv}$. □

O próximo resultado relaciona os coeficientes A_j e B_j com as diagonais da matriz de x na base normal integral

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

no caso em que $\tilde{t}=p-1$. Com as notações do teorema anterior temos que:

Corolário 4.2.5. *Se $\tilde{t}=p-1$, segue que:*

$$
\begin{aligned}
Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(x^2) &= n\sum_{i,j=0}^{p-1}a_{ij}^2+\frac{(m_1-1)(m_2-1)}{p^2}\left(\sum_{i,j=0}^{p-1}a_{ij}\right)^2\\
&- \frac{m_1(m_2-1)}{p}\left(\sum_{j=0}^{p-1}A_j^2\right)-\frac{m_2(m_1-1)}{p}\left(\sum_{j=0}^{p-1}B_j^2\right),
\end{aligned}
$$

onde $A_j = a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv(j-v)\ (mod\ p)}}^{p-1} a_{uv}$ *e* $B_j = a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv(p-1)(j-v)\ (mod\ p)}}^{p-1} a_{uv}$. *Além disso, considerando a matriz* $\mathcal{M}=\begin{bmatrix} M & M\end{bmatrix}$, *com*

$$
M=\begin{bmatrix}
a_{00} & a_{01} & \ldots & a_{0(p-1)}\\
a_{10} & a_{11} & \ldots & a_{1(p-1)}\\
\vdots & \vdots & \ddots & \vdots\\
a_{(p-2)0} & a_{(p-2)1} & \ldots & a_{(p-2)(p-1)}\\
a_{(p-1)0} & a_{(p-1)1} & \cdots & a_{(p-1)(p-1)}
\end{bmatrix},
$$

temos que B_j é a soma dos elementos da diagonal principal da matriz $\mathcal{M}_j$, resultante da matriz $\mathcal{M}$ retirando as primeiras j-ésimas colunas e A_j é a soma dos elementos da diagonal secundária da matriz $\mathcal{M}'_j$, resultante da matriz $\mathcal{M}$ retirando as últimas $p-(j+1)$-ésimas colunas, para $j=1,2,\ldots,p-1$.

Exemplo 4.2.6. Se p=3, temos que

$$M = \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}.$$

$$\mathcal{M} = \left[\begin{array}{cccccc} a_{00} & a_{01} & a_{02} & a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} & a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} & a_{20} & a_{21} & a_{22} \end{array}\right] \begin{array}{cccccc} D_0 & D_1 & D_2 & E_0 & E_1 & E_2 \end{array}.$$

Dessa forma, considerando a matriz acima, para cada $j=0,1,2$, segue que A_j é a soma dos elementos da diagonal secundária D_j e B_j é a soma dos elementos da diagonal principal E_j.

Corolário 4.2.7. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números abelianos distintos, ambos de condutor n, com $[\mathbb{K}:\mathbb{Q}]=[\mathbb{L}:\mathbb{Q}]=3$, sendo 3 não ramificado em $\mathbb{K}$ e nem em $\mathbb{L}$. Se $n=p_1p_2p_3$ é livre de quadrados, p_1,p_2 e p_3 são primos inteiros, então existe uma base normal integral $\{(\theta_1^i\circ\theta_2^j)(t);\ i,j=0,1,2\}$ de $\mathcal{O}_{\mathbb{KL}}$, tal que escrevendo $x\in\mathcal{O}_{\mathbb{KL}}$ como*

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

obtemos que existe $p_i\in\{p_1,p_2,p_3\}$ tal que:

$$\begin{aligned} Tr_{\mathbb{KL}/\mathbb{Q}}(x^2) &= n\sum_{i,j=0}^{2}a_{ij}^2+\frac{(p_i-1)\left(\frac{n}{p_i}-1\right)}{9}\left(\sum_{i,j=0}^{2}a_{ij}\right)^2 \\ &- \frac{p_i\left(\frac{n}{p_i}-1\right)}{3}\left(\sum_{i=0}^{2}A_j^2\right)-\frac{\frac{n}{p_i}(p_i-1)}{3}\left(\sum_{i=0}^{2}B_j^2\right), \end{aligned}$$

onde $A_j=a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv(j-v)\ (mod\ 3)}}^{2} a_{uv}$ *e* $B_j=a_{0j}+\sum\limits_{\substack{u=1,v=0\\ u\equiv 2(j-v)\ (mod\ 3)}}^{2} a_{uv}$.

Demonstração. Pelo Corolário 3.5.7, basta verificarmos que $\mathbb{K}_i\subseteq\mathbb{KL}$, para algum $i\in\{1,2,3\}$, onde $\mathbb{K}_i$ é a única 3-extensão abeliana não ramificada em $\mathbb{Q}(\zeta_{p_i})$. Note inicialmente que $\mathbb{KL}$ possuí $\frac{3^2-1}{3-1}=4$ 3-extensões abelianas não ramificadas distintas, sendo duas delas $\mathbb{K}$ e $\mathbb{L}$.

Suponha que $\mathbb{K}_1,\mathbb{K}_2,\mathbb{K}_3\not\subset\mathbb{KL}$, logo

$$\mathbb{K}_1\mathbb{K}_2\mathbb{K}_3=\mathbb{K}^*=\mathbb{L}^*=\mathbb{K}_1\mathbb{KL}=\mathbb{K}_2\mathbb{KL},$$

dessa forma, $\mathbb{K}_3 \subseteq \mathbb{K}_1\mathbb{K}\mathbb{L} = \mathbb{K}_2\mathbb{K}\mathbb{L}$. Pelo Lema 3.1.6, existem 3-extensões $\mathbb{K}', \mathbb{K}'' \subseteq \mathbb{K}\mathbb{L}$, de forma que $\mathbb{K}_3 \subseteq \mathbb{K}_1\mathbb{K}'$ e $\mathbb{K}_3 \subseteq \mathbb{K}_2\mathbb{K}''$, logo $\text{cond}(\mathbb{K}') = p_1p_3$ e $\text{cond}(\mathbb{K}'') = p_2p_3$.

Por outro lado, $\mathbb{K}_1 \subseteq \mathbb{K}_2\mathbb{K}\mathbb{L}$ e assim, existe uma 3-extensão $\mathbb{K}''' \subseteq \mathbb{K}\mathbb{L}$, de maneira que, $\mathbb{K}_1 \subseteq \mathbb{K}_2\mathbb{K}'''$, com isso, $\text{cond}(\mathbb{K}''') = p_1p_2$. Dessa forma, $\mathbb{K}, \mathbb{L}, \mathbb{K}', \mathbb{K}'', \mathbb{K}'''$ são 3-extensões abelianas não ramificadas distintas contidas em $\mathbb{K}\mathbb{L}$, um absurdo.

Portanto, $\mathbb{K}_1, \mathbb{K}_2$ ou $\mathbb{K}_3$ é uma 3−extensão contida em $\mathbb{K}\mathbb{L}$. □

4.3 Condutores das p-extensões contidas em $\mathbb{K}\mathbb{K}_{m_1}$

Na seção 3.5, vimos que dada uma p-extensão abeliana não ramificada $\mathbb{K}$ de condutor $n = p_1p_2 \dots p_s$, poderíamos "subir" adequadamente até seu Corpo de Gênero $\mathbb{K}^* = \mathbb{K}_1\mathbb{K}_2 \cdots \mathbb{K}_{s-1}\mathbb{M}_{s-1}$ pela torre de compósito dada na Figura 4.6, onde para cada $i = 1, 2, \dots, s-1$, $\mathbb{K}_i$ é a única p-extensão abeliana não ramificada de condutor p_i e $\mathbb{M}_i = \mathbb{M}_{i-1}\mathbb{K}_i \cap \mathbb{Q}(\zeta_{p_{i+1}p_{i+2}\cdots p_s})$ é a única p-extensão abeliana não ramificada de condutor $p_{i+1}p_{i+2} \cdots p_s$ contida no compósito $\mathbb{K}_i\mathbb{M}_{i-1}$, considerando $\mathbb{M}_0 = \mathbb{K}$.

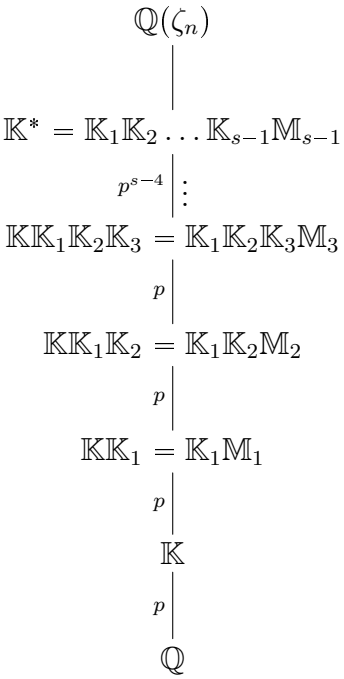

Figura 4.6: Torre ramificada de p-extensões abelianas não ramificadas.
Fonte: Próprio autor.

Se $\mathbb{K}_{p_1p_2}$ é uma p-extensão abeliana não ramificada com $\text{cond}(\mathbb{K}_{p_1p_2}) = p_1p_2$ e $\mathbb{K}_i$ é a única p-extensão abeliana não ramificada de condutor p_i, então $\mathbb{K}_{p_1p_2} \subseteq \mathbb{K}_1\mathbb{K}_2 \subset \mathbb{K}^* = \mathbb{K}_1\mathbb{K}_2 \dots \mathbb{K}_s = \mathbb{K}\mathbb{K}_2\mathbb{K}_3 \dots \mathbb{K}_s$. Pelo Lema 3.1.6, existe uma p-extensão $\mathbb{P} \subseteq \mathbb{K}_2\mathbb{K}_3 \dots \mathbb{K}_s$ tal que $\mathbb{K}_{p_1p_2} \subset \mathbb{K}\mathbb{P}$, conforme a Figura 4.7. Note que nesse caso teremos duas possibilidades para o condutor de $\mathbb{P}$: $\text{cond}(\mathbb{P}) = p_3p_4 \dots p_s$ ou $\text{cond}(\mathbb{P}) = p_2p_3 \dots p_s$ e que $\text{cond}(\mathbb{P}) = p_2p_3 \dots p_s$ se, e somente se, a extensão $\mathbb{K}_2\mathbb{K}_3 \dots \mathbb{K}_s/\mathbb{P}$ é não ramificada, ou equivalentemente, $\mathbb{P}^* = \mathbb{K}_2\mathbb{K}_3 \dots \mathbb{K}_s$.

Queremos analisar uma forma mais geral para essa configuração: Seja $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ um compósito, tal que $\text{mdc}(m_1, m_2) = p_k$, sendo $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2 \dots p_k$ e $m_2 = p_kp_{k+1} \dots p_s$, respectivamente, de

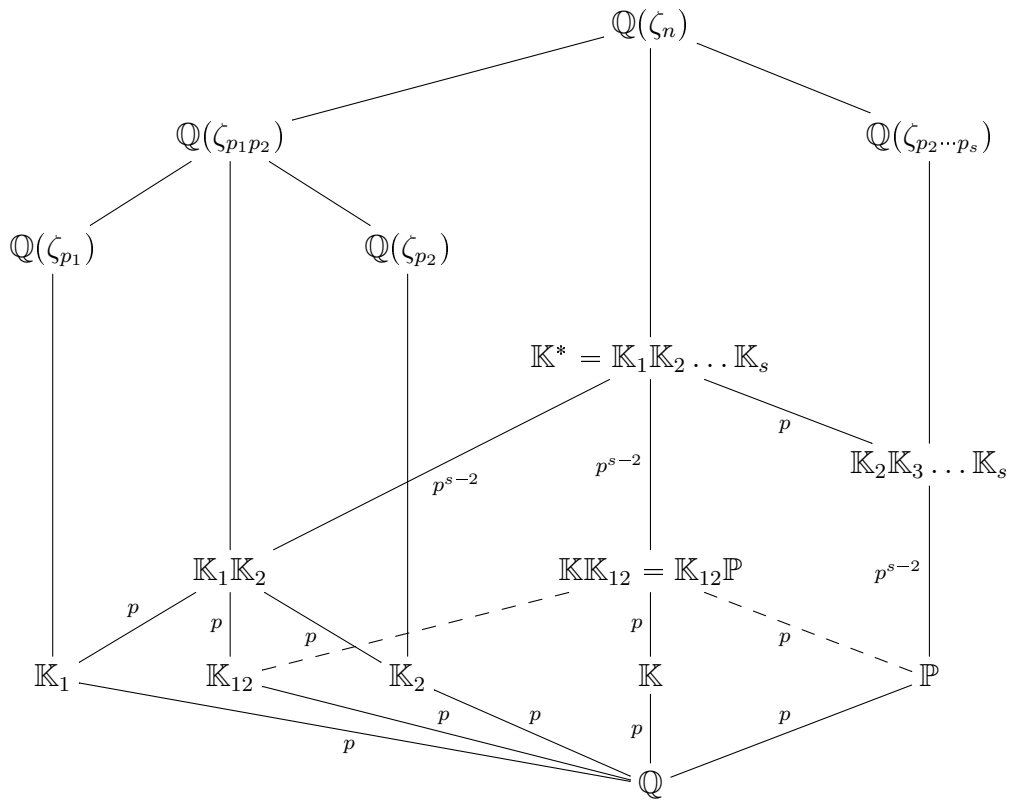

Figura 4.7: Condutor de $\mathbb{P}$.
Fonte: Próprio autor.

maneira que exista uma p-extensão abeliana não ramificada $\mathbb{P} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$ de condutor m_1m_2/p_k. Para isso vejamos alguns resultados.

Proposição 4.3.1. *Sejam $\mathbb{K}$, $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $n = p_1p_2\ldots p_s$, $m_1 = p_1p_2\ldots p_k$ e $m_2 = p_{k+1}p_{k+2}\ldots p_s$, respectivamente, com $k < s$, de forma que*

$$\mathbb{K}\mathbb{K}_{m_1} = \mathbb{K}_{m_1}\mathbb{K}_{m_2}.$$

Então, $\mathbb{K}_{m_2} = \mathbb{M}_k$, onde $\mathbb{M}_i = \mathbb{M}_{i-1}\mathbb{K}_i \cap \mathbb{Q}(\zeta_{(p_{i+1})(p_{i+2})\cdots p_s})$, $\mathbb{K}_i$ é a única p-extensão de condutor p_i e $\mathbb{M}_1 = \mathbb{K}\mathbb{K}_1 \cap \mathbb{Q}(\zeta_{p_2p_3\cdots p_s})$.

Demonstração. Sejam $\mathbb{K}$, $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ como no enunciado, então

$$\mathbb{K}_{m_2} \subseteq \mathbb{K}\mathbb{K}_{m_1} \subseteq \mathbb{K}\mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_k = \mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_k\mathbb{M}_k.$$

Assim, pelo Lema 3.1.6, existe uma p-extensão $\mathbb{P} \subseteq \mathbb{K}_1\mathbb{K}_2\ldots\mathbb{K}_k$ de forma que

$$\mathbb{K}_{m_2} \subseteq \mathbb{P}\mathbb{M}_k.$$

Se $\mathbb{K}_{m_2} \neq \mathbb{M}_k$, então

$$[\mathbb{K}_{m_2}\mathbb{M}_k : \mathbb{Q}] = p^2 = [\mathbb{P}\mathbb{M}_k : \mathbb{Q}],$$

ou seja,

$$\mathbb{P} \subseteq \mathbb{P}\mathbb{M}_k = \mathbb{K}_{m_2}\mathbb{M}_k,$$

o que é um absurdo, pois $\text{cond}(\mathbb{K}_{m_2}\mathbb{M}_k) = m_2 = p_{k+1}p_{k+2}\ldots p_s$ e o condutor de $\mathbb{P}$ divide $m_1 = p_1p_2\ldots p_k$. Portanto, $\mathbb{K}_{m_2} = \mathbb{M}_k$. □

Da proposição anterior obtemos:

Corolário 4.3.2. *Sejam* $\mathbb{K}$, $\mathbb{K}_{m_1}$ *e* $\mathbb{K}_{m_2}$ *p-extensões abelianas não ramificadas de condutores* $n = p_1p_2\dots p_s$, $m_1 = p_1p_2\dots p_k$ *e* $m_2 = \frac{n}{m_1}$, *com* $k < s$, *respectivamente, de forma que* $\mathbb{K}\mathbb{K}_{m_1} = \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. *Então,* $\mathbb{K}_{m_1} = \mathbb{M}_k^{-1}$, *onde*

$$\mathbb{M}_i^{-1} = \mathbb{M}_{i+1}^{-1}\mathbb{K}_i \cap \mathbb{Q}(\zeta_{p_1p_2\cdots p_{i-1}p_i}),$$

$\mathbb{K}_i$ *é a única p-extensão de condutor* p_i *e*

$$\mathbb{M}_s^{-1} = \mathbb{K}\mathbb{K}_s \cap \mathbb{Q}(\zeta_{p_1p_2\cdots p_{s-1}}).$$

Note que alterando a ordem dos fatores de $n = p_1p_2\dots p_s$ para $n = p_sp_{s-1}\dots p_2p_1$, pelo corolário anterior $\mathbb{K}_{m_1} = \mathbb{M}_k$, onde $m_1 = p_1p_2\dots p_s$ e $\mathbb{K}_{m_2} = \mathbb{M}_k^{-1}$. Consequentemente obtemos:

Corolário 4.3.3. *Dada uma p-extensão abeliana não ramificada* $\mathbb{K}$ *de condutor* $n = p_1p_2\dots p_s$, *para cada par de inteiros positivos* m_1, m_2, *satisfazendo* $n = m_1m_2$ (*note que* $mdc(m_1, m_2) = 1$) *existem únicas p-extensões abelianas não ramificadas* $\mathbb{K}_{m_1}$ *e* $\mathbb{K}_{m_2}$ *de condutores* m_1 *e* m_2, *respectivamente, de forma que* $\mathbb{K} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. *A saber, fixada a ordem da fatoração de* $n = p_1p_2\dots p_s$, *de maneira que* $m_1 = p_1p_2\dots p_k$, *então* $\mathbb{K}_{m_2} = \mathbb{M}_k$ *e* $\mathbb{K}_{m_1} = \mathbb{M}_k^{-1}$.

Agora, sejam $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\dots p_k$ e $m_2 = p_kp_{k+1}\dots p_s$, respectivamente e $\mathbb{K} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$ uma p-extensão abeliana não ramificada de condutor $n = m_1m_2/p_k = p_1p_2\dots p_s$. Note que neste caso $\mathbb{K}_{m_1} \neq \mathbb{M}_k^{-1}$ e $\mathbb{K}_{m_2} \neq \mathbb{M}_k$ (considerando a construção feita anteriormente sobre o corpo $\mathbb{K}$). Além disso, como

$$\mathbb{K}_{m_1} \subseteq \mathbb{K}^* = \mathbb{K}\mathbb{K}_1\mathbb{K}_2\dots\mathbb{K}_{k-1}\mathbb{K}_{k+1}\dots\mathbb{K}_s,$$

segue pelo Lema 3.1.6 que existe uma p-extensão abeliana não ramificada

$$\mathbb{K}_{m_3} \subseteq \mathbb{K}_1\mathbb{K}_2\dots\mathbb{K}_{k-1}\mathbb{K}_{k+1}\dots\mathbb{K}_s,$$

de condutor m_3, tal que $\mathbb{K}_{m_1} \subseteq \mathbb{K}\mathbb{K}_{m_3}$. Uma vez que

$$\mathbb{K}_{m_1}, \mathbb{K}_{m_2} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_3} = \mathbb{K}\mathbb{K}_{m_3} = \mathbb{K}_{m_2}\mathbb{K}_{m_3},$$

obtemos que $m_3 = n/p_k = p_1p_2\dots p_{k-1}p_{k+1}\dots p_s$. Observe que, $\mathbb{K}_{m_1}, \mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ são as únicas p-extensões abelianas contidas no compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ de condutor menor que n.

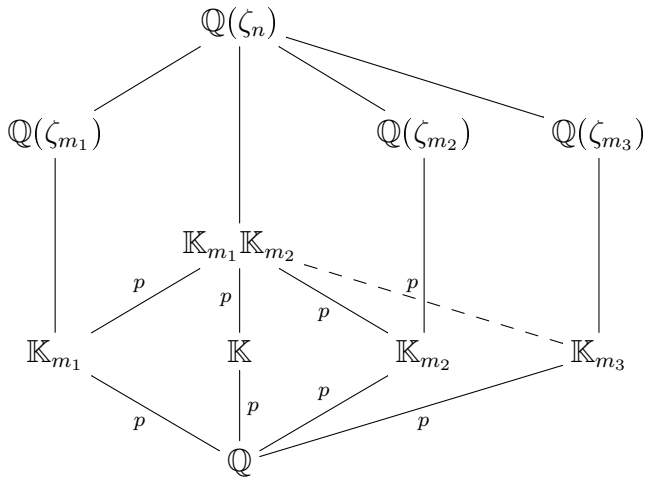

Figura 4.8: p-extensões abelianas não ramificadas de condutores menores que n.
Fonte: Próprio autor

Observação 4.3.4. Pelo Teorema 3.1.4, o compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ contém $p-3$ p-extensões abelianas não ramificadas distintas de $\mathbb{K}$ de condutor cheio n.

4.4 Forma Traço Integral do compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$, com mdc$(m_1, m_2) = p_k$

Considere $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\dots p_k$ e $m_2 = p_kp_{k+1}\dots p_s$, respectivamente, com $\text{mdc}(m_1, m_2) = p_k$, de forma que exista uma (e portanto a única) p-extensão abeliana não ramificada

$$\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2},$$

com $\text{cond}(\mathbb{K}_{m_3}) = \frac{n}{p_k}$, sendo $n = \frac{m_1m_2}{p_k}$ e H o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$.

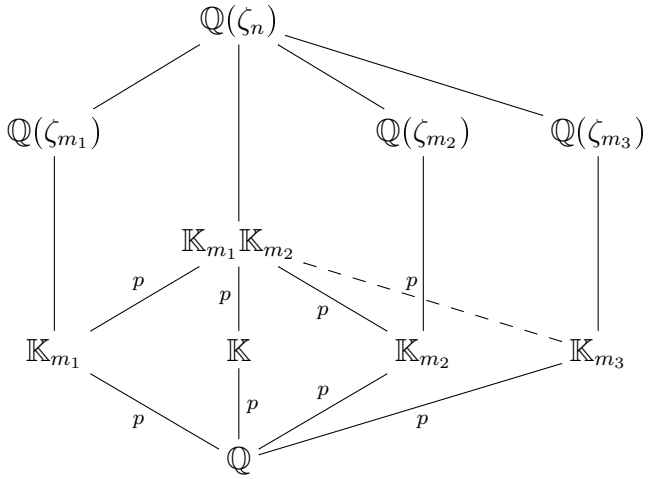

Figura 4.9: Compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ com $\text{mdc}(m_1, m_2) = p_k$.
Fonte: Próprio autor

Assim, a obtenção da forma traço integral do compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$, apresentado no Teorema 4.4.4, será dividida em três lemas auxiliares (como feito na seção 4.2). De maneira a não sobrecarregar esta seção, estes lemas auxiliares, assim como alguns resultados de contagens de elementos de H, terão sua prova apresentada no Apêndice **??**, na Seção 5.

Lema 4.4.1. *Sejam $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\dots p_k$, $m_2 = p_kp_{k+1}\dots p_s$ e $m_3 = m_1m_2/p_k^2$, respectivamente, com $mdc(m_1, m_2) = p_k$ de forma que $\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\dots p-1}$ é o grupo de Galois de $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ sobre $\mathbb{Q}$, satisfazendo:*

1. *$\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$;*
2. *$\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$;*
3. *$(\theta_1 \circ \theta_2)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$,*

então o valor de $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t^2)$ *é:*

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)+m_3\left(p_k-1\right)}{p}+n,$$

onde $n=m_1m_2/p_k$ *e* $t=Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$.

Demonstração. Sua prova encontra-se na Seção 5, Lema 5.0.14. □

Lema 4.4.2. *Sejam* $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ *e* $\mathbb{K}_{m_3}$ *p-extensões abelianas não ramificadas de condutores* $m_1=p_1p_2\ldots p_k$, $m_2=p_kp_{k+1}\ldots p_s$ *e* $m_3=m_1m_2/p_k^2$, *respectivamente, com* $mdc(m_1,m_2)=p_k$ *de forma que* $\mathbb{K}_{m_3}\subseteq\mathbb{K}_{m_1}\mathbb{K}_{m_2}$. *Se* $G=\{\theta_1^i\circ\theta_2^j\}_{i,j=0\ldots p-1}$ *é o grupo de Galois de* $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ *sobre* $\mathbb{Q}$, *satisfazendo:*

1. $\theta_1|_{\mathbb{K}_{m_2}}$ *é um gerador de* $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, *com* $\theta_1|_{\mathbb{K}_{m_1}}=Id_{\mathbb{K}_{m_1}}$;
2. $\theta_2|_{\mathbb{K}_{m_1}}$ *é um gerador de* $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, *com* $\theta_2|_{\mathbb{K}_{m_2}}=Id_{\mathbb{K}_{m_2}}$;
3. $(\theta_1\circ\theta_2)|_{\mathbb{K}_{m_3}}=Id_{\mathbb{K}_{m_3}}$,

então:

1. *Para* $1\leqslant i\leqslant p-1$, *o valor de* $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t\theta_1^i(t))$ *é:*

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_1\left(\frac{m_2}{p_k}-1\right)}{p};$$

2. *Para* $1\leqslant j\leqslant p-1$, *o valor de* $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t\theta_2^j(t))$ *é:*

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_2\left(\frac{m_1}{p_k}-1\right)}{p},$$

onde $t=Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$.

Demonstração. Sua prova encontra-se na Seção 5, Lema 5.0.15. □

Lema 4.4.3. *Sejam* $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ *e* $\mathbb{K}_{m_3}$ *p-extensões abelianas não ramificadas de condutores* $m_1=p_1p_2\ldots p_k$, $m_2=p_kp_{k+1}\ldots p_s$ *e* $m_3=m_1m_2/p_k^2$, *respectivamente, com* $mdc(m_1,m_2)=p_k$ *de forma que* $\mathbb{K}_{m_3}\subseteq\mathbb{K}_{m_1}\mathbb{K}_{m_2}$. *Se* $G=\{\theta_1^i\circ\theta_2^j\}_{i,j=0\ldots p-1}$ *é o grupo de Galois de* $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ *sobre* $\mathbb{Q}$, *satisfazendo:*

1. $\theta_1|_{\mathbb{K}_{m_2}}$ *é um gerador de* $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, *com* $\theta_1|_{\mathbb{K}_{m_1}}=Id_{\mathbb{K}_{m_1}}$;
2. $\theta_2|_{\mathbb{K}_{m_1}}$ *é um gerador de* $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, *com* $\theta_2|_{\mathbb{K}_{m_2}}=Id_{\mathbb{K}_{m_2}}$;
3. $(\theta_1\circ\theta_2)|_{\mathbb{K}_{m_3}}=Id_{\mathbb{K}_{m_3}}$,

então, para $1\leqslant i,j\leqslant p-1$, *temos que:*

$$Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\begin{cases}\dfrac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}, & se\ i\neq j\\ \dfrac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\dfrac{m_3\left(p_k-1\right)}{p}, & se\ i=j\end{cases},$$

onde $t=Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$.

Demonstração. Sua prova encontra-se na Seção 5, Lema 5.0.16. □

Fazendo uso destes três lemas, enunciaremos agora o principal teorema desta seção como segue:

Teorema 4.4.4. *Sejam $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\dots p_k$, $m_2 = p_kp_{k+1}\dots p_s$ e $m_3 = m_1m_2/p_k^2$, respectivamente, com $mdc(m_1, m_2) = p_k$ de forma que $\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\dots p-1}$ é o grupo de Galois de $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ sobre $\mathbb{Q}$, satisfazendo:*

1. *$\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$;*
2. *$\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$;*
3. *$(\theta_1 \circ \theta_2)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$.*

Então, dado $n = m_1m_2/p_k$, $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$ e escrevendo $x \in \mathcal{O}_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}}$ como

$$x = \sum_{i,j=0}^{p-1} a_{ij} \left(\theta_1^i \circ \theta_2^j\right)(t),$$

temos que

$$\begin{aligned} Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}\left(x^2\right) &= n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{m_1\left(\frac{m_2}{p_k}-1\right) + m_2\left(\frac{m_1}{p_k}-1\right) - m_3 + 1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2 \\ &- \frac{m_1\left(\frac{m_2}{p_k}-1\right)}{p}\sum_{j=0}^{p-1} A_j^2 - \frac{m_2\left(\frac{m_1}{p_k}-1\right)}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{m_3\left(p_k-1\right)}{p}\sum_{j=0}^{p-1} C_j^2, \end{aligned}$$

onde $A_j = \sum_{i=0}^{p-1} a_{ij}$, $B_j = \sum_{i=0}^{p-1} a_{ji}$ *e* $C_j = a_{0j} + \sum_{\substack{u=1,v=0 \\ u\equiv(j-v) \pmod p}}^{p-1} a_{uv}$.

Demonstração. Considere

$$\tilde{m}_1 = m_1(\frac{m_2}{p_k} - 1),\ \tilde{m}_2 = m_2(\frac{m_1}{p_k} - 1) \text{ e } \tilde{m}_3 = m_3(p_k - 1).$$

Utilizando os lemas anteriores temos que o valor de $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(x^2)$ é:

$$\sum_{i,j=0}^{p-1} a_{ij}^2 Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}\left(t^2\right) + \sum_{i=0}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{iv} Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_2^{j-v})(t))$$

$$+ \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{j=0}^{p-1} a_{ij}a_{uj} Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^{i-u})(t)) + \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{uv} Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^{i-u}\circ\theta_2^{j-v})(t))$$

$$= \sum_{i,j=0}^{p-1} a_{ij}^2\left[\frac{\tilde{m}_1+\tilde{m}_2-m_3+1}{p^2} - \frac{\tilde{m}_1+\tilde{m}_2+\tilde{m}_3}{p} + n\right]$$

$$+ \sum_{i=0}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{iv}\left[\frac{\tilde{m}_1+\tilde{m}_2-m_3+1}{p^2} - \frac{\tilde{m}_2}{p}\right]$$

$$+ \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{j=0}^{p-1} a_{ij}a_{uj}\left[\frac{\tilde{m}_1+\tilde{m}_2-m_3+1}{p^2} - \frac{\tilde{m}_1}{p}\right]$$

$$+ \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{p-1} a_{ij}a_{uv}\left[\frac{\tilde{m}_1+\tilde{m}_2-m_3+1}{p^2}\right]$$

$$+ \left[\sum_{j=0}^{p-1}\left(a_{0j} + \sum_{\substack{u=1,v=0\\ u\equiv(j-v)\pmod p}}^{p-1} a_{uv}\right)^2 - \sum_{i,j=0}^{p-1} a_{ij}^2\right]\left[-\frac{\tilde{m}_3}{p}\right]$$

$$= n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{\tilde{m}_1+\tilde{m}_2-m_3+1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2$$

$$- \frac{\tilde{m}_2}{p}\sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-1} a_{ij}\right)^2 - \frac{\tilde{m}_1}{p}\sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1} a_{ij}\right)^2 - \frac{\tilde{m}_3}{p}\sum_{j=0}^{p-1}\left(a_{0j} + \sum_{\substack{u=1,v=0\\ u\equiv(j-v)\pmod p}}^{p-1} a_{uv}\right)^2.$$

Portanto,

$$Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(x^2) = n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2$$

$$- \frac{m_1\left(\frac{m_2}{p_k}-1\right)}{p}\sum_{j=0}^{p-1} A_j^2 - \frac{m_2\left(\frac{m_1}{p_k}-1\right)}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{m_3\left(p_k-1\right)}{p}\sum_{j=0}^{p-1} C_j^2,$$

onde $A_j = \sum_{i=0}^{p-1} a_{ij}$, $B_j = \sum_{i=0}^{p-1} a_{ji}$ e $C_j = a_{0j} + \sum_{\substack{u=1,v=0\\ u\equiv(j-v)\pmod p}}^{p-1} a_{uv}$. □

5 Considerações finais

Se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana de grau n, $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{K}$ e $\mathcal{M} \subseteq \mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n, então a densidade de centro do Reticulado Algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é dada por

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

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

$$|\sigma_{\mathbb{K}}(x)|^2 = \begin{cases} Tr_{\mathbb{K}/\mathbb{Q}}(x^2) & \text{se } \mathbb{K} \text{ é totalmente real;} \\ \dfrac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) & \text{se } \mathbb{K} \text{ é totalmente imaginário.} \end{cases}$$

Dessa forma, conhecer o valor do discriminante de $\mathbb{K}$, do índice do $\mathbb{Z}$-módulo $\mathcal{M}$ em $\mathcal{O}_{\mathbb{K}}$ e a forma traço integral são grandes ferramentas no estudo de reticulados algébricos. A proposta deste trabalho foi o de apresentar uma contribuição no estudo da forma traço integral, sobretudo sobre compósitos de p-extensões abelianas não ramificadas de grau p^2. Contudo, para se obter a densidade de centro de um reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{M})$ é necessário conhecermos o menor valor que a forma traço integral tem nos elementos de $\mathcal{M}$. Esse estudo se mostrou complexo no caso dos compósitos aqui estudados, proporcionando assim um desafio futuro: descrever $\mathbb{Z}$-módulos livres $\mathcal{M}$, de posto finito n, a fim de minimizar as formas traço integral obtidas no Capítulo 4, com relação a estes módulos, visando a obtenção de reticulados algébricos com boas densidades de centro.

Seja p um número primo ímpar e $n = p_1p_2 \ldots p_s$ um inteiro livre de quadrados, com $p_i \equiv 1(\mod p)$, para cada $1 \leqslant i \leqslant s$. Fixado $k \in \{1, 2 \ldots s\}$, considere $m_1 = p_1p_2 \ldots p_{k-1}$, $m_2 = p_{k+1}p_{k+2} \ldots p_s$, $m_3 = m_1m_2 = n/p_k$, $\tilde{m}_1 = m_1p_k$ e $\tilde{m}_2 = m_2p_k$. Se $\mathbb{K}_{\tilde{m}_1}, \mathbb{K}_{\tilde{m}_2}, \mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ são p-extensões abelianas não ramificadas de condutores $\tilde{m}_1$, $\tilde{m}_2$, m_2 e m_3, respectivamente, então os compósitos $\tilde{\mathbb{M}} = \mathbb{K}_{\tilde{m}_1}\mathbb{K}_{\tilde{m}_2}$ e $\mathbb{M} = \mathbb{K}_{\tilde{m}_1}\mathbb{K}_{m_2}$ são ambos corpos de números de grau p^2 e condutor n. Suponha ainda que exista uma, e portanto a única, p-extensão abeliana não ramificada $\mathbb{K}_{m_3}$ de condutor m_3, de forma que $\mathbb{K}_{m_3} \subseteq \tilde{\mathbb{M}}$. Logo, se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$ é o grupo de Galois de $\tilde{\mathbb{M}}$ sobre $\mathbb{Q}$, satisfazendo:

1. $\theta_1|_{\mathbb{K}_{\tilde{m}_2}}$ é um gerador de $\mathrm{Gal}(\mathbb{K}_{\tilde{m}_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{\tilde{m}_1}} = Id_{\mathbb{K}_{\tilde{m}_1}}$;
2. $\theta_2|_{\mathbb{K}_{\tilde{m}_1}}$ é um gerador de $\mathrm{Gal}(\mathbb{K}_{\tilde{m}_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{\tilde{m}_2}} = Id_{\mathbb{K}_{\tilde{m}_2}}$;
3. $(\theta_1^i \circ \theta_2^i)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$, para todo $i = 0, 1, \ldots, p-1$.

Então, dado $t = Tr_{\mathbb{Q}(\zeta_n)/\tilde{\mathbb{M}}}(\zeta_n)$ e escrevendo $x \in \mathcal{O}_{\tilde{\mathbb{M}}}$ como $x = \sum_{i,j=0}^{p-1} a_{ij}(\theta_1^i \circ \theta_2^j)(t)$,

$$\begin{aligned}
Tr_{\tilde{\mathbb{M}}/\mathbb{Q}}(x^2) &= n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{2n-\tilde{m}_1-\tilde{m}_2-m_3+1}{p^2}\Big(\sum_{i,j=0}^{p-1} a_{ij}\Big)^2 \\
&- \frac{\tilde{m}_1(m_2-1)}{p}\sum_{j=0}^{p-1} A_j^2 - \frac{\tilde{m}_2(m_1-1)}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{m_3(p_k-1)}{p}\sum_{j=0}^{p-1} C_j^2 \\
&= n\sum_{i,j=0}^{p-1} a_{ij}^2 + \frac{(\tilde{m}_1-1)(m_2-1)+(m_3-m_2)(p_k-1)}{p^2}\Big(\sum_{i,j=0}^{p-1} a_{ij}\Big)^2 \\
&- \frac{\tilde{m}_1(m_2-1)}{p}\sum_{j=0}^{p-1} A_j^2 - \frac{m_2(\tilde{m}_1-1)-m_2(p_k-1)}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{m_3(p_k-1)}{p}\sum_{j=0}^{p-1} C_j^2 \\
&= n\sum_{i,j=0}^{p-1} a_{ij}^2 - \frac{\tilde{m}_1(m_2-1)}{p}\sum_{j=0}^{p-1} A_j^2 \\
&- \frac{m_2(\tilde{m}_1-1)}{p}\sum_{j=0}^{p-1} B_j^2 + \frac{(\tilde{m}_1-1)(m_2-1)}{p^2}\Big(\sum_{i,j=0}^{p-1} a_{ij}\Big)^2 \\
&+ m_2(p_k-1)\left[\frac{1}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2\right] - m_3(p_k-1)\left[\frac{1}{p}\sum_{j=0}^{p-1} C_j^2 - \frac{1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2\right],
\end{aligned}$$

onde $A_j = \sum_{i=0}^{p-1} a_{ij}$, $B_j = \sum_{i=0}^{p-1} a_{ji}$ e $C_j = a_{0j} + \sum_{\substack{u=1,v=0 \\ u\equiv(j-v)\ (mod\ p)}}^{p-1} a_{uv}$.

Assim, se $G' = \left\{{\theta_1'}^i \circ {\theta_2'}^j\right\}_{i,j=0\ldots p-1}$ é o grupo de Galois de $\mathbb{M}$ sobre $\mathbb{Q}$, onde $\theta_1'|_{\mathbb{K}_{\tilde{m}_1}}$ é um gerador de $\mathbb{K}_{\tilde{m}_1}$, $\theta_1'|_{\mathbb{K}_{m_2}}$ é um gerador de $\mathbb{K}_{m_2}$, com $\theta_1', \theta_2' \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $x' = \sum_{i,j=0}^{p-1} a_{ij}({\theta_1'}^i \circ {\theta_2'}^j)\left(\tilde{t}\right)$, com $\tilde{t} = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)$, então pela Proposição 3.5.8, segue que

$$\begin{aligned}
Tr_{\tilde{\mathbb{M}}/\mathbb{Q}}(x^2) &= Tr_{\mathbb{M}/\mathbb{Q}}(x'^2) + m_2(p_k-1)\left[\frac{1}{p}\sum_{j=0}^{p-1} B_j^2 - \frac{1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2\right] \\
&- m_3(p_k-1)\left[\frac{1}{p}\sum_{j=0}^{p-1} C_j^2 - \frac{1}{p^2}\left(\sum_{i,j=0}^{p-1} a_{ij}\right)^2\right].
\end{aligned}$$

Uma questão a ser discutida é: dado um $\mathbb{Z}$-módulo livre $\mathcal{M}$, constituído de matrizes quadradas de ordem $p-1$, é comparável os mínimos das formas traços relativo a esse módulo? Se sim, em qual caso obtemos reticulados com maior densidade de centro? Essa é uma questão a ser pesquisada futuramente.

Referências

[1] Araujo, R. R., **Reticulados Algébricos e aplicações a códigos e criptografia**. Tese (doutorado) - Instituto de Matemática Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2018.

[2] Bahttacharya, P.B., Jain, S.K., Nagpaul, S.R., **Basic Abstract Algebra 2. ed.** Cambridge University Press, 1994.

[3] Chagas, A. C. M. M., **Uma contribuição a teoria dos números e reticulados**. Tese (doutorado) - UNESP, São José do Rio Preto, 2015.

[4] Ishida, M., **Some unramified abelian extensions of algebraic number fields**. Journal für die reine und angewandte Mathematik (Crelles Journal), p. 165-173, 1974.

[5] Xianke, Z., **A Simple Construction of Genus Fields of Abelian Number Fields**. American Mathematical Society v.94, p. 393-395, 1985.

[6] Moro, E. M., **Forma Traço Integral de um Corpo de Números com grau e condutor ímpares e livres de quadrados**. Tese (doutorado) - UNESP, São José do Rio Preto, 2020.

[7] Oliveira, E. L., **Torres de Extensões Abelianas de grau primo ímpar não ramificado**. Tese (doutorado) - UNESP, São José do Rio Preto, 2015.

[8] Marcus, D. A., **Number Fields 1. ed.** Springer-Verlag. New York, 1977.

[9] Lang, S., **Algebraic Number Theory 2. ed.** Serie Graduate Texts in Mathematics 110, Spring-Verlag, New York, 1994

[10] Nóbrega Neto, T. P., Lopes, J. O. P., Interlando, J. C., **The Discriminant of Abelian Number Fields**. Journal of Algebra and its Applications v.05, p. 35-41, 2006.

[11] Leopoldt, H. W., **Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers**. J. reine angew, Math. 201, p. 119-149, 1959.

[12] Ishida, M., **The Genus Fields of Algebraic Number Fields 1. ed.** Serie Lecture notes in mathematics, Springer-Verlag, New York, 1976.

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

[14] Samuel, P., **Algebraic theory os numbers**. Hermann, Paris, 1970.

[15] Stewart, I. N., **Galois Theory 4. ed.** Chapman Hall/Crc Mathematics, Boca Raton, FL, 2015.

[16] Washington, L. C., **Introduction to Cyclotomic Fields 2. ed.** Spring-Verlag, New York, 1982.

[17] Conway, J. H., Sloane, J. N. A., **Sphere packing, lattices and groups 3. ed.** Spring-Verlag, New York, 1999.

[18] Helmut, H, **Number Theory: Algebraic Numbers and Functions 1. ed.** American Mathematical Society, Providence, Rhode Island, 2000.

Apêndice A: Caso linearmente disjunto

A fim de não sobrecarregar o capítulo 4 com demasiadas contas e tirar o foco dos principais resultados, propusemos a criação deste apêndice a fim de auxiliar na compreensão deste material. Este capítulo será refente ao caso do compósito de p-extensões abelianas não ramificadas $\mathbb{L}_1$ e $\mathbb{L}_2$ de mesmo condutor n, admitindo a existência de p-extensões abelianas não ramificadas $\mathbb{K}, \mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$ de condutores m_1 e m_2, respectivamente, com $\text{mdc}(m_1, m_2) = 1$ e $n = m_1m_2$. O segundo caso, será abordar algumas contagens de elementos considerando p-extensões abelianas não ramificadas $\mathbb{K}$ e $\mathbb{L}$ de condutores m_1 e m_2, respectivamente, de maneira que $\text{mdc}(m_1, m_2) = p_1$, com p_1 um número primo.

Iniciamos destacando um resultado bastante conhecido, o qual foi utilizado nas teses de doutorado citadas nos capítulos anteriores. Tal resultado será útil nas seções seguintes e por isso deixaremos aqui sua prova.

Proposição 5.0.1. *Dado um inteiro positivo u, temos que*

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

Em particular,

$$-\binom{u}{u-1} + \binom{u}{u-2} - \cdots + (-1)^{u-1}\binom{u}{1} = \begin{cases} 0, & \textit{se } u \textit{ é ímpar} \\ -2, & \textit{se } u \textit{ é par} \end{cases}.$$

Demonstração. Temos que $(-1)^u\binom{u}{0} = \begin{cases} -1, & \text{se } u \text{ é ímpar} \\ 1, & \text{se } u \text{ é par} \end{cases}$.

Se u é ímpar, então para cada $1 \leqslant a \leqslant \dfrac{u-1}{2}$, segue que

$$(-1)^a\binom{u}{u-a} = -(-1)^{u-a}\binom{u}{a}$$

e assim,

$$\begin{aligned} \sum_{k=1}^{u-1}(-1)^k\binom{u}{u-k} &= \sum_{k=1}^{\frac{u-1}{2}}\left[(-1)^k\binom{u}{u-k} + (-1)^{u-k}\binom{u}{k}\right] \\ &= \sum_{k=1}^{\frac{u-1}{2}} 0 \\ &= 0. \end{aligned}$$

Logo,

$$\sum_{k=1}^{u}(-1)^k \left(\begin{array}{c} u \\ u-k \end{array} \right) = -1.$$

Se u é par, então $u-1$ é ímpar e pelo caso anterior

$$\sum_{k=1}^{u-2}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) = 0.$$

Além disso, a relação de Stifel diz que $\left(\begin{array}{c} u \\ u-k \end{array} \right) = \left(\begin{array}{c} u-1 \\ u-k \end{array} \right) + \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right)$. Dessa forma,

$$\begin{aligned} \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u \\ u-k \end{array} \right) &= \sum_{k=1}^{u-1}(-1)^k \left[\left(\begin{array}{c} u-1 \\ u-k \end{array} \right) + \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) \right] \\ &= \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u-1 \\ u-k \end{array} \right) + \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right). \end{aligned}$$

Por outro lado,

$$\begin{aligned} \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u-1 \\ u-k \end{array} \right) &= -\sum_{k=0}^{u-2}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) \\ &= -\sum_{k=1}^{u-2}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) - (-1)^0 \left(\begin{array}{c} u-1 \\ u-1 \end{array} \right) \\ &= -0-1 = -1. \end{aligned}$$

E,

$$\begin{aligned} \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) &= \sum_{k=1}^{u-2}(-1)^k \left(\begin{array}{c} u-1 \\ (u-1)-k \end{array} \right) + (-1)^{u-1} \left(\begin{array}{c} u-1 \\ 0 \end{array} \right) \\ &= 0 + (-1) = -1. \end{aligned}$$

Logo,

$$\sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u \\ u-k \end{array} \right) = -1 + (-1) = -2.$$

Portanto,

$$\sum_{k=1}^{u}(-1)^k \left(\begin{array}{c} u \\ u-k \end{array} \right) = \sum_{k=1}^{u-1}(-1)^k \left(\begin{array}{c} u \\ u-k \end{array} \right) + (-1)^u \left(\begin{array}{c} u \\ 0 \end{array} \right) = -2 + 1 = -1.$$

□

Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ p-extensões abelianas não ramificadas de mesmo condutor $n = p_1p_2\dots p_s$, de forma que existam duas p-extensões abelianas não ramificadas $\mathbb{K}, \mathbb{L} \subseteq \mathbb{L}_1\mathbb{L}_2$, com $\text{cond}(\mathbb{K}) = m_1 = p_1p_2\dots p_{s_1}$, $\text{cond}(\mathbb{L}) = m_2 = p'_1p'_2\dots p'_{s_2}$, $s = s_1 + s_2$, $\text{mdc}(m_1, m_2) = 1$ e $n = m_1m_2$. Considere ainda os conjuntos Y, Y', P, P', L e L' como no Lema 4.1.1, e $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_s) \in H$, sendo H o subgrupo de $\mathbb{Z}_n^*$ isormorfo a $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{L}_1\mathbb{L}_2$. Nessa seção estamos interessados em obter a quantidade $S^{i,j}_{L\times L'}$ de elementos $\beta \in H$ de forma que $r_1^i r_2^j\beta$ coincide com $-\alpha$ exatamente nas coordenadas $y_1, y_2, \dots, y_u, y'_1, y'_1, \dots, y'_{u'}$ (isto é, nas coordenadas de $Y \times Y'$). Também faremos o uso da notação $S^{i,j}_{l_1,l_2,\dots,l_{s_1-u},l'_1,l'_2,\dots,l'_{s_2-u'}}$ para descrever a quantidade $S^{i,j}_{L\times L'}$.

O próximo teorema fornecerá os valores de $S^{i,j}_{L\times L'}$ por meio das quantidades $A_{\tilde{L}\times\tilde{L}'}$, onde $\tilde{L}$ e $\tilde{L}'$ são subconjuntos de L e L', respectivamente. Considere $q_{l_0} = q_{l'_0} = 1$. Note também que $A_0 = 1$, pois $A_0 = A_{L\times L'}$, quando $Y = P$ e $Y' = P'$.

Teorema 5.0.2. *Com as notações do Lema 4.1.1, sejam* $\tilde{u} = u + u'$ *e* $l_{s_1-u+1} = l'_1, l_{s_1-u+2} = l'_2, \dots, l_{s-\tilde{u}} = l'_{s_2-u'}$. *Então:*

1. Para $i = j = 0$, *temos que*

$$S^{0,0}_{l_1,l_2,\dots,l_{s-\tilde{u}}} = \sum_{k=0}^{s-\tilde{u}}\left[(-1)^k \sum_{1\leqslant t_1<t_2<\dots<t_{s-\tilde{u}-k}\leqslant s-\tilde{u}} A_{l_{t_1},l_{t_2},\dots,l_{t_{s-\tilde{u}-k}}}\right].$$

2. Para $i \neq 0$ *e* $j = 0$ *ou* $i = 0$ *e* $j \neq 0$,

2-a)Temos que

$$S^{i,j}_{l_{t_1},l_{t_2},\dots,l_{t_k}} = 0 \text{ e } S^{i,j}_{l'_{t'_1},l'_{t'_2},\dots,l'_{t'_{k'}}} = 0,$$

para todo $k = 0, 1, \dots, s_1 - u$, $k' = 0, 1, \dots, s_2 - u'$, *com*

$$l_1 \leqslant l_{t_1}, l_{t_2}, \dots, l_{t_k} \leqslant l_{s_1-u} \text{ e } l'_1 \leqslant l'_{t'_1}, l'_{t'_2}, \dots, l'_{t'_{k'}} \leqslant l_{s_2-u'}.$$

2-b)Se $1 \leqslant u \leqslant s_1 - 1$ *e* $1 \leqslant u' \leqslant s_2 - 1$, *temos que*

$$S^{i,j}_{l_1,l_2,\dots,l_{s_1-u},l'_1,l'_2,\dots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u-1}\sum_{k'=0}^{s_2-u'-1}(-1)^{k+k'}\tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ *é a quantidade*

$$\sum_{1\leqslant t_1<t_2<\dots<t_{s_1-u-k}\leqslant s_1-u \text{ e } 1\leqslant t'_1<t'_2<\dots<t'_{s_2-u'-k'}\leqslant s_2-u'} A_{l_{t_1},l_{t_2}\dots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\dots,l'_{t'_{s_2-u'-k'}}}.$$

3. Para $i \neq 0$ *e* $j \neq 0$,

3-a)Se $i \not\equiv -j \pmod p$ *e* $i \not\equiv -\tilde{t}j \pmod p$ *então:*

i)Temos que

$$S^{i,j}_{l_{t_1},l_{t_2},\dots,l_{t_k}} = S^{i,j}_{l'_{t'_1},l'_{t'_2},\dots,l'_{t'_{k'}}} = 0,$$

para todo $k = 0, 1, \dots, s_1 - u$ *e* $k' = 0, 1, \dots, s_2 - u'$.

ii)Se $1 \leqslant u \leqslant s_1 - 1$ *e* $1 \leqslant u' \leqslant s_2 - 1$, *temos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u-1} \sum_{k'=0}^{s_2-u'-1} (-1)^{k+k'} \tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ *é a quantidade*

$$\sum_{1 \leqslant t_1 < t_2 < \cdots < t_{s_1-u-k} \leqslant s_1-u \text{ e } 1 \leqslant t'_1 < t'_2 < \cdots < t'_{s_2-u'-k'} \leqslant s_2-u'} A_{l_{t_1},l_{t_2}\ldots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}}.$$

3-b)Se $i \equiv -j \ (mod\ p)$ *então:*

i)Temos que

$$S^{i,j}_{l_{t_1},l_{t_2},\ldots,l_{t_k}} = 0,$$

para todo $k = 0, 1, \ldots, s_1 - u$.

ii)Se $0 \leqslant u' \leqslant s_2 - 1$ *obtemos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u} \sum_{k'=0}^{s_2-u'-1} (-1)^{k+k'} \tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ *é a quantidade*

$$\sum_{1 \leqslant t_1 < t_2 < \cdots < t_{s_1-u-k} \leqslant s_1-u \text{ e } 1 \leqslant t'_1 < t'_2 < \cdots < t'_{s_2-u'-k'} \leqslant s_2-u'} A_{l_{t_1},l_{t_2}\ldots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}},$$

se $0 \leqslant k \leqslant s_1 - u - 1$ *e,*

$$\tilde{A}_{(s_1-u),k'} \sum_{1 \leqslant t'_1 < t'_2 < \cdots < t'_{s_2-u'-k'} \leqslant s_2-u'} A_{l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}}.$$

3-c)Se $i \equiv -tj \ (mod\ p)$ *então:*

i)Temos que

$$S^{i,j}_{l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{k'}}} = 0,$$

para todo $k' = 0, 1, \ldots, s_2 - u'$.

ii)Se $0 \leqslant u \leqslant s_1 - 1$ *obtemos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u-1} \sum_{k'=0}^{s_2-u'} (-1)^{k+k'} \tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ *é a quantidade*

$$\sum_{1 \leqslant t_1 < t_2 < \cdots < t_{s_1-u-k} \leqslant s_1-u \text{ e } 1 \leqslant t'_1 < t'_2 < \cdots < t'_{s_2-u'-k'} \leqslant s_2-u'} A_{l_{t_1},l_{t_2}\ldots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}},$$

se $0 \leqslant k' \leqslant s_2 - u' - 1$ *e,*

$$\tilde{A}_{k,(s_2-u')} \sum_{1 \leqslant t_1 < t_2 < \cdots < t_{s_1-u-k} \leqslant s_1-u} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s_1-u-k}}}.$$

Demonstração.

1. Temos que

$$S^{0,0}_{l_1,\ldots,l_{s-\tilde{u}}} = A_{l_1,\ldots,l_{s-\tilde{u}}} - \sum_{k=1}^{s-\tilde{u}} \left[\sum_{1\leqslant t_1<t_2<\cdots<t_{s-\tilde{u}-k}\leqslant s-\tilde{u}} S^{0,0}_{l_{t_1},\ldots,l_{t_{s-\tilde{u}-k}}} \right]. \tag{5.1}$$

Além disso,

$$\sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} = \sum_{t=1}^{s-\tilde{u}} A_{l_t} - \left(\begin{array}{c} s-\tilde{u} \\ 1 \end{array} \right) S^{0,0}_0,$$

$$\sum_{1\leqslant t_1<t_2\leqslant s-\tilde{u}} S^{0,0}_{l_{t_1},l_{t_2}} = \sum_{1\leqslant t_1<t_2\leqslant s-\tilde{u}} A_{l_{t_1},l_{t_2}} - \left(\begin{array}{c} s-\tilde{u}-1 \\ 1 \end{array} \right) \sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} - \left(\begin{array}{c} s-\tilde{u} \\ 2 \end{array} \right) S^{0,0}_0,$$

$$\begin{aligned} \sum_{1\leqslant t_1<t_2<t_3\leqslant s-\tilde{u}} S^{0,0}_{l_{t_1},l_{t_2},l_{t_3}} &= \sum_{1\leqslant t_1<t_2<t_3\leqslant s-\tilde{u}} A_{l_{t_1},l_{t_2},l_{t_3}} - \left(\begin{array}{c} s-\tilde{u}-2 \\ 1 \end{array} \right) \sum_{1\leqslant t_1<t_2\leqslant s-\tilde{u}} S^{0,0}_{l_{t_1},l_{t_2}} \\ &- \left(\begin{array}{c} s-\tilde{u}-1 \\ 2 \end{array} \right) \sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} - \left(\begin{array}{c} s-\tilde{u} \\ 3 \end{array} \right) S^{0,0}_0. \end{aligned}$$

Continuando o processo, para todo $1 \leqslant k \leqslant s-\tilde{u}$, o valor de

$$\sum_{t_1<t_2<\ldots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\cdots,l_{t_{s-\tilde{u}-k}}}$$

é dado por

$$\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}} - \sum_{d=0}^{s-\tilde{u}-k-1} \left[\left(\begin{array}{c} k+(d+1) \\ d+1 \end{array} \right) \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k-1-d}} S^{0.0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k-1-d}}} \right].$$

Assim, substituindo o valor de $\sum_{t_1<t_2<\ldots<t_{s-\tilde{u}-1}} S^{0,0}_{l_{t_1},l_{t_2},\cdots,l_{t_{s-\tilde{u}-1}}}$, obtido acima, na equação (5.1) temos que

$$\begin{aligned} S^{0,0}_{l_1,l_2\ldots,l_{s-\tilde{u}}} &= A_{l_1,l_2\ldots,l_{s-\tilde{u}}} - \Bigg[\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-1}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-1}}} \\ &- \left(\begin{array}{c} 2 \\ 1 \end{array} \right) \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-2}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-2}}} - \left(\begin{array}{c} 3 \\ 2 \end{array} \right) \sum_{t_1<\ldots<t_{s-\tilde{u}-3}} S^{0,0}_{l_{t_1},\ldots,l_{t_{s-\tilde{u}-3}}} - \cdots \\ &\cdots - \left(\begin{array}{c} s-\tilde{u}-2 \\ s-\tilde{u}-3 \end{array} \right) \sum_{t_1<t_2} S^{0,0}_{l_{t_1},l_{t_2}} - \left(\begin{array}{c} s-\tilde{u}-1 \\ s-\tilde{u}-2 \end{array} \right) \sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} - \left(\begin{array}{c} s-\tilde{u} \\ s-\tilde{u}-1 \end{array} \right) S^{0,0}_0 \Bigg] \\ &- \sum_{t_1<\ldots<t_{s-\tilde{u}-2}} S^{0,0}_{l_{t_1},\ldots,l_{t_{s-\tilde{u}-2}}} - \cdots - \sum_{t_1<t_2} S^{0,0}_{l_{t_1},l_{t_2}} - \sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} - S^{0,0}_0 \\ &= A_{l_1,l_2,\ldots,l_{s-\tilde{u}}} - \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-1}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-1}}} + \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-2}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-2}}} \\ &- \left[1 - \left(\begin{array}{c} 3 \\ 2 \end{array} \right) \right] \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-3}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-3}}} - \cdots \\ &\cdots - \left[1 - \left(\begin{array}{c} s-\tilde{u}-2 \\ s-\tilde{u}-3 \end{array} \right) \right] \sum_{t_1<t_2} S^{0,0}_{l_{t_1},l_{t_2}} - \left[1 - \left(\begin{array}{c} s-\tilde{u}-1 \\ s-\tilde{u}-2 \end{array} \right) \right] \sum_{t=1}^{s-\tilde{u}} S^{0,0}_{l_t} \\ &- \left[1 - \left(\begin{array}{c} s-\tilde{u} \\ s-\tilde{u}-1 \end{array} \right) \right] S^{0,0}_0. \end{aligned}$$

Dessa forma, substituindo o valor de $\sum_{t_1<t_2<\ldots<t_{s-\tilde{u}-2}} S^{0,0}_{l_{t_1},l_{t_2},\cdots,l_{t_{s-\tilde{u}-2}}}$, temos que

$$\begin{aligned}
S^{0,0}_{l_1,l_2\ldots,l_{s-\tilde{u}}} &= A_{l_1,l_2\ldots,l_{s-\tilde{u}}} - \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-1}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-1}}} \\
&+ \left[\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-2}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-2}}} - \binom{3}{1} \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-3}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-3}}} - \cdots\right. \\
&\cdots \left. - \binom{s-\tilde{u}-2}{s-\tilde{u}-4} \sum_{t_1<t_2} S^{0,0}_{l_{t_1},l_{t_2}} - \binom{s-\tilde{u}-1}{s-\tilde{u}-3} \sum_{t=1}^{s-u} S^{0,0}_{l_t} - \binom{s-\tilde{u}}{s-\tilde{u}-2} S^{0,0}_0\right] \\
&- \left[1-\binom{3}{2}\right] \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-3}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-3}}} - \cdots \\
&\cdots - \left[1-\binom{s-\tilde{u}-2}{s-\tilde{u}-3}\right] \sum_{t_1<t_2} S^{0,0}_{l_{t_1},l_{t_2}} - \left[1-\binom{s-\tilde{u}-1}{s-\tilde{u}-2}\right] \sum_{t=1}^{s-u} S^{0,0}_{l_t} \\
&- \left[1-\binom{s-\tilde{u}}{s-\tilde{u}-1}\right] S^{0,0}_0 \\
&= \sum_{k=0}^{2} \left[(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right] \\
&- \sum_{k=3}^{s-\tilde{u}} \left(\left[-\binom{k}{k-1} + \binom{k}{k-2} + 1\right] \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right).
\end{aligned}$$

Pela Proposição 5.0.1,

$$\left[-\binom{3}{2} + \binom{3}{1} + 1\right] = 0 + 1 = 1.$$

Logo,

$$\begin{aligned}
S^{0,0}_{l_1,l_2\ldots,l_{s-\tilde{u}}} &= \sum_{k=0}^{2} \left[(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right] \\
&- \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-3}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-3}}} \\
&- \sum_{k=4}^{s-\tilde{u}} \left(\left[-\binom{k}{k-1} + \binom{k}{k-2} + 1\right] \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right) \\
&= \sum_{k=0}^{2} \left[(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right] \\
&- \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-3}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-3}}} \\
&+ \sum_{d=0}^{s-\tilde{u}-4} \left[\binom{3+(d+1)}{d+1} \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-4-d}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-4-d}}}\right] \\
&- \sum_{k=4}^{s-\tilde{u}} \left(\left[-\binom{k}{k-1} + \binom{k}{k-2} + 1\right] \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{3}\left[(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right] \\
&- \sum_{k=4}^{s-\tilde{u}}\left[\left(\sum_{v=1}^{3}\left[(-1)^s\begin{pmatrix} k \\ k-v \end{pmatrix}\right]+1\right)\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right].
\end{aligned}
$$

Observe que pela Proposição 5.0.1, para todo inteiro k,

$$
\sum_{v=1}^{k-1}\left[(-1)^v\begin{pmatrix} k \\ k-v \end{pmatrix}\right]+1 = \begin{cases} 1, & \text{se } k \text{ é ímpar} \\ -1 & \text{se } k \text{ é par} \end{cases}.
$$

Logo,

$$
\begin{aligned}
S^{0,0}_{l_1,l_2\ldots,l_{s-\tilde{u}}} &= \sum_{k=0}^{4}\left[(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right] \\
&- \sum_{k=5}^{s-u}\left[\left(\sum_{v=1}^{4}\left[(-1)^v\begin{pmatrix} k \\ k-v \end{pmatrix}\right]+1\right)\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}\right].
\end{aligned}
$$

Portanto, continuando o processo

$$
\begin{aligned}
S^{0,0}_{l_1,l_2\ldots,l_{s-\tilde{u}}} &= \sum_{k=0}^{s-\tilde{u}-1}(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}} \\
&- \left(\sum_{v=1}^{s-\tilde{u}}\left[(-1)^v\begin{pmatrix} k \\ k-v \end{pmatrix}\right]+1\right)\sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} S^{0,0}_0 \\
&= \sum_{k=0}^{s-\tilde{u}}(-1)^k \sum_{t_1<t_2<\cdots<t_{s-\tilde{u}-k}} A_{l_{t_1},l_{t_2},\ldots,l_{t_{s-\tilde{u}-k}}}.
\end{aligned}
$$

2. Faremos a prova para o caso $i \neq 0$ e $j = 0$, o caso $i = 0$ e $j \neq 0$ seguirá de maneira análoga bastando observar que $r_2^j = (r^j_{1_1}, r^j_{1_2}, \ldots, r^j_{1_{s_1}}, r^{\tilde{t}j}_{1_{s_1+1}}, r^{\tilde{t}j}_{1_{s_1+2}}, \ldots, r^{\tilde{t}j}_{1_s})$.

2.a) Se $\beta = (\beta_1, \beta_2, \ldots, \beta_s) \in \mathbb{Z}_n^*$ satisfaz $\alpha + \beta r_1^i = 0$, então $-\beta r_1^i = \alpha \in H$, ou ainda, $\beta = -\alpha r_1^{n-i}$. Como, $n \equiv 0\ (mod\ p)$, então $n - i \equiv -i\ (mod\ p)$ e assim, $-\alpha \in H$ e $r_1^{n-i} \notin H$. Logo $\beta \notin H$ e dessa forma, não existe $\beta \in H$ tal que $\alpha + \beta r_1^i = 0$, portanto $S_0^{i,0} = 0$, para $1 \leqslant i \leqslant p-1$.

Suponhamos agora que $\beta = (\beta_1, \beta_2, \ldots, \beta_s) \in \mathbb{Z}_n^*$ satisfaz $r^i_{1_k}\beta_k = -\alpha_k$, para todo $1 \leqslant k \leqslant s_1$, então

$$
\begin{aligned}
(r^i_{1_1}, r^i_{1_2}, \ldots, r^i_{1_{s_1}}, 1, \ldots, 1)(\beta_1, \beta_2, \ldots, \beta_{s_1}, 1, \ldots, 1) &= (-\alpha_1, -\alpha_2, \ldots, -\alpha_{s_1}, 1, \ldots, 1) \\
&= \Pi_P(-\alpha) \times \Pi_{P'}(1) \in H.
\end{aligned}
$$

Contudo, pelo Corolário 4.1.6,

$$
(r^i_{1_1}, r^i_{1_2}, \ldots, r^i_{1_{s_1}}, 1, \ldots, 1) \notin H,
$$

dessa forma

$$(\beta_1, \beta_2, \ldots, \beta_{s_1}, 1, \ldots, 1) \notin H$$

e assim, $\beta \notin H$. Portanto, $S^{i,0}_{l'_{t'_1}, l'_{t'_2}, \ldots, l'_{t'_{k'}}} = 0$, para todo $k' = 1, 2, \ldots, s_2 - u'$.

De forma análoga, segue que $S^{i,0}_{l_{t_1}, l_{t_2}, \ldots, l_{t_k}} = 0$, para $k = 1, 2, \ldots, s_1 - u$, bastando notar que $(1, 1, \ldots, 1, r^i_{1_{s_1+1}}, r^i_{1_{s_1+2}}, \ldots, r^i_{1_s}) \notin H$.

2.b) Para cada $l_t \in L$, $l'_{t'} \in L'$, considere $Y_t = P \backslash \{l_t\}$ e $Y'_{t'} = P' \backslash \{l'_{t'}\}$, temos que

$$\left(-\alpha_1 r^{n-i}_{1_1}, -\alpha_2 r^{n-i}_{1_2}, \ldots, -\alpha_{l_{t-1}} r^{n-i}_{1_{l_{t-1}}}, -\alpha_{l_{t+1}} r^{n-i}_{1_{l_{t+1}}}, \ldots, -\alpha_{s_1} r^{n-i}_{1_{s_1}}\right),$$

e

$$\left(-\alpha_{s_1+1} r^{n-i}_{1_{s_1+1}}, -\alpha_{s_1+2} r^{n-i}_{1_{s_1+2}}, \ldots, -\alpha_{s_1+l'_{t'-1}} r^{n-i}_{1_{s_1+l'_{t'-1}}}, -\alpha_{s_1+l'_{t'+1}} r^{n-i}_{1_{s_1+l'_{t'+1}}}, \ldots, -\alpha_s r^{n-i}_{1_s}\right),$$

são elementos de $\mathbb{Z}^*_{\left(m_1/p_{l_t}\right)}$ e $\mathbb{Z}^*_{\left(m_2/p'_{l'_{t'}}\right)}$, respectivamente. Como

$$\mathbb{Z}^*_{\left(m_1/p_{l_t}\right)} \times \mathbb{Z}^*_{\left(m_2/p'_{l'_{t'}}\right)} = Z_{Y_t} \times Z_{Y'_{t'}} = \Pi_{Y_t}(H) \times \Pi_{Y'_{t'}}(H) = \Pi_{Y_t \times Y'_{t'}}(H),$$

existe $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_s) \in H$ de forma que para todo $k \in \{1, 2, \ldots, s\} \backslash \{l_{t_1}, l'_{t'_1}\}$ temos que $r^i_{1_k} \gamma_k = -\alpha_k$, e pelo item 2.a) $r^i_{1_{l_t}} \gamma_{l_t} \neq -\alpha_{l_t}$ e $r^i_{1_{l'_{t'}}} \gamma_{l'_{t'}} \neq -\alpha_{l'_{t'}}$.

Portanto,

$$\begin{aligned} S^{i,0}_{l_t, l'_{t'}} &= |\Pi^{-1}_{Y_t \times Y'_{t'}}(\gamma)| - S^{i,0}_{l_t} - S^{i,0}_{l'_{t'}} - S^{i,0}_0 \\ &= A_{l_t, l'_{t'}} - 0 - 0 - 0 \\ &= A_{l_t, l'_{t'}}. \end{aligned}$$

Agora, sejam $l_1 \leqslant l_{t_1} < l_{t_2} < l_{t_3} \leqslant l_{s-u}$, com $l_{t_1} \in L$ e $l_{t_3} \in L'$ (tomamos l_{t_3} ao invés de $l'_{t'}$ para facilitar as contas). Assim como no argumento acima, existe $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_s) \in H$ de forma que para todo $t \in \{1, 2, \ldots, s\} \backslash \{l_{t_1}, l_{t_2}, l_{t_3}\}$ temos que $r^i_{1_t} \gamma_t = -\alpha_t$. Logo,

$$\begin{aligned} S^{i,0}_{l_{t_1}, l_{t_2}, l_{t_3}} &= A_{l_{t_1}, l_{t_2}, l_{t_3}} - S^{i,0}_{l_{t_1}, l_{t_2}} - S^{i,0}_{l_{t_1}, l_{t_3}} - S^{i,0}_{l_{t_2}, l_{t_3}} - S^{i,0}_{l_{t_1}} - S^{i,0}_{l_{t_2}} - S^{i,0}_{l_{t_3}} - S^{i,0}_0 \\ &= \begin{cases} A_{l_{t_1}, l_{t_2}, l_{t_3}} - A_{l_{t_1}, l_{t_3}} - A_{l_{t_2}, l_{t_3}} & , \text{se} \quad l_{t_2} \in L \\ A_{l_{t_1}, l_{t_2}, l_{t_3}} - A_{l_{t_1}, l_{t_2}} - A_{l_{t_1}, l_{t_3}} & , \text{se} \quad l_{t_2} \in L' \end{cases}. \end{aligned}$$

Generalizando, temos que o fator $S^{i,0}_{l_1, l_2, \ldots, l_{s_1-u}, l'_1, l'_2, \ldots, l'_{s_2-u'}}$ é dado por

$$A_{l_1, l_2, \ldots, l_{s_1-u}, l'_1, l'_2, \ldots, l'_{s_2-u'}} - \sum_{\substack{t_1 < t_2 < \ldots < t_e \text{ e } t'_1 < t'_2 < \ldots < t'_{e'} \\ e + e' = s - \tilde{u} - 1}} S^{i,0}_{l_{t_1}, l_{t_2} \ldots, l_{t_e}, l'_1, l'_2, \ldots, l'_{e'}}$$

$$- \sum_{\substack{t_1 < t_2 < \ldots < t_e \text{ e } t'_1 < t'_2 < \ldots < t'_{e'} \\ e + e' = s - \tilde{u} - 2}} S^{i,0}_{l_{t_1}, l_{t_2} \ldots, l_{t_e}, l_{t'_1}, l_{t'_2} \ldots, l_{t'_{e'}}} - \cdots$$

$$\cdots \quad - \left(\sum_{t_1<t_2<t_3} S^{i,0}_{l_{t_1},l_{t_2},l_{t_3}} + \sum_{t_1<t_2,\ l_{t'}\in L'} S^{i,0}_{l_{t_1},l_{t_2},l'_{t'}} + \sum_{t'_1<t'_2,\ l_t\in L} S^{i,0}_{l_t,l'_{t'_1},l'_{t'_2}} + \sum_{t'_1<t'_2<t'_3} S^{i,0}_{l'_{t'_1},l'_{t'_2},l'_{t'_3}} \right)$$

$$- \quad \left(\sum_{t_1<t_2} S^{i,0}_{l_{t_1},l_{t_2}} + \sum_{l_t\in L,\ l_{t'}\in L'} S^{i,0}_{l_t,l'_{t'}} + \sum_{t'_1<t'_2} S^{i,0}_{l'_{t'_1},l'_{t'_2}} \right)$$

$$- \quad \left(\sum_{t=1}^{s_1-u} S^{i,0}_{l_t} + \sum_{t'=1}^{s_2-u'} S^{i,0}_{l'_{t'}} \right) - S^{i,0}_0,$$

onde $e, e' \geqslant 0$.

Pelo item 2.a) podemos descartar as parcelas em que $e = 0$ ou $e' = 0$, assim, $S^{i,0}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}}$ é igual a

$$A_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} - \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-1}} S^{i,0}_{l_{t_1},l_{t_2}\ldots,l_{t_d},l'_1,l'_2,\ldots,l'_{d'}}$$

$$- \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-2}} S^{i,0}_{l_{t_1},l_{t_2}\ldots,l_{t_d},l_{t'_1},l_{t'_2}\ldots,l_{t'_{d'}}} - \cdots$$

$$\cdots \quad - \left(\sum_{t_1<t_2,\ l_{t'}\in L'} S^{i,0}_{l_{t_1},l_{t_2},l'_{t'}} + \sum_{t'_1<t'_2,\ l_t\in L} S^{i,0}_{l_t,l'_{t'_1},l'_{t'_2}} \right) - \sum_{l_t\in L,\ l_{t'}\in L'} S^{i,0}_{l_t,l'_{t'}},$$

com $d, d' \geqslant 1$.

Logo, de forma análoga ao caso 1., segue que $S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}}$ é

$$A_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} - \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-1}} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},l'_1,l'_2,\ldots,l'_{d'}}$$

$$+ \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-2}} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},l_{t'_1},l_{t'_2}\ldots,l_{t'_{d'}}} - \cdots$$

$$\cdots \quad +(-1)^{s-\tilde{u}-3} \left(\sum_{t_1<t_2,\ l_{t'}\in L'} A_{l_{t_1},l_{t_2},l'_{t'}} + \sum_{t'_1<t'_2,\ l_t\in L} A_{l_t,l'_{t'_1},l'_{t'_2}} \right)$$

$$+ \quad (-1)^{s-\tilde{u}-2} \sum_{l_t\in L,\ l_{t'}\in L'} A_{l_t,l'_{t'}},$$

com $d, d' \geqslant 1$. Ou ainda,

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u-1} \sum_{k'=0}^{s_2-u'-1} (-1)^{k+k'} \tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ é a quantidade

$$\sum_{1\leqslant t_1<t_2<\cdots<t_{s_1-u-k}\leqslant s_1-u \text{ e } 1\leqslant t'_1<t'_2<\cdots<t'_{s_2-u'-k'}\leqslant s_2-u'} A_{l_{t_1},l_{t_2}\ldots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}}.$$

3. Seja $i \neq 0$ e $j \neq 0$.

3.a) Pelo Corolário 4.1.6, desde que $i \not\equiv -j \pmod p$ e $i \not\equiv -\tilde{t}j \pmod p$ temos que

$$(r_{1_1}^{i+j}, r_{1_2}^{i+j}, \ldots, r_{1_{s_1}}^{i+j}, 1, 1, \ldots, 1) \notin H \text{ e } (1, 1, \ldots, 1, r_{1_{s_1+1}}^{i+\tilde{t}j}, r_{1_{s_1+2}}^{i+\tilde{t}j}, \ldots, r_{1_s}^{i+\tilde{t}j}) \notin H.$$

Portanto, o resultado segue de forma análoga ao caso 2.

3.b) Para $i \equiv -j \pmod p$.

i) Note inicialmente que $i \not\equiv -\tilde{t}j \pmod p$. Logo, pelo Corolário 4.1.6 , segue que $(r_{1_1}^{i+j}, r_{1_2}^{i+j}, \ldots, r_{1_{s_1}}^{i+j}, 1, 1, \ldots, 1) \in H$ e $(1, 1, \ldots, 1, r_{1_{s_1+1}}^{i+\tilde{t}j}, r_{1_{s_1+2}}^{i+\tilde{t}j}, \ldots, r_{1_s}^{i+\tilde{t}j}) \notin H$. Dessa forma, assim como no caso 2.a), segue que

$$S^{i,0}_{l_{t_1}, l_{t_2}, \ldots, l_{t_k}} = 0,$$

para todo $k = 0, 1, \ldots, s_1 - u$.

ii) Suponha que $u' \neq s_2$. Logo, utilizando a construção feita em 2. observando o item *i*), obtemos que o valor de

$$S^{i,j}_{l_1, l_2, \ldots, l_{s_1-u}, l'_1, l'_2, \ldots, l'_{s_2-u'}}$$

é dado por:

$$\begin{aligned}
& A_{l_1, l_2, \ldots, l_{s_1-u}, l'_1, l'_2, \ldots, l'_{s_2-u'}} - \sum_{\substack{t_1<t_2<\ldots<t_e \text{ e } t'_1<t'_2<\ldots<t'_{e'} \\ d+d'=s-\tilde{u}-1}} S^{i,j}_{l_{t_1}, l_{t_2}\ldots, l_{t_d}, l'_1, l'_2, \ldots, l'_{d'}} \\
- & \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-2}} S^{i,j}_{l_{t_1}, l_{t_2}\ldots, l_{t_d}, l_{t'_1}, l_{t'_2}\ldots, l_{t'_{d'}}} - \cdots \\
\cdots - & \left(\sum_{t_1<t_2,\ l_{t'}\in L'} S^{i,j}_{l_{t_1}, l_{t_2}, l'_{t'}} + \sum_{t'_1<t'_2,\ l_t\in L} S^{i,j}_{l_t, l'_{t'_1}, l'_{t'_2}} + \sum_{t'_1<t'_2<t'_3} S^{i,j}_{l'_{t'_1}, l'_{t'_2}, l'_{t'_3}} \right) \\
- & \left(\sum_{l_t\in L,\ l_{t'}\in L'} S^{i,j}_{l_t, l'_{t'}} + \sum_{t'_1<t'_2} S^{i,j}_{l'_{t'_1}, l'_{t'_2}} \right) - \sum_{t'=1}^{s_2-u'} S^{i,j}_{l'_{t'}},
\end{aligned}$$

com $d \geqslant 0$ e $d' \geqslant 1$. Ou seja,

$$\begin{aligned}
& A_{l_1, l_2, \ldots, l_{s_1-u}, l'_1, l'_2, \ldots, l'_{s_2-u'}} - \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-1}} A_{l_{t_1}, l_{t_2}\ldots, l_{t_d}, l'_1, l'_2, \ldots, l'_{d'}} \\
+ & \sum_{\substack{t_1<t_2<\ldots<t_d \text{ e } t'_1<t'_2<\ldots<t'_{d'} \\ d+d'=s-\tilde{u}-2}} A_{l_{t_1}, l_{t_2}\ldots, l_{t_d}, l_{t'_1}, l_{t'_2}\ldots, l_{t'_{d'}}} - \cdots \\
\cdots + & (-1)^{s-\tilde{u}-3} \left(\sum_{t_1<t_2,\ l_{t'}\in L'} A_{l_{t_1}, l_{t_2}, l'_{t'}} + \sum_{t'_1<t'_2,\ l_t\in L} A_{l_t, l'_{t'_1}, l'_{t'_2}} + \sum_{t'_1<t'_2<t'_3} A_{l'_{t'_1}, l'_{t'_2}, l'_{t'_3}} \right) \\
+ & (-1)^{s-\tilde{u}-2} \left(\sum_{l_t\in L,\ l_{t'}\in L'} A_{l_t, l'_{t'}} + \sum_{t'_1<t'_2} A_{l'_{t'_1}, l'_{t'_2}} \right) + (-1)^{s-\tilde{u}-1} \sum_{t'=1}^{s_2-u'} A_{l'_{t'}},
\end{aligned}$$

com $d \geqslant 0$ e $d' \geqslant 1$. Dessa forma,

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k=0}^{s_1-u} \sum_{k'=0}^{s_2-u'-1} (-1)^{k+k'} \tilde{A}_{k,k'},$$

onde $\tilde{A}_{k,k'}$ é a quantidade

$$\sum_{1\leqslant t_1<t_2<\cdots<t_{s_1-u-k}\leqslant s_1-u \text{ e } 1\leqslant t'_1<t'_2<\cdots<t'_{s_2-u'-k'}\leqslant s_2-u'} A_{l_{t_1},l_{t_2}\ldots,l_{t_{s_1-u-k}},l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}},$$

se $0 \leqslant k \leqslant s_1 - u - 1$ e,

$$\tilde{A}_{(s_1-u),k'} \sum_{1\leqslant t'_1<t'_2<\cdots<t'_{s_2-u'-k'}\leqslant s_2-u'} A_{l'_{t'_1},l'_{t'_2},\ldots,l'_{t'_{s_2-u'-k'}}}.$$

3.c) Segue de forma análoga ao caso 3.b), apenas observando que se $i \equiv -\tilde{t}j \pmod p$, então $i \not\equiv -j \pmod p$. □

Substituindo as quantidade $A_{\tilde{L}\times\tilde{L}'}$ obtidas no Lema 4.1.1 no teorema anterior, segue que:

Corolário 5.0.3. *Com as notações do teorema anterior, considerando*

$$D_L := D_{l_1,l_2,\ldots,l_{s_1-u}} = \sum_{k=0}^{s_1-u-1} \left[(-1)^k \sum_{t_1<t_2<\ldots<t_{s_1-u-k}} \frac{\prod_{t=t_1}^{t_{s_1-u-k}} q_{l_t}}{p} \right]$$

e,

$$D'_{L'} := D_{l'_1,l'_2,\ldots,l'_{s_2-u'}} = \sum_{k'=0}^{s_2-u'-1} \left[(-1)^{k'} \sum_{t'_1<t'_2<\ldots<t_{s'_2-u'-k'}} \frac{\prod_{t'=t'_1}^{t'_{s_2-u'-k'}} q'_{l'_{t'}}}{p} \right].$$

Então,

1. *Para $\tilde{u} = s$, temos que $S^{0,0}_0 = 1$ e $S^{i,j}_0 = 0$, se $(i,j) \neq (0,0)$.*
2. *Para $0 \leqslant u \leqslant s_1 - 1$ e $u' = s_2$,*
   (a) *Se $i \not\equiv -\tilde{t}j \pmod p$, temos que*
   $$S^{i,j}_{l_1,l_2\ldots,l_{s_1-u}} = 0.$$
   (b) *Se $i = j = 0$, temos que*
   $$S^{0,0}_{l_1,l_2\ldots,l_{s_1-u}} = D_L + (-1)^{s_1-u}.$$

(c) Se $i \equiv -\tilde{t}j \pmod p$, *com* $(i,j) \neq (0,0)$, *temos que*

$$S^{0,0}_{l_1,l_2\ldots,l_{s_1-u}} = D_L.$$

3. Para $u = s_1$ *e* $0 \leqslant u' \leqslant s_2 - 1$,

(a) Se $i \not\equiv -j \pmod p$, *temos que*

$$S^{i,j}_{l'_1,l'_2\ldots,l'_{s_2-u'}} = 0.$$

(b) Se $i = j = 0$, *temos que*

$$S^{0,0}_{l'_1,l'_2\ldots,l'_{s_2-u'}} = D'_{L'} + (-1)^{s_2-u'}.$$

(c) $i \equiv -j \pmod p$, *com* $(i,j) \neq (0,0)$, *temos que*

$$S^{i,j}_{l'_1,l'_2\ldots,l'_{s_2-u'}} = D'_{L'}.$$

4. Para $0 \leqslant u \leqslant s_1 - 1$ *e* $0 \leqslant u' \leqslant s_2 - 1$.

(a) Se $i = j = 0$, *temos que*

$$S^{0,0}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \left(D_L + (-1)^{s_1-u}\right)\left(D'_{L'} + (-1)^{s_2-u'}\right).$$

(b) Se $i \not\equiv -j \pmod p$ *e* $i \not\equiv -\tilde{t}j \pmod p$ *temos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = D_L D'_{L'}.$$

(c) Se $i \equiv -j \pmod p$, *com* $(i,j) \neq (0,0)$, *temos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = \left(D_L + (-1)^{s_1-u}\right) D'_{L'}.$$

(d) Se $i \equiv -tj \pmod p$, *com* $(i,j) \neq (0,0)$, *temos que*

$$S^{i,j}_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} = D_L\left(D'_{L'} + (-1)^{s_2-u'}\right).$$

Faremos uso destes resultados para verificarmos a veracidade de três lemas auxiliares destacados no Capítulo 4 (Lemas 4.2.1, 4.2.2 e 4.2.3) a fim de obtermos a forma traço integral, para isso denotaremos $h = |H| = \frac{\phi(n)}{p^2}$ e utilizaremos a expressão

$$\begin{aligned} S'_{l_1,l_2,\ldots,l_{s_1-u},l'_1,l'_2,\ldots,l'_{s_2-u'}} &= (-1)^{s-\tilde{u}} \prod_{k=1}^{u} Tr_{\mathbb{Q}(\zeta_{p_{y_k}})/\mathbb{Q}}\left(\zeta^0_{p_{y_k}}\right) \prod_{k'=1}^{u'} Tr_{\mathbb{Q}\left(\zeta_{p'_{y'_{k'}}}\right)/\mathbb{Q}}\left(\zeta^0_{p'_{y'_{k'}}}\right) \\ &= (-1)^{s-\tilde{u}} \prod_{k=1}^{u} q_{y_k} \prod_{k'=1}^{u'} q'_{y'_{k'}} \\ &= (-1)^{s-\tilde{u}} \frac{\phi(n)}{\prod_{t=1}^{s_1-u} q_{l_t} \prod_{t'=1}^{s_2-u'} q'_{l'_{t'}}}, \end{aligned} \tag{5.2}$$

para $(u,u') \neq (0,0)$ e

$$S'_0 = \prod_{k=1}^{s_1} q_{y_k} \prod_{k'=1}^{s_2} q'_{y'_{k'}} = \phi(m_1)\phi(m_2) = \phi(n).$$

Lema 5.0.4. *Com as notações do Lema 4.2.1, temos que*

$$\begin{aligned} Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2) &= \frac{1}{h} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) \\ &= \frac{(m_1-1)(m_2-1)}{p^2} - \frac{m_1(m_2-1)+(m_1-1)m_2}{p} + n. \end{aligned}$$

Demonstração. Pela equação (4.1) temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) = T_1^0 + T_1^1 + T_1^2 + \cdots + T_1^{s-1} + T_1^s,$$

onde

$$T_1^u = h \left[\sum_{\substack{l_1<l_2<\ldots<l_d,\ l'_1<l'_2<\ldots<l'_{d'} \\ d+d'=u}} S'_{l_1,l_2,\ldots,l_d,l'_1,l'_2,\ldots,l'_{d'}} S^{0,0}_{l_1,l_2,\ldots,l_d,l'_1,l'_2,\ldots,l'_{d'}} \right].$$

Conforme o Corolário 5.0.3, temos que $S_0^{0,0} = 1$, assim

$$T_1^0 = hS'_0S_0^{0,0} = h.\phi(n).$$

Para o caso T_1^1, temos que $S'_l = -\frac{\phi(n)}{q_l}$ e $S'_{l'} = -\frac{\phi(n)}{q'_{l'}}$, para $l \in P$ e $l' \in P'$. Logo,

$$\begin{aligned} T_1^1 &= h\left[\sum_{l=1}^{s_1} S'_l S_l^{0,0} + \sum_{l'=1}^{s_2} S'_{l'} S_{l'}^{0,0}\right] \\ &= h\left[\sum_{l=1}^{s_1} -\frac{\phi(n)}{q_l}\left(\frac{q_l}{p}-1\right) + \sum_{l'=1}^{s_2} -\frac{\phi(n)}{q'_{l'}}\left(\frac{q'_{l'}}{p}-1\right)\right] \\ &= h\left[\sum_{l=1}^{s_1}\left(-\frac{\phi(n)}{p}+\frac{\phi(n)}{q_l}\right) + \sum_{l'=1}^{s_2}\left(-\frac{\phi(n)}{p}+\frac{\phi(n)}{q'_{l'}}\right)\right] \\ &= -h\left[\frac{1}{p}\left[\begin{pmatrix} s_1 \\ s_1-1 \end{pmatrix} + \begin{pmatrix} s_2 \\ s_2-1 \end{pmatrix}\right]\phi(n) - \sum_{k=1}^{s}\frac{\phi(n)}{q_k}\right]. \end{aligned}$$

Note que, $S'_{l_1,l_2} = \frac{\phi(n)}{q_{l_1}q_{l_2}}$, $S'_{l,l'} = \frac{\phi(n)}{q_l q'_{l'}}$ e $S'_{l'_1,l'_2} = \frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}$, para $l, l_1, l_2 \in P$ e $l', l'_1, l'_2 \in P'$. Assim, a parcela T_1^2 é igual a

$$
\begin{aligned}
& h\left[\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}\left(\frac{q_{l_1}q_{l_2}}{p}-\frac{q_{l_1}+q_{l_2}}{p}+1\right)+\sum_{l\in P,\ l'\in P'}\frac{\phi(n)}{q_l q'_{l'}}\left(\frac{q_l q'_{l'}}{p^2}-\frac{q_l+q'_{l'}}{p}+1\right)\right.\\
+\quad & \left.\sum_{l'_1<l'_2}\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}\left(\frac{q'_{l'_1}q'_{l'_2}}{p}-\frac{q'_{l'_1}-q'_{l'_2}}{p}+1\right)\right]\\
=\quad & h\left[\sum_{l\in P,\ l'\in P'}\frac{\phi(n)}{p^2}+\sum_{l_1<l_2}\frac{\phi(n)}{p}+\sum_{l'_1<l'_2}\frac{\phi(n)}{p}-\sum_{l_1<l_2}\left(\frac{\phi(n)}{pq_{l_1}}+\frac{\phi(n)}{pq_{l_2}}\right)-\sum_{l'_1<l'_2}\left(\frac{\phi(n)}{pq'_{l'_1}}+\frac{\phi(n)}{pq'_{l'_2}}\right)\right.\\
-\quad & \left.\sum_{l\in P,l'\in P'}\left(\frac{\phi(n)}{pq_l}+\frac{\phi(n)}{pq'_{l'}}\right)+\sum_{1\leqslant k_1<k_2\leqslant s}\frac{\phi(n)}{q_{k_1}q_{k_2}}\right]\\
=\quad & h\left[\frac{1}{p^2}s_1s_2\phi(n)+\frac{1}{p}\left(\left[\binom{s_1}{s_1-2}+\binom{s_2}{s_2-2}\right]\phi(n)-(s_1-1)\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}-(s_2-1)\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right.\right.\\
-\quad & \left.\left.s_2\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}-s_1\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right)+\sum_{1\leqslant k_1<k_2\leqslant s}\frac{\phi(n)}{q_{k_1}q_{k_2}}\right]\\
=\quad & h\left[\frac{1}{p^2}\left(\binom{s_1}{s_1-1}\binom{s_2}{s_2-1}\right)\phi(n)+\frac{1}{p}\left(\left[\binom{s_1}{s_1-2}+\binom{s_2}{s_2-2}\right]\phi(n)\right.\right.\\
-\quad & \left.\left.\left[\binom{s_1-1}{s_1-2}+\binom{s_2}{s_2-1}\right]\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}-\left[\binom{s_2-1}{s_2-2}+\binom{s_1}{s_1-1}\right]\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right)\right.\\
+\quad & \left.\sum_{1\leqslant k_1<k_2\leqslant s}\frac{\phi(n)}{q_{k_1}q_{k_2}}\right].
\end{aligned}
$$

De forma análoga, olhando para os elementos de H que coincidem com $-\alpha$ em exatamente três coordenadas, temos que a parcela correspondente a T_1^3, na expressão (4.1), é igual a

$$
\begin{aligned}
& h\left[\sum_{l_1<l_2<l_3}-\frac{\phi(n)}{q_{l_1}q_{l_2}q_{l_3}}\left(\frac{q_{l_1}q_{l_2}q_{l_3}-q_{l_1}q_{l_2}-q_{l_1}q_{l_3}-q_{l_2}q_{l_3}+q_{l_1}+q_{l_2}+q_{l_3}}{p}-1\right)\right.\\
+\quad & \sum_{l_1<l_2,\ l'\in P'}-\frac{\phi(n)}{q_{l_1}q_{l_2}q'_{l'}}\left(\frac{q_{l_1}q_{l_2}q'_{l'}-q_{l_1}q_{l'}-q_{l_2}q_{l'}}{p^2}+\frac{-q_{l_1}q_{l_2}+q_{l_1}+q_{l_2}+q'_{l'}}{p}-1\right)\\
+\quad & \sum_{l\in P,\ l'_1<l'_2}-\frac{\phi(n)}{q_l q'_{l'_1}q'_{l'_2}}\left(\frac{q_l q'_{l'_1}q'_{l'_2}-q_l q_{l'_1}-q_l q_{l'_2}}{p^2}+\frac{-q'_{l'_1}q'_{l'_2}+q_l+q'_{l'_1}+q'_{l'_2}}{p}-1\right)\\
+\quad & \left.\sum_{l'_1<l'_2<l'_3}-\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}q'_{l'_3}}\left(\frac{q'_{l'_1}q'_{l'_2}q'_{l'_3}-q'_{l'_1}q'_{l'_2}-q'_{l'_1}q'_{l'_3}-q'_{l'_2}q'_{l'_3}+q'_{l'_1}+q'_{l'_2}+q'_{l'_3}}{p}-1\right)\right]\\
=\quad & -h\left[\frac{1}{p^2}\left(\left[\binom{s_1}{s_1-1}\binom{s_2}{s_2-2}+\binom{s_1}{s_1-2}\binom{s_2}{s_2-1}\right]\phi(n)\right.\right.\\
-\quad & \left.\left.\binom{s_1-1}{s_1-2}\binom{s_2}{s_2-1}\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}+\binom{s_1}{s_1-1}\binom{s_2-1}{s_2-2}\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right)\right.\\
+\quad & \frac{1}{p}\left(\left[\binom{s_1}{s_1-3}+\binom{s_2}{s_2-3}\right]\phi(n)-\left[\binom{s_1-1}{s_1-3}+\binom{s_2}{s_2-2}\right]\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}\right.\\
-\quad & \left.\left.\left[\binom{s_2-1}{s_2-3}+\binom{s_1}{s_1-2}\right]\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}+\left[\binom{s_1-2}{s_1-3}+\binom{s_2}{s_2-1}\right]\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}\right.\right.
\end{aligned}
$$

$$+ \quad \left[\binom{s_1-1}{s_1-2} + \binom{s_2-1}{s_2-2} \right] \sum_{l\in P<l'\in P'} \frac{\phi(n)}{q_l q'_{l'}} + \left[\binom{s_2-2}{s_2-3} + \binom{s_1}{s_1-1} \right] \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} \Bigg)$$

$$- \quad \sum_{1\leqslant k_1<k_2<k_3\leqslant s} \frac{\phi(n)}{q_{k_1} q_{k_2} q_{k_3}} \Bigg].$$

Generalizando esse processo, analisando quando $0 \leqslant \tilde{u} \leqslant s-1$ coordenadas de $-\alpha$ coincidem com elementos de H, precisamos tomar alguns cuidados com os índices. Sejam $0 \leqslant u \leqslant s_1$, $0 \leqslant u' \leqslant s_2$, $d, d' \geqslant 1$

$$d_{\tilde{u}} = \begin{cases} s_1 - 1, & \text{se } \tilde{u} > s_1 \\ \tilde{u} - 2, & \text{se } \tilde{u} \leqslant s_1 \end{cases}, \quad d'_{\tilde{u}} = \begin{cases} s_2 - 1, & \text{se } \tilde{u} > s_2 \\ \tilde{u} - 2, & \text{se } \tilde{u} \leqslant s_2 \end{cases}$$

e considere que

$$\binom{s_i}{s_i - c} = 0,$$

se $c \geqslant s_i$, para $i = 1, 2$. Logo,

$$\begin{aligned}
T_1^{\tilde{u}} &= (-1)^{\tilde{u}} h \Bigg[\frac{1}{p^2} \Bigg(\Bigg[\sum_{d+d'=\tilde{u}} \binom{s_1}{s_1-d} \binom{s_2}{s_2-d'} \Bigg] \phi(n) \\
&- \Bigg[\sum_{d+d'=\tilde{u}-1} \binom{s_1-1}{(s_1-1)-d} \binom{s_2}{s_2-d'} \Bigg] \sum_{l=1}^{s_1} \frac{\phi(n)}{q_l} \\
&+ \Bigg[\sum_{d+d'=\tilde{u}-2} \binom{s_1-2}{(s_1-2)-d} \binom{s_2}{s_2-d'} \Bigg] \sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}} \\
&- \Bigg[\sum_{d+d'=\tilde{u}-3} \binom{s_1-3}{(s_1-3)-d} \binom{s_2}{s_2-d'} \Bigg] \sum_{l_1<l_2<l_3} \frac{\phi(n)}{q_{l_1} q_{l_2} q_{l_3}} + \cdots \\
\cdots &+ (-1)^{d_{\tilde{u}}} \Bigg[\sum_{d+d'=\tilde{u}-d_{\tilde{u}}} \binom{s_1-d_{\tilde{u}}}{(s_1-d_{\tilde{u}})-d} \binom{s_2}{s_2-d'} \Bigg] \sum_{l_1<l_2<\cdots<l_{d_{\tilde{u}}}} \frac{\phi(n)}{q_{l_1} q_{l_2} \cdots q_{l_{d_{\tilde{u}}}}} \\
&- \Bigg[\sum_{d+d'=\tilde{u}-1} \binom{s_1}{s_1-d} \binom{s_2-1}{(s_2-1)-d'} \Bigg] \sum_{l'=1}^{s_2} \frac{\phi(n)}{q'_{l'}} \\
&+ \Bigg[\sum_{d+d'=\tilde{u}-2} \binom{s_1}{s_1-d} \binom{s_2-2}{(s_2-2)-d'} \Bigg] \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} \\
&- \Bigg[\sum_{d+d'=\tilde{u}-3} \binom{s_1}{s_1-d} \binom{s_2-3}{(s_2-3)-d'} \Bigg] \sum_{l'_1<l'_2<l'_3} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2} q'_{l'_3}} + \cdots \\
\cdots &+ (-1)^{d'_{\tilde{u}}} \Bigg[\sum_{d+d'=\tilde{u}-d'_{\tilde{u}}} \binom{s_1}{s_1-d} \binom{s_2-d'_{\tilde{u}}}{(s_2-d'_{\tilde{u}})-d'} \Bigg] \sum_{l'_1<l'_2<\cdots<l'_{d'_{\tilde{u}}}} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{d'_{\tilde{u}}}}} \\
&+ \Bigg[\sum_{d+d'=\tilde{u}-2} \binom{s_1-1}{(s_1-1)-d} \binom{s_2-1}{(s_2-1)-d'} \Bigg] \sum_{l\in P, l'\in P'} \frac{\phi(n)}{q_l q'_{l'}} - \cdots \Bigg)
\end{aligned}$$

$$
\begin{aligned}
&+ \frac{1}{p}\left(\left[\begin{pmatrix} s_1 \\ s_1-\tilde{u}\end{pmatrix}+\begin{pmatrix} s_2 \\ s_2-\tilde{u}\end{pmatrix}\right]\phi(n)\right.\\
&- \left[\begin{pmatrix} s_1-1 \\ (s_1-1)-(\tilde{u}-1)\end{pmatrix}+\begin{pmatrix} s_2 \\ s_2-(\tilde{u}-1)\end{pmatrix}\right]\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}\\
&- \left[\begin{pmatrix} s_2-1 \\ (s_2-1)-(\tilde{u}-1)\end{pmatrix}+\begin{pmatrix} s_1 \\ s_1-(\tilde{u}-1)\end{pmatrix}\right]\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\\
&+ \left[\begin{pmatrix} s_1-2 \\ s_1-\tilde{u}\end{pmatrix}+\begin{pmatrix} s_2 \\ s_2-(\tilde{u}-2)\end{pmatrix}\right]\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}\\
&+ \left[\begin{pmatrix} s_1-1 \\ (s_1-1)-(\tilde{u}-2)\end{pmatrix}+\begin{pmatrix} s_2-1 \\ (s_2-1)-(\tilde{u}-2)\end{pmatrix}\right]\sum_{l\in P, l'\in P'}\frac{\phi(n)}{q_l q'_{l'}}\\
&+ \left.\left[\begin{pmatrix} s_2-2 \\ s_2-\tilde{u}\end{pmatrix}+\begin{pmatrix} s_1 \\ s_1-(\tilde{u}-2)\end{pmatrix}\right]\sum_{l'_1<l'_2}\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}-\cdots\right)\\
&+ \left.\sum_{1\leqslant k_1<k_2<\cdots<k_{\tilde{u}}\leqslant s}\frac{\phi(n)}{q_{k_1}q_{k_2}\ldots q_{k_{\tilde{u}}}}\right).
\end{aligned}
$$

Assim, $T_1^{\tilde{u}}$ é dado por:

$$
(-1)^{\tilde{u}}h\left[\frac{1}{p^2}\sum_{u+u'=0}^{\tilde{u}-2}(-1)^{u+u'}\Gamma_{u,u'}+\frac{1}{p}\sum_{u+u'=0}^{\tilde{u}-1}(-1)^{u+u'}\Delta_{u,u'}+\sum_{u+u'=\tilde{u}}(-1)^{u+u'}\Omega_{u,u'}\right],
$$

onde

$$
\Omega_{u,u'}=\sum_{\substack{L\in\mathcal{P}(P),\ L'\in\mathcal{P}(P')\\ |L|=u \text{ e } |L'|=u'}}\frac{\phi(n)}{\prod_{l=1}^{u}q_l\prod_{l'=1}^{u'}q'_{l'}},
$$

$$
\Gamma_{u,u'}=\left[\sum_{d+d'=\tilde{u}-(u+u')}\begin{pmatrix} s_1-u \\ (s_1-u)-d\end{pmatrix}\begin{pmatrix} s_2-u' \\ (s_2-u')-d'\end{pmatrix}\right]\Omega_{u,u'}
$$

e,

$$
\Delta_{u,u'}=\left[\begin{pmatrix} s_1-u \\ s_1-(\tilde{u}-u')\end{pmatrix}\begin{pmatrix} s_2-u' \\ s_2-u'\end{pmatrix}+\begin{pmatrix} s_1-u \\ s_1-u\end{pmatrix}\begin{pmatrix} s_2-u' \\ s_2-(\tilde{u}-u)\end{pmatrix}\right]\Omega_{u,u'},
$$

sendo $\mathcal{P}(P)$ e $\mathcal{P}(P')$ o conjuntos de todos os subconjuntos de P e P', respectivamente.

Observe que para $\tilde{u} > s_1$, os termos $\phi(m_2)$, $\frac{\phi(m_2)}{q'_{l'}}$, $\frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}},\ldots,\frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}\cdots q'_{l'_{\tilde{u}-s_1-1}}}$, não aparecem multiplicando $\frac{1}{p^2}$ mas aparecem multiplicando $\frac{1}{p}$. Da mesma forma, para $\tilde{u} > s_2$, os termos $\phi(m_1)$, $\frac{\phi(m_1)}{q_l}$, $\frac{\phi(m_1)}{q_{l_1}q_{l_2}},\ldots,\frac{\phi(m_1)}{q_{l_1}q_{l_2}\cdots q_{l_{\tilde{u}-s_2-1}}}$ não aparecem multiplicando $\frac{1}{p^2}$ mas aparecem multiplicando $\frac{1}{p}$.

O termo T_1^s é dado por:

$$
\begin{aligned}
h\left[S'_{1,2\ldots,s}S^{0,0}_{1,2\ldots,s}\right] &= h\left[(-1)^s\frac{\phi(n)}{q_1q_2\ldots q_s}\left(D_P+(-1)^{s_1}\right)\left(D'_{P'}+(-1)^{s_2}\right)\right]\\
&= (-1)^s h\left(\frac{1}{p^2}\left[\phi(n)-\left(\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}+\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right)\right.\right.
\end{aligned}
$$

$$
\begin{aligned}
&+ \quad \left(\sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}} + \sum_{l\in P, l'\in P'} \frac{\phi(n)}{q_l q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} \right) - \cdots \\
&\cdots \quad + (-1)^{s-2} \sum_{l_1<l_2<\ldots<l_{s_1-1}, l'_1<l'_2<\ldots<l'_{s_2-1}} \frac{\phi(n)}{q_{l_1} q_{l_2} \cdots q_{l_{s_1-1}} q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} \Bigg] \\
&+ \quad \frac{1}{p} \Bigg[(-1)^{s_1} \phi(m_2) + (-1)^{s_1-1} \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + (-1)^{s_1-2} \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots \\
&\cdots \quad - \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} + (-1)^{s_2} \phi(m_1) + (-1)^{s_2-1} \sum_{l=1}^{s_1} \frac{\phi(m_1)}{q_l} \\
&+ \quad (-1)^{s_2-2} \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots - \sum_{l_1<l_2<\cdots<l_{s_1-1}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{s_1-1}}} \Bigg] + 1 \Bigg).
\end{aligned}
$$

Desse modo, considerando

$$
a_{u,d} = (-1)^d \begin{pmatrix} s_1 - u \\ (s_1 - u) - d \end{pmatrix} \text{ e } b_{u',d'} = (-1)^{d'} \begin{pmatrix} s_2 - u' \\ (s_2 - u') - d' \end{pmatrix},
$$

temos que o valor $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) = T_1^0 + T_1^1 + T_1^2 + \cdots + T_1^{s-1} + T_1^s$ é dado por:

$$
\begin{aligned}
& h \left(\left[\frac{\sum_{d=1}^{s_1} a_{0,d} + \sum_{d'=1}^{s_2} b_{0,d'}}{p} + \frac{\sum_{d=1}^{s_1} a_{0,d} \left(\sum_{d'=1}^{s_2} b_{0,d'} \right)}{p^2} \right] \phi(n) \right. \\
&+ \left[\frac{\sum_{d=1}^{s_1-1} a_{1,d} + \sum_{d'=1}^{s_2} b_{0,d'}}{p} + \frac{\sum_{d=1}^{s_1-1} a_{a_{1,d}} \left(\sum_{d'=1}^{s_2} b_{0,d'} \right)}{p^2} \right] \sum_{l=1}^{s_1} \frac{\phi(n)}{q_l} \\
&+ \left[\frac{\sum_{d=1}^{s_1} a_{0,d} + \sum_{d'=1}^{s_2-1} b_{1,d'}}{p} + \frac{\sum_{d=1}^{s_1} a_{a_{0,d}} \left(\sum_{d'=1}^{s_2-1} b_{1,d'} \right)}{p^2} \right] \sum_{l'=1}^{s_2} \frac{\phi(n)}{q'_{l'}} \\
&+ \left[\frac{\sum_{d=1}^{s_1-2} a_{2,d} + \sum_{d'=1}^{s_2} b_{0,d'}}{p} + \frac{\sum_{d=1}^{s_1-2} a_{2,d} \left(\sum_{d'=1}^{s_2} b_{0,d'} \right)}{p^2} \right] \sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}} \\
&+ \left. \left[\frac{\sum_{d=1}^{s_1-1} a_{1,d} + \sum_{d'=1}^{s_2-1} b_{1,d'}}{p} + \frac{\sum_{d=1}^{s_1-1} a_{1,d} \left(\sum_{d'=1}^{s_2-1} b_{1,d'} \right)}{p^2} \right] \sum_{l\in P, l'\in P'} \frac{\phi(n)}{q_l q'_{l'}} \right.
\end{aligned}
$$

$$+ \quad \left[\frac{\sum_{d=1}^{s_1} a_{0,d} + \sum_{d'=1}^{s_2-2} b_{2,d'}}{p} + \frac{\sum_{d=1}^{s_1} a_{0,d} \left(\sum_{d'=1}^{s_2-2} b_{2,d'} \right)}{p^2} \right] \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} + \cdots$$

$$\cdots \quad + \frac{\sum_{d'=1}^{s_2} b_{0,d'}}{p} \phi(m_2) + \frac{\sum_{d'=1}^{s_2-1} b_{1,d'}}{p} \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + \cdots + \frac{b_{s_2-1,1}}{p} \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{\prod_{t'=1}^{s_2-1} q'_{l'_{t'}}}$$

$$+ \quad \frac{\sum_{d=1}^{s_1} a_{0,d}}{p} \phi(m_1) + \frac{\sum_{d=1}^{s_1-1} a_{1,d}}{p} \sum_{l=1}^{s_1} \frac{\phi(m_1)}{q_l} + \cdots + \frac{a_{s_1-1,1}}{p} \sum_{l_1<l_2<\cdots<l_{s_1-1}} \frac{\phi(m_2)}{\prod_{t=1}^{s_1-1} q_{l_t}}$$

$$+ \quad \phi(n) + \sum_{k=1}^{s} \frac{\phi(n)}{q_k} + \sum_{k_1<k_2} \frac{\phi(n)}{q_{k_1} q_{k_2}} + \cdots + \sum_{k_1<k_2<\ldots<k_{s-1}} \frac{\phi(n)}{q_{k_1} q_{k_2} \cdots q_{k_{s-1}}} + 1.$$

Como

$$\sum_{d=1}^{s_1-u} a_{u,d} = -1 = \sum_{d'=1}^{s_2-u'} b_{u',d'},$$

segue pela Proposição 5.0.1, que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é igual a

$$h \Bigg[\left(-\frac{2}{p} + \frac{1}{p^2} \right) \left(\phi(n) + \sum_{k=1}^{s} \frac{\phi(n)}{q_k} + \sum_{k_1<k_2} \frac{\phi(n)}{q_{k_1} q_{k_2}} + \cdots + \sum_{k_1<k_2<\cdots<k_{s-1}} \frac{\phi(n)}{q_{k_1} q_{k_2} \cdots q_{k_{s-1}}} \right)$$

$$+ \quad \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_1) + \sum_{l=1}^{s_1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{s_1-1}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{s_1-1}}} \right)$$

$$+ \quad \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_2) + \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots + \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} \right)$$

$$+ \quad \phi(n) + \sum_{k=1}^{s} \frac{\phi(n)}{q_k} + \sum_{k_1<k_2} \frac{\phi(n)}{q_{k_1} q_{k_2}} + \cdots + \sum_{k_1<k_2<\ldots<k_{s-1}} \frac{\phi(n)}{q_{k_1} q_{k_2} \cdots q_{k_{s-1}}} + 1 \Bigg].$$

No entanto,

$$\begin{aligned} m_1 m_2 &= (q_1+1)(q_2+1)\cdots(q_{s_1}+1)(q'_1+1)(q'_2+1)\cdots(q'_{s_2}+1) \\ &= \phi(n) + \sum_{k=1}^{s} \frac{\phi(n)}{q_k} + \sum_{k_1<k_2} \frac{\phi(n)}{q_{k_1} q_{k_2}} + \cdots + \sum_{k_1<k_2<\cdots<k_{s-1}} \frac{\phi(n)}{q_{k_1} q_{k_2} \cdots q_{k_{s-1}}} + 1, \end{aligned}$$

$$\begin{aligned} m_1 &= (q_1+1)(q_2+1)\cdots(q_{s_1}+1) \\ &= \phi(m_1) + \sum_{l=1}^{s_1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{s_1-1}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{s_1-1}}} + 1, \end{aligned}$$

e

$$\begin{aligned} m_2 &= (q'_1+1)(q'_2+1)\cdots(q'_{s_2}+1) \\ &= \phi(m_2) + \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots + \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} + 1, \end{aligned}$$

Assim, o valor de $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é

$$\begin{aligned} & h\left[\frac{m_1m_2-1-(m_1-1)-(m_2-1)}{p^2}-\frac{2(m_1m_2-1)-(m_1-1)-(m_2-1)}{p}+n\right] \\ = \; & h\left[\frac{(m_1-1)(m_2-1)}{p^2}-\frac{m_1(m_2-1)+(m_1-1)m_2}{p}+n\right]. \end{aligned}$$

Portanto, como $Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2)=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$, segue que

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2)=\frac{(m_1-1)(m_2-1)}{p^2}-\frac{m_1(m_2-1)+(m_1-1)m_2}{p}+n.$$

□

Lema 5.0.5. *Com as notações do Lema 4.2.2, para $1\leqslant i,j\leqslant p-1$ temos que*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i)(t))=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i)(t))=\frac{(m_1-1)(m_2-1)}{p^2},$$

e

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_2^j)(t))=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_2^j)(t))=\frac{(m_1-1)(m_2-1)}{p^2}.$$

Demonstração. Basta observar que nesses casos, pelo Corolário 5.0.3, os termos que aparecem na soma de $T_2^0+T_2^1+\cdots+T_2^s$ são exatamente os que multiplicam o fator $\frac{1}{p^2}$ (coincidindo com os termos que aparecem multiplicando $\frac{1}{p^2}$ do lema anterior), pois $i\not\equiv j \pmod p$ e $i\not\equiv \tilde{t}j \pmod p$. □

Por fim, o terceiro lema auxiliar é:

Lema 5.0.6. *Com as notações do Lema 4.2.3 temos que:*

1. *Se $i\not\equiv -j \pmod p$ e $i\not\equiv -\tilde{t}j \pmod p$, então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{(m_1-1)(m_2-1)}{p^2}.$$

2. *Se $i\equiv -j \pmod p$, então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{(m_1-1)(m_2-1)}{p^2}-\frac{m_1(m_2-1)}{p}.$$

3. *Se $i\equiv -\tilde{t}j \pmod p$, então*

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=\frac{(m_1-1)(m_2-1)}{p^2}-\frac{(m_1-1)m_2}{p}.$$

Demonstração. Pela equação (4.1), temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i\circ\theta_2^j)(t))=T_3^0+T_3^1+T_3^2+\cdots+T_3^{s-1}+T_3^s,$$

onde

$$T_3^u=h\left[\sum_{k_1<k_2<\ldots<k_u}S'_{k_1,k_2,\ldots,k_u}S^{i,j}_{k_1,k_2,\ldots,k_u}\right].$$

Aqui vamos separar em três casos:

Caso 1: $i \not\equiv -j \ (mod\ p)$ e $i \not\equiv -\tilde{t}j \ (mod\ p)$. Note que este caso é parecido com o feito no Lema 5.0.5. Assim,

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{(m_1-1)(m_2-1)}{p^2}.$$

Caso 2: $i \equiv -j \ (mod\ p)$.

Observe inicialmente que $i \not\equiv -\tilde{t}j \ (mod\ p)$.

Para T_3^0, segue do Corolário 5.0.3 que $T_3^0 = hS_0'S_0^{i,j} = h.\phi(n).0 = 0$. Para o caso T_3^1 temos que,

$$\begin{aligned} T_3^1 &= h\left[\sum_{l=1}^{s_1} S_l' S_l^{i,j} + \sum_{l'=1}^{s_2} S_{l'}' S_{l'}^{i,j}\right] \\ &= h\left[\sum_{l=1}^{s_1} -\frac{\phi(n)}{q_l}.0 + \sum_{l'=1}^{s_2} -\frac{\phi(n)}{q_{l'}'}.\frac{q_{l'}'}{p}\right] \\ &= h\left[\sum_{l'=1}^{s_2} -\frac{\phi(n)}{p}\right] \\ &= -h\left[\frac{1}{p}\begin{pmatrix} s_2 \\ s_2-1 \end{pmatrix}\phi(n)\right]. \end{aligned}$$

Além disso, $S'_{l_1,l_2} = \frac{\phi(n)}{q_{l_1}q_{l_2}}$, $S'_{l_1,l_1'} = \frac{\phi(n)}{q_{l_1}q'_{l_1'}}$ e $S'_{l_1',l_2'} = \frac{\phi(n)}{q'_{l_1'}q'_{l_2'}}$, para $l_1, l_2 \in P$ e $l_1', l_2' \in P'$. Assim, pelo Corolário 5.0.3, a parcela T_3^2 é igual a:

$$\begin{aligned} & h\left[\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}0 + \sum_{l\in P,\ l'\in P'}\frac{\phi(n)}{q_l q_{l'}'}\left(\frac{q_l q_{l'}'}{p^2} - \frac{q_{l'}'}{p}\right) + \sum_{l_1'<l_2'}\frac{\phi(n)}{q_{l_1'}'q_{l_2'}'}\left(\frac{q_{l_1'}'q_{l_2'}'}{p} - \frac{q_{l_1'}' - q_{l_2'}'}{p}\right)\right] \\ = \ & h\left[\sum_{l\in P,\ l'\in P'}\frac{\phi(n)}{p^2} + \sum_{l_1'<l_2'}\frac{\phi(n)}{p} - \sum_{l_1'<l_2'}\left(\frac{\phi(n)}{pq'_{l_1'}} + \frac{\phi(n)}{pq'_{l_2'}}\right) - \sum_{l\in P, l'\in P'}\frac{\phi(n)}{pq_l}\right] \\ = \ & h\left[\frac{1}{p^2}s_1s_2\phi(n) + \frac{1}{p}\left(\begin{pmatrix} s_2 \\ s_2-2 \end{pmatrix}\phi(n) - (s_2-1)\sum_{l'=1}^{s_2}\frac{\phi(n)}{q_{l'}'} - s_2\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}\right)\right]. \end{aligned}$$

Logo,

$$\begin{aligned} T_3^2 &= h\left(\frac{1}{p^2}\left[\begin{pmatrix} s_1 \\ s_1-1 \end{pmatrix}\begin{pmatrix} s_2 \\ s_2-1 \end{pmatrix}\right]\phi(n)\right. \\ &+ \left.\frac{1}{p}\left[\begin{pmatrix} s_2 \\ s_2-2 \end{pmatrix}\phi(n) - \begin{pmatrix} s_2 \\ s_2-1 \end{pmatrix}\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l} - \begin{pmatrix} s_2-1 \\ s_2-2 \end{pmatrix}\sum_{l'=1}^{s_2}\frac{\phi(n)}{q_{l'}'}\right]\right). \end{aligned}$$

De forma análoga, o valor de T_3^3 é:

$$
\begin{aligned}
& h\left[\sum_{l_1<l_2<l_3} -\frac{\phi(n)}{q_{l_1}q_{l_2}q_{l_3}}0 + \sum_{l_1<l_2,\ l'\in P'} -\frac{\phi(n)}{q_{l_1}q_{l_2}q'_{l'}}\left(D_{l_1,l_2}+1\right)D'_{l'}\right.\\
+ & \sum_{l\in P,\ l'_1<l'_2} -\frac{\phi(n)}{q_l q'_{l'_1}q'_{l'_2}}\left(D_l-1\right)D'_{l'_1,l'_2} + \left.\sum_{l'_1<l'_2<l'_3} -\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}q'_{l'_3}}D'_{l'_1,l'_2,l'_3}\right]\\
= & h\left[\sum_{l_1<l_2,\ l'\in P'} -\frac{\phi(n)}{q_{l_1}q_{l_2}q'_{l'}}\left(\frac{q_{l_1}q_{l_2}q'_{l'}-q_{l_1}q_{l'}-q_{l_2}q_{l'}}{p^2}+\frac{q'_{l'}}{p}\right)\right.\\
+ & \sum_{l\in P,\ l'_1<l'_2} -\frac{\phi(n)}{q_l q'_{l'_1}q'_{l'_2}}\left(\frac{q_l q'_{l'_1}q'_{l'_2}-q_l q_{l'_1}-q_l q_{l'_2}}{p^2}+\frac{-q'_{l'_1}q'_{l'_2}+q'_{l'_1}+q'_{l'_2}}{p}\right)\\
& \left.+ \sum_{l'_1<l'_2<l'_3} -\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}q'_{l'_3}}\left(\frac{q'_{l'_1}q'_{l_2}q'_{l'_3}-q'_{l'_1}q'_{l'_2}-q'_{l'_1}q'_{l'_3}-q'_{l'_2}q'_{l'_3}+q'_{l'_1}+q'_{l'_2}+q'_{l'_3}}{p}\right)\right].
\end{aligned}
$$

Ou seja,

$$
\begin{aligned}
T_3^3 = & -h\left[\frac{1}{p^2}\left(\left[\begin{pmatrix} s_1 \\ s_1-1\end{pmatrix}\begin{pmatrix} s_2 \\ s_2-2\end{pmatrix}+\begin{pmatrix} s_1 \\ s_1-2\end{pmatrix}\begin{pmatrix} s_2 \\ s_2-1\end{pmatrix}\right]\phi(n)\right.\right.\\
& \left.\left.-\begin{pmatrix} s_1-1 \\ s_1-2\end{pmatrix}\begin{pmatrix} s_2 \\ s_2-1\end{pmatrix}\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}+\begin{pmatrix} s_1 \\ s_1-1\end{pmatrix}\begin{pmatrix} s_2-1 \\ s_2-2\end{pmatrix}\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right)\right.\\
& +\frac{1}{p}\left[\begin{pmatrix} s_2 \\ s_2-3\end{pmatrix}\phi(n)-\begin{pmatrix} s_2 \\ s_2-2\end{pmatrix}\sum_{l=1}^{s_1}\frac{\phi(n)}{q_l}-\begin{pmatrix} s_2-1 \\ s_2-3\end{pmatrix}\sum_{l'=1}^{s_2}\frac{\phi(n)}{q'_{l'}}\right.\\
& \left.\left.+\begin{pmatrix} s_2 \\ s_2-1\end{pmatrix}\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}+\begin{pmatrix} s_2-1 \\ s_2-2\end{pmatrix}\sum_{l\in P<l'\in P'}\frac{\phi(n)}{q_l q'_{l'}}+\begin{pmatrix} s_2-2 \\ s_2-3\end{pmatrix}\sum_{l'_1<l'_2}\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}\right].
\end{aligned}
$$

Para generalizar esse processo, analisando quando $0 \leqslant \tilde{u} \leqslant s-1$ coordenadas de $-\alpha r_1^{-i}r_2^{-j}$ coincidem com elementos de H, sejam $0 \leqslant u \leqslant s_1$, $0 \leqslant u' \leqslant s_2$, $d, d' \geqslant 1$ e

$$
\begin{pmatrix} s_i \\ s_i-c\end{pmatrix}=0,
$$

se $c \geqslant s_i$, para $i=1,2$. Então,

$$
T_3^{\tilde{u}} = (-1)^{\tilde{u}}h\left[\frac{1}{p^2}\sum_{u+u'=0}^{\tilde{u}-2}(-1)^{u+u'}\Gamma_{u,u'}+\frac{1}{p}\sum_{u+u'=0}^{\tilde{u}-1}(-1)^{u+u'}\Delta^j_{u,u'}\right],
$$

onde

$$
\Gamma_{u,u'}=\left[\sum_{d+d'=\tilde{u}-(u+u')}\begin{pmatrix} s_1-u \\ (s_1-u)-d\end{pmatrix}\begin{pmatrix} s_2-u' \\ (s_2-u')-d'\end{pmatrix}\right]\Omega_{u,u'},
$$

$$
\Delta^j_{u,u'}=\begin{pmatrix} s_2-u' \\ s_2-(\tilde{u}-u)\end{pmatrix}\Omega_{u,u'},
$$

e,

$$\Omega_{u,u'} = \sum_{\substack{L\in\mathcal{P}(P),\ L'\in\mathcal{P}(P') \\ |L|=u \text{ e } |L'|=u'}} \frac{\phi(n)}{\prod_{k=1}^{u} q_{l_k} \prod_{k'=1}^{u'} q'_{l'_{k'}}},$$

sendo $\mathcal{P}(P)$ e $\mathcal{P}(P')$ o conjuntos de todos os subconjuntos de P e P', respectivamente.

Observe que para $\tilde{u} > s_1$, os termos $\phi(m_2)$, $\frac{\phi(m_2)}{q'_{l'}}$, $\frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}}, \ldots,$ $\frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{\tilde{u}-s_1-1}}}$, não aparecem multiplicando $\frac{1}{p^2}$ mas aparecem multiplicando $\frac{1}{p}$. Já para $\tilde{u} > s_2$, os termos $\phi(m_1)$, $\frac{\phi(m_1)}{q'_{l'}}$, $\frac{\phi(m_1)}{q'_{l'_1} q'_{l'_2}}, \ldots,$ $\frac{\phi(m_1)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{\tilde{u}-s_1-1}}}$, não aparecem multiplicando $\frac{1}{p^2}$ nem $\frac{1}{p}$.

Agora, para o índice s temos que, $T_3^s = h\left[(-1)^s \frac{\phi(n)}{q_1 q_2 \ldots q_s} \left(D_P + (-1)^{s_1} D'_{P'}\right)\right]$, ou seja,

$$\begin{aligned}
T_3^s &= (-1)^s h \left(\frac{1}{p^2} \left[\phi(n) - \left(\sum_{l=1}^{s_1} \frac{\phi(n)}{q_l} + \sum_{l'=1}^{s_2} \frac{\phi(n)}{q'_{l'}} \right) \right.\right. \\
&+ \left(\sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}} + \sum_{l\in P, l'\in P'} \frac{\phi(n)}{q_l q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} \right) - \cdots \\
&\cdots + (-1)^{s-2} \left.\left. \sum_{l_1<l_2<\ldots<l_{s_1-1}, l'_1<l'_2<\ldots<l'_{s_2-1}} \frac{\phi(n)}{q_{l_1} q_{l_2} \ldots q_{l_{s_1-1}} q'_{l'_1} q'_{l'_2} \ldots q'_{l'_{s_2-1}}} \right] \right. \\
&+ \frac{1}{p} \left((-1)^{s_1} \phi(m_2) + (-1)^{s_1-1} \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + (-1)^{s_1-2} \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots \right. \\
&\cdots - \left.\left. \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} \right) \right].
\end{aligned}$$

Somando todos os termos, obtemos pela Proposição 5.0.1 que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)/h$ é:

$$\begin{aligned}
&\left(-\frac{1}{p} + \frac{1}{p^2}\right) \left(\phi(n) + \sum_{k=1}^{s} \frac{\phi(n)}{q_k} + \sum_{k_1<k_2} \frac{\phi(n)}{q_{k_1} q_{k_2}} + \cdots + \sum_{k_1<k_2<\cdots<k_{s-1}} \frac{\phi(n)}{q_{k_1} q_{k_2} \cdots q_{k_{s-1}}} \right) \\
+ &\left(\frac{1}{p} - \frac{1}{p^2}\right) \left(\phi(m_1) + \sum_{l=1}^{s_1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{s_1-1}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{s_1-1}}} \right) \\
- &\frac{1}{p^2} \left(\phi(m_2) + \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots + \sum_{l'_1<l'_2<\cdots<l'_{s_2-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s_2-1}}} \right).
\end{aligned}$$

Assim,

$$\begin{aligned}
Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) &= h\left[\frac{m_1 m_2 - 1 - (m_1 - 1) - (m_2 - 1)}{p^2} - \frac{(m_1 m_2 - 1) - (m_1 - 1)}{p} \right] \\
&= h\left[\frac{(m_1 - 1)(m_2 - 1)}{p^2} - \frac{m_1 (m_2 - 1)}{p} \right].
\end{aligned}$$

Portanto, neste caso

$$Tr_{\mathbb{L}_1\mathbb{L}_2/\mathbb{Q}}(t^2) = \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) = \frac{(m_1-1)(m_2-1)}{p^2} - \frac{m_1(m_2-1)}{p}.$$

Caso 3: $i \equiv -\tilde{t}j \ (mod\ p)$.
Segue de forma análoga ao **Caso 2**. □

Apêndice B: Caso mdc$(m_1, m_2) = q$, com q primo

Para esta capítulo iremos considerar p-extensões abelianas não ramificadas $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ de condutores $m_1 = p_1 p_2 \dots p_k$ e $m_2 = p_k p_{k+1} \dots p_s$, respectivamente, com $p_1, p_2, \dots, p_s$ inteiros primos distintos (em particular, mdc$(m_1, m_2) = p_k$) e $\mathbb{K}_{m_3}$ a única p-extensão abeliana não ramificada de condutor

$$m_3 = \frac{m_1 m_2}{p_k^2} = p_1 p_2 \dots p_{k-1} p_{k+1} \dots p_s,$$

contida em $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Sejam $n = m_1 m_2 / p_k$ e H o subgrupo de $\mathbb{Z}_n^*$ que é isomorfo a $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2})$, ou seja, H é o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Considere ainda os subgrupos

$$J_1 \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}), J_2 \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_2}), J_3 \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_3}) \leqslant \mathbb{Z}_n^*,$$

conforme a Figura 5.1:

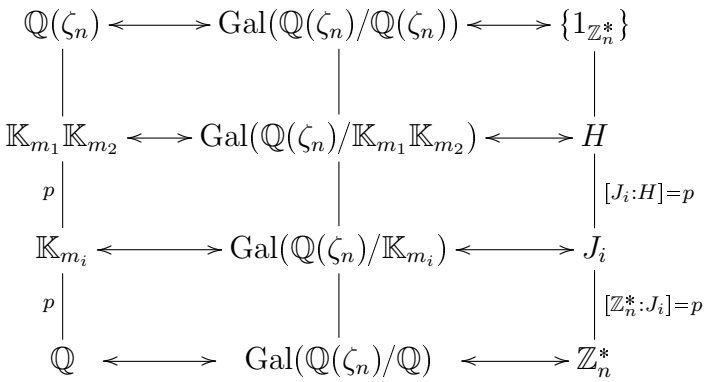

Figura 5.1: Correspondência de Galois de J_1, J_2 e J_3.
Fonte: Próprio autor

O próximo lema é um resultado semelhante ao Lema 4.1.1, apresentado no capítulo 4, o qual teve o propósito de analisar o núcleo das projeções canônicas sobre o grupo H que fixava o compósito $\mathbb{L}_1\mathbb{L}_2$. Observe que para o caso estudado neste capítulo, a diferença é que o grupo $\mathbb{Z}_n^*$ possui três subgrupos não triviais (a saber, J_1, J_2 e J_3) contendo o subgrupo H (que aqui fixa $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$) fixando p-extensões de condutores menores que n, ou equivalentemente, o compósito $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ contem três p-extensões abelianas não ramificadas de condutor não cheio ($\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$).

Lema 5.0.7. *Sejam $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1 p_2 \dots p_k$ e $m_2 = p_k p_{k+1} \dots p_s$, respectivamente, com $mdc(m_1, m_2) = p_k$, de forma que exista uma (e portanto a única) p-extensão abeliana não ramificada*

$$\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2},$$

com $cond(\mathbb{K}_{m_3}) = \frac{n}{p_k}$, sendo $n = \frac{m_1 m_2}{p_k}$. Tome $X = \{1, 2, \dots, s\}$, $Y = \{y_i\}_{i=1}^{u} \subsetneq X$, com

$$1 \leqslant y_1 < y_2 < \ldots < y_u \leqslant s,$$

e a projeção canônica

$$\begin{array}{rccc} \Pi_Y : & H & \longrightarrow & Z_Y = \mathbb{Z}^*_{p_{y_1}} \times \mathbb{Z}^*_{p_{y_2}} \times \cdots \times \mathbb{Z}^*_{p_{y_u}} \\ & \alpha = (\alpha_1, \alpha_2, \dots, \alpha_s) & \longmapsto & \Pi_Y(\alpha) = (\alpha_{y_1}, \alpha_{y_2}, \dots, \alpha_{y_u}) \end{array}.$$

Então,

$$\Pi_Y(H) = \begin{cases} Z_Y, & se\ P_1, P_2, P_3 \nsubseteq Y \\ \tilde{J}_i \times Z_{Y \setminus P_i} & se\ P_i \subseteq Y \end{cases},$$

para $i = 1, 2, 3$, onde $P_1 = \{1, 2, \dots, k\}$, $P_2 = \{k, k+1, \dots, s\}$, $P_3 = X \setminus \{k\}$ e $\tilde{J}_i$ é o subgrupo de $\mathbb{Z}^*_{m_i}$ isomorfo a $Gal(\mathbb{Q}(\zeta_{m_i})/\mathbb{K}_{m_i})$.

Demonstração. Note que, se $i \neq j$, então $P_i \cup P_j = X$, e assim $P_i \cup P_j \nsubseteq Y$.

Se $P_i \nsubseteq Y$, para $i = 1, 2, 3$ então $\Pi_Y(H) = Z_Y$, pois caso contrário,

$$H \leqslant \Pi_Y(H) \times Z_{X \setminus Y} \leqslant \mathbb{Z}^*_n,$$

com $[\mathbb{Z}^*_n : H] = p^2$, logo $[\mathbb{Z}^*_n : \Pi_Y(H) \times Z_{X \setminus Y}] = p$ ou p^2. Supondo que

$$[\mathbb{Z}^*_n : \Pi_Y(H) \times Z_{X \setminus Y}] = p,$$

temos que $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ possuí uma p-extensão abeliana não ramificada de condutor m, com m dividindo $p_{y_1} p_{y_2} \dots p_{y_u}$ e como $P_i \nsubseteq Y$, então $m \neq n$ e $m \neq m_i$, para $i = 1, 2, 3$. O que é um absurdo.

Supondo que

$$[\mathbb{Z}^*_n : \Pi_Y(H) \times Z_{X \setminus Y}] = p^2,$$

então $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ possuí condutor $m < n$, absurdo. Dessa forma, $\Pi_Y(H) = Z_Y$.

Se $P_i \subseteq Y$, para algum $i = 1, 2, 3$, então $P_j \nsubseteq Y \setminus P_i$, para $j = 1, 2, 3$. Logo, pelo argumento anterior, segue que $\Pi_{Y \setminus P_i}(H) = Z_{Y \setminus P_i}$. De forma análoga ao feito no Lema 4.1.1, obtemos que $\Pi_{P_i}(H) = \tilde{J}_i$, assim $\Pi_Y(H) = \tilde{J}_i \times Z_{Y \setminus P_i}$. □

Seguem diretamente do lema anterior:

Corolário 5.0.8. *Com as notações do lema anterior:*

$$A_{X \setminus Y} = |\ker \Pi_Y| = \begin{cases} \dfrac{\prod\limits_{j \in X \setminus Y} (p_j - 1)}{p^2}, & se\ P_1, P_2, P_3 \nsubseteq Y \\ \dfrac{\prod\limits_{j \in X \setminus Y} (p_j - 1)}{p}, & se\ P_i \subseteq Y \end{cases},$$

para algum $i = 1, 2, 3$.

Corolário 5.0.9. *Dados os grupos J_1, J_2, J_3 e $\tilde{J}_1, \tilde{J}_2, \tilde{J}_3$, como anteriormente definidos. Então,*

1. $J_1 = \Pi_{P_1}(H) \times \Pi_{X\setminus P_1}(H) = \tilde{J}_1 \times Z_{X\setminus P_1} = \tilde{J}_1 \times \mathbb{Z}_{p_{k+1}} \times \mathbb{Z}_{p_{k+2}} \times \ldots \times \mathbb{Z}_{p_s}$;
2. $J_2 = \Pi_{P_2}(H) \times \Pi_{X\setminus P_2}(H) = \tilde{J}_2 \times Z_{X\setminus P_2} = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_{k-1}} \times \tilde{J}_2$;
3. $J_3 = \Pi_{P_3}(H) \times \Pi_{X\setminus P_3}(H) = \tilde{J}_3 \times Z_{X\setminus P_3} = \tilde{J}_3 \times \mathbb{Z}_{p_k}$.

Além disso, $H = J_1 \cap J_2 = J_1 \cap J_3 = J_2 \cap J_3$.

Considere $G = \text{Gal}(\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}) = \left\{\theta_1^i \circ \theta_2^j\right\}_{i,j=0,1\ldots p-1}$, onde $\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $\text{Gal}(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$ e $\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $\text{Gal}(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$. Podemos considerar r_1 e r_2 em $\mathbb{Z}_n^*$ tal que seus correspondentes em $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ são σ_{r_1} e σ_{r_2}, respectivamente, sendo $\sigma_{r_i}|_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}} = \theta_i$, para $i = 1, 2$.

Vejamos algumas relações entre os elementos r_1^i e r_2^j com os grupos J_1, J_2 e J_3, para $1 \leqslant i, j \leqslant p-1$. Inicialmente, observe que r_1 fixa $\mathbb{K}_{m_1}$ e restrito a $\mathbb{K}_{m_2}$ gera $\text{Gal}(\mathbb{K}_{m_2}/\mathbb{Q})$, ou seja, $r_1 \in J_1$ e $r_1 \notin J_2, J_3$. De forma análoga, r_2 fixa $\mathbb{K}_{m_2}$ e restrito a $\mathbb{K}_{m_1}$ gera $\text{Gal}(\mathbb{K}_{m_1}/\mathbb{Q})$, ou seja, $r_2 \in J_2$ e $r_2 \notin J_1, J_3$. Assim, pelo Corolário 5.0.9, temos que para todo $i = 1, 2, \ldots, p-1$:

1. $(1, 1, \ldots, 1, \gamma_{k+1}^i, \gamma_{k+2}^i, \ldots, \gamma_s^i) \in J_1$, para cada combinação γ_t valendo r_{1_t} ou 1, com $k+1 \leqslant t \leqslant s$;
2. $(\gamma_1^i, \gamma_2^i, \ldots, \gamma_{k-1}^i, 1, 1, \ldots, 1) \in J_2$, para cada combinação γ_t valendo r_{1_t} ou 1, com $1 \leqslant t \leqslant k-1$;
3. $(1, 1, \ldots, 1, r_{1_k}^i, 1, 1, \ldots, 1) \in J_3$.

Além disso, como $r_1 \in J_1$ e $r_1 \notin J_2, J_3$, segue que:

4. $(r_{1_1}^i, r_{1_2}^i, \ldots, r_{1_k}^i, \gamma_{k+1}^i, \gamma_{k+2}^i, \ldots, \gamma_s^i) \in J_1$, para cada combinação γ_t valendo r_{1_t} ou 1, com $k+1 \leqslant t \leqslant s$;
5. $(\gamma_1^i, \gamma_2^i, \ldots, \gamma_{k-1}^i, r_{1_k}^i, r_{1_{k+1}}^i, \ldots, r_{1_s}^i) \notin J_2$, para cada combinação γ_t valendo r_{1_t} ou 1, com $1 \leqslant t \leqslant k-1$;
6. $(r_{1_1}^i, r_{1_2}^i, \ldots, r_{1_k}^i, 1, r_{1_{k+1}}^i, r_{1_{k+2}}^i, \ldots, r_{1_s}^i) \notin J_3$.

Relacionando agora os produtos $r_1^i r_2^j$ com J_1, J_2 e J_3, temos diretamente que $r_1^i r_2^j \in J_1$, se e somente se, $j = 0$ e $r_1^i r_2^j \in J_2$, se e somente se, $i = 0$. Já para $r_1^i r_2^j \in J_3$, temos que:

Afirmação: Para cada $i = 1, 2, \ldots, p-1$ existe um único $j_i \in \{1, 2, \ldots, p-1\}$ tal que $r_1^i r_2^{j_i} \in J_3$. Além disso, $j_i = i.j_1$.

Com efeito, dados $0 \leqslant j, v \leqslant p-1$ segue que, $r_1 r_2^j J_3 = r_1 r_2^v J_3$ se, e somente se, $r_2^{j-v} \in J_3$, o que ocorre se, e somente se, $j = v$. Assim, $\bigcup_{j=0}^{p-1} r_1 r_2^j J_3$ é uma união disjunta. Logo,

$$\left|\bigcup_{j=0}^{p-1} r_1 r_2^j J_3\right| = \sum_{j=0}^{p-1} |J_3| = p\frac{\phi(n)}{p} = \phi(n) = |\mathbb{Z}_n^*|.$$

Ou seja,

$$\bigcup_{j=0}^{p-1} r_1 r_2^j J_3 = \mathbb{Z}_n^*.$$

Logo, existe $j_1 \in \{1, 2, \ldots, p-1\}$ tal que $r_1 r_2^{j_1} \in J_3$ (note que $r_1 \notin J_3$, assim não pode ocorrer de $j_1 = 0$).

Por fim, como $r_1 r_2^{j_1} \in J_3$, então $(r_1 r_2^{j_1})^i = r_1^i r_2^{j_1 . i} \in J_3$. A unicidade do par $(i, j_i) = (i, i.j_1)$ é imediata.

Observação 5.0.10. Note que, tomando $\theta_2' = \theta_2^{j_1}$, temos que

$$\mathrm{Gal}(\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}) = \{\theta_1^i \circ (\theta_2')^j\}_{i,j=0}^{p-1},$$

com $r_1 r_2'$ fixando $\mathbb{K}_{m_3}$, onde $r_2' = r_2^{j_1}$.

A partir deste ponto em todo o resto deste capítulo estaremos sempre exigindo que a base $\mathrm{Gal}(\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i,j=0}^{p-1}$, também satisfaça a Observação 5.0.10 ($r_1 r_2 \in J_3$), isto é, o índice j_1, como na **Afirmação** é $j_1 = 1$.

O próximo resultado é uma adaptação de um lema apresentado na tese [7], o qual nos será útil a seguir. Como sua prova pode ser feita de forma idêntica a encontrada na referência, ela será aqui omitida.

Lema 5.0.11 ([7], pág. 35)**.** *Sejam $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{s_i}) \in \tilde{J}_i \leqslant Z_{P_i}$, $1 \leqslant q < s_i = \#(P_i)$ e a projeção*

$$\begin{array}{rccc} \Pi: & \tilde{J}_i & \longrightarrow & \mathbb{Z}_{p_{j_1}}^* \times \mathbb{Z}_{p_{j_2}}^* \times \cdots \times \mathbb{Z}_{p_{j_q}}^* \\ & (\alpha_1, \alpha_2, \ldots, \alpha_{s_i}) & \longmapsto & \Pi(\alpha) = (\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_q}) \end{array},$$

com $1 \leqslant j_1 < j_2 < \ldots < j_q \leqslant s_i$. Então,

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

onde $1 \leqslant i_1 < i_2 < \ldots < i_r \leqslant s_i$ são as coordenadas de α distintas dos $j_1, j_2, \ldots, j_q$.

Observação 5.0.12. Para facilitar as contas, para cada $\tilde{J}_i$, com $i = 1, 2, 3$ e Π como no lema anterior, consideraremos

$$A_{i_1, i_2, \ldots, i_r}^{\tilde{J}_i} := |\ker \Pi| = \frac{q_{i_1} q_{i_1} \cdots q_{i_r}}{p}.$$

Neste ponto queremos estabelecer um resultado semelhante ao Corolário 5.0.3 apresentado no capítulo anterior, readequando-o ao caso agora estudado. Dados os conjuntos $P_1' = P_1 \backslash \{k\}$, $P_2' = P_2 \backslash \{k\}$, $L_1 = \{l_1, l_2, \ldots, l_{\tilde{t}_1}\} \subseteq P_1'$ e $L_2 = \{l_1', l_2', \ldots, l_{\tilde{t}_2}'\} \subseteq P_2'$, com

$$1 \leqslant l_1 < l_2 < \ldots < l_{\tilde{t}_1} < k < l_1' < l_2' < \ldots < l_{\tilde{t}_2} \leqslant s,$$

considere $Y_1' = \{y_1, y_2, \ldots, y_{t_1}\} = P_1' \backslash L_1'$, $Y_2' = \{y_1', y_2', \ldots, y_{t_2}'\} = P_2' \backslash L_2'$, com

$$1 \leqslant y_1 < y_2 < \ldots < y_{t_1} < k < y_1', y_2' < \ldots < y_{t_2}' \leqslant s.$$

Note que, $t_1 + \tilde{t}_1 = k - 1$ e $t_2 + \tilde{t}_2 = s - k$. Podemos ainda destacar os seguintes conjuntos: $Y = Y_1 \cup Y_2$, $L = L_1 \cup L_2$ e $X = \{1, 2, \ldots, s\}$.

Dado $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_s) \in H$, queremos determinar os números

$$S_L^{i,j} := S_{l_1, l_2, \ldots, l_{\tilde{t}_1}, l_1', l_2', \ldots, l_{\tilde{t}_2}'}^{i,j} \text{ e } S_{L \bigcup \{k\}}^{i,j} := S_{l_1, l_2, \ldots, l_{\tilde{t}_1}, k, l_1', l_2', \ldots, l_{\tilde{t}_2}'}^{i,j},$$

da quantidade de elementos $\beta \in H$ de forma que $r_1^i r_2^j \beta$ coincide com $-\alpha$ exatamente nas coordenadas de $X \backslash L = Y \bigcup \{k\}$ e $X \backslash (L \bigcup \{k\}) = Y$, respectivamente. Como a coordenada k é onde temos uma alteração nas contagens ela necessita ter uma atenção extra, por isso a divisão da contagem de $S^{i,j}$.

Proposição 5.0.13. *Com as notações acima estalecidas e considerando*

$$D_{L_1} := D_{l_1,l_2,\ldots,l_{\tilde{t}_1}} = \sum_{d=1}^{\tilde{t}_1} \left[(-1)^{(\tilde{t}_1-d)} \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} \frac{\prod_{t=t_1}^{t_d} q_{l_t}}{p} \right],$$

$$D_{L_2} := D_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} = \sum_{d'=1}^{\tilde{t}_2} \left[(-1)^{(\tilde{t}_2-d')} \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} \frac{\prod_{t'=t'_1}^{t'_{d'}} q'_{l'_{t'}}}{p} \right],$$

temos que:

1. $$S_0^{i,j} = \begin{cases} 1, & se\ i = 0\ e\ j = 0; \\ 0, & se\ i \neq 0\ ou\ j \neq 0; \end{cases}$$

2. $$S_k^{i,j} = \begin{cases} \frac{q_k}{p} - 1, & se\ i = 0\ e\ j = 0; \\ 0, & se\ i = 0\ e\ j \neq 0,\ ou\ se\ i \neq 0\ e\ j = 0; \\ 0, & se\ i \neq 0\ e\ j \neq 0, com\ i \neq j; \\ \frac{q_k}{p}, & se\ i \neq 0\ e\ j \neq 0, com\ i = j; \end{cases}$$

3. $$S_{L_1}^{i,j} = \begin{cases} D_{L_1} + (-1)^{\tilde{t}_1}, & se\ i = 0\ e\ j = 0; \\ 0, & se\ i \neq 0\ e\ j = 0; \\ D_{L_1}, & se\ i = 0\ e\ j \neq 0; \\ 0, & se\ i \neq 0\ e\ j \neq 0; \end{cases}$$

4. $$S_{L_1\cup\{k\}}^{i,j} = \begin{cases} \left(D_{L_1} + (-1)^{\tilde{t}_1}\right)\left(\frac{q_k}{p} - 1\right), & se\ i = 0\ e\ j = 0; \\ D_{L_1}\frac{q_k}{p}, & se\ i \neq 0\ e\ j = 0; \\ D_{L_1}\left(\frac{q_k}{p} - 1\right), & se\ i = 0\ e\ j \neq 0; \\ D_{L_1}\frac{q_k}{p}, & se\ i \neq 0\ e\ j \neq 0,\ com\ i \neq j; \\ \left(D_{L_1} + (-1)^{\tilde{t}_1}\right)\frac{q_k}{p}, & se\ i \neq 0\ e\ j \neq 0,\ com\ i = j; \end{cases}$$

5. $$S_{L_2}^{i,j} = \begin{cases} D_{L_2} + (-1)^{\tilde{t}_2}, & se\ i = 0\ e\ j = 0; \\ D_{L_2}, & se\ i \neq 0\ e\ j = 0; \\ 0, & se\ i = 0\ e\ j \neq 0; \\ 0, & se\ i \neq 0\ e\ j \neq 0 \end{cases}$$

6.

$$S^{i,j}_{L_2\cup\{k\}} = \begin{cases} \left(D_{L_2} + (-1)^{\tilde{t}_2}\right)\left(\dfrac{q_k}{p} - 1\right), & se\ i = 0\ e\ j = 0; \\ D_{L_2}\left(\dfrac{q_k}{p} - 1\right), & se\ i \neq 0\ e\ j = 0; \\ D_{L_2}\dfrac{q_k}{p}, & se\ i = 0\ e\ j \neq 0; \\ D_{L_2}\dfrac{q_k}{p}, & se\ i \neq 0\ e\ j \neq 0,\ com\ i \neq j; \\ \left(D_{L_2} + (-1)^{\tilde{t}_2}\right)\dfrac{q_k}{p}, & se\ i \neq 0\ e\ j \neq 0,\ com\ i = j; \end{cases}$$

7.

$$S^{i,j}_{L_1\cup L_2} = \begin{cases} \left(D_{L_1} + (-1)^{\tilde{t}_1}\right)\left(D_{L_2} + (-1)^{\tilde{t}_2}\right), & se\ i = 0\ e\ j = 0; \\ \left(D_{L_1} + (-1)^{\tilde{t}_1}\right)D_{L_2}, & se\ i \neq 0\ e\ j = 0; \\ D_{L_1}\left(D_{L_2} + (-1)^{\tilde{t}_2}\right), & se\ i = 0\ e\ j \neq 0; \\ D_{L_1}D_{L_2}, & se\ i \neq 0\ e\ j \neq 0; \end{cases}$$

8. Para $S^{i,j}_{L_1\cup\{k\}\cup L_2}$*, segue que*

(a) $S^{0,0}_{L_1\cup\{k\}\cup L_2}$ *é dado por:*

$$\left(\frac{q_k}{p} - 1\right)\left(D_{L_1} + (-1)^{\tilde{t}_1}\right)\left(D_{L_2} + (-1)^{\tilde{t}_2}\right) - D_{L_1}D_{L_2}\frac{q_k}{p} + D_{L_1}D_{L_2}q_k;$$

(b) $S^{i,0}_{L_1\cup\{k\}\cup L_2}$*, com* $i \neq 0$ *é dado por:*

$$\left(\frac{q_k}{p} - 1\right)\left(D_{L_1} + (-1)^{\tilde{t}_1}\right)D_{L_2} - D_{L_1}D_{L_2}\frac{q_k}{p} + D_{L_1}D_{L_2}q_k + (-1)^{\tilde{t}_2}D_{L_1}\frac{q_k}{p};$$

(c) $S^{0,j}_{L_1\cup\{k\}\cup L_2}$*, com* $j \neq 0$ *é dado por:*

$$\left(\frac{q_k}{p} - 1\right)D_{L_1}\left(D_{L_2} + (-1)^{\tilde{t}_2}\right) - D_{L_1}D_{L_2}\frac{q_k}{p} + D_{L_1}D_{L_2}q_k + (-1)^{\tilde{t}_1}D_{L_2}\frac{q_k}{p};$$

(d) $S^{i,j}_{L_1\cup\{k\}\cup L_2}$*, com* $1 \leqslant i, j \leqslant p-1$ *e* $i \neq j$ *é dado por*

$$D_{L_1}D_{L_2}q_k - D_{L_1}D_{L_2} + (-1)^{\tilde{t}_2}D_{L_1}\frac{q_k}{p} + (-1)^{\tilde{t}_1}D_{L_2}\frac{q_k}{p};$$

(e) $S^{i,j}_{L_1\cup\{k\}\cup L_2}$*, com* $1 \leqslant i, j \leqslant p-1$ *e* $i = j$ *é dado por*

$$D_{L_1}D_{L_2}q_k - D_{L_1}D_{L_2} + (-1)^{\tilde{t}_2}D_{L_1}\frac{q_k}{p} + (-1)^{\tilde{t}_1}D_{L_2}\frac{q_k}{p} + (-1)^{\tilde{t}_1+\tilde{t}_2}\frac{q_k}{p}.$$

Demonstração. O caso $S^{0,0}$, segue utilizando o Teorema 5.0.2. Faremos uma abordagem mais explanada para os casos $S^{i,0}$ e $S^{i,j}$, com $1 \leqslant i, j \leqslant p-1$. O caso $S^{0,j}$ pode ser obtido de forma análogo ao caso $S^{i,0}$.

Caso $S^{i,0}$, com $1 \leqslant i \leqslant p-1$: Desde que $r_1^i \notin H$, para $1 \leqslant i \leqslant p-1$, segue que

$$J_1 = \dot{\bigcup}_{i=0}^{p-1} r_1^i H,$$

ou seja, $r_1^i H \bigcap H = \varnothing$, logo $r_1^i \beta \neq -\alpha$, para todo elemento $\beta \in H$, isto é, $S_0^{i,0} = 0$.

Para analisar o valor de $S_{L_1}^{i,0}$, veja que $\Pi_{P_2}(\pm\alpha) = \pm(\alpha_k, \alpha_{k+1}, \ldots, \alpha_s) \in \tilde{J}_2$ e assim,

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}, -\alpha_k, -\alpha_{k+1}, \ldots, -\alpha_s) \in J_2, \ \forall \beta_t \in \mathbb{Z}_{p_t}^*, \text{ com } 1 \leqslant t \leqslant k-1.$$

Logo, se $\beta = (\beta_1, \beta_2, \ldots, \beta_s) \in \mathbb{Z}_n^*$ é tal que $r_1^i \beta$ coincide com $-\alpha$ ao menos nas últimas $s-k+1$ coordenadas (ou seja, coincide ao menos em todo o conjunto P_2), então $r_1^i \beta \in J_2$, como $r_1^{-i} \notin J_2$, então $\beta = r_1^{-i} r_1^i \beta \notin J_2$, em particular, $\beta \notin H$. Ou seja,

$$S_{L_1}^{i,0} = S_{l_1, l_2, \ldots, l_{\tilde{t}_1}}^{i,0} = 0. \tag{5.3}$$

Como $\Pi_{P_1' \cup P_2'}(\pm\alpha) = \Pi_{P_3}(\pm\alpha) \in \tilde{J}_3$, então

$$(-\alpha_1, -\alpha_2, \ldots, -\alpha_{k-1}, \theta_k, -\alpha_{k+1}, \ldots, -\alpha_s) \in J_3, \ \forall \theta_k \in \mathbb{Z}_{p_k}^*.$$

Assim, se $\beta \in \mathbb{Z}_n^*$ é tal que $r_1^i \beta = (-\alpha_1, -\alpha_2, \ldots, -\alpha_{k-1}, r_{1_k}^i \beta_k, -\alpha_{k+1}, \ldots, -\alpha_s) \in J_3$, então $\beta = r_1^{-i} r_1^i \beta \notin J_3$, uma vez que $r_1^{-i} \notin J_3$, em particular, $\beta \notin H$. Logo,

$$S_k^{i,0} = 0. \tag{5.4}$$

Queremos determinar agora o valor de $S_{L_1 \cup \{k\}}^{i,0}$. Se $L_1 = \{l\}$, tome $\beta_t = -r_{1_t}^{-i} \alpha_t$, para todo $t \in (P_1' \backslash \{l\}) \cup P_2' = X \backslash \{l, k\}$, logo

$$(\beta_{k+1}, \beta_{k+2}, \ldots, \beta_s) \in Z_{P_2'} = \Pi_{P_2'}(H),$$

e assim, pelo Lema 5.0.11, existem $A_k^{\tilde{J}_2} = \frac{q_k}{p}$ elementos distintos $\beta_k \neq -r_{1_k}^{-i} \alpha_t$ em $\mathbb{Z}_{p_k}^*$ de forma que

$$(\beta_k, \beta_{k+1}, \ldots, \beta_s) \in \tilde{J}_2.$$

Por outro lado, para cada um desses β_k,

$$(\beta_1, \beta_2, \ldots, \beta_{l-1}, \beta_{l+1}, \ldots \beta_k) \in Z_{P_1 \backslash \{l\}} = \Pi_{P_1 \backslash \{l\}}(H),$$

assim, existem $A_l^{\tilde{J}_1} = \frac{q_l}{p}$ elementos distintos β_l em $\mathbb{Z}_{p_l}^*$ de forma que

$$(\beta_1, \beta_2, \ldots \beta_k) \in \tilde{J}_1.$$

Logo, para cada uma das escolhas de β_l e β_k, temos que

$$\beta = (\beta_1, \beta_2, \ldots \beta_s) \in J_1 \cap J_2 = H,$$

observe que $\beta_l \neq -r_{1_l}^{-i} \alpha_l$, pois $S_k^{i,0} = 0$, conforme equação (5.4). Dessa forma, existem $A_{l,k} = \frac{q_l}{p} \frac{q_k}{p}$ elementos distintos β de forma que $r_1^{-i} \beta$ coincide com $-\alpha$ nas coordenadas $X \backslash \{l, k\}$, ou seja,

$$S_{l,k}^{i,0} = A_{l,k} - S_l^{i,0} - S_k^{i,0} = \frac{q_l q_k}{p^2}.$$

Estendendo essa construção para $L_1 = \{l_1, l_2, \ldots, l_{\tilde{t}_1}\}$, temos que o valor de

$$S^{i,0}_{L_1\cup\{k\}} = S^{i,0}_{l_1,l_2,\ldots,l_{\tilde{t}_1},k},$$

é dado por:

$$\begin{aligned} & A_{l_1,l_2,\ldots,l_{\tilde{t}_1},k} - \sum_{d=1}^{\tilde{t}_1-1} \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} S^{i,0}_{l_{t_1},l_{t_2}\ldots,l_{t_d},k} - \sum_{d=1}^{\tilde{t}_1} \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} S^{i,0}_{l_{t_1},l_{t_2}\ldots,l_{t_d}} - S^{i,0}_k \\ = \; & A_{l_1,l_2,\ldots,l_{\tilde{t}_1},k} - \sum_{d=1}^{\tilde{t}_1-1} \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} S^{i,0}_{l_{t_1},l_{t_2}\ldots,l_{t_d},k} \end{aligned}$$

Assim, conforme visto no Teorema 5.0.2, segue que

$$S^{i,0}_{L_1\cup\{k\}} = \sum_{d=1}^{\tilde{t}_1} \left[(-1)^{\tilde{t}_1-d} \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},k} \right], \tag{5.5}$$

onde pelo Corolário 5.0.8

$$A_{l_{t_1},l_{t_2}\ldots,l_{t_d},k} = \frac{q_{l_{t_1}} q_{l_{t_2}} \cdots q_{l_{t_d}} q_k}{p^2}.$$

Vamos analisar agora o valor de $S^{i,0}_{L_2}$. Se $L_2 = \{l'\}$, tome $\beta_t = -r_{1_t}^{-i}\alpha_t \in \mathbb{Z}^*_{p_t}$, para todo $t \in P_1 \cup (P_2'\backslash\{l'\}) = X\backslash\{l\}$, logo

$$(\beta_1, \beta_2, \ldots, \beta_k) \in \tilde{J}_1,$$

e assim,

$$(\beta_1, \beta_2, \ldots, \beta_k, \theta_{k+1}, \theta_{k+2}, \ldots, \theta_s) \in J_1, \text{ para todo } \theta_{t'} \in \mathbb{Z}_{p_{t'}}, \text{ com } k+1 \leqslant t' \leqslant s.$$

Por outro lado,

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}, \beta_{k+1} \ldots, \beta_{l'-1}, \beta_{l'+1}, \ldots, \beta_s) \in Z_{P_3\backslash\{l'\}} = \Pi_{P_3\backslash\{l'\}}(H),$$

assim, pelo Lema 5.0.11, existem $A^{\tilde{J}_3}_{l'} = \frac{q_{l'}}{p}$ elementos distintos $\beta_{l'}$ em $\mathbb{Z}^*_{p_{l'}}$ de forma que

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}, \beta_{k+1} \ldots, \beta_s) \in \tilde{J}_3.$$

Repare que $\beta_{l'} \neq -r_{1_{l'}}^{-i}\alpha_{l'}$, pois $(r^i_{1_1}, r^i_{1_2}, \ldots, r^i_{1_k}, r^i_{1_{k+1}}, r^i_{1_{k+2}}, \ldots, r^i_{1_s}) \notin \tilde{J}_3$. Logo, para cada uma das escolhas de $\beta_{l'}$, temos que

$$\beta = (\beta_1, \beta_2, \ldots \beta_s) \in J_1 \cap J_3 = H,$$

dessa forma, existem $A_{l'} = \frac{q'_{l'}}{p}$ elementos distintos $\beta \in H$ de forma que $r_1^{-i}\beta$ coincide com $-\alpha$ nas coordenadas $Y = X\backslash\{l'\}$, ou seja,

$$S^{i,0}_{l'} = A_{l'} = \frac{q'_{l'}}{p}.$$

Estendendo essa construção para $L_2 = \{l'_1, l'_2, \ldots, l'_{\tilde{t}_2}\}$, temos que o valor de

$$S^{i,0}_{L_2} = S^{i,0}_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}},$$

é dado por:

$$A_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} - \sum_{d'=1}^{\tilde{t}_2-1} \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant \tilde{t}_2} S^{i,0}_{l'_{t'_1},l_{t'_2}\ldots,l'_{t'_{d'}}}.$$

Assim, conforme visto no Teorema 5.0.2, segue que

$$S^{i,0}_{L_2} = \sum_{d'=1}^{\tilde{t}_2} \left[(-1)^{\tilde{t}_2-d'} \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant \tilde{t}_2} A_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}} \right], \tag{5.6}$$

onde pelo Corolário 5.0.8

$$A_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}} = \frac{q'_{l'_{t'_1}} q'_{l'_{t'_2}} \ldots q'_{l'_{t'_{d'}}}}{p}.$$

Determinemos agora o valor de $S^{i,0}_{\{k\}\cup L_2}$, quando $L_2 = \{l'_1, l'_2, \ldots, l'_{\tilde{t}_2}\}$.
Para cada $t \in P'_1 \cup Y'_2 = X\backslash(\{k\} \cup L_2)$ seja $\beta_t = -r_{1_t}^{-i}\alpha_t$, logo

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}) \in Z_{P'_1} = \Pi_{P'_1}(H).$$

Dessa forma, existem $A_k^{\tilde{J}_1} = \frac{q_k}{p}$ elementos distintos $\beta_k \in \mathbb{Z}^*_{p_k}$ (incluindo $\beta_k = -r_{1_k}^{-i}\alpha_k$), de forma que

$$(\beta_1, \beta_2, \ldots, \beta_k, \theta_{k+1}, \theta_{k+2}, \ldots, \theta_s) \in J_1, \text{ para todo } \theta_{t'} \in \mathbb{Z}_{p_{t'}}, \text{ com } k+1 \leqslant t' \leqslant s.$$

Por outro lado,

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}, \beta_{y'_1}, \beta_{y'_2}, \ldots, \beta_{y'_{t_2}}) \in Z_{P'_1\cup Y_2} = \Pi_{P'_1\cup Y'_2}(H).$$

Assim, pelo Lema 5.0.11, existem $A^{\tilde{J}_3}_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} = \frac{q_{l'_1} q_{l'_2} \ldots q_{l'_{\tilde{t}_2}}}{p}$ elementos distintos

$$(\beta_{l'_1}, \beta_{l'_2}, \ldots, \beta_{l'_{\tilde{t}_2}}) \in Z_{L'_2} = \Pi_{L'_2}(H),$$

de forma que

$$(\beta_1, \beta_2, \ldots, \beta_{k-1}, \beta_{k+1} \ldots, \beta_s) \in \tilde{J}_3.$$

Logo, para cada uma das escolhas de $(\beta_{l'_1}, \beta_{l'_2}, \ldots, \beta_{l'_{\tilde{t}_2}})$ e β_k, temos que

$$\beta = (\beta_1, \beta_2, \ldots \beta_s) \in J_1 \cap J_3 = H,$$

dessa forma, existem

$$A_{k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} = \frac{q'_{l'_1} q'_{l'_2} \ldots q'_{l'_{\tilde{t}_2}} q_k}{p^2}$$

elementos distintos β de forma que $r_1^{-i}\beta$ coincide com $-\alpha$ nas coordenadas do conjunto $X\backslash(L_2 \cup \{k\})$, ou seja, o valor de

$$S^{i,0}_{\{k\}\cup L_2} = S^{i,0}_{k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}},$$

é dado por:

$$A_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2},k} - \sum_{d'=1}^{\tilde{t}_2-1} \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} S^{i,0}_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}},k} - \sum_{d'=1}^{\tilde{t}_2} \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} S^{i,0}_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}}.$$

Assim, conforme visto no Teorema 5.0.2, segue que

$$S^{i,0}_{\{k\}\cup L_2} = \left(\frac{q_k}{p}-1\right)\sum_{d'=1}^{\tilde{t}_2}\left[(-1)^{\tilde{t}_2-d'}\sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} A_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}}\right], \tag{5.7}$$

onde pelo Corolário 5.0.8

$$A_{l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}} = \frac{q'_{l'_{t'_1}}q'_{l'_{t'_2}}\cdots q'_{l'_{t'_{d'}}}}{p}.$$

Agora, para cada $t \in Y'_1 \cup \{k\} \cup Y'_2 = X\backslash L$, seja $\beta_t = -r_{1_t}^{-i}\alpha_t$. Assim,

$$(\beta_{y_1}, \beta_{y_2}, \ldots, \beta_{y_{t_1}}, \beta_k) \in Z_{Y'_1\cup\{k\}} = \Pi_{Y'_1\cup\{k\}}(H),$$

e dessa forma, pelo Lema 5.0.11, existem $A^{\tilde{J}_1}_{l_1,l_2,\ldots,l_{\tilde{t}_1}} = \frac{q_{l_1}q_{l_2}\cdots q_{l_{\tilde{t}_1}}}{p}$ elementos distintos $(\beta_{l_1}, \beta_{l_2}, \ldots, \beta_{l_{\tilde{t}_1}}) \in Z_{L'_1}$, tais que:

$$(\beta_1, \beta_2, \ldots, \beta_k, \theta_{k+1}, \theta_{k+2}, \ldots, \theta_s) \in J_1, \text{ para todo } (\theta_{k+1}, \theta_{k+2}, \ldots, \theta_s) \in Z_{P'_2}.$$

De forma análoga, obtemos que existem $A^{\tilde{J}_2}_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} = \frac{q'_{l'_1}q'_{l'_2}\cdots q'_{l'_{\tilde{t}_2}}}{p}$ elementos distintos $(\beta_{l'_1}, \beta_{l'_2}, \ldots, \beta_{l'_{\tilde{t}_2}})$ em $Z_{L'_2}$, tais que:

$$(\theta_1, \theta_2, \ldots, \theta_{k-1}, \beta_k, \beta_{k+1}, \ldots, \beta_s) \in J_2, \text{ para todo } (\theta_1, \theta_2, \ldots, \theta_{k-1}) \in Z_{P'_1}.$$

Portanto, para cada uma dessas $A^{\tilde{J}_1}_{l_1,l_2,\ldots,l_{\tilde{t}_1}} A^{\tilde{J}_2}_{l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} = A_{L_1\cup L_2}$ escolhas temos que $\beta \in J_1 \cap J_2 = H$. Assim, para $Y = Y'_1 \cup \{k\} \cup Y'_2 = X\backslash L$, temos que

$$S^{i,0}_{L'_1\cup L'_2} = \sum_{d=0}^{\tilde{t}_1}\sum_{d'=1}^{\tilde{t}_2}(-1)^{(d+d'-(\tilde{t}_1+\tilde{t}_2))}A_{d,d'}, \tag{5.8}$$

onde a quantidade $A_{d,d'}$ é dada por

$$\sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1 \text{ e } 1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}},$$

isto é,

$$A_{d,d'} = \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1 \text{ e } 1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} \frac{q_{l_{t_1}}q_{l_{t_2}}\cdots q_{l_{t_d}}}{p}\frac{q_{l'_{t'_1}}q_{l'_{t'_2}}\cdots q_{l'_{t'_{d'}}}}{p}.$$

Por fim, para encerrarmos o caso $S^{i,0}$, devemos verificar quando $r_1^i\beta$ coincide com $-\alpha$ exatamente nas coordenadas de $Y = Y'_1 \cup Y'_2$, para $\beta \in H$, em outras palavras,

queremos determinar $S^{i,0}_{L'_1\cup\{k\}\cup L'_2}$. Seguindo com as mesmas construções anteriores temos que,

$$\begin{aligned} S^{i,0}_{L'_1\cup\{k\}\cup L'_2} &= S^{i,0}_{l_1,l_2,\ldots,l_{\tilde{t}_1},k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} \\ &= \sum_{d=0}^{\tilde{t}_1}\sum_{d'=1}^{\tilde{t}_2}(-1)^{(d+d'-(\tilde{t}_1+\tilde{t}_2))}A_{d,d',k} + \sum_{d=0}^{\tilde{t}_1}\sum_{d'=1}^{\tilde{t}_2}(-1)^{(d+d'-(\tilde{t}_1+\tilde{t}_2)-1)}A_{d,d'} \\ &+ \sum_{d=1}^{\tilde{t}_1}(-1)^{\tilde{t}_1-d}A_{d,k}, \end{aligned}$$

onde

$$A_{d,d',k} = \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1 \text{ e } 1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},k,l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}},$$

$$A_{d,d'} = \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1 \text{ e } 1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}},$$

$$A_{d,k} = \sum_{1\leqslant t_1<t_2<\ldots<t_d\leqslant\tilde{t}_1} A_{l_{t_1},l_{t_2}\ldots,l_{t_d},k},$$

e,

$$A_{d',k} = \sum_{1\leqslant t'_1<t'_2<\ldots<t'_{d'}\leqslant\tilde{t}_2} A_{k,l'_{t'_1},l'_{t'_2}\ldots,l'_{t'_{d'}}}.$$

Caso $S^{i,j}$, com $1 \leqslant i, j \leqslant p-1$: Observe que $r_1^i r_2^j H = r_1^u r_2^v H$ se, e somente se, $r_1^{i-u} r_2^{j-v} \in H$, o que por sua vez ocorre se, e somente se, $i = u$ e $j = v$, ou seja

$$\left|\bigcup_{i,j=0}^{p-1} r_1^i r_2^j H\right| = \sum_{i,j=0}^{p-1}|H| = p^2\frac{\phi(n)}{p^2} = \phi(n) = |\mathbb{Z}_n^*|.$$

Logo,

$$\mathbb{Z}_n^* = \dot{\bigcup}_{i,j=0}^{p-1} r_1^i r_2^j H.$$

Dessa forma, $r_1^i r_2^j H \cap H = \varnothing$, para todo $1 \leqslant i, j \leqslant p-1$, ou seja,

$$S_0^{i,j} = 0. \tag{5.9}$$

Conforme o caso $S^{i,0}$ e analogamente $S^{0,j}$, como $r_1^i r_2^j \notin J_1$ e $r_1^i r_2^j \notin J_2$, então

$$S^{i,j}_{L_1} = S^{i,j}_{L_2} = 0. \tag{5.10}$$

Como $\Pi_{P'_1\cup P'_2}(\pm\alpha) = \Pi_{P_3}(\pm\alpha) \in \tilde{J}_3$, então

$$(-\alpha_1, -\alpha_2, \ldots, -\alpha_{k-1}, \theta_k, -\alpha_{k+1}, \ldots, -\alpha_s) \in J_3, \ \forall\theta_k \in \mathbb{Z}^*_{p_k}.$$

Assim, como $r_1^i r_2^j \in J_3$ se, e somente se, $i = j$, segue que

$$S_k^{i,j} = \begin{cases} 0, & \text{se } i \neq j \\ \dfrac{q_k}{p}, & \text{se } i = j \end{cases}. \tag{5.11}$$

Note que dado $l \in P_1'$, $S_{l,k}^{i,j} = A_{l,k} - S_l^{i,j} - S_k^{i,j} - S_0^{i,j}$. Assim,

$$S_{l,k}^{i,j} = \begin{cases} \dfrac{q_l}{p}\dfrac{q_k}{p}, & \text{se } i \neq j \\ \left(\dfrac{q_l}{p} - 1\right)\dfrac{q_k}{p}, & \text{se } i = j \end{cases}. \tag{5.12}$$

Generalizando, temos que

$$S_{L_1\cup\{k\}}^{i,j} = \begin{cases} D_{L_1}\dfrac{q_k}{p}, & \text{se } i \neq j \\ \left(D_{L_1} + (-1)^{\tilde{t}_1}\right)\dfrac{q_k}{p}, & \text{se } i = j \end{cases}. \tag{5.13}$$

De maneira semelhante,

$$S_{\{k\}\cup L_2}^{i,j} = \begin{cases} D_{L_2}\dfrac{q_k}{p}, & \text{se } i \neq j \\ \left(D_{L_2} + (-1)^{\tilde{t}_2}\right)\dfrac{q_k}{p}, & \text{se } i = j \end{cases}. \tag{5.14}$$

Além disso, a partir do exposto no caso $S_{L_1\cup L_2}^{i,0}$ segue que

$$S_{L_1\cup L_2}^{i,j} = D_{L_1}D_{L_2}. \tag{5.15}$$

Por fim, para encerrarmos o caso $S^{i,j}$, devemos determinar $S_{L_1\cup\{k\}\cup L_2}^{i,j}$. Seguindo com as mesmas construções anteriores temos que:

1. Se $i \neq j$, então $S_{L_1\cup\{k\}\cup L_2}^{i,j}$ é dado por

$$D_{L_1}D_{L_2}q_k - D_{L_1}D_{L_2} + (-1)^{\tilde{t}_2}D_{L_1}\frac{q_k}{p} + (-1)^{\tilde{t}_1}D_{L_2}\frac{q_k}{p}. \tag{5.16}$$

2. Se $i = j$, então $S_{L_1\cup\{k\}\cup L_2}^{i,j}$ é dado por

$$D_{L_1}D_{L_2}q_k - D_{L_1}D_{L_2} + (-1)^{\tilde{t}_2}D_{L_1}\frac{q_k}{p} + (-1)^{\tilde{t}_1}D_{L_2}\frac{q_k}{p} + (-1)^{\tilde{t}_1+\tilde{t}_2}\frac{q_k}{p}. \tag{5.17}$$

□

A partir da contagem estabelecida na Proposição 5.0.13, podemos introduzir os lemas auxiliares para a obtenção da forma traço integral. Estes lemas são adaptações dos Lemas 5.0.4, 5.0.5 e 5.0.6, obtidos na seção anterior. Antes, considere $h = |H| = \frac{\phi(n)}{p^2}$ e

$$S'_{v_1,v_2,\ldots,v_{\tilde{u}}} = (-1)^{\tilde{u}}\frac{\phi(n)}{\prod_{k'=1}^{\tilde{u}} q_{v_{k'}}}, \tag{5.18}$$

sendo $S_0' = \phi(n)$.

Considere $\mathbb{K}_{m_1}$ e $\mathbb{K}_{m_2}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\ldots p_k$ e $m_2 = p_kp_{k+1}\ldots p_s$, respectivamente, com mdc$(m_1, m_2) = p_k$, de forma que exista uma (e portanto a única) p-extensão abeliana não ramificada

$$\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2},$$

com cond$(\mathbb{K}_{m_3}) = \frac{n}{p_k}$, sendo $n = \frac{m_1m_2}{p_k}$ e H o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$.

Lema 5.0.14. *Sejam $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\dots p_k$, $m_2 = p_kp_{k+1}\dots p_s$ e $m_3 = m_1m_2/p_k^2$, respectivamente, com $mdc(m_1, m_2) = p_k$ de forma que $\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\dots p-1}$ é o grupo de Galois de $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ sobre $\mathbb{Q}$, satisfazendo:*

1. *$\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$;*
2. *$\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$;*
3. *$(\theta_1 \circ \theta_2)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$,*

$n = m_1m_2/p_k$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$, então o valor de $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t^2)$ é:

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)+m_3\left(p_k-1\right)}{p}+n.$$

Demonstração. Pela equação (4.1) temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2) \;=\; T_1^0+T_1^1+T_1^2+\cdots+T_1^{s-1}+T_1^s,$$

onde

$$T_1^u = h\left[\sum_{\substack{l_1<l_2<\dots<l_{\tilde{t}_1},\ l'_1<l'_2<\dots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=u}} S'_{\tilde{t}_1,\tilde{t}_2}S^{0,0}_{\tilde{t}_1,\tilde{t}_2}+\sum_{\substack{l_1<l_2<\dots<l_{\tilde{t}_1},\ l'_1<l'_2<\dots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=u-1}} S'_{\tilde{t}_1,k,\tilde{t}_2}S^{0,0}_{\tilde{t}_1,k,\tilde{t}_2}\right],$$

com $S'_{\tilde{t}_1,\tilde{t}_2} = S'_{l_1,l_2,\dots,l_{\tilde{t}_1},l'_1,l'_2,\dots,l'_{\tilde{t}_2}}$, $S_{\tilde{t}_1,\tilde{t}_2} = S^{0,0}_{l_1,l_2,\dots,l_{\tilde{t}_1},l'_1,l'_2,\dots,l'_{\tilde{t}_2}}$, $S'_{\tilde{t}_1,k,\tilde{t}_2} = S'_{l_1,l_2,\dots,l_{\tilde{t}_1},k,l'_1,l'_2,\dots,l'_{\tilde{t}_2}}$ e $S_{\tilde{t}_1,k,\tilde{t}_2} = S^{0,0}_{l_1,l_2,\dots,l_{\tilde{t}_1},k,l'_1,l'_2,\dots,l'_{\tilde{t}_2}}$.

Conforme a Proposição 5.0.13, temos que $S_0^{0,0} = 1$, assim

$$T_1^0 = hS'_0S_0^{0,0} = h.\phi(n).$$

Para o caso em que $\beta \in H$ coincide com $-\alpha$, exceto em uma de suas coordenadas temos o fator representante T_1^1. Note que $S'_l = -\frac{\phi(n)}{q_l}$, $S'_k = -\frac{\phi(n)}{q_k}$ e $S'_{l'} = -\frac{\phi(n)}{q'_{l'}}$, para $l \in P'_1$ e $l' \in P'_2$. Logo,

$$\begin{aligned}
T_1^1 &= h\left[\sum_{l=1}^{k-1}S'_lS_l^{0,0}+S'_kS_k^{0,0}+\sum_{l'=1}^{s-k}S'_{l'}S_{l'}^{0,0}\right]\\
&= h\left[\sum_{l=1}^{k-1}-\frac{\phi(n)}{q_l}\left(\frac{q_l}{p}-1\right)-\frac{\phi(n)}{q_k}\left(\frac{q_k}{p}-1\right)+\sum_{l'=1}^{s-k}-\frac{\phi(n)}{q'_{l'}}\left(\frac{q'_{l'}}{p}-1\right)\right]\\
&= -h\left(\frac{1}{p}\left[\binom{k-1}{(k-1)-1}+1+\binom{s-k}{(s-k)-1}\right]\phi(n)-\sum_{v=1}^{s}\frac{\phi(n)}{q_v}\right).
\end{aligned}$$

A quantidade de elementos $\beta \in H$ de forma que β_v coincide com $-\alpha_v$ exatamente em $s-2$ de suas coordenadas (equivalentemente, difere de $-\alpha$ exatamente em duas de suas coordenadas) é representada pelo fator:

$$
\begin{aligned}
T_1^2 &= h\Bigg[\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}\left(\frac{q_{l_1}q_{l_2}}{p}-\frac{q_{l_1}+q_{l_2}}{p}+1\right)+\sum_{l\in P,\ l'\in P'}\frac{\phi(n)}{q_l q'_{l'}}\left(\frac{q_l q'_{l'}}{p^2}-\frac{q_l+q'_{l'}}{p}+1\right)\\
&+ \sum_{l'_1<l'_2}\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}\left(\frac{q'_{l'_1}q'_{l'_2}}{p}-\frac{q'_{l'_1}-q'_{l'_2}}{p}+1\right)+\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l q_k}\left(\frac{q_l q_k}{p^2}-\frac{q_l+q_k}{p}+1\right)\\
&+ \sum_{l'=k+1}^{s-k}\frac{\phi(n)}{q'_{l'}q_k}\left(\frac{q'_{l'}q_k}{p^2}-\frac{q'_{l'}+q_k}{p}+1\right)\Bigg]\\
&= h\Bigg(\frac{1}{p^2}\left[\binom{k-1}{(k-1)-1}\binom{s-k}{(s-k)-1}\right.\\
&+ \left.\binom{k-1}{(k-1)-1}+\binom{s-k}{(s-k)-1}\right]\phi(n)\\
&+ \frac{1}{p}\Bigg(\left[\binom{k-1}{(k-1)-2}+\binom{s-k}{(s-k)-2}\right]\phi(n)\\
&- \left[\binom{k-2}{(k-2)-1}+\binom{s-k}{(s-k)-1}+1\right]\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}\\
&- \left[\binom{s-k-1}{(s-k-1)-1}+\binom{k-1}{(k-1)-1}+1\right]\sum_{l'=1}^{s-k}\frac{\phi(n)}{q'_{l'}}\\
&- \left[\binom{k-1}{(k-1)-1}+\binom{s-k}{(s-k)-1}\right]\frac{\phi(n)}{q_k}\Bigg)+\sum_{1\leqslant v_1<v_2\leqslant s}\frac{\phi(n)}{q_{v_1}q_{v_2}}\Bigg).
\end{aligned}
$$

Olhando para os elementos de H que coincidem com $-\alpha$ em exatamente três coordenadas, temos que a parcela correspondente a T_1^3, na expressão (4.1), é igual a

$$
\begin{aligned}
&-h\Bigg[\frac{1}{p^2}\Bigg(\left[\binom{k-1}{(k-1)-2}\binom{s-k}{(s-k)-1}+\binom{k-1}{(k-1)-1}\binom{s-k}{(s-k)-2}\right.\\
&+ \left.\binom{k-1}{(k-1)-2}+\binom{s-k}{(s-k)-2}+\binom{k-1}{(k-1)-1}\binom{s-k}{(s-k)-1}\right]\phi(n)\\
&- \left[\binom{k-2}{(k-2)-1}\binom{s-k}{(s-k)-1}+\binom{k-2}{(k-2)-1}+\binom{s-k}{(s-k)-1}\right]\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}\\
&- \left[\binom{s-k-1}{(s-k-1)-1}+\binom{k-1}{(k-1)-1}\binom{s-k-1}{(s-k-1)-1}+\binom{k-1}{(k-1)-1}\right]\sum_{l'=1}^{s-k}\frac{\phi(n)}{q'_{l'}}\\
&- \binom{k-1}{(k-1)-1}\binom{s-k}{(s-k)-1}\frac{\phi(n)}{q_k}\Bigg)\\
&+ \frac{1}{p}\Bigg(\left[\binom{k-1}{(k-1)-3}+\binom{s-k}{(s-k)-3}\right]\phi(n)\\
&- \left[\binom{k-2}{(k-2)-2}+\binom{s-k}{(s-k)-2}\right]\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}\\
&- \left[\binom{s-k-1}{(s-k-1)-2}+\binom{k-1}{(k-1)-2}\right]\sum_{l'=1}^{s-k}\frac{\phi(n)}{q'_{l'}}\\
&- \left[\binom{k-1}{(k-1)-2}+\binom{s-k}{(s-k)-2}\right]\frac{\phi(n)}{q_k}
\end{aligned}
$$

$$
\begin{aligned}
&+ \left[\binom{k-3}{(k-3)-1} + \binom{(s-k)}{(s-k)-1} + 1 \right] \sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}} \\
&+ \left[\binom{k-2}{(k-2)-1} + \binom{s-k-1}{(s-k-1)-1} + 1 \right] \sum_{l \in P_1' < l' \in P_2'} \frac{\phi(n)}{q_l q_{l'}'} \\
&+ \left[\binom{s-k-2}{(s-k-2)-1} + \binom{k-1}{(k-1)-1} + 1 \right] \sum_{l_1'<l_2'} \frac{\phi(n)}{q_{l_1}' q_{l_2}'} \\
&+ \left[\binom{k-2}{(k-2)-1} + \binom{s-k}{(s-k)-1} \right] \sum_{l=1}^{k-1} \frac{\phi(n)}{q_l q_k} \\
&+ \left[\binom{k-1}{(k-1)-1} + \binom{s-k-1}{(s-k-1)-1} \right] \left(\sum_{l'=1}^{s-k} \frac{\phi(n)}{q_{l'}' q_k} \right) - \sum_{1 \leqslant v_1 < v_2 < v_3 \leqslant s} \frac{\phi(n)}{q_{v_1} q_{v_2} q_{v_3}} \Bigg].
\end{aligned}
$$

A fim de expressar uma generalização para o termo $T_1^{\tilde{u}}$, sejam d e d' inteiros positivos não nulos, $0 \leqslant u \leqslant k-1$, $0 \leqslant u' \leqslant s-k$ e considere

$$\binom{a}{a-b} = 0,$$

se $b \geqslant a$. Logo, $T_1^{\tilde{u}} = (-1)^{\tilde{u}} h \left(\lambda_{\tilde{u}_1} - \lambda_{\tilde{u}_2} + \lambda_{\tilde{u}_3} \right)$, onde

$$\lambda_{\tilde{u}_1} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \Gamma_{u,u'} + \frac{1}{p} \sum_{u+u'=0}^{\tilde{u}-1} (-1)^{u+u'} \Delta_{u,u'} + \sum_{u+u'=\tilde{u}} (-1)^{u+u'} \Omega_{u,u'}, \tag{5.19}$$

$$\lambda_{\tilde{u}_2} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-3} (-1)^{u+u'} \Gamma_{u,u',k} + \frac{1}{p} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \Delta_{u,u',k} + \sum_{u+u'=\tilde{u}-1} (-1)^{u+u'} \frac{\Omega_{u,u'}}{q_k}, \tag{5.20}$$

$$\lambda_{\tilde{u}_3} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \tilde{\Gamma}_{u,u'} + \frac{1}{p} \sum_{u+u'=\tilde{u}-1} (-1)^{u+u'} \Omega_{u,u'}, \tag{5.21}$$

sendo

$$\Omega_{u,u'} = \sum_{\substack{L_1 \in \mathcal{P}(P_1'),\ L_2 \in \mathcal{P}(P_2') \\ |L_1|=u \text{ e } |L_2|=u'}} \frac{\phi(n)}{\prod_{l=1}^{u} q_l \prod_{l'=1}^{u'} q_{l'}'},$$

$$\Gamma_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')} \binom{k-1-u}{(k-1-u)-d} \binom{s-k-u'}{(s-k-u')-d'} \right] \Omega_{u,u'},$$

$$\Gamma_{u,u',k} = \left[\sum_{d+d'=\tilde{u}-(u+u')-1} \binom{k-1-u}{(k-1-u)-d} \binom{s-k-u'}{(s-k-u')-d'} \right] \frac{\Omega_{u,u'}}{q_k},$$

$$\tilde{\Gamma}_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')+1} \binom{k-1-u}{(k-1-u)-(d-1)} \binom{s-k-u'}{(s-k-u')-(d'-1)} \right] \Omega_{u,u'},$$

$$\Delta_{u,u'} = \left[\binom{k-1-u}{k-1-(\tilde{u}-u')} + \binom{s-k-u'}{s-k-(\tilde{u}-u)} \right] \Omega_{u,u'},$$

$$\Delta_{u,u',k} = \left[\begin{pmatrix} k-1-u \\ k-1-(\tilde{u}-u'-1)\end{pmatrix} + \begin{pmatrix} s-k-u' \\ s-k-(\tilde{u}-u-1)\end{pmatrix}\right]\frac{\Omega_{u,u'}}{q_k},$$

onde $\mathcal{P}(P_1')$ e $\mathcal{P}(P_2')$ o conjuntos de todos os subconjuntos de P_1' e P_2', respectivamente.

Além disso,

$$T_1^s = h\left[(-1)^s\frac{\phi(n)}{q_1q_2\dots q_s}\left(\left(D_{P_1'}+(-1)^{k-1}\right)\left(D_{P_2'}+(-1)^{s-k}\right)\left(\frac{q_k}{p}-1\right)\right.\right.$$
$$\left.\left. - \quad D_{P_1'}D_{P_2'}\frac{q_k}{p}+D_{P_1'}D_{P_2'}q_k\right)\right].$$

Logo, o termo $\dfrac{(-1)^sT_1^s}{h}$ é dado por:

$$\frac{1}{p^2}\left[\phi(n)-\left(\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}+\sum_{l'=1}^{s-k}\frac{\phi(n)}{q_{l'}'}\right)+\left(\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}+\sum_{l\in P_1',l'\in P_2'}\frac{\phi(n)}{q_lq_{l'}'}+\sum_{l_1'<l_2'}\frac{\phi(n)}{q_{l_1'}'q_{l_2'}'}\right)-\cdots\right.$$
$$\left.\cdots\quad+(-1)^{s-2}\sum_{l_1<l_2<\ldots<l_{k-2},l_1'<l_2'<\ldots<l_{s-k-1}'}\frac{\phi(n)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}q_{l_1'}'q_{l_2'}'\cdots q_{l_{s-k-1}'}'}\right]$$
$$-\quad\frac{1}{p^2q_k}\left[\phi(n)-\left(\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}+\sum_{l'=1}^{s-k}\frac{\phi(n)}{q_{l'}'}\right)+\left(\sum_{l_1<l_2}\frac{\phi(n)}{q_{l_1}q_{l_2}}+\sum_{l\in P_1',l'\in P_2'}\frac{\phi(n)}{q_lq_{l'}'}+\sum_{l_1'<l_2'}\frac{\phi(n)}{q_{l_1'}'q_{l_2'}'}\right)-\cdots\right.$$
$$\left.\cdots\quad+(-1)^{s-3}\sum_{l_1<l_2<\ldots<l_{k-2},l_1'<l_2'<\ldots<l_{s-k-1}'}\frac{\phi(n)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}q_{l_1'}'q_{l_2'}'\cdots q_{l_{s-k-1}'}'}\right]$$

$$+\quad\frac{1}{p^2}\left[(-1)^{k-1}\phi(m_2)+(-1)^{k-2}\sum_{l'=1}^{s-k}\frac{\phi(m_2)}{q_{l'}'}+(-1)^{k-3}\sum_{l_1'<l_2'}\frac{\phi(m_2)}{q_{l_1'}'q_{l_2'}'}+\cdots\right.$$
$$\cdots\quad+(-1)^{-s}\sum_{l_1'<l_2'<\cdots<l_{s-k-1}'}\frac{\phi(m_2)}{q_{l_1'}'q_{l_2'}'\cdots q_{l_{s-k-1}'}'}+(-1)^{s-k}\phi(m_1)+(-1)^{s-k-1}\sum_{l=1}^{k-1}\frac{\phi(m_1)}{q_l}$$
$$\left.+\quad(-1)^{s-k-2}\sum_{l_1<l_2}\frac{\phi(m_1)}{q_{l_1}q_{l_2}}+\cdots+(-1)^{s+2}\sum_{l_1<l_2<\cdots<l_{k-2}}\frac{\phi(m_1)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}}\right]$$
$$+\quad\frac{1}{pq_k}\left[(-1)^k\phi(m_2)+(-1)^{k-1}\sum_{l'=1}^{s-k}\frac{\phi(m_2)}{q_{l'}'}+(-1)^{k-2}\sum_{l_1'<l_2'}\frac{\phi(m_2)}{q_{l_1'}'q_{l_2'}'}+\cdots\right.$$
$$\cdots\quad-\sum_{l_1'<l_2'<\cdots<l_{s_2-1}'}\frac{\phi(m_2)}{q_{l_1'}'q_{l_2'}'\cdots q_{l_{s-k-1}'}'}+(-1)^{s-k+1}\phi(m_1)+(-1)^{s-k}\sum_{l=1}^{k-1}\frac{\phi(m_1)}{q_l}$$
$$\left.+\quad(-1)^{s-k-1}\sum_{l_1<l_2}\frac{\phi(m_1)}{q_{l_1}q_{l_2}}+\cdots-\sum_{l_1<l_2<\cdots<l_{k-2}}\frac{\phi(m_1)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}}\right]$$
$$+\quad(-1)^{s-1}\frac{1}{p}\frac{\phi(n)}{q_1q_2\dots q_{k-1}q_1'q_2'\dots q_{s-k}'}+(-1)^s.$$

Desse modo, considerando

$$a_{u,d}=(-1)^d\begin{pmatrix} k-1-u \\ (k-1-u)-d\end{pmatrix}\text{ e }b_{u',d'}=(-1)^{d'}\begin{pmatrix} s-k-u' \\ (s-k-u')-d'\end{pmatrix},$$

temos que o valor

$$\frac{Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)}{h} = \frac{T_1^0 + T_1^1 + T_1^2 + \cdots + T_1^{s-1} + T_1^s}{h}$$

é dado por:

$$\left[\frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k} b_{0,d'} - 1}{p} - \frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k} b_{0,d'}}{p^2}\right] \phi(n)$$

$$+ \left[\frac{\sum_{d=1}^{k-2} a_{1,d} + \sum_{d'=1}^{s-k} b_{0,d'} - 1}{p} - \frac{\sum_{d=1}^{k-2} a_{1,d} + \sum_{d'=1}^{s-k} b_{0,d'}}{p^2}\right] \sum_{l=1}^{k-1} \frac{\phi(n)}{q_l}$$

$$+ \left[\frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k-1} b_{1,d'} - 1}{p} - \frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k-1} b_{1,d'}}{p^2}\right] \sum_{l'=1}^{s-k} \frac{\phi(n)}{q'_{l'}}$$

$$+ \left[\frac{\sum_{d=1}^{k-3} a_{2,d} + \sum_{d'=1}^{s-k} b_{0,d'} - 1}{p} - \frac{\sum_{d=1}^{k-3} a_{2,d} + \sum_{d'=1}^{s-k} b_{0,d'}}{p^2}\right] \sum_{l_1<l_2} \frac{\phi(n)}{q_{l_1} q_{l_2}}$$

$$+ \left[\frac{\sum_{d=1}^{k-2} a_{1,d} + \sum_{d'=1}^{s-k-1} b_{1,d'} - 1}{p} - \frac{\sum_{d=1}^{k-2} a_{1,d} + \sum_{d'=1}^{s-k-1} b_{1,d'}}{p^2}\right] \sum_{l\in P'_1, l'\in P'_2} \frac{\phi(n)}{q_l q'_{l'}}$$

$$+ \left[\frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k-2} b_{2,d'} - 1}{p} - \frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k-2} b_{2,d'}}{p^2}\right] \sum_{l'_1<l'_2} \frac{\phi(n)}{q'_{l'_1} q'_{l'_2}} + \cdots$$

$$\cdots + \left[\frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k} b_{0,d'}}{p} + \frac{\sum_{d=1}^{k-1} a_{0,d} \left(\sum_{d'=1}^{s-k} b_{0,d'}\right)}{p^2}\right] \frac{\phi(n)}{q_k}$$

$$+ \left[\frac{\sum_{d=1}^{k-2} a_{1,d} + \sum_{d'=1}^{s-k} b_{0,d'}}{p} + \frac{\sum_{d=1}^{k-2} a_{1,d} \left(\sum_{d'=1}^{s-k} b_{0,d'}\right)}{p^2}\right] \sum_{l=1}^{k-1} \frac{\phi(n)}{q_l q_k}$$

$$+ \quad \left[\frac{\sum_{d=1}^{k-1} a_{0,d} + \sum_{d'=1}^{s-k-1} b_{1,d'}}{p} + \frac{\sum_{d=1}^{k-1} a_{0,d} \left(\sum_{d'=1}^{s-k-1} b_{1,d'} \right)}{p^2} \right] \sum_{l'=1}^{s-k} \frac{\phi(n)}{q'_{l'} q_k} + \cdots$$

$$\cdots \quad + \phi(n) + \sum_{v=1}^{s} \frac{\phi(n)}{q_v} + \sum_{v_1<v_2} \frac{\phi(n)}{q_{v_1} q_{v_2}} + \cdots + \sum_{v_1<v_2<\ldots<v_{s-1}} \frac{\phi(n)}{q_{v_1} q_{v_2} \cdots q_{v_{s-1}}} + 1.$$

Repare que para os termos $\phi(m_2)$, $\frac{\phi(m_2)}{q'_{l'}}$, $\frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}}$, $\ldots$, $\frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s-k-1}}}$ obtemos:

$$\left[\frac{\sum_{d'=1}^{s-k} b_{0,d'} - 1}{p} - \frac{\sum_{d'=1}^{s-k} b_{0,d'}}{p^2} \right] \phi(m_2) + \left[\frac{\sum_{d'=1}^{s-k-1} b_{1,d'} - 1}{p} - \frac{\sum_{d'=1}^{s-k-1} b_{1,d'}}{p^2} \right] \sum_{l'=1}^{s_2} \frac{\phi(m_2)}{q'_{l'}} + \cdots$$

$$\cdots \quad + \left[\frac{b_{s-k-1,1} - 1}{p} + \frac{b_{s-k-1,1}}{p^2} \right] \sum_{l'_1<l'_2<\cdots<l'_{s-k-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s-k-1}}}.$$

Equivalentemente, para os termos $\phi(m_1)$, $\frac{\phi(m_1)}{q_l}$, $\frac{\phi(m_1)}{q_{l_1} q_{l_2}}$, $\ldots$, $\frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{k-2}}}$ obtemos:

$$\left[\frac{\sum_{d=1}^{k-1} a_{0,d} - 1}{p} - \frac{\sum_{d=1}^{k-1} a_{0,d}}{p^2} \right] \phi(m_1) + \left[\frac{\sum_{d=1}^{k-2} a_{1,d} - 1}{p} - \frac{\sum_{d=1}^{k-2} a_{1,d}}{p^2} \right] \sum_{l=1}^{k-1} \frac{\phi(m_1)}{q_l} + \cdots$$

$$\cdots \quad + \left[\frac{a_{k-2,1} - 1}{p} - \frac{a_{k-2,1}}{p^2} \right] \sum_{l_1<l_2<\cdots<l_{k-2}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{k-2}}}.$$

Pela Proposição 5.0.1, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é igual a

$$h \quad \left[\left(-\frac{3}{p} + \frac{2}{p^2} \right) \left(\phi(n) + \sum_{v=1}^{s} \frac{\phi(n)}{q_v} + \sum_{v_1<v_2} \frac{\phi(n)}{q_{v_1} q_{v_2}} + \cdots + \sum_{v_1<v_2<\cdots<v_{s-1}} \frac{\phi(n)}{q_{v_1} q_{v_2} \cdots q_{v_{s-1}}} \right) \right.$$

$$+ \quad \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_1) + \sum_{l=1}^{k-1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{k-2}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \cdots q_{l_{k-2}}} \right)$$

$$+ \quad \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_2) + \sum_{l'=1}^{s-k} \frac{\phi(m_2)}{q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2}} + \cdots + \sum_{l'_1<l'_2<\cdots<l'_{s-k-1}} \frac{\phi(m_2)}{q'_{l'_1} q'_{l'_2} \cdots q'_{l'_{s-k-1}}} \right)$$

$$+ \quad \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_3) + \sum_{\substack{v=1 \\ v \neq k}}^{s} \frac{\phi(m_3)}{q_v} + \sum_{\substack{v_1<v_2 \\ v_1,v_2 \neq k}} \frac{\phi(m_2)}{q_{v_1} q_{v_2}} + \cdots + \sum_{\substack{v_1<v_2<\cdots<v_{s-2} \\ v_1,v_2,\ldots,v_{s-2} \neq k}} \frac{\phi(m_2)}{q_{v_1} q_{v_2} \cdots q_{v_{s-2}}} \right)$$

$$+ \quad \left. \phi(n) + \sum_{v=1}^{s} \frac{\phi(n)}{q_v} + \sum_{v_1<v_2} \frac{\phi(n)}{q_{v_1} q_{v_2}} + \cdots + \sum_{v_1<v_2<\ldots<v_{s-1}} \frac{\phi(n)}{q_{v_1} q_{v_2} \cdots q_{v_{s-1}}} + 1 \right].$$

No entanto,

$$\begin{aligned} n &= (q_1+1)(q_2+1)\cdots(q_{k-1}+1)(q_k+1)(q'_1+1)(q'_2+1)\cdots(q'_{s-k}+1) \\ &= \phi(n) + \sum_{v=1}^{s} \frac{\phi(n)}{q_v} + \sum_{v_1<v_2} \frac{\phi(n)}{q_{v_1} q_{v_2}} + \cdots + \sum_{v_1<v_2<\cdots<v_{s-1}} \frac{\phi(n)}{q_{v_1} q_{v_2} \cdots q_{v_{s-1}}} + 1, \end{aligned}$$

$$\begin{aligned} m_1 &= (q_1+1)(q_2+1)\cdots(q_{k-1}+1) \\ &= \phi(m_1) + \sum_{l=1}^{k-1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1}q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{k-2}} \frac{\phi(m_1)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}} + 1, \end{aligned}$$

$$\begin{aligned} m_2 &= (q'_1+1)(q'_2+1)\cdots(q'_{s-k}+1) \\ &= \phi(m_2) + \sum_{l'=1}^{s-k} \frac{\phi(m_2)}{q'_{l'}} + \sum_{l'_1<l'_2} \frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}} + \cdots + \sum_{l'_1<l'_2<\cdots<l'_{s-k-1}} \frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}\cdots q'_{l'_{s-k-1}}} + 1, \end{aligned}$$

e

$$\begin{aligned} m_3 &= (q_1+1)(q_2+1)\cdots(q_{k-1}+1)(q'_1+1)(q'_2+1)\cdots(q'_{s-k}+1) \\ &= \phi(m_3) + \sum_{\substack{v=1 \\ v\neq k}}^{s} \frac{\phi(m_3)}{q_v} + \sum_{\substack{v_1<v_2 \\ v_1,v_2\neq k}} \frac{\phi(m_2)}{q_{v_1}q_{v_2}} + \cdots + \sum_{\substack{v_1<v_2<\cdots<v_{s-2} \\ v_1,v_2,\ldots,v_{s-2}\neq k}} \frac{\phi(m_2)}{q_{v_1}q_{v_2}\cdots q_{v_{s-2}}} + 1, \end{aligned}$$

Assim, o valor de $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é:

$$\begin{aligned} & h\left[\frac{2n-m_1-m_2-m_3+1}{p^2} + \frac{-3(n-1)+(m_1-1)+(m_2-1)+(m_3-1)}{p} + n\right] \\ = \; & h\left[\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2} - \frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)+m_3\left(p_k-1\right)}{p}\right] \\ + \; & hn. \end{aligned}$$

Portanto, $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t^2) = \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é dado por:

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2} - \frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)+m_3\left(p_k-1\right)}{p} + n.$$

□

Lema 5.0.15. *Sejam $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\ldots p_k$, $m_2 = p_kp_{k+1}\ldots p_s$ e $m_3 = m_1m_2/p_k^2$, respectivamente, com $mdc(m_1, m_2) = p_k$ de forma que $\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$ é o grupo de Galois de $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ sobre $\mathbb{Q}$, satisfazendo:*

1. *$\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$;*
2. *$\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$;*
3. *$(\theta_1 \circ \theta_2)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$,*

e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$, então:

1. *Para $1 \leqslant i \leqslant p-1$, o valor de $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t\theta_1^i(t))$ é:*

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2} - \frac{m_1\left(\frac{m_2}{p_k}-1\right)}{p}.$$

2. Para $1 \leqslant j \leqslant p-1$, o valor de $Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t\theta_2^j(t))$ é:

$$\frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_2\left(\frac{m_1}{p_k}-1\right)}{p}.$$

Demonstração. Faremos a prova apenas para o caso 1., o outro caso é análogo. Pela equação (4.1) temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\theta_1^i(t)) \;=\; T_2^0+T_2^1+T_2^2+\cdots+T_2^{s-1}+T_2^s,$$

onde

$$T_2^{\tilde{u}} \;=\; h\left[\sum_{\substack{l_1<l_2<\ldots<l_{\tilde{t}_1},\ l'_1<l'_2<\ldots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=\tilde{u}}} S'_{l_1,l_2,\ldots,l_{\tilde{t}_1},l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} S^{i,0}_{l_1,l_2,\ldots,l_{\tilde{t}_1},l'_1,l'_2,\ldots,l'_{\tilde{t}_2}}\right.$$

$$\left.+\sum_{\substack{l_1<l_2<\ldots<l_{\tilde{t}_1},\ l'_1<l'_2<\ldots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=\tilde{u}-1}} S'_{l_1,l_2,\ldots,l_{\tilde{t}_1},k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} S^{i,0}_{l_1,l_2,\ldots,l_{\tilde{t}_1},k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}}\right].$$

Conforme a Proposição 5.0.13, temos que $S_0^{i,0}=0$, assim

$$T_2^0 = hS'_0S_0^{i,0}=0.$$

Para o caso T_2^1, segue que

$$T_2^1 \;=\; h\left[\sum_{l'=1}^{s-k} S'_{l'}S_{l'}^{0,0}\right]=h\left[\sum_{l'=1}^{s-k}-\frac{\phi(n)}{q'_{l'}}\frac{q'_{l'}}{p}\right]=-h\frac{1}{p}\begin{pmatrix} s-k \\ (s-k)-1\end{pmatrix}\phi(n).$$

A parcela T_2^1 é igual a

$$\begin{aligned}
& h\left[\sum_{l\in P'_1,\ l'\in P'_2}\frac{\phi(n)}{q_lq'_{l'}}\left(\frac{q_lq'_{l'}}{p^2}-\frac{q'_{l'}}{p}\right)+\sum_{l'_1<l'_2}\frac{\phi(n)}{q'_{l'_1}q'_{l'_2}}\left(\frac{q'_{l'_1}q'_{l'_2}}{p}-\frac{q'_{l'_1}-q'_{l'_2}}{p}\right)+\sum_{l=1}^{k-1}\frac{\phi(n)}{q_lq_k}\left(\frac{q_lq_k}{p^2}\right)\right.\\
+\;& \left.\sum_{l'=1}^{s-k}\frac{\phi(n)}{q'_{l'}q_k}\left(\frac{q'_{l'}q_k}{p^2}-\frac{q'_{l'}}{p}\right)\right]\\
=\;& h\left(\frac{1}{p^2}\left[\begin{pmatrix} k-1 \\ (k-1)-1\end{pmatrix}\begin{pmatrix} s-k \\ (s-k)-1\end{pmatrix}+\begin{pmatrix} k-1 \\ (k-1)-1\end{pmatrix}+\begin{pmatrix} s-k \\ (s-k)-1\end{pmatrix}\right]\phi(n)\right.\\
+\;& \frac{1}{p}\left[\begin{pmatrix} s-k \\ (s-k)-2\end{pmatrix}\phi(n)-\begin{pmatrix} s-k \\ (s-k)-1\end{pmatrix}\sum_{l=1}^{k-1}\frac{\phi(n)}{q_l}-\begin{pmatrix} s-k-1 \\ (s-k-1)-1\end{pmatrix}\sum_{l'=1}^{s-k}\frac{\phi(n)}{q'_{l'}}\right.\\
-\;& \left.\left.\begin{pmatrix} s-k \\ (s-k)-1\end{pmatrix}\frac{\phi(n)}{q_k}\right]\right).
\end{aligned}$$

Sejam $0\leqslant u\leqslant k-1$, $0\leqslant u'\leqslant s-k$, $d,d'\geqslant 1$ e considere que

$$\begin{pmatrix} a \\ a-b\end{pmatrix}=0,$$

se $b \geqslant a$. Logo, o termo geral, para $1 \leqslant \tilde{u} \leqslant s-1$ é dado por:

$$T_2^{\tilde{u}} = (-1)^{\tilde{u}} h \left(\lambda_{\tilde{u}_1} - \lambda_{\tilde{u}_2} + \lambda_{\tilde{u}_3}\right),$$

onde

$$\lambda_{\tilde{u}_1} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \Gamma_{u,u'} + \frac{1}{p} \sum_{u+u'=0}^{\tilde{u}-1} (-1)^{u+u'} \Delta_{u,u'}, \tag{5.22}$$

$$\lambda_{\tilde{u}_2} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-3} (-1)^{u+u'} \Gamma_{u,u',k} + \frac{1}{p} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \Delta_{u,u',k}, \tag{5.23}$$

$$\lambda_{\tilde{u}_3} = \frac{1}{p^2} \sum_{u+u'=0}^{\tilde{u}-2} (-1)^{u+u'} \tilde{\Gamma}_{u,u'}, \tag{5.24}$$

sendo

$$\Omega_{u,u'} = \sum_{\substack{L_1 \in \mathcal{P}(P_1'),\ L_2 \in \mathcal{P}(P_2') \\ |L_1|=u \text{ e } |L_2|=u'}} \frac{\phi(n)}{\prod_{l=1}^{u} q_l \prod_{l'=1}^{u'} q_{l'}'},$$

$$\Gamma_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')} \binom{k-1-u}{(k-1-u)-d} \binom{s-k-u'}{(s-k-u')-d'} \right] \Omega_{u,u'},$$

$$\Gamma_{u,u',k} = \left[\sum_{d+d'=\tilde{u}-(u+u')-1} \binom{k-1-u}{(k-1-u)-d} \binom{s-k-u'}{(s-k-u')-d'} \right] \frac{\Omega_{u,u'}}{q_k},$$

$$\tilde{\Gamma}_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')+1} \binom{k-1-u}{(k-1-u)-(d-1)} \binom{s-k-u'}{(s-k-u')-(d'-1)} \right] \Omega_{u,u'},$$

$$\Delta_{u,u'} = \left[\binom{s-k-u'}{s-k-(\tilde{u}-u)} \right] \Omega_{u,u'},$$

$$\Delta_{u,u',k} = \left[\binom{s-k-u'}{s-k-(\tilde{u}-u-1)} \right] \frac{\Omega_{u,u'}}{q_k},$$

onde $\mathcal{P}(P_1')$ e $\mathcal{P}(P_2')$ o conjuntos de todos os subconjuntos de P_1' e P_2', respectivamente. Temos também que,

$$\begin{aligned} T_2^s = \; & h \left[(-1)^s \frac{\phi(n)}{q_1 q_2 \dots q_s} \left(\left(D_{P_1'} + (-1)^{k-1} \right) D_{P_2'} \left(\frac{q_k}{p} - 1 \right) - D_{P_1'} D_{P_2'} \frac{q_k}{p} \right. \right. \\ + \; & \left. \left. D_{P_1'} D_{P_2'} q_k + (-1)^{s-k} D_{P_1'} \frac{q_k}{p} \right) \right]. \end{aligned}$$

Logo,

$$T_2^s = (-1)^s h \left(\frac{1}{p^2} - \frac{1}{p^2 q_k}\right)\left[\sum_{u+u'=0}^{s-1}(-1)^{u+u'}\Omega_{u,u'}\right] + \frac{1}{pq_k}\left[\sum_{u'=0}^{s-k-1}(-1)^{k+u'}\Omega_{k-1,u'}\right].$$

Assim, pela Proposição 5.0.1, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\theta_1^i(t))$ é igual a

$$\begin{aligned}
h \quad & \left[\left(-\frac{1}{p}+\frac{2}{p^2}\right)\left(\phi(n)+\sum_{v=1}^{s}\frac{\phi(n)}{q_v}+\sum_{v_1<v_2}\frac{\phi(n)}{q_{v_1}q_{v_2}}+\cdots+\sum_{v_1<v_2<\cdots<v_{s-1}}\frac{\phi(n)}{q_{v_1}q_{v_2}\cdots q_{v_{s-1}}}\right)\right. \\
+ \quad & \left(\frac{1}{p}-\frac{1}{p^2}\right)\left(\phi(m_1)+\sum_{l=1}^{k-1}\frac{\phi(m_1)}{q_l}+\sum_{l_1<l_2}\frac{\phi(m_1)}{q_{l_1}q_{l_2}}+\cdots+\sum_{l_1<l_2<\cdots<l_{k-2}}\frac{\phi(m_1)}{q_{l_1}q_{l_2}\cdots q_{l_{k-2}}}\right) \\
+ \quad & -\frac{1}{p^2}\left(\phi(m_2)+\sum_{l'=1}^{s-k}\frac{\phi(m_2)}{q'_{l'}}+\sum_{l'_1<l'_2}\frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}}+\cdots+\sum_{l'_1<l'_2<\cdots<l'_{s-k-1}}\frac{\phi(m_2)}{q'_{l'_1}q'_{l'_2}\cdots q'_{l'_{s-k-1}}}\right) \\
+ \quad & \left.-\frac{1}{p^2}\left(\phi(m_3)+\sum_{\substack{v=1\\v\neq k}}^{s}\frac{\phi(m_3)}{q_v}+\sum_{\substack{v_1<v_2\\v_1,v_2\neq k}}\frac{\phi(m_2)}{q_{v_1}q_{v_2}}+\cdots+\sum_{\substack{v_1<v_2<\cdots<v_{s-2}\\v_1,v_2,\ldots,v_{s-2}\neq k}}\frac{\phi(m_2)}{q_{v_1}q_{v_2}\cdots q_{v_{s-2}}}\right)\right].
\end{aligned}$$

Portanto,

$$\begin{aligned}
Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t\theta_1^i(t)) &= \frac{1}{h}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\theta_1^i(t)) \\
&= \frac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\frac{m_1\left(\frac{m_2}{p_k}-1\right)}{p}.
\end{aligned}$$

□

Lema 5.0.16. *Sejam $\mathbb{K}_{m_1}$, $\mathbb{K}_{m_2}$ e $\mathbb{K}_{m_3}$ p-extensões abelianas não ramificadas de condutores $m_1 = p_1p_2\ldots p_k$, $m_2 = p_kp_{k+1}\ldots p_s$ e $m_3 = m_1m_2/p_k^2$, respectivamente, com $mdc(m_1, m_2) = p_k$ de forma que $\mathbb{K}_{m_3} \subseteq \mathbb{K}_{m_1}\mathbb{K}_{m_2}$. Se $G = \{\theta_1^i \circ \theta_2^j\}_{i,j=0\ldots p-1}$ é o grupo de Galois de $\mathbb{K}_{m_1}\mathbb{K}_{m_2}$ sobre $\mathbb{Q}$, satisfazendo:*

1. *$\theta_1|_{\mathbb{K}_{m_2}}$ é um gerador de $Gal(\mathbb{K}_{m_2}/\mathbb{Q})$, com $\theta_1|_{\mathbb{K}_{m_1}} = Id_{\mathbb{K}_{m_1}}$;*
2. *$\theta_2|_{\mathbb{K}_{m_1}}$ é um gerador de $Gal(\mathbb{K}_{m_1}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}_{m_2}} = Id_{\mathbb{K}_{m_2}}$;*
3. *$(\theta_1 \circ \theta_2)|_{\mathbb{K}_{m_3}} = Id_{\mathbb{K}_{m_3}}$,*

e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}_{m_1}\mathbb{K}_{m_2}}(\zeta_n)$, então, para $1 \leqslant i, j \leqslant p-1$, temos que:

$$Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \begin{cases} \dfrac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}, & \text{se } i \neq j \\ \dfrac{m_1\left(\frac{m_2}{p_k}-1\right)+m_2\left(\frac{m_1}{p_k}-1\right)-m_3+1}{p^2}-\dfrac{m_3\,(p_k-1)}{p}, & \text{se } i = j \end{cases}.$$

Demonstração. Pela equação (4.1) temos que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = T_3^0 + T_3^1 + T_3^2 + \cdots + T_3^{s-1} + T_3^s,$$

onde

$$T_3^{\tilde{u}} = h\left[\sum_{\substack{l_1<l_2<\ldots<l_{\tilde{t}_1},\ l'_1<l'_2<\ldots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=\tilde{u}}} S'_{l_1,l_2,\ldots,l_{\tilde{t}_1},l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} S^{i,j}_{l_1,l_2,\ldots,l_{\tilde{t}_1},l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} + \sum_{\substack{l_1<l_2<\ldots<l_{\tilde{t}_1},\ l'_1<l'_2<\ldots<l'_{\tilde{t}_2}\\ \tilde{t}_1+\tilde{t}_2=\tilde{u}-1}} S'_{l_1,l_2,\ldots,l_{\tilde{t}_1},k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}} S^{i,j}_{l_1,l_2,\ldots,l_{\tilde{t}_1},k,l'_1,l'_2,\ldots,l'_{\tilde{t}_2}}\right].$$

Note que, $T_3^0 = 0$. Faremos aqui uma divisão em dois casos:

Caso 1: Se $i \neq j$.

Repare que neste caso, pela Proposição 5.0.13, os valores não nulos são exatamente os que aparecem multiplicando $\frac{1}{p^2}$ nos dois lemas auxiliares anteriores, dessa forma:

$$Tr_{\mathbb{K}_{m_1}\mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{m_1\left(\frac{m_2}{p_k}-1\right) + m_2\left(\frac{m_1}{p_k}-1\right) - m_3 + 1}{p^2}.$$

Caso 2: Se $i = j$.

Sejam $0 \leqslant u \leqslant k-1$, $0 \leqslant u' \leqslant s-k$, $d, d' \geqslant 1$ e considere que

$$\begin{pmatrix} a \\ a-b \end{pmatrix} = 0,$$

se $b \geqslant a$. Logo, o termo geral $T_3^{\tilde{u}} = (-1)^{\tilde{u}} h\,(\lambda_{\tilde{u}_1} - \lambda_{\tilde{u}_2} + \lambda_{\tilde{u}_3})$, onde

$$\lambda_{\tilde{u}_1} = \frac{1}{p^2}\sum_{u+u'=0}^{\tilde{u}-2}(-1)^{u+u'}\Gamma_{u,u'}, \tag{5.25}$$

$$\lambda_{\tilde{u}_2} = \frac{1}{p^2}\sum_{u+u'=0}^{\tilde{u}-3}(-1)^{u+u'}\Gamma_{u,u',k}, \tag{5.26}$$

$$\lambda_{\tilde{u}_3} = \frac{1}{p^2}\sum_{u+u'=0}^{\tilde{u}-2}(-1)^{u+u'}\tilde{\Gamma}_{u,u'} + \frac{1}{p}\sum_{u+u'=\tilde{u}-1}(-1)^{u+u'}\Omega_{u,u'}, \tag{5.27}$$

sendo

$$\Omega_{u,u'} = \sum_{\substack{L_1\in\mathcal{P}(P'_1),\ L_2\in\mathcal{P}(P'_2)\\ |L_1|=u \text{ e } |L_2|=u'}} \frac{\phi(n)}{\prod_{l=1}^{u} q_l \prod_{l'=1}^{u'} q'_{l'}},$$

$$\Gamma_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')}\begin{pmatrix} k-1-u \\ (k-1-u)-d \end{pmatrix}\begin{pmatrix} s-k-u' \\ (s-k-u')-d' \end{pmatrix}\right]\Omega_{u,u'},$$

$$\Gamma_{u,u',k} = \left[\sum_{d+d'=\tilde{u}-(u+u')-1}\begin{pmatrix} k-1-u \\ (k-1-u)-d \end{pmatrix}\begin{pmatrix} s-k-u' \\ (s-k-u')-d' \end{pmatrix}\right]\frac{\Omega_{u,u'}}{q_k},$$

$$\tilde{\Gamma}_{u,u'} = \left[\sum_{d+d'=\tilde{u}-(u+u')+1} \binom{k-1-u}{(k-1-u)-(d-1)} \binom{s-k-u'}{(s-k-u')-(d'-1)}\right] \Omega_{u,u'},$$

onde $\mathcal{P}(P_1')$ e $\mathcal{P}(P_2')$ o conjuntos de todos os subconjuntos de P_1' e P_2', respectivamente.

Além disso, o termo $\dfrac{T_3^s}{h}$ é dado por:

$$(-1)^s \frac{\phi(n)}{q_1 q_2 \dots q_s} \left(D_{P_1'} D_{P_2'} q_k - D_{P_1'} D_{P_2'} + (-1)^{s-k} D_{P_1'} \frac{q_k}{p} + (-1)^{k-1} D_{P_2'} \frac{q_k}{p} + (-1)^{s-1} \frac{q_k}{p} \right).$$

Logo,

$$T_3^s = (-1)^s h \left(\frac{1}{p^2} - \frac{1}{p^2 q_k} \right) \left[\sum_{u+u'=0}^{s-1} (-1)^{u+u'} \Omega_{u,u'} \right] + (-1)^{s-1} \frac{q_k}{p}.$$

Pela Proposição 5.0.1, temos que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t^2)$ é igual a

$$\begin{aligned}
h \quad & \left[\left(-\frac{1}{p} + \frac{2}{p^2} \right) \left(\phi(n) + \sum_{v=1}^{s} \frac{\phi(n)}{q_v} + \sum_{v_1<v_2} \frac{\phi(n)}{q_{v_1} q_{v_2}} + \cdots + \sum_{v_1<v_2<\cdots<v_{s-1}} \frac{\phi(n)}{q_{v_1} q_{v_2} \dots q_{v_{s-1}}} \right) \right. \\
- \quad & \frac{1}{p^2} \left(\phi(m_1) + \sum_{l=1}^{k-1} \frac{\phi(m_1)}{q_l} + \sum_{l_1<l_2} \frac{\phi(m_1)}{q_{l_1} q_{l_2}} + \cdots + \sum_{l_1<l_2<\cdots<l_{k-2}} \frac{\phi(m_1)}{q_{l_1} q_{l_2} \dots q_{l_{k-2}}} \right) \\
- \quad & \frac{1}{p^2} \left(\phi(m_2) + \sum_{l'=1}^{s-k} \frac{\phi(m_2)}{q_{l'}'} + \sum_{l_1'<l_2'} \frac{\phi(m_2)}{q_{l_1'}' q_{l_2'}'} + \cdots + \sum_{l_1'<l_2'<\cdots<l_{s-k-1}'} \frac{\phi(m_2)}{q_{l_1'}' q_{l_2'}' \dots q_{l_{s-k-1}'}'} \right) \\
+ \quad & \left. \left(\frac{1}{p} - \frac{1}{p^2} \right) \left(\phi(m_3) + \sum_{\substack{v=1 \\ v \neq k}}^{s} \frac{\phi(m_3)}{q_v} + \sum_{\substack{v_1<v_2 \\ v_1, v_2 \neq k}} \frac{\phi(m_2)}{q_{v_1} q_{v_2}} + \cdots + \sum_{\substack{v_1<v_2<\cdots<v_{s-2} \\ v_1, v_2, \dots, v_{s-2} \neq k}} \frac{\phi(m_2)}{q_{v_1} q_{v_2} \dots q_{v_{s-2}}} \right) \right].
\end{aligned}$$

Portanto,

$$Tr_{\mathbb{K}_{m_1} \mathbb{K}_{m_2}/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \frac{m_1 \left(\frac{m_2}{p_k} - 1 \right) + m_2 \left(\frac{m_1}{p_k} - 1 \right) - m_3 + 1}{p^2} - \frac{m_3 (p_k - 1)}{p}.$$

□

Índice Remissivo