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

Eliton Mendonça Moro

Forma traço integral de um corpo de números com grau e condutor ímpares e livres de quadrados

São José do Rio Preto
2020

Eliton Mendonça Moro

Forma traço integral de um corpo de números com grau e condutor ímpares e livres de quadrados

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.

Orientador: Prof. Dr. Antonio Aparecido de Andrade
Coorientadora: Profa. Dra. Carina Alves Severo

Financiadora: CAPES

São José do Rio Preto
2020

M867f

Moro, Eliton Mendonça

Forma traço integral de um corpo de números com grau e condutor ímpares e livres de quadrados / Eliton Mendonça Moro. -- São José do Rio Preto, 2020

73 p.

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

Orientador: Antonio Aparecido de Andrade

Coorientadora: Carina Alves Severo

1. Corpo de números. 2. Reticulados algébricos. 3. Forma traço integral. 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.

Eliton Mendonça Moro

Forma traço integral de um corpo de números com grau e condutor ímpares e livres de quadrados

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

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Orientador

Prof. Dr. Agnaldo José Ferrari
UNESP - Bauru

Profa. Dra. Ana Cláudia Machado Mendonça Chagas
UFGD - Dourados

Prof. Dr. Edson Donizete de Carvalho
UNESP - São José do Rio Preto

Prof. Dr. Trajano Pires da Nóbrega Neto
UNESP - São José do Rio Preto

São José do Rio Preto
28 de fevereiro de 2020

Aos meus pais, Dorival e Paula,
ao meu irmão Elton e a
minha namorada Tatiana,
dedico

AGRADECIMENTOS

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

Ao meu orientador, Prof. Dr. Antonio, pela orientação, pelos conselhos, pela confiança e pela amizade durante todos esses anos de doutorado.

A minha coorientadora, Profa. Dra. Carina, pela caminhada desde a graduação, pela amizade, pelo incentivo, confiança e apoio.

Ao Prof. Dr. Trajano e ao Daniel, pelas amizade e pelos encontros semanais que contribuíram muito com minha formação e amadurecimento do conhecimento na área.

Aos meus pais Dorival e Paula, meu irmão Elton e a minha namorada Tatiana e a toda minha família por me apoiar ao longo desse trajeto.

Aos meus amigos Ana, André Antunes, André Carvalho, Carol, Cheienne, Dienes, Eduardo, Gustavo, Harison, Heloísa, Jéssica, Junior, Jarne, Laura, Lucas Arakaki, Lucas Ueno, Luiz, Otávio, Plínio, Ronisio, Rodrigo Bononi, Rodrigo Ishisaka, Samuel, Willian e todos aos alunos da pós-graduação pelas amizades, conversas, risadas, jogatinas, campeonatos, e por tudo mais ao longo da minha pós-graduação.

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

RESUMO

Os reticulados vem ganhando cada vez mais importância devido às suas aplicações em criptografia e na teoria da informação. Dentre as diversas maneiras de se construir reticulados, uma delas é a construção via extensão de corpos. Visando a densidade de centro de um reticulado, a maior dificuldade de construí-los via extensões de corpos é calcular o raio de empacotamento. Desta forma, neste trabalho apresentamos a forma traço integral de uma extensão abeliana finita dos racionais com grau e condutor ímpar e livres de quadrados. Ao minimizar a forma traço integral em um $\mathbb{Z}$-módulo do anel de inteiros obtemos o raio de empacotamento, e assim, podemos calcular a densidade de centro do reticulado.

Palavras-chave: Corpo de números, Reticulados algébricos, Forma traço integral.

ABSTRACT

Lattices are becoming increasingly important due to their applications in cryptography and information theory. Among the various ways of constructing lattices, one of them is a construction via field extension. Aiming the density of the center of a lattice, the greatest difficulty in constructing them through field extensions is the calculation of the packing radius. Thus, in this work we present an integral trace form of a finite abelian extension of rationals with odd and square-free degree and conductor. By minimizing an integral trace form in a $\mathbb{Z}$-module of the integer ring obtains the packing radius and thus the density of the center of the lattice can be calculated.

Keywords: Number field, Algebraic lattices, Integral trace form.

Sumário

Introdução **15**

1 Conceitos preliminares **17**
1.1 Módulos 17
1.2 Extensão de corpos 18
1.3 Traço, norma e discriminante 21
1.4 Decomposição de ideais 25
1.5 Considerações finais do capítulo 27

2 Reticulados **29**
2.1 Empacotamento esférico 30
2.2 Reticulados algébricos 31
2.2.1 Homomorfismo torcido 32
2.2.2 Reticulados sobre corpos de números 33
2.3 Considerações finais do capítulo 35

3 Forma traço integral **37**
3.1 Caracterização do condutor e contagem dos subcorpos 37
3.2 Caso ramificado de grau p 38
3.3 Caso não ramificado de grau p 39
3.4 Caso não ramificado de grau pq 40
3.5 Caso não ramificado de grau $p_1 \cdots p_r$ 46
3.6 Considerações finais do capítulo 54

4 Mínimo da forma traço integral **57**
4.1 Módulos em um compósito de corpos de graus primos distintos e condutores iguais 57
4.2 Módulos em um compósito de dois corpos de condutores m_1 e $m_2 = rm_1$ . . . 59
4.3 Considerações finais do capítulo 63

5 Considerações finais do trabalho e perspectivas futuras **65**
5.1 Homomorfismo torcido 65
5.2 Mínimo da forma traço 68
5.3 Condutor com termos quadráticos 68

Referências **71**

Índice Remissivo **73**

Introdução

A teoria dos números é um dos mais antigos campos de estudo em matemática, antes mesmo de existir qualquer formalização da matemática, os povos antigos vinham tentando resolver problemas associados a esta teoria como por exemplo Pitágoras (570-500 a.c.) que fundou, na atual região da Itália, uma escola, conhecida como Ordem Pitagórica. Os pitagóricos devotaram considerável atenção aos números primos e muitos problemas da teoria dos números foram formulados por eles.

Ao decorrer do tempo, estudos foram sendo desenvolvidos e diversos resultados foram sendo apresentados, como por exemplo, o último teorema de Fermat. A teoria algébrica dos números é um ramo da teoria dos números em que o conceito de número é expandido para o conceito de número algébrico, que são raízes de polinômios com coeficientes racionais (ou inteiros, dependendo do contexto). Évariste Galois (1811-1832) desenvolveu a teoria de Galois, uma importante ferramenta que molda a atual teoria algébrica dos números.

Ao longo do tempo, a matemática foi criando diversas ramificações de estudos, cada uma dessas ramificações com sua devida importância. Entre as diversas linhas que surgiram, uma delas foi a dos reticulados. Reticulados é um conjunto de pontos espalhados no $\mathbb{R}^n$ e fixando um raio r, construímos bolas de raio r centradas nesses pontos de forma que quaisquer duas bolas se interceptem no máximo em um ponto. Um dos interesses no estudo de reticulados é construí-los de forma que as bolas ocupem a maior parte do espaço possível. Em 1948, Claude Elwood Shannon (1916-2001) publicou um artigo que estabelece as bases teóricas para o estudo de esquemas de transmissão de informação eficientes e seguros, dando assim aos reticulados uma notável importância por desempenharem um importante papel na teoria da informação.

A teoria algébrica dos números vem ganhado cada vez mais importância prática ao produzir aplicações importantes à teoria de códigos e à criptografia, dentre elas, a construções de reticulados com boas densidade de centro. Os reticulados podem ser construídos de diversas formas, porém neste trabalho vamos focar na construção de reticulados algébricos, isto é, reticulados construídos via o homomorfismo canônico (ou torcido) a partir de uma extensão finita dos racionais. Construir um reticulado algébrico é simples, basta conhecer os homomorfismo de uma extensão de corpos, contudo uma dificuldade nos estudos de reticulados está em calcular sua densidade de centro.

A densidade de centro de um reticulado algébrico, no caso do homomorfismo canônico, possui quatro parâmetros: o número correspondente a metade da quantidade de homomorfismo complexos da extensão; o raio de empacotamento; o discriminante do corpo estendido; o índice do $\mathbb{Z}$-módulo no anel de inteiros. Dentre esses parâmetros dois se destacam pela dificuldade de calcula-los, o discriminante e o raio de empacotamento. Existem diversos trabalhos a respeito do discriminante de um corpo, embora ainda tenha muito a ser explorado. Nosso foco, neste trabalho, é descrever o raio de empacotamento, cujo comportamento é dado pela forma traço integral.

No Capítulo 1, apresentamos uma revisão teórica de alguns dos principais pré-requisitos para poder ter uma melhor compreensão sobre o trabalho. Dentre eles estão alguns tópicos da teoria de Galois e módulos.

No Capítulo 2, abordamos o assunto de reticulados, algumas formas de se construir e como calcular a densidade de centro de reticulados em certas construções. Dentre as formas de se construir reticulados, damos destaque aos reticulados algébricos construídos sobre uma extensão dos racionais que será o foco principal deste trabalho.

No Capítulo 3, apresentamos alguns resultados já existentes na literatura sobre a forma traço integral, como, por exemplo, alguns resultados presentes em [1],[2] e [3] que abordam a forma traço integral de uma extensão abeliana dos racionais de grau p ramificada, e em [14] e [15] que abordam a forma traço integral de uma extensão abeliana dos racionais de grau p não ramificada, onde p é um número primo impar em ambos os casos. Além disso, apresentamos nossas principais contribuições deste trabalho. As seções 3.4 e 3.5, consistem em estudar a forma traço integral de uma extensão $\mathbb{M}/\mathbb{Q}$. Na Seção 3.4 o grau da extensão é pq, com $p \neq q$ e na Seção 3.5 e $p_1 \cdots p_r$, com $p_i \neq p_j$ se $i \neq j$.

No Capítulo 4, considerando os Teoremas 3.12 e 3.14, apresentamos o mínimo da forma traço integral em certos $\mathbb{Z}$-módulos e construímos reticulados a partir desses $\mathbb{Z}$-módulos.

No Capítulo 5, apresentamos uma conclusão do trabalho e uma perspectiva futura sobre o homomorfismo torcido e outros condutores para a forma traço integral.

1 Conceitos preliminares

Neste capítulo, introduzimos alguns conceitos básicos da teoria de Galois e da teoria algébrica dos números para a compreensão e desenvolvimento dos próximos capítulos. Os conceitos de traço, módulo e reticulados são essenciais para a compreensão do Capítulo 3, no qual está a nossa principal contribuição para o assunto. A demonstração de alguns resultados está omitida, mas inserimos a referência nos que seguem sem demonstração.

1.1 Módulos

Nesta seção, apresentamos o conceito de um módulo sobre um anel, com o enfoque para $\mathbb{Z}$-módulos livres de posto n. As definições de módulos e submódulos são necessárias no contexto de reticulados, pois a partir da estrutura de um módulo é que construímos exemplos de reticulados utilizando os resultados apresentados nas Seções 3.4, 3.5, 4.1 e 4.2. No que segue, consideramos A sendo um anel comutativo com unidade.

Definição 1.1. Seja A um anel. Um grupo abeliano aditivo $(M, +)$ munido de um produto

$$\cdot : A \times M \to M$$

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

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

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

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

iv) $1x = x$,

para todo $a, b \in A$ e $x, y \in M$.

Um subgrupo N de M é chamado de um A-submódulo de M, se para todo $a \in A$ e $x \in N$ tivermos $ax \in N$. Note que todo anel A é um A-módulo, todo espaço vetorial sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo e todo grupo abeliano é um $\mathbb{Z}$-módulo.

Definição 1.2. Seja M um A-módulo.

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

ii) Dizemos que um subconjunto $B = \{x_1, \ldots, x_n\} \subset M$ é linearmente independente sobre A se $a_1x_1 + \cdots + a_nx_n = 0$, com $a_i \in A$, então $a_i = 0$, para $i = 1, \ldots, n$.

iii) Um conjunto $B = \{x_1, \ldots, x_n\} \subset M$ é dito uma base de M quando o conjunto B é formado por geradores linearmente independente sobre A. Se M possui uma base, o módulo M é chamado um A-módulo livre e o número de elementos da base é chamado posto de M.

Teorema 1.3. ([17], pag. 21) sejam A um anel principal, M um A-módulo livre de posto n e N um A-submódulo de M.

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

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

1.2 Extensão de corpos

Nesta seção, abordamos conceitos da teoria de Galois sobre extensões de corpos. Os reticulados construídos no Capítulo 3 são construídos a partir de um módulo dentro do anel de inteiros $\mathcal{O}_{\mathbb{L}}$, onde $\mathbb{L}$ é um corpo de números, e esta construção utiliza os conceito de homomorfismo canônico e torcido. Assim, para ter um bom domínio sobre essas estruturas primeiro caracterizamos extensões de corpos, o anel de inteiros de um corpo de números e corpos ciclotômicos.

Definição 1.4. Dizemos que um corpo $\mathbb{L}$ é uma extensão de um corpo $\mathbb{K}$ se $\mathbb{K} \subset \mathbb{L}$. Podemos considerar $\mathbb{L}$ como um $\mathbb{K}$-espaço vetorial, e assim, chamamos $dim_{\mathbb{K}}\mathbb{L} = [\mathbb{L} : \mathbb{K}]$ o grau da extensão de $\mathbb{L}$ sobre $\mathbb{K}$. Se o grau da extensão for finita dizemos que $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$. Denotamos a extensão $\mathbb{L}$ sobre $\mathbb{K}$ por $\mathbb{L}/\mathbb{K}$.

Definição 1.5. Seja $\mathbb{Q}$ o corpo dos números racionais. Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$ de grau n, dizemos que $\mathbb{K}$ é um corpo de números de grau n, e $\mathbb{K}$ é chamado de uma n-extensão.

Definição 1.6. Seja $\mathbb{K}$ um corpo de números. O anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é definido como o conjunto dos elementos de $\mathbb{K}$ que são raízes de polinômios mônicos sobre $\mathbb{Z}$. Um elemento $x \in \mathcal{O}_{\mathbb{K}}$ é chamado de elemento inteiro de $\mathbb{K}$.

Proposição 1.7. ([17], pag. 40) Se $\mathbb{K}$ é um corpo de números de grau n, então $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n.

Definição 1.8. Seja $\mathbb{K}$ um corpo de números. Uma base de $\mathcal{O}_{\mathbb{K}}$ como um $\mathbb{Z}$-módulo é chamada base integral de $\mathbb{K}$.

A seguir, começamos a exibir resultados que permitem compreender o Teorema da Correspondência de Galois.

Proposição 1.9. ([17], pag. 31) Se $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ são extensões de corpos, então $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Definição 1.10. Sejam $\mathbb{K}$ um corpo de números e $\alpha \notin \mathbb{C}$. O menor corpo que contém $\mathbb{K}$ e α é definido por $\mathbb{K}(\alpha)$ e $[\mathbb{K}(\alpha) : \mathbb{K}]$ =grau$(p(x))$, onde $p(x) = min_{\alpha,\mathbb{K}}(x)$ é o polinômio minimal de α sobre $\mathbb{K}$ e $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]/(p(x))$.

Teorema 1.11. ([17], pag. 33) Se $\mathbb{K}$ é um corpo de números, $\mathbb{L}$ uma extensão de grau n de $\mathbb{K}$ e $\mathbb{M}$ um corpo algebricamente fechado contendo $\mathbb{K}$, então existem n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{M}$.

Teorema 1.12. ([16], pag. 20)(Lema de Dedekind) Se $\mathbb{L}/\mathbb{K}$ é uma extensão finita de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ num corpo algebricamente fechado $\mathbb{M}$ contendo $\mathbb{K}$, então $\{\sigma_1, \ldots, \sigma_n\}$ é linearmente independente sobre $\mathbb{M}$, isto é, se existem elementos $a_1, \ldots, a_n \in \mathbb{M}$ tais que $\sum_{i=1}^{n} a_i\sigma_i(x) = 0$, para todo $x \in \mathbb{L}$, então necessariamente $a_1 = \cdots = a_n = 0$.

Teorema 1.13. ([17], pag. 34)(Teorema do elemento primitivo) Se $\mathbb{L}/\mathbb{K}$ é uma extensão finita, então existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$, onde α é chamado de elemento primitivo.

Seja $Aut(\mathbb{L}) = \{\sigma : \mathbb{L} \to \mathbb{L} \mid \sigma \text{ é um isomorfismo}\}$.

Definição 1.14. Seja $\mathbb{L}/\mathbb{K}$ uma extensão finita de corpos. O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é o conjunto de todos os $\mathbb{K}$-automorfismos de $\mathbb{L}$, ou seja, é o conjunto $\{\sigma \in Aut(\mathbb{L}) \mid \sigma|_{\mathbb{K}} = id_{\mathbb{K}}\}$. Denotamos este grupo por $Gal(\mathbb{L}/\mathbb{K})$.

Definição 1.15. Uma extensão finita $\mathbb{L}$ de $\mathbb{K}$ é dita uma extensão galoisiana, ou de Galois, se $[\mathbb{L} : \mathbb{K}] = \circ(Gal(\mathbb{L}/\mathbb{K}))$. Uma extensão de Galois é dita abeliana (ou cíclica) se o grupo de Galois é abeliano (ou cíclico).

Teorema 1.16. ([18], Teo. 12.1)(Teorema de Correspondência de Galois) Seja $\mathbb{L}/\mathbb{K}$ uma extensão de Galois.

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

ii) Se $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, então $\mathbb{L}/\mathbb{M}$ é de Galois e $Gal(\mathbb{L}/\mathbb{M})$ é o único subgrupo de $Gal(\mathbb{L}/\mathbb{K})$ que satisfaz
$$[\mathbb{L} : \mathbb{M}] = \frac{\circ(Gal(\mathbb{L}/\mathbb{K}))}{\circ(Gal(\mathbb{L}/\mathbb{M}))}.$$

iii) Se $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, então $\mathbb{M}/\mathbb{K}$ é de Galois se, e somente se, $Gal(\mathbb{L}/\mathbb{M})$ é um subgrupo normal de $Gal(\mathbb{L}/\mathbb{K})$. Neste caso,
$$Gal(\mathbb{M}/\mathbb{K}) \simeq \frac{Gal(\mathbb{L}/\mathbb{K})}{Gal(\mathbb{L}/\mathbb{M})}.$$

Com base no Teorema 1.16, se $\mathbb{L}/\mathbb{K}$ é uma extensão de Galois, então temos o seguinte diagrama:

$$\begin{tikzcd}
\mathbb{L} \arrow[r, leftrightarrow] \arrow[d, dash, "m"] & \{id\} \arrow[d, dash, "m"] \\
\mathbb{M} \arrow[r, leftrightarrow] \arrow[d, dash, "n"] & Gal(\mathbb{L}/\mathbb{M}) \arrow[d, dash, "n"] \\
\mathbb{K} \arrow[r, leftrightarrow] & Gal(\mathbb{L}/\mathbb{K})
\end{tikzcd}$$

Definição 1.17. Sejam $\mathbb{L}$ e $\mathbb{M}$ extensões de um corpo $\mathbb{K}$. O menor corpo que contém $\mathbb{L}$ e $\mathbb{M}$ é chamado de compósito dos corpos $\mathbb{L}$ e $\mathbb{M}$ e denotado por $\mathbb{LM}$.

Teorema 1.18. ([16], pag. 17)(Irracionalidade Natural) Se $\mathbb{L}/\mathbb{K}$ é uma extensão de Galois e $\mathbb{M}/\mathbb{K}$ é uma extensão arbitrária, então $\mathbb{LM}/\mathbb{M}$ é de Galois e $Gal(\mathbb{LM}/\mathbb{M}) \simeq Gal(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$.

$$\begin{tikzcd}
 & \mathbb{LM} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{L} \arrow[dr, dash] & & \mathbb{M} \arrow[dl, dash] \\
 & \mathbb{L} \cap \mathbb{M} \arrow[d, dash] & \\
 & \mathbb{K} &
\end{tikzcd}$$

Teorema 1.19. ([16], pag. 17) Se $\mathbb{L}/\mathbb{K}$ e $\mathbb{M}/\mathbb{K}$ são extensões de Galois, então $\mathbb{LM}/\mathbb{K}$ é uma extensão de Galois.

Definição 1.20. Seja $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$.

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

ii) Se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, para todo $i = 1, \ldots, n$, dizemos que $\mathbb{K}$ é um corpo totalmente real.
Se $\sigma_i(\mathbb{K}) \not\subset \mathbb{R}$, para todo $i = 1, \ldots, n$, dizemos que $\mathbb{K}$ é um corpo totalmente complexo.

Observação 1.21. Se $\mathbb{K}/\mathbb{Q}$ é uma extensão de Galois de grau n, então os $\mathbb{Q}$-monomorfismos σ_i, com $i = 1, \ldots, n$, que compõem o grupo de Galois leva $\mathbb{K}$ em $\mathbb{K}$, ou seja, $\sigma_i(\mathbb{K}) = \mathbb{K}$. Desta forma, $\mathbb{K}$ é totalmente real ou totalmente complexo, e observamos que os monomorfismos complexos sempre aparecem aos pares.

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

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

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

Teorema 1.22. ([16], pag. 273)(Teorema de Kronecker-Weber) Se $\mathbb{K}/\mathbb{Q}$ é uma extensão abeliana finita, então existe uma raiz n-ésima da unidade ζ_n tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$.

Definição 1.23. Seja $\mathbb{K}/\mathbb{Q}$ uma extensão abeliana finita. O menor inteiro positivo n tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ é chamado de condutor do corpo $\mathbb{K}$ e o denotamos por $cond(\mathbb{K}) = n$.

Sejam $\mathbb{Z}_n^*$ é o grupo das classes residuais invertíveis módulo n e

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

onde $n > 1$ é um inteiro positivo, então $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$ via o isomorfismo natural $\sigma_i \mapsto \bar{i}$.

Teorema 1.24. ([16], pag. 44) O grupo $\mathbb{Z}_n^*$ é cíclico se, e somente se, $n = 2$, 4, p^r ou $2p^r$, onde p é um primo ímpar e $r \geq 1$.

1.3 Traço, norma e discriminante

Nesta seção, apresentamos os conceitos de norma, traço, discriminante e algumas de suas propriedades. A teoria apresentada aqui é essencial para o desenvolvimento dos resultados principais deste trabalho. O traço, $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$, está relacionado com o raio de empacotamento de um reticulado algébrico, e o discriminante de um corpo está relacionado com a densidade de centro de um reticulado algébrico.

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

Definição 1.25. A norma e o traço de um elemento $\alpha \in \mathbb{L}$ na extensão $\mathbb{L}/\mathbb{K}$ é definido da seguinte forma:

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

Seja $\mathbb{M}/\mathbb{L}$ um extensão finita. Se $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, $a \in \mathbb{K}$, $\alpha, \beta \in \mathbb{L}$ e , $\gamma \in \mathbb{M}$, então valem as seguintes propriedades:

1) $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$;

2) $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}/\mathbb{K}}(\alpha)$;

3) $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$;

4) $Tr_{\mathbb{M}/\mathbb{K}}(\gamma) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\gamma))$;

5) $Tr_{\mathbb{M}/\mathbb{K}}(\alpha) = [\mathbb{M} : \mathbb{L}]Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$;

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

7) $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$;

8) $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$;

9) $N_{\mathbb{M}/\mathbb{K}}(\gamma) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\gamma))$;

10) $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha)^{[\mathbb{M}:\mathbb{L}]}$.

Proposição 1.26. ([17], pag. 36) Se $\mathbb{K}$ é um corpo de números, $\mathbb{L}$ uma extensão de grau n de $\mathbb{K}$, $\alpha \in \mathbb{L}$ e $\alpha_1, \ldots, \alpha_n$ raízes do polinômio minimal de α sobre $\mathbb{K}$, então

$$Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n \text{ e } N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n.$$

Proposição 1.27. ([16], pag. 28) Se $\mathbb{K} \subset \mathbb{L}$ são corpos de números e $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de $\mathcal{O}_{\mathbb{K}}$.

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

$$disc_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) = det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j)),$$

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

Proposição 1.28. ([17], pag. 39) Se $\sigma_1, \ldots, \sigma_n$ são os $\mathbb{K}$-monomorfismos de $\mathbb{L}$ num corpo algebricamente fechado, então

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

Se $\alpha_1, \ldots, \alpha_n$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então $disc_{\mathbb{L}/\mathbb{K}}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Proposição 1.29. ([17], pag. 38) Se $(\beta_1, \ldots, \beta_n)$ é uma n-upla de elementos em $\mathbb{L}$ tal que $\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i$ com $a_{ij} \in \mathbb{K}$, para $j = 1, \ldots, n$, então

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

Para definir o discriminante de um corpo, precisamos do conceito de base integral normal.

Definição 1.30. Seja $\mathbb{K}/\mathbb{Q}$ uma extensão de Galois com

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

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

Definição 1.31. Seja $\mathbb{K}$ um corpo de números. O discriminante em $\mathbb{K}/\mathbb{Q}$ de uma base integral de $\mathbb{K}$ é chamado de discriminante do corpo $\mathbb{K}$ e denotado por $disc(\mathbb{K})$.

Proposição 1.32. ([13], pag. 37) Se $\mathbb{K}$ é um corpo de números abeliano de grau primo p e condutor n, então

$$|disc(\mathbb{K})| = n^{p-1}.$$

Teorema 1.33. ([13], pag. 38) Se $\mathbb{K}$ é um corpo de números abeliano de condutor $n = p_1^{a_1} \cdots p_s^{a_s}$, então

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

Observação 1.34. Note que

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

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

$$|disc(\mathbb{K})| = p_1^{\alpha_1} \cdots p_s^{\alpha_s},$$

onde

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

Definição 1.35. Sejam $\mathbb{K}_1$ e $\mathbb{K}_2$ corpos de números de grau m_1 e m_2, respectivamente. Dizemos que $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos quando $[\mathbb{K}_1\mathbb{K}_2 : Q] = m_1m_2$. Se $\mathbb{K}_1$ e $\mathbb{K}_2$ são disjuntos e seus discriminantes são relativamente primos, então os corpos $\mathbb{K}_1$ e $\mathbb{K}_2$ são chamados linearmente disjuntos.

Proposição 1.36. ([10], pag. 68) Se $\mathbb{K}_1$ e $\mathbb{K}_2$ são corpos de números linearmente disjuntos de graus m_1 e m_2, respectivamente, então

(i) $\mathcal{O}_{\mathbb{K}_1\mathbb{K}_2} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2}$;

(ii) $disc(\mathbb{K}_1\mathbb{K}_2) = disc(\mathbb{K}_1)^{m_2} disc(\mathbb{K}_2)^{m_1}$.

Nos próximos resultados, consideramos ζ_n uma raiz n-ésima primitiva da unidade.

Proposição 1.37. ([14], pag. 29) Sejam n um inteiro livre de quadrados e s a quantidade de primos distintos que dividem n, então

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

Demonstração. Se $n = p_1$, com p_1 um primo, então o resultado segue do fato de que $x^{p_1-1} + x^{p_1-2} + \cdots + 1$ é o polinômio minimal de ζ_n. Se $n = p_1 \cdots p_s$, então

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) &= Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{p_1})}(\zeta_{p_1}\zeta_{n/p1})) \\ &= Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1} Tr_{\mathbb{Q}(\zeta_{n/p1})/\mathbb{Q}}(\zeta_{n/p1})) \\ &= Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}) Tr_{\mathbb{Q}(\zeta_{n/p1})/\mathbb{Q}}(\zeta_{n/p1}) \\ &= Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}) \cdots Tr_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}) \\ &= (-1)\cdots(-1) = (-1)^s, \end{aligned}$$

o que prova a proposição. □

Os próximos resultados caracterizam os subcorpos de um corpo ciclotômico e exibem uma base integral normal.

Proposição 1.38. ([14], pag. 29) Se $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$, onde n é livre de quadrados e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então $\mathbb{K} = \mathbb{Q}(t)$.

Demonstração. Como $t \in \mathbb{K}$, segue que $\mathbb{Q}(t) \subset \mathbb{K}$. Assim, pela Proposição 1.37, segue que

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

Logo, $[\mathbb{K} : \mathbb{Q}(t)] = 1$, pois $[\mathbb{K} : \mathbb{Q}(t)]$ e $Tr_{\mathbb{Q}(t)/\mathbb{Q}}(t)$ são inteiros. □

Lema 1.39. ([14], pag. 29) Se n é livre de quadrados, então o conjunto $\{\zeta_n^i \mid i = 1, \ldots, n, mdc(i, n) = 1\}$ é um base integral normal do corpo $\mathbb{Q}(\zeta_n)$.

Demonstração. Seja $n = p_1 \cdots p_s$, com p_i primos distintos. Faremos a prova por indução sobre s. Se $s = 1$, então ζ_{p_1} é raiz do polinômio minimal $x^{p_1-1} + x^{p_1-2} + \cdots + 1$. Como os coeficientes do polinômio minimal são inteiros, segue que todas as raízes desse polinômio estão no anel de inteiros $\mathcal{O}_{\mathbb{L}}$. Assim, $\{\zeta_{p_1}, \zeta_{p_1}^2, \ldots, \zeta_{p_1}^{p_1-1}\}$ pertence ao anel de inteiros $\mathcal{O}_{\mathbb{L}}$. O conjunto $\{1, \zeta_{p_1}, \zeta_{p_1}^2, \ldots, \zeta_{p_1}^{p_1-2}\}$ é linearmente independente, pois caso não fosse existiriam inteiros a_i tal que

$$a_0 + a_1\zeta_{p_1} + \cdots + a_{p_1-2}^{p_1-2} = 0.$$

Logo, ζ_{p_1} é uma raiz do polinômio $a_{p_1-2}x^{p_1-2} + \cdots + a_1 x + a_0$, o que é um absurdo. Como $\{1, \zeta_{p_1}, \zeta_{p_1}^2, \ldots, \zeta_{p_1}^{p_1-2}\}$ é linearmente independente, segue que $\{\zeta_{p_1}, \zeta_{p_1}^2, \ldots, \zeta_{p_1}^{p_1-1}\}$ também

o é. Logo, este conjunto é uma base integral normal. Continuando o processo de indução, suponhamos que

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

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

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

Note que $\zeta_{n/p_s}^i \zeta_{p_s}^j = \zeta_n^{ip_s} \zeta_n^{j\frac{n}{p_s}}$ e $mdc(ip_s + j\frac{n}{p_s}, n) = 1$. Como B tem cardinalidade $\phi(\frac{n}{p_s}\phi(p_s))$ $= \phi(n)$, segue que $B = \{\zeta_n^i \ / \ i = 1, \ldots, n,\ mdc(i, n) = 1\}$. □

Teorema 1.40. ([14], pag. 30) Se $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$, com n livre de quadrados, $[\mathbb{K} : \mathbb{Q}] = r$ e $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_r\}$, então

$$\{\sigma_1(t), \ldots \sigma_r(t)\}$$

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

Demonstração. Para cada $\sigma_i \in Gal(\mathbb{K}/\mathbb{Q})$ existe $\varphi_i \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que $\sigma_i = \varphi_i|_{\mathbb{K}}$. Seja $Gal(\mathbb{Q}(\zeta_n)/\mathbb{K}) = \{\theta_j\}_{j=1}^e$, onde $e = \phi(n)/r$, onde ϕ é a função de Euler. Logo, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\phi_i \circ \theta_j\}_{i=1,\ldots,r}^{j=1,\ldots,e}$ e cada elemento é escrito de forma única, pois se $\phi_i \circ \theta_j = \phi_u \circ \theta_v$, então $\phi_u^{-1} \circ \phi_i = \theta_v \circ \theta_j^{-1} \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{K})$ e quando restrito a $\mathbb{K}$ é um elemento do grupo $Gal(\mathbb{K}/\mathbb{Q})$. Logo, $\phi_u^{-1} \circ \phi_i = \theta_v \circ \theta_j^{-1} = Id|_{\mathbb{K}}$. Deste modo, $u = i$, e assim, $j = v$. Seja $x \in \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Pelo Lema 1.39, segue que

$$\begin{aligned} x &= \sum_{\substack{u=1 \\ (u,n)=1}}^{n} a_u \zeta_n^u \\ &= \sum_{i=1}^{r} \sum_{j=1}^{e} a_{i,j} (\phi_i \circ \theta_j)(\zeta_n) \\ &= \phi_1 \left(\sum_{j=1}^{e} a_{1,j} \theta_j(\zeta_n) \right) + \cdots + \phi_r \left(\sum_{j=1}^{e} a_{r,j} \theta_j(\zeta_n) \right). \end{aligned}$$

Observemos que $a_{i,1} = a_{i,j}$, para qualquer j, pois para qualquer $\theta \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{K})$, segue que

$$x = \phi_1 \left(\sum_{j=1}^{e} a_{1,j} \theta_j(\zeta_n) \right) + \cdots + \phi_r \left(\sum_{j=1}^{e} a_{r,j} \theta_j(\zeta_n) \right)$$

$$x = \theta(x) = \phi_1 \left(\sum_{j=1}^{e} a_{1,j} (\theta \circ \theta_j)(\zeta_n) \right) + \cdots + \phi_r \left(\sum_{j=1}^{e} a_{r,j} (\theta \circ \theta_j)(\zeta_n) \right),$$

ou seja, uma reordenação nos índices j de $a_{i,j}$ não interfere na forma de escrever o elemento x, mas a base integral normal nos garante a unicidade da escrita. Portanto, $a_{i,1} = a_{i,j}$ para qualquer j entre 1 e e. Deste modo, $x = a_{1,1}\phi_1(t) + \cdots + a_{r,1}\phi_r(t)$. Além disso, $\phi_i \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e da independência linear de $\{\zeta_n^i \mid i = 1, \ldots, n,\ mdc(i, n) = 1\}$, segue que $\{\phi_1(t), \ldots, \phi(t)\}$ também é linearmente independente. □

O Teorema 1.40 é uma parte de uma demonstração alternativa para a recíproca do Teorema de Hilbert-Speiser, o qual diz que uma extensão abeliana finita $\mathbb{K}/\mathbb{Q}$ tem uma base normal integral se, e somente se, o condutor de $\mathbb{K}$ é ímpar livre de quadrados.

1.4 Decomposição de ideais

Nesta seção, abordamos alguns conceitos sobre decomposição de ideais. O foco deste trabalho não está diretamente relacionado com este tema, mas a caracterização do condutor de uma extensão de grau p primo ímpar está diretamente relacionado com a ramificação do ideal gerado por p. Deste modo, nesta seção, abordamos os resultados de decomposição de ideais necessários para compreender o desenvolvimento do trabalho.

Sejam $\mathbb{K}$ um corpo de números de grau m e $\mathbb{L}$ uma extensão finita de grau n sobre $\mathbb{K}$.

Teorema 1.41. ([16], pag. 128) Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$, então o ideal $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ de $\mathcal{O}_{\mathbb{L}}$ pode ser escrito unicamente na forma

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

onde os $\mathfrak{P}_i$ são ideais primos distintos de $\mathcal{O}_{\mathbb{L}}$, e os e_i's são elementos inteiros positivos.

Os ideais $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathfrak{P}_i \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$. Além disso, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$. Neste caso, dizemos que os ideais $\mathfrak{P}_i$'s são os ideais de $\mathcal{O}_{\mathbb{L}}$ que estão acima de $\mathfrak{p}$, [17].

Proposição 1.42. ([16], pag. 141) Se $\mathfrak{P}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, acima de $p\mathbb{Z}$, com p primo, então $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}$ é uma extensão finita de $\mathbb{Z}_p$ e $\left[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}} : \mathbb{Z}_p\right] \leq m$.

Definição 1.43. Seja $\mathfrak{p}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Chamamos de norma do ideal $\mathfrak{p}$ o número de elementos do anel quociente $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}$ e denotamos por $N_{\mathbb{K}}(\mathfrak{p})$, ou simplesmente, $N(\mathfrak{p})$.

Proposição 1.44. ([16], pag. 141) Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ que está acima de $p\mathbb{Z}$, com p primo, então $N(\mathfrak{p}) = p^f$, onde $f = \left[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} : \mathbb{Z}_p\right]$.

Consideremos, no que segue, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, onde $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$.

Definição 1.45. O grau $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_{\mathrm{i}}} : \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}\right]$ é chamado grau de inércia de $\mathfrak{P}_i$ e denotado por $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. O expoente $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ é chamado índice de ramificação de $\mathfrak{P}_i$. Quando pelo menos um dos índices de ramificação e_i é maior que 1, dizemos que $\mathfrak{p}$ se ramifica ou é ramificado em $\mathbb{L}$.

Teorema 1.46. ([6], pag. 104)(Teorema da Igualdade Fundamental) Se $\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, então

$$\sum_{i=1}^{r} e_i f_i = n.$$

Definição 1.47. Dizemos que o ideal $\mathfrak{p}$ é:

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

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

iii) Inerte em $\mathbb{L}$, quando $f_i = n$ para algum $i = 1, \ldots, r$, neste caso $r = e_i = 1$.

Quando $\mathbb{L}/\mathbb{K}$ é uma extensão de Galois, segue que $e_1 = \cdots = e_r$ e $f_1 = \cdots = f_r$ ([6] Teorema 20.2). Denotando $e = e_1$ e $f = f_1$, segue que a igualdade fundamental é dada por

$$efr = n.$$

Se n é primo, então os casos da Definição 1.47 são os únicos possíveis.

Teorema 1.48. ([12], pag. 65) Sejam $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ corpos de números e $\mathfrak{p}$, $\mathfrak{P}$ e $\mathfrak{P}'$ ideais primos dos respectivos anéis de inteiros de cada corpo. Se $\mathfrak{P}'$ está acima de $\mathfrak{P}$, então

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

ii) Neste caso, $e(\mathfrak{P}'/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$ e $f(\mathfrak{P}'/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$.

Teorema 1.49. [4] Seja $\mathbb{K}$ um corpo de números. Um número primo p se ramifica em $\mathbb{K}$ se, e somente se, p divide o discriminante $disc(\mathbb{K})$.

Definição 1.50. Sejam A um anel e $f(x) = \sum_{i=1}^{n} a_i x^i \in A[x]$. Denotamos por $\overline{f}(x)$ o polinômio $\sum_{i=1}^{n}(a_i + \mathfrak{p})x^i \in (A/\mathfrak{p})[x]$, onde $\mathfrak{p}$ é um ideal primo não nulo de A.

Proposição 1.51. ([10], pag. 25) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão separável de $\mathbb{K}$ de grau n, $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A tal que $\mathcal{O}_{\mathbb{L}} = A[\beta]$, para algum $\beta \in \mathbb{L}$ e $\mathfrak{p}$ um ideal primo não nulo de A. Se $f(x) = min_{\mathbb{K},\beta}(x)$ e $f_1, \cdots, f_r$ são polinômios mônicos em $A[x]$ tal que a fatoração de $\overline{f}$ em polinômios irredutíveis distintos em $(A/\mathfrak{p})[x]$ seja dada por

$$\overline{f} = \overline{f}_1^{e_1} \cdots \overline{f}_r^{e_r},$$

então os ideais primos, dois a dois distintos, $\mathfrak{P}_1 \cdots, \mathfrak{P}_r$ de $\mathcal{O}_{\mathbb{L}}$, que estão acima de $\mathfrak{p}$ e satisfazem

$$\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_j \cong (A/\mathfrak{p})[\overline{\beta}_j],$$

onde $\overline{\beta}_j$ é uma raiz de $\overline{f}$. Além disso, $f(\mathfrak{P}_j/\mathfrak{p}) = grau(f_j)$, para $j = 1, \cdots, r$.

Teorema 1.52. ([10], pag. 25) (Kummer) Nas condições da Proposição 1.51, se $\overline{f} = \overline{f}_1^{e_1} \cdots \overline{f}_r^{e_r}$ é a fatoração de $\overline{f}$ em polinômios irredutíveis em $A/\mathfrak{p}[x]$, então

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

onde $\mathfrak{P}_j = \mathfrak{p}\mathcal{O}_{\mathbb{L}} + f_j(\beta)\mathcal{O}_{\mathbb{L}}$, para $j = 1, \cdots, r$, $e(\mathfrak{P}_j/\mathfrak{p}) = e_j$, para $j = 1, \cdots, r$ e $f(\mathfrak{P}_j/\mathfrak{p}) =$grau$(f_j)$, para $j = 1, \cdots, r$.

Teorema 1.53. ([8], pag. 384) Seja $\mathbb{L}/\mathbb{K}$ um extensão finita de corpos de números de grau ímpar. Se $cond(\mathbb{K}) = cond(\mathbb{L})$, então

$$Tr_{\mathbb{L}/\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{K}}.$$

Como no Teorema 1.53 o traço é sobrejetor, vamos analisar o traço em certos ideais de $\mathcal{O}_{\mathbb{L}}$

Exemplo 1.54. Sejam $\mathbb{K}$ o corpo gerado pelas raízes do polinômio $f(x) = x^2 + x - 3$ sobre $\mathbb{Q}$ e $\mathbb{L}$ uma extensão de $\mathbb{K}$ gerada pelas raízes do polinômio $g(x) = x^3 + x^2 - 4x + 1$ sobre $\mathbb{Q}$. Note que $cond(\mathbb{K}) = cond(\mathbb{L}) = 13$. Seja $\mathfrak{p} = \langle 5 \rangle$ um ideal primo em $\mathcal{O}_{\mathbb{K}}$. Fatorando o polinômio minimal de $\mathbb{L}$, segue que

$$g(x) = x^3 + x^2 - 4x + 1 \equiv (x-2)(x-3)(x-4) \ \left(\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}\right).$$

Logo, pelo Teorema de Kummer 1.52, segue que

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$$

e

$$\mathfrak{P}_1 = \langle 5, z-2 \rangle, \ \mathfrak{P}_2 = \langle 5, z-3 \rangle \text{ e } \mathfrak{P}_3 = \langle 5, z-4 \rangle,$$

onde z é uma raiz de $g(x) = x^3 + x^2 - 4x + 1$. Como

$$Tr_{\mathbb{L}/\mathbb{K}}(\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3) = Tr_{\mathbb{L}/\mathbb{K}}(\mathfrak{p}\mathcal{O}_{\mathbb{L}}) = \mathfrak{p}Tr_{\mathbb{L}/\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) = \mathfrak{p}\mathcal{O}_{\mathbb{K}} = \mathfrak{p},$$

e pelo polinômio minimal $g(x)$, segue que

$$Tr_{\mathbb{L}/\mathbb{K}}(z-2) = -1.$$

Com isso, concluímos que $Tr_{\mathbb{L}/\mathbb{K}}(\mathfrak{P}_1) = \mathcal{O}_{\mathbb{K}}$.

1.5 Considerações finais do capítulo

Neste capítulo, apresentamos alguns dos principais resultados básicos necessários para a compreensão do trabalho, dentre os assuntos abordados se destacam tópicos da teoria de Galois e da teoria algébrica dos números. No próximo capítulo, apresentamos alguns tópicos sobre reticulados, dando destaque aos reticulados algébricos. Como o objetivo deste trabalho é construir reticulados e calcular suas densidades de centro, o próximo capítulo é essencial para o desenvolvimento do trabalho.

2 Reticulados

O conceito de reticulado surgiu a partir do problema de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio, de forma que quaisquer duas esferas se toquem no máximo em um ponto e ocupem a maior parte do espaço possível.

Apesar de problemas relacionados aos reticulados serem estudados pelo menos desde o século XVII, a formalização da teoria da maneira como a conhecemos é relativamente recente, devido aos trabalhos de matemáticos como Fejes Tóth e Rogers, de meados do século XX [9]. Antes disso, a maioria das referências no tema trata de construções para problemas específicos e não é raro encontrar resultados relevantes acerca de reticulados enunciados em outros contextos como: equações diofantinas, formas quadráticas e teoria dos números.

Intuitivamente, entende-se por um reticulado como sendo um subconjunto discreto do $\mathbb{R}^n$ que tem estrutura de um $\mathbb{Z}$-módulo de posto finito n.

Definição 2.1. Seja $\{v_1, v_2, ..., v_m\}$ um conjunto de vetores linearmente independentes do $\mathbb{R}^n$, com $m \leq n$. O conjunto de pontos

$$\Lambda = \left\{ \mathbf{x} = \sum_{i=1}^{m} z_i v_i, z_i \in \mathbb{Z}, \text{ para } i = 1, \ldots, m \right\},$$

é chamado reticulado de dimensão m e $\{v_1, v_2, ..., v_m\}$ é chamado de uma base do reticulado.

Definição 2.2. O paralelepípedo formado pelos pontos

$$\theta_1 v_1 + \cdots + \theta_m v_m, \text{ com } 0 \leq \theta_i < 1,$$

é chamado um paralelepípedo fundamental ou região fundamental do reticulado, e seu volume é denotado por $Vol(\Lambda)$.

Uma importante característica de um reticulado é que a base não é única. A proposição seguinte dá uma condição necessária e suficiente para que um conjunto de vetores linearmente independentes seja uma base de um dado reticulado.

Proposição 2.3. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\{v_1, \ldots, v_n\}$ e $\{e_1, \ldots, e_n\}$ um conjunto de vetores de Λ linearmente independentes tal que $e_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Assim, $\{e_1, \ldots, e_n\}$ é uma base de Λ se, e somente se, $det(A) = \pm 1$, onde $A = (a_{ij})_{i,j=1,\ldots,n}$.

Demonstração. Como

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

segue que $\{e_1 \ldots, e_n\}$ é uma base de Λ se, e somente se, $A = (a_{ij})_{i,j=1,\ldots,n}$ é a matriz mudança de base, o que é equivalente a $det(A) = \pm 1$. $\square$

Definição 2.4. Seja $\{v_1, \ldots, v_m\}$ uma base de um reticulado Λ. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \cdots, m$, a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

é chamada de uma matriz geradora para o reticulado. A matriz $G = MM^t$ é chamada de uma matriz de Gram para o reticulado, onde t denota a transposição. Quando $m = n$, o volume de Λ é dado por $Vol(\Lambda) = |det(M)|$.

Observação 2.5. Existe mais de uma base que determinam o mesmo reticulado Λ, e assim, mais de uma matriz geradora pode determina-lo. No entanto, o módulo do determinante de qualquer matriz geradora de Λ é sempre o mesmo. De fato, sejam $\{f_1, \ldots, f_n\}$ e $\{v_1, \ldots, v_n\}$ duas bases de um reticulado Λ tal que $f_i = (f_{i1}, \ldots, f_{in})$ e $v_i = (v_{i1}, \ldots, v_{in})$, para todo $i = 1, \ldots, n$. Se $f_i = \sum_{j=2}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$, então

$$|det(f_{ij})_{i,j=1,\ldots,n}| = |det(a_{ij})_{i,j=1,\ldots,n}||det(v_{ij})_{i,j=1,\ldots,n}| = |det(v_{ij})_{i,j=1,\ldots,n}|,$$

pois $|det(a_{ij})| = 1$. Portanto, o módulo do determinante da matriz geradora de um reticulado é um invariante algébrico, ou seja, independente da escolha da base.

Observação 2.6. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e M, N duas matrizes geradoras de Λ. Sejam $G_1 = MM^t$ e $G_2 = NN^t$ matrizes de Gram de Λ. Assim, existe uma matriz inversível A tal que $M = AN$. Logo, $G_1 = ANN^tA^t$. Desta forma, $det(G_1) = det(ANN^tA^t) = (det(A))^2 det(NN^t) = (det(A))^2 det(G_2)$. Como A é inversível, segue que $det(A) = \pm 1$. Assim, $det(G_1) = det(G_2)$. Portanto, o determinante da matriz de Gram independe da matriz geradora utilizada.

Definição 2.7. O determinante de um reticulado Λ é definido como sendo o determinante da matriz G, isto é,

$$det(\Lambda) = det(G).$$

2.1 Empacotamento esférico

Dado uma métrica d em $\mathbb{R}^n$, a densidade de empacotamento fornece uma medida de quanto do espaço pode ser coberto por esferas de mesmo raio na métrica d de forma que estas esferas ou não se interceptam, ou se interceptam apenas no bordo. Em cada dimensão busca-se pelo reticulado com a maior densidade de empacotamento possível e são poucas as dimensões em que tais reticulados são conhecidos, sendo a métrica euclidiana a métrica mais amplamente estudada.

Definição 2.8.

1. Um empacotamento esférico, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas se interceptem no máximo em um ponto.

2. O raio de um empacotamento esférico é chamado de raio de empacotamento.

3. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ no $\mathbb{R}^n$.

Definição 2.9. Seja $B(\rho)$ a esfera com centro na origem e raio ρ. A densidade de empacotamento de um reticulado Λ é definida por

$$\Delta(\Lambda) = \frac{\text{volume da região coberta por uma esfera}}{\text{volume da região fundamental}} = \frac{Vol(B(\rho)}{Vol(\Lambda)} = \frac{Vol(B(1))\rho^n}{Vol(\Lambda)}.$$

Definição 2.10. A densidade de centro de um reticulado Λ é definida por

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

Exemplo 2.11. Se $\beta = \{(1,0,0),(0,2,0),(1,0,3)\}$ e Λ o reticulado gerado por β, então

$$\Lambda = \{a(1,0,0) + b(0,2,0) + c(1,0,3); a,b,c \in \mathbb{Z}\} = \{(a+c, 2b, 3c); a,b,c \in \mathbb{Z}\}.$$

Assim, $\Lambda_{min} = min\{|\lambda|, \lambda \in \Lambda, \lambda \neq 0\} = 1$, o que implica que $\rho = \dfrac{\Lambda_{min}}{2} = \dfrac{1}{2}$ é o maior raio para o qual é possível obter um empacotamento. Além disso,

$$\begin{aligned}
Vol(\Lambda) &= \left| det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \right| = 6, \\
\Delta(\Lambda) &= \frac{Vol(B(1))\rho^3}{Vol(\Lambda)} = \frac{(\frac{4}{3})\pi(\frac{1}{2^3})}{6} = \frac{\pi}{36} \approx 0,0873 \text{ e} \\
\delta(\Lambda) &= \frac{(\frac{1}{2^3})}{6} = \frac{1}{48} \approx 0,020833.
\end{aligned}$$

2.2 Reticulados algébricos

Nesta seção, apresentamos um método para gerar reticulados no $\mathbb{R}^n$ a partir de um corpo de números $\mathbb{K}$. O método consiste em aplicar determinados homomorfismos em $\mathbb{Z}$-módulos livres de posto n contidos em $\mathbb{K}$. Os reticulados gerados por este método são conhecidos como reticulados algébricos.

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

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

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

é chamado de homomorfismo canônico ou homomorfismo de Minkowski, onde Re representa a parte real e Im representa a parte imaginária de um número complexo.

Exemplo 2.12. Sejam o corpo $\mathbb{K} = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a+bi) = a - bi$, com $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 0$ e $r_2 = 1$. Para $x = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, segue que

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

Teorema 2.13. ([17], pag. 56) Se $M \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M, então $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$, com uma $\mathbb{Z}$-base dada por $\{\sigma_{\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{K}}(x_n)\}$ e o volume é dado por

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

Corolário 2.14. ([17], pag. 57) Se $M \subset \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(M)$ são reticulados no $\mathbb{R}^n$, cujos volumes são, respectivamente, dados por

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

Definição 2.15. Seja $M \subset \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. O reticulado $\sigma_{\mathbb{K}}(M)$ é chamado reticulado algébrico.

Seja $M \subset \mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n. Pelo Corolário 2.14, segue que a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(M)$ é dada por

$$\delta(\sigma_{\mathbb{K}}(M)) = \frac{2^{r_2}\rho^n}{|disc(\mathbb{K})|^{\frac{1}{2}}[\mathcal{O}_{\mathbb{K}} : M]}, \tag{2.1}$$

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

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

Observemos que se $\mathbb{K}/\mathbb{Q}$ é uma extensão de Galois de grau ímpar, então $\mathbb{K}$ é totalmente real ([5], pag. 225), visto que os homomorfismos complexos aparecem aos pares.

2.2.1 Homomorfismo torcido

A fim de construir reticulados com densidade de centro melhores, podemos perturbar o homomorfismo canônico multiplicando cada entrada dos vetores do reticulado por um escalar apropriado.

Definição 2.16. Sejam $\mathbb{K}$ um corpo de números e $\alpha \in \mathbb{K}$. O elemento α é chamado totalmente positivo se $\sigma_i(\alpha) > 0$, para $i = 1, \ldots, n$.

Definição 2.17. Seja $\alpha \in \mathbb{K}$ um elemento totalmente positivo. O homomorfismo $\sigma_{\alpha,\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$ definido por

$$\sigma_{\alpha,\mathbb{K}}(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_{r_1}}(\alpha)\sigma_{r_1}(x), \sqrt{\sigma_{r_1+1}}(\alpha)Re(\sigma_{r_1+1}(x)), \ldots, \sqrt{\sigma_{r_1+r_2}}(\alpha)Im(\sigma_{r_1+r_2}(x))), \tag{2.2}$$

é chamado de homomorfismo torcido.

Teorema 2.18. ([17], pag. 57) Se M é um $\mathbb{Z}$-submódulo livre de posto n de $\mathcal{O}_{\mathbb{K}}$ com $\{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base de M, então $\sigma_{\alpha,\mathbb{K}}(M)$ é um reticulado em $\mathbb{R}^n$ com uma $\mathbb{Z}$-base dada por $\{\sigma_{\alpha,\mathbb{K}}(v_1), \ldots, \sigma_{\alpha,\mathbb{K}}(v_n)\}$.

Neste caso, o volume do reticulado $\sigma_{\alpha,\mathbb{K}}(M)$ é

$$Vol(\sigma_{\alpha,\mathbb{K}}(M)) = 2^{-r_2}|disc(\mathbb{K})|^{\frac{1}{2}}|N(\alpha)|^{\frac{1}{2}}[\mathcal{O}_{\mathbb{K}} : M],$$

onde $N(\alpha) = |\frac{\mathcal{O}_{\mathbb{K}}}{\alpha\mathcal{O}_{\mathbb{K}}}|$. Desta forma,

$$\delta(\sigma_{\alpha,\mathbb{K}}(M)) = \frac{2^{r_2}\rho^n}{|disc(\mathbb{K})|^{\frac{1}{2}}|N(\alpha)|^{\frac{1}{2}}[\mathcal{O}_{\mathbb{K}} : M]}. \tag{2.3}$$

2.2.2 Reticulados sobre corpos de números

Afim de construir reticulados com boas densidades de centro, também podemos mudar o corpo base no qual o estamos construindo. Até o momento, consideramos as formulas para densidades de centro de reticulados construídos via o homomorfismo canônico ou o homomorfismo torcido considerando o corpo base sendo os racionais. Porém podemos mudar esse corpo base e torna-lo um corpo de números qualquer. Desta forma, analisamos o caso onde o corpo base é um corpo de números totalmente real.

Definição 2.19. Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subset \mathbb{K}$ um anel e $\{v_1, \ldots, v_m\}$ um conjunto de vetores de V linearmente independentes sobre $\mathbb{K}$. Chama-se reticulado com base $\{v_1, \ldots, v_m\}$ o conjunto dos elementos de V da forma

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

que será denotado por $\mathcal{H}$.

Definição 2.20. Um subgrupo $\mathcal{H}$ do $\mathbb{R}^n$ é discreto se para qualquer subconjunto compacto C do $\mathbb{R}^n$, tivermos $\mathcal{H} \cap C$ finito.

Teorema 2.21. ([17], pag. 53) Se H é um subgrupo discreto do $\mathbb{R}^n$, então H é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$.

Pelo Teorema 2.21, segue que um subgrupo discreto do $\mathbb{R}^n$ é um reticulado. Seja $\mathbb{K} \subset \mathbb{L}$ corpos de números. De modo análogo ao homomorfismo injetivo, definimos $\sigma_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \to \mathbb{R}^n$ por

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

Teorema 2.22. Sejam $\mathbb{L}/\mathbb{K}$ uma extensão, de grau n, de corpos de números com $\mathbb{K}$ totalmente real. Se $M \subset \mathbb{L}$ é um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M linearmente independente sobre $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$, com uma $\mathbb{Z}$-base $\{\sigma_{\mathbb{L}/\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{L}/\mathbb{K}}(x_n)\}$ e volume dado por

$$Vol(\sigma_{\mathbb{L}/\mathbb{K}}(M)) = 2^{-r_2}|det(\sigma_i(x_j))_{i,j=1}^n| = 2^{-r_2} disc_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n)^{\frac{1}{2}},$$

onde $[\mathbb{L} : \mathbb{K}] = n = r_1 + 2r_2$.

Demonstração. Seja G uma matriz $n \times n$, onde cada linha é $\sigma_{\mathbb{L}/\mathbb{K}}(x_i)$. Como $Re(z) = \frac{1}{2}(z + \overline{z})$ e $Im(z) = \frac{1}{2}(z - \overline{z})$, manipulando a matriz, concluímos que $det(G) = (2i)^{-r_2}|\sigma_i(x_j)|$.

Como $\mathbb{K}$ é o corpo de frações de $\mathcal{O}_{\mathbb{K}}$, segue que $\{x_1, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, pela Proposição 1.28, segue que $disc_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) = |\sigma_i(x_j)|^2 \neq 0$. Portanto, $\{\sigma_{\mathbb{L}/\mathbb{K}}(x_1), \ldots, \sigma_{\mathbb{L}/\mathbb{K}}(x_n)\}$ é um conjunto linearmente independente. Logo, $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é um reticulado com uma matriz geradora dada por G. □

Note que estamos tomando M um $\mathbb{Z}$-módulo para que o volume do reticulado M fique bem definido, uma vez que, as matrizes geradoras de um reticulado possuem o mesmo determinante a menos de uma unidade, e ao considerar o anel de inteiros de um corpo de números, as unidades podem ser algo além de ± 1. Desta forma, também garantimos que o reticulado $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ será discreto, e portanto, é possível calcular o raio de empacotamento do reticulado.

Corolário 2.23. Sejam $\mathbb{L}/\mathbb{K}$ uma extensão de grau n de corpos de números com $\mathbb{K}$ totalmente real e $M \subset N \subset \mathcal{O}_{\mathbb{L}}$ $\mathbb{Z}$-módulos livres de posto n. Se $\{x_1, \ldots, x_n\}$ é uma base de N linearmente independente sobre $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é um reticulado em $\mathbb{R}^n$ com volume

$$Vol(\sigma_{\mathbb{L}/\mathbb{K}}(M)) = Vol(\sigma_{\mathbb{L}/\mathbb{K}}(N))[N : M].$$

Demonstração. Pelo Teorema 2.22, segue que $\sigma_{\mathbb{L}/\mathbb{K}}(N)$ é um reticulado. Para calcularmos o volume de $\sigma_{\mathbb{L}/\mathbb{K}}(M)$, observemos que $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é um subgrupo de $\sigma(N)$ cujo índice é dado por $[N : M]$ uma vez que $N/M \simeq \sigma_{\mathbb{L}/\mathbb{K}}(N)/\sigma_{\mathbb{L}/\mathbb{K}}(M)$. Logo, concluímos o resultado.

□

Proposição 2.24. Se $\mathbb{K}$ é totalmente real, então

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

Demonstração. Seja $\{\sigma_1, \ldots, \sigma_n\} = Gal(\mathbb{L}/\mathbb{K})$. Se $\mathbb{L}$ é totalmente real, então $\sigma_{\mathbb{L}/\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_n(x))$ e

$$\begin{aligned} |\sigma_{\mathbb{L}/\mathbb{K}}(x)|^2 &= \sigma_1(x)^2 + \cdots + \sigma_n(x)^2 \\ &= \sigma_1(x^2) + \cdots + \sigma_n(x^2) \\ &= Tr_{\mathbb{L}/\mathbb{K}}(x^2). \end{aligned}$$

Se $\mathbb{L}$ é totalmente imaginário, então $\sigma_{\mathbb{L}/\mathbb{K}}(x) = (Re(\sigma_1(x)), Im(\sigma_1(x)), \ldots, Re(\sigma_m(x)), Im(\sigma_{\frac{n}{2}}(x)))$ e

$$\begin{aligned} |\sigma_{\mathbb{L}/\mathbb{K}}(x)|^2 &= (Re(\sigma_1(x)))^2 + (Im(\sigma_1(x)))^2 + \cdots + (Re(\sigma_{\frac{n}{2}}(x)))^2 + (Im(\sigma_{\frac{n}{2}}(x)))^2 \\ &= \sigma_1(x)\sigma_1(\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x)\sigma_{\frac{n}{2}}(\overline{x}) \\ &= \sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x}) \\ &= \tfrac{1}{2}(\sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x}) + \sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x})) \\ &= \tfrac{1}{2}(\sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x}) + \sigma_{\frac{n}{2}+1}(\overline{x}x) + \ldots + \sigma_{\frac{n}{2}+\frac{n}{2}}(\overline{x}x)) \\ &= \tfrac{1}{2}Tr_{\mathbb{L}/\mathbb{K}}(x\overline{x}), \end{aligned}$$

visto que $\sigma_i = \overline{\sigma_{\frac{n}{2}+i}}$ e $(Re(\sigma_1(x)))^2 + (Im(\sigma_1(x)))^2 = \sigma(x)\sigma(\overline{x})$, pois $\mathbb{K}$ é totalmente real. □

Sejam $M \subset \mathcal{O}_{\mathbb{L}}$ um $\mathbb{Z}$-módulo livre de posto n e $\{x_1, \ldots, x_n\}$ uma $\mathbb{Z}$-base de M linearmente independente sobre $\mathcal{O}_{\mathbb{K}}$. Como $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é um reticulado discreto, segue que a densidade de centro do reticulado algébrico $\sigma_{\mathbb{L}/\mathbb{K}}(M)$ é dada por

$$\delta(\sigma_{\mathbb{L}/\mathbb{K}}(M)) = \frac{2^{r_2}\rho^n}{|disc_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n)|^{\frac{1}{2}}}, \tag{2.4}$$

onde $\rho = \frac{1}{2}\min\{|\sigma_{\mathbb{L}/\mathbb{K}}(x)|,\ x \in M,\ n \neq 0\}$.

2.3 Considerações finais do capítulo

Neste capítulo, abordamos o assunto de reticulados, dando destaque aos reticulados algébricos. Embora tenhamos apresentado a fórmula da densidade de centro de um reticulado construído via o homomorfismo canônico sobre uma extensão de um corpo de números, o objetivo deste trabalho não aborda tais construções. Estamos interessados em construir reticulados tomando como corpo base os racionais. Assim, no próximo capítulo, apresentamos as principais contribuições deste trabalho juntamente com alguns resultados que já foram desenvolvidos neste mesmo assunto. O objetivo principal é a caracterização da forma traço integral de uma extensão de grau ímpar livre de quadrados cujo condutor também é livre de quadrados.

3 Forma traço integral

Neste capítulo, apresentamos alguns resultados já conhecidos sobre a forma traço integral e as nossas principais contribuições para o assunto. Na Seção 2.1, vimos que o $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$ está relacionado com o raio de empacotamento de um reticulado. Nos trabalhos [2] e [15] foram apresentados a forma traço integral de um corpo de grau p, onde p é um primo ímpar. Assim, pensando em dar continuidade a estes trabalhos, nosso objetivo é generalizar o resultado para corpos cujo grau e condutor são ímpares e livres de quadrados.

3.1 Caracterização do condutor e contagem dos subcorpos

Para caracterizar a forma traço integral, uma das questões importantes é a contagem de subcorpos. Assim, nesta seção apresentamos a contagem de subcorpos a partir do condutor. Para isso, consideremos $\mathbb{K}$ e $\mathbb{L}$ corpos de números de condutores n_1 e n_2, respectivamente, e $\mathbb{M} = \mathbb{K}\mathbb{L}$.

Proposição 3.1. ([14], pag. 33) Se $n = p_1^{a_1} \cdots p_u^{a_u}$ é um inteiro positivo e

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

onde ϕ é a Função de Euler, então $\mathbb{Q}(\zeta_n)$ contém $\frac{p^s-1}{p-1}$ extensões de grau p sobre $\mathbb{Q}$.

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

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_u^{a_u}}^*$$

contém $\frac{p^s-1}{p-1}$ subgrupos de ordem p, isto é, contém $p^s - 1$ elementos de ordem p. O grupo $\mathbb{Z}_{p_i^{a_i}}$ é cíclico, e pelo Teorema 1.24, tem ordem $\phi(p_i^{a_i})$, para cada $i = 1, \ldots, u$. Assim, se p divide $\phi(p_i^{a_i})$, então $\mathbb{Z}_{p_i^{a_i}}^*$ possui um elemento de ordem p. Logo, esse elemento gera um grupo de ordem p. Se p não divide $\phi(p_i^{a_i})$, então não existe elemento de ordem p em $\mathbb{Z}_{p_i^{a_i}}^*$. Deste modo, a equação $(x_1, \ldots, x_u)^p = (1, \ldots, 1)$ tem $p^s - 1$ soluções não triviais. $\square$

Proposição 3.2. ([14], pag. 33) Se $[\mathbb{K} : \mathbb{Q}] = p$ é um primo ímpar, então:

i) p se ramifica em $\mathbb{K}$ se, e somente se, o condutor $n_1 = p^2 p_1 \cdots p_s$;

ii) p não se ramifica em $\mathbb{K}$ se, e somente se, o condutor $n_1 = p_1 \cdots p_s$,

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

Observamos que no decorrer deste trabalho sempre que consideramos um corpo de números de grau p, onde p é um primo ímpar, estamos considerando um corpo não ramificado, ou seja, um corpo de números com condutor $p_1 \cdots p_s$.

Lema 3.3. Sejam $cond(\mathbb{K}) = n_1$ e $cond(\mathbb{L}) = n_2$. Se $mdc(n_1, n_2) = r$, então $cond(\mathbb{M}) = \frac{n_1 n_2}{r}$, onde $\mathbb{M} = \mathbb{K}\mathbb{L}$.

Demonstração. Se $n = \frac{n_1 n_2}{r}$, então $\mathbb{K} \subset \mathbb{Q}(\zeta_{n_1}) \subset \mathbb{Q}(\zeta_n)$ e $\mathbb{L} \subset \mathbb{Q}(\zeta_{n_1}) \subset \mathbb{Q}(\zeta_n)$, e portanto, $\mathbb{M} \subset \mathbb{Q}(\zeta_n)$. Suponhamos que exista $n' < n$ tal que $\mathbb{M} \subset \mathbb{Q}(\zeta_{n'})$. Como $cond(\mathbb{K}) = n_1$ e $\mathbb{K} \subset \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n'}) = \mathbb{Q}(\zeta_{mdc(n_1,n')})$, segue que $mdc(n_1, n') = n_1$. Assim, n_1 divide n'. Analogamente, concluímos que n_2 divide n'. Portanto, $n = \frac{n_1 n_2}{r}$ divide n', ou seja $n \leq n'$, o que é um absurdo. Logo, $cond(\mathbb{M}) = \frac{n_1 n_2}{r}$. $\square$

Observação 3.4. Sejam $n_1 = p_1 \cdots p_s$ e $\overline{K}$ o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{K}$. Assim,

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^* \times \cdots \times \mathbb{Z}_{p_s}^*.$$

Seja H o subgrupo correspondente de $\overline{K}$ em $\mathbb{Z}_n^*$ e suponhamos que $H \simeq H' \times \mathbb{Z}_m^*$, onde H' é um subgrupo de $\mathbb{Z}_{n/m}^*$. Considere o seguinte diagrama

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_{n/m}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_m) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

onde $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \mathbb{Z}_m^*$ e $Gal(\mathbb{Q}(\zeta_{n/m})/\mathbb{Q}) \simeq \mathbb{Z}_{n/m}^*$. Assim, H' pode ser visto como um subgrupo de $Gal(\mathbb{Q}(\zeta_{n/m})/\mathbb{Q})$, e portanto, concluímos que $cond(\mathbb{K}) \leq n/m$, o que é um absurdo. Logo, não podemos escrever H como $H' \times \mathbb{Z}_m^*$.

Observação 3.5. Seja $\sigma : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Com uma apropriada restrição, segue que $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Se $[\mathbb{K} : \mathbb{Q}]$ é ímpar, então $\mathbb{K}$ é totalmente real, e portanto, $\sigma \in H$, onde $H < Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é um subgrupo que fixa $\mathbb{K}$. Assim, $\sigma = (\sigma_1, \ldots, \sigma_s)$, onde $\sigma_j \neq 1$ para todo j. Como $\sigma^2 = Id$, segue que $\sigma = (-1, \ldots, -1)$, isto é, $(-1, \ldots, -1) \in H$.

3.2 Caso ramificado de grau p

A forma traço integral de um corpo de grau p, onde p é ramificado é abordada em [1], [2] e [3] e é utilizado o Teorema de Leopoldt para caracterizar o anel de inteiros deste corpo. Nesta seção, consideramos $\mathbb{K}$ uma p-extensão ramificada de condutor n_1.

Definição 3.6. Sejam A uma anel e G um grupo. Um anel de grupo $A[G]$ é o conjunto de todas as combinações lineares

$$\alpha = \sum_{g \in G} a_g g,$$

onde $a_g \in A$ e somente um número finito de a_g's são não nulos.

Definimos a soma e produto de $\alpha, \beta \in A[G]$ da seguinte forma:

$$\alpha + \beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g,$$
$$\alpha\beta = \sum_{g\in G} a_g g + \sum_{h\in G} b_h h = \sum_{g,h\in G}(a_g b_h)gh,$$
$$\lambda\alpha = \lambda(\sum_{g\in G} a_g g) = \sum_{g\in G}(\lambda a_g)g, \text{ com } \lambda \in A.$$

Com essas operações, tem-se que $A[G]$ é um anel.

Teorema 3.7. ([11], pag. 167)(Teorema de Leopoldt) Seja $\mathbb{F}$ um corpo de números abeliano de condutor m. Considere

$$D(m) = \{d \in \mathbb{Z}_{>0},\ P_m|d,\ d|m \text{ e } d \not\equiv 2\ (mod\ 4)\},$$

onde P_m denota o produto de todos os números primos ímpares distintos e divisores de m. Para cada d no conjunto $D(m)$, sejam $\mathbb{F}_d = \mathbb{F} \cap \mathbb{Q}(\zeta_d)$ e

$$\eta_d = Tr_{\mathbb{Q}(\zeta_d)/\mathbb{F}_d}(\zeta_d).$$

O anel de inteiros de $\mathbb{F}$ é dado por

$$\mathcal{O}_{\mathbb{F}} = \bigoplus_{d\in D(n)} \mathbb{Z}[Gal(\mathbb{F}/\mathbb{Q})]\eta_d.$$

Se $\mathbb{K}$ é uma p-extensão ramificada de grau p, onde p é um primo ímpar, pelo Teorema 3.7 e pela referência [2], segue que se $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então $\{1, \sigma(t), \ldots, \sigma^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, onde σ é um gerador do $Gal(\mathbb{K}/\mathbb{Q})$. Assim, todo elemento de $\mathcal{O}_{\mathbb{K}}$ pode ser escrito como

$$x = a_0 + \sum_{i=1}^{p-1} a_i\sigma^i(t),\ \text{com } a_i \in \mathbb{Z}, \text{para } i = 0, \ldots, p-1.$$

Desta forma, temos o seguinte teorema.

Teorema 3.8. ([2], pag. 4) Seja $\mathbb{K}$ uma p-extensão ramificada com condutor n_1. Se $x \in \mathcal{O}_{\mathbb{K}}$ com $x = a_0 + \sum_{i=1}^{p-1} a_i\sigma^i(t)$, com $a_i \in \mathbb{Z}$, para $i = 0, \ldots, p-1$, então

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = pa_0^2 + \frac{n_1}{p}\left(\sum_{i=1}^{p-1} a_i^2 + \sum_{1\le i<j\le p-1}(a_i - a_j)^2\right).$$

3.3 Caso não ramificado de grau p

A forma traço integral de um corpo de grau p, onde p é não ramificado, é abordada em [14] e [15] e é utilizado o Teorema de Hilbert-Speiser para caracterizar o anel de inteiros deste corpo. Para isso, nesta seção, consideremos $\mathbb{K}$ uma p-extensão não ramificada de condutor n_1, com p ímpar.

Teorema 3.9. (Teorema de Hilbert-Speiser) Um corpo de números abeliano $\mathbb{F}$ tem base integral normal se, e somente se, o condutor de $\mathbb{F}$ é livre de quadrados. Neste caso, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[Gal(\mathbb{F}/\mathbb{Q})]t$, onde $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{F}}(\zeta_n)$ e $n = cond(\mathbb{F})$.

Observamos que este resultado é uma versão mais forte do Teorema 1.40. Se $\mathbb{K}$ é uma p-extensão não ramificada com p primo ímpar, pelo Teorema 3.9, segue que se $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, então $\{t, \sigma(t), \ldots, \sigma^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, onde σ é um gerador do grupo $Gal(\mathbb{K}/\mathbb{Q})$. Assim, todo elemento de $\mathcal{O}_{\mathbb{K}}$ pode ser escrito como

$$x = \sum_{i=0}^{p-1} a_i \sigma^i(t), \text{ com } a_i \in \mathbb{Z}, \text{ para } i = 0, \ldots, p-1.$$

Desta forma, temos o seguinte teorema.

Teorema 3.10. ([15], pag. 1081) Seja $\mathbb{K}$ uma p-extensão não ramificada com condutor n_1. Se $x \in \mathcal{O}_{\mathbb{K}}$ com $x = \sum_{i=0}^{p-1} a_i \sigma^i(t)$, com $a_i \in \mathbb{Z}$, para $i = 0, \ldots, p-1$, então

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = n_1 \sum_{i=0}^{p-1} a_i^2 - \frac{n_1 - 1}{p} \left(\sum_{i=0}^{p-1} a_i \right)^2.$$

3.4 Caso não ramificado de grau pq

Nosso objetivo, nesta seção, é estender os resultados da forma traço integral para o caso não ramificado. Para isso, nesta seção, consideramos $\mathbb{K}$ uma p-extensão não ramificada de condutor n_1, $\mathbb{L}$ uma q-extensão não ramificada de condutor n_2, $\mathbb{M} = \mathbb{K}\mathbb{L}$ uma pq-extensão de condutor n, com $p \neq q$ primos ímpares, e consideramos H o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{M}$.

Lema 3.11. Sejam $cond(\mathbb{K}) = n_1 = r_1 \cdots r_a$, $cond(\mathbb{L}) = n_2 = r_{a+1} \cdots r_b$, onde os r_i são primos e $\Pi : H \to \mathbb{Z}_{y_1}^* \times \cdots \times \mathbb{Z}_{y_j}^*$, definida por $\Pi(\alpha_1, \ldots, \alpha_c) = (\alpha_{y_1}, \ldots, \alpha_{y_j})$.
$i)$ Se $\{r_1, \ldots, r_a\} \not\subset \{y_1, \ldots, y_j\}$ e $\{r_{a+1}, \ldots, r_b\} \not\subset \{y_1, \ldots, y_j\}$, então

$$|\mathrm{Ker}\Pi| = \frac{\prod_{i=1}^{e}(r_{d_i} - 1)}{pq}.$$

$ii)$ Se $\{r_1, \ldots, r_a\} \subset \{y_1, \ldots, y_j\}$ e $\{r_{a+1}, \ldots, r_b\} \not\subset \{y_1, \ldots, y_j\}$, então

$$|\mathrm{Ker}\Pi| = \frac{\prod_{i=1}^{e}(r_{d_i} - 1)}{q}.$$

$iii)$ Se $\{r_1, \ldots, r_a\} \not\subset \{y_1, \ldots, y_j\}$ e $\{r_{a+1}, \ldots, r_b\} \subset \{y_1, \ldots, y_j\}$, então

$$|\mathrm{Ker}\Pi| = \frac{\prod_{i=1}^{e}(r_{d_i} - 1)}{p},$$

onde $d_1, \ldots, d_e$ são as coordenadas de α que são distintas de $y_1, \ldots, y_j$.

Demonstração. Sejam $Z = \mathbb{Z}_{y_1}^* \times \cdots \times \mathbb{Z}_{y_j}^*$ e $Z^c = \mathbb{Z}_{d_1}^* \times \cdots \times \mathbb{Z}_{d_e}^*$, ou seja, Z^c é o complementar de Z em $\mathbb{Z}_n^*$. Temos os seguintes casos:
$i)$ Como H é um subgrupo de $\Pi(H) \times Z^c < \mathbb{Z}_n^*$ e $[\mathbb{Z}_n^* : H] = pq$, segue que $[\mathbb{Z}_n^* : \Pi(H) \times Z^c] = 1$, p, q ou pq. Se o índice for pq, então $H = \Pi(H) \times Z^c$. Pela Obervação 3.4, segue que isso é um absurdo, pois $cond(\mathbb{K}\mathbb{L}) = n$. Se o índice for p, então $\Pi(H) \times Z^c$ fixa o corpo $\mathbb{K}$. Usando a Obervação 3.4, concluímos que existe um primo r_s que aparece no condutor de $\mathbb{K}$ e que não

aparece nas coordenadas de $\Pi(H)$, o que é um absurdo. Se o índice for q, o resultado segue de modo análogo. Portanto, concluímos que o índice é 1. Logo $H/\mathrm{Ker}\Pi \simeq Z$, e assim,

$$|\mathrm{Ker}\Pi| = \frac{\phi(n)}{pq}\frac{1}{(r_{y_1}-1)\cdots(r_{y_j}-1)} = \frac{\prod_{i=1}^{e}(r_{d_i}-1)}{pq}.$$

$ii)$ Como H é um subgrupo de $\Pi(H)\times Z^c < \mathbb{Z}_n^*$ e $[\mathbb{Z}_n^* : H] = pq$, segue que $[\mathbb{Z}_n^* : \Pi(H)\times Z^c] = 1$, p, q ou pq. Se o índice for pq, então $H = \Pi(H)\times Z^c$. Pela Obervação 3.4, segue que isso é um absurdo, pois $cond(\mathbb{K}\mathbb{L}) = n$. Se o índice for q, então $\Pi(H)\times Z^c$ fixa o corpo $\mathbb{L}$, mas usando a Obervação 3.4, concluímos que existe um primo r_s que aparece no condutor de $\mathbb{L}$ e que não aparece nas coordenadas de $\Pi(H)$, o que é um absurdo. Se o índice for 1, então Π é sobrejetora. Definindo $\Pi_2 : \mathbb{Z}_n^* \to Z$, segue que $\Pi_2(H) = \Pi(H)$. Logo, $\Pi_2(H) = Z$. Se I é o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{K}$, então H é um subgrupo de I. Logo $Z = \Pi_2(H) \subset \Pi_2(I)$. Assim, $\Pi_2(I) = Z$ o que é um absurdo, pois o índice de I em $\mathbb{Z}_{n_1}^*$ é p. Portanto, o índice de $\Pi(H)$ é p, e assim, $|\Pi(H)| = |Z|/[Z : \Pi(H)]$ e $H/\mathrm{Ker}\Pi \simeq \Pi(H)$. Logo,

$$|\mathrm{Ker}\Pi| = \frac{\phi(n)}{pq}\frac{p}{((r_{y_1}-1)\cdots(r_{y_j}-1))} = \frac{\prod_{i=1}^{e}(r_{d_i}-1)}{q}.$$

$iii)$ Segue de modo análogo ao item (ii), e portanto,

$$|\mathrm{Ker}\Pi| = \frac{\phi(n)}{pq}\frac{q}{((r_{y_1}-1)\cdots(r_{y_j}-1))} = \frac{\prod_{i=1}^{e}(r_{d_i}-1)}{p},$$

o que prova o teorema. □

Sejam $Gal(\mathbb{M}/\mathbb{Q}) = \{\theta_1^i \circ \theta_2^j\}_{i=0,\ldots,p-1}^{j=0,\ldots,q-1}$, onde $\theta_1|_{\mathbb{K}}$ é um gerador de $Gal(\mathbb{K}/\mathbb{Q})$, com $\theta_1|_{\mathbb{L}} = Id_{\mathbb{L}}$ e $\theta_2|_{\mathbb{L}}$ é um gerador de $Gal(\mathbb{L}/\mathbb{Q})$, com $\theta_2|_{\mathbb{K}} = Id_{\mathbb{K}}$. Se $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)$, então

$$Tr_{\mathbb{M}/\mathbb{Q}}((\theta_1^i \circ \theta_2^u(t))(\theta_1^j \circ \theta_2^v(t))) = Tr_{\mathbb{M}/\mathbb{Q}}(t(\theta_1^{i-j} \circ \theta_2^{u-v})(t)).$$

Teorema 3.12. Sejam $\mathbb{K}$ uma p-extensão não ramificada de condutor n_1, $\mathbb{L}$ uma q-extensão não ramificada de condutor n_2 com $p \neq q$, e $\mathbb{M} = \mathbb{K}\mathbb{L}$. Se $x \in \mathcal{O}_{\mathbb{M}}$ com $x = \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}(\theta_1^i \circ \theta_2^j(t))$, então

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

Demonstração. Se $x \in \mathcal{O}_{\mathbb{M}}$, então

$$Tr_{\mathbb{M}/\mathbb{Q}}(x^2) = \sum_{i,u=0}^{p-1}\sum_{j,v=0}^{q-1} a_{ij}a_{uv}Tr_{\mathbb{M}/\mathbb{Q}}\left(t(\theta_1^{i-u} \circ \theta_2^{j-v})(t)\right).$$

Para provar o resultado, vamos fazer um processo de contagem nas potências $i-u$ e $j-v$.

Para isso, denotamos $n_1 = p_1 \cdots p_a w_1 \cdots w_b$, e $n_2 = q_1 \cdots q_c w_1 \cdots w_b$ onde $p_i \equiv 1 \pmod p$, $q_j \equiv 1 \pmod q$ e $w_r \equiv 1 \pmod{pq}$. Logo, $n = s_1 \cdots s_{a+b+c}$, onde

$$s_i = \begin{cases} p_i, & \text{se } 1 \leq i \leq a \\ w_{i-a}, & \text{se } a+1 \leq i \leq a+b \\ q_{i-a-b}, & \text{se } a+b+1 \leq i \leq a+b+c. \end{cases}$$

Como $\mathbb{M} \subset \mathbb{Q}(\zeta_n)$, segue que existem $\varphi_{r_1}, \varphi_{r_2} \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que $\varphi_{r_1}|_{\mathbb{M}} = \theta_1$ e $\varphi_{r_2}|_{\mathbb{M}} = \theta_2$, onde $\varphi_{r_y}(\zeta_n) = \zeta_n^{r_y}$ para $y = 1, 2$. Considerando φ_{r_1} em $\mathbb{Z}_n^*$, segue que φ_{r_1} não altera as últimas c coordenadas e φ_{r_2} não altera as primeiras a coordenadas. Se H é o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{M}$, então

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

Considerando $d = \frac{n}{s_1} + \cdots + \frac{n}{s_{a+b+c}}$, segue que $\zeta_n^d = \zeta_{s_1} \cdots \zeta_{s_{a+b+c}}$, e desta forma, $\zeta_n^{\alpha + \beta r_1^i r_2^j}$ é uma raiz primitiva da unidade se, e somente se,

$$\zeta_n^{d(\alpha + \beta r_1^i r_2^j)} = \zeta_{s_1}^{\alpha + \beta r_1^i} \cdots \zeta_{s_a}^{\alpha + \beta r_1^i} \zeta_{s_{a+1}}^{\alpha + \beta r_1^i r_2^j} \cdots \zeta_{s_{a+b}}^{\alpha + \beta r_1^i r_2^j} \zeta_{s_{a+b+1}}^{\alpha + \beta r_2^j} \cdots \zeta_{s_{a+b+c}}^{\alpha + \beta r_2^j}$$

também o é. Denotando $\alpha = (\alpha_1, \ldots, \alpha_{a+b+c})$, $\beta = (\beta_1, \ldots, \beta_{a+b+c})$, $r_1 = (r_{1_1}, \ldots, r_{1_{a+b+c}})$, $r_2 = (r_{2_1}, \ldots, r_{2_{a+b+c}}) \in \mathbb{Z}_n^* \simeq \mathbb{Z}_{s_1}^* \times \ldots \times \mathbb{Z}_{s_{a+b+c}}^*$, segue que $\alpha + \beta r_1^i r_2^j \equiv \alpha_k + \beta_k r_{1_k}^i r_{2_k}^j \pmod{s_k}$. Portanto, tomando $e = a + b + c$, segue que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^i \circ \theta_2^j)(t)) = \sum_{\alpha, \beta \in H} Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i} \cdots \zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j}).$$

Mas

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i} \cdots \zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j}) = Tr_{\mathbb{Q}(\zeta_{\frac{n}{s_1}})/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{\frac{n}{s_1}})}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i} \cdots \zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j})),$$

onde

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{\frac{n}{s_1}})}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i} \cdots \zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j}) = \zeta_{s_2}^{\alpha_2 + \beta_2 r_{1_2}^i} \cdots \zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j} Tr_{\mathbb{Q}(\zeta_{s_1})/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i}).$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\theta_1^i \circ \theta_2^j(t)) = \sum_{\alpha, \beta \in H} Tr_{\mathbb{Q}(\zeta_{s_1})/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1 + \beta_1 r_{1_1}^i}) \cdots Tr_{\mathbb{Q}(\zeta_{s_e})/\mathbb{Q}}(\zeta_{s_e}^{\alpha_e + \beta_e r_{2_e}^j}), \tag{3.1}$$

onde

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

para $k = 1, \ldots, e$. No que segue, vamos dividir a provar em quatro casos, ou sejam para $i = 0$ e $j = 0$, $i = 0$ e $j \neq 0$, $i \neq 0$ e $j = 0$, e $i \neq 0$ e $j \neq 0$.

Caso (i): $i = 0$ e $j = 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_e) \in H$. Como $\mathbb{M}$ é totalmente real, pela Observação 3.5, segue que a conjugação complexa pertence a H. Logo, $(-1, \ldots, -1) \in H$, e

portanto, $\beta = (-\alpha_1, \ldots, -\alpha_e) \in H$. Além disso, β é o único elemento de H tal que $\alpha + \beta = 0$. Deste modo, $\alpha_k + \beta_k = 0$, para $k = 1, \ldots, e$. Assim, denotando $s_k - 1 = f_k$, segue que

$$Tr_{\mathbb{Q}(\zeta_{s_1})/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1+\beta_1 r_{1_1}^i}) \cdots Tr_{\mathbb{Q}(\zeta_{s_e})/\mathbb{Q}}(\zeta_{s_e}^{\alpha_e+\beta_e r_{2_e}^j}) = f_1 \cdots f_e = \phi(n).$$

Como para cada $\alpha \in H$, existe um único $\beta \in H$ tal que $\alpha + \beta = 0$, segue que ocorrem $h = |H| = \frac{\phi(n)}{pq}$ parcelas iguais a $\phi(n)$ quando fazemos o somatório da Equação 3.1. Deste modo, a soma desses termos é $T_0^1 = h\phi(n)$. Pelo Lema 3.11, para cada $\alpha \in H$, segue que existem $\frac{f_k}{pq} - 1$ ou $\frac{f_k}{p} - 1$ ou $\frac{f_k}{q} - 1$ (dependendo da coordenada) elementos de H com uma coordenada diferente e a as outras iguais. Assim,

$$Tr_{\mathbb{Q}(\zeta_{s_1})/\mathbb{Q}}(\zeta_{s_1}^{\alpha_1+\beta_1 r_{1_1}^i}) \cdots Tr_{\mathbb{Q}(\zeta_{s_e})/\mathbb{Q}}(\zeta_{s_e}^{\alpha_e+\beta_e r_{2_e}^j}) = f_1 \cdots f_{k-1}(-1)f_{k+1} \cdots f_e = -\frac{\phi(n)}{f_k}.$$

Logo, na Equação 3.1, segue que a soma da parcela é

$$\begin{aligned}
T_1^1 &= h\left(\sum_{k=1}^{a} -\frac{\phi(n)}{f_k}\left(\frac{f_k}{p} - 1\right) + \sum_{k=a+1}^{a+b} -\frac{\phi(n)}{f_k}\left(\frac{f_k}{pq} - 1\right)\right. \\
&\quad \left. + \sum_{k=a+b+1}^{a+b+c} -\frac{\phi(n)}{f_k}\left(\frac{f_k}{q} - 1\right)\right) \\
&= h\left(\sum_{k=1}^{a}\left(-\frac{\phi(n)}{p} + \frac{\phi(n)}{f_k}\right) + \sum_{k=a+1}^{a+b}\left(-\frac{\phi(n)}{pq} + \frac{\phi(n)}{f_k}\right)\right. \\
&\quad \left. + \sum_{k=a+b+1}^{a+b+c}\left(-\frac{\phi(n)}{q} + \frac{\phi(n)}{f_k}\right)\right) \\
&= h\left(-a\frac{\phi(n)}{p} - b\frac{\phi(n)}{pq} - c\frac{\phi(n)}{q} + \sum_{k=1}^{a+b+c}\frac{\phi(n)}{f_k}\right) \\
&= -h\left(\binom{a}{a-1}\frac{\phi(n)}{p} + \binom{b}{b-1}\frac{\phi(n)}{pq} + \binom{c}{c-1}\frac{\phi(n)}{q} - \sum_{k=1}^{a+b+c}\frac{\phi(n)}{f_k}\right).
\end{aligned}$$

De forma geral, sendo Π a projeção do Lema 3.11, segue que

$$\begin{aligned}
T_u^1 &= (-1)^u \sum_{k_1<\cdots<k_u} \frac{\phi(n)}{f_{k_1}\cdots f_{k_u}}\left(|\mathrm{Ker}\Pi_{\hat{k_1}\cdots\hat{k_u}}|\right. \\
&\quad - \sum_{k_1 \le k_l \le k_u} |\mathrm{Ker}\Pi_{\hat{k_1}\cdots\hat{k_{l-1}}\hat{k_{l+1}}\cdots\hat{k_u}}| + \cdots \\
&\quad \left. +(-1)^{u-1}\sum_{l=1}^{u}|\mathrm{Ker}\Pi_{\hat{k_l}}| + (-1)^u\right),
\end{aligned}$$

onde $\Pi_{\hat{k_1}\cdots\hat{k_u}}$ é a projeção nas coordenadas de $\mathbb{Z}_n^*$ com exceção das coordenadas $k_1, \cdots, k_u$. Observamos que, neste caso, aparecem os termos $\frac{1}{p}$, $\frac{1}{pq}$, $\frac{1}{q}$ e 1.

Caso (ii): $i = 0$ e $j \neq 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_e) \in H$. Suponhamos que exista $\beta \in H$ tal que $\alpha + \beta r_2^j = 0$. Assim, $-\beta r_2^j = \alpha \in H$. Por outro lado, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) =$

$H\dot{\cup}\varphi_{r_1}\varphi_{r_2}H\dot{\cup}\cdots\dot{\cup}\varphi_{r_1}^{p-1}\varphi_{r_2}^{q-1}H$, ou seja, $\mathbb{Z}_n^* = H\dot{\cup}r_1r_2H\dot{\cup}\cdots\dot{\cup}r_1^{p-1}r_2^{q-1}H$ é uma união de classes laterais disjuntas. Deste modo, $\alpha = -\beta r_2^j \in r_2^jH$, o que é um absurdo. Logo, não existe $\beta \in H$ tal que $\alpha + \beta r_2^j = 0$, e deste modo, $T_0^2 = 0$. Agora, analisamos a existência de β tal que $\alpha_k + \beta_k r_{2_k}^j = 0$ em todas as coordenadas exceto em uma coordenada, digamos l. Observamos que

$$\beta r_2^j = (\beta_1, \ldots, \beta_a, \beta_{a+1}r_{2_{a+1}}^j, \ldots, \beta_e r_{2_e}^j).$$

Para $1 \leq l \leq a$, suponhamos que existe $\beta \in H$ tal que

$$\beta = (-\alpha_1, \ldots, -\alpha_{l-1}, \beta_l, -\alpha_{l+1}, \ldots, -\alpha_a, -\alpha_{a+1}r_{2_{a+1}}^{-j}, \ldots, -\alpha_e r_{2_e}^{-j}).$$

Se $I \subset \mathbb{Z}_n^*$ é o grupo que fixa $\mathbb{L}$, então $\alpha, \beta \in H \subset I$. Pela Observação 3.4, segue que $I \simeq \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_a}^* \times \overline{I}$. Como $\alpha \in I$, segue que $r_2^{-j}\alpha \in r_2^{-j}I$, onde $r_2^{-j}I$ é uma classe lateral de I. Como $\mathbb{Z}_{p_l}^*$ é um fator de I, segue que $\beta \in r_2^{-j}I$, o que é um absurdo. Logo, não existe um elemento β nestas condições. Se $a+1 \leq l \leq a+b$, pelo Lema 3.11, segue que a projeção $\Pi : H \to \mathbb{Z}_{n/p_l}^*$ é sobrejetora. Portanto, existe um elemento β nestas condições. Agora, sejam $a+b+1 \leq l \leq e$, $J \subset \mathbb{Z}_n^*$ o grupo que fixa $\mathbb{K}$ e $\Pi : \mathbb{Z}_n^* \to \mathbb{Z}_{n/p_l}^*$. Como $H \subset J$, segue que $\Pi(H) \subset \Pi(J)$. Pela Observação 3.4 e pelo Lema 3.11, segue que $|\Pi(H)| = |\Pi(J)|$. Logo, $\Pi(H) = \Pi(J)$. Dado $\alpha \in H \subset J$, segue que $r_2^{-j}\alpha \in J$, e assim, $\Pi(r_2^{-j}\alpha) \in \Pi(J) = \Pi(H)$, e portanto, $\beta \in \Pi^{-1}(\Pi(r_2^{-j}\alpha))$. Concluímos, assim, que existe um elemento β nestas condições. Desta forma,

$$T_1^2 = -h\left(\binom{b}{b-1}\frac{\phi(n)}{pq} + \binom{c}{c-1}\frac{\phi(n)}{q}\right).$$

De um modo geral, obtemos que T_u^2 é uma cópia de T_u^1, porém copiando somente os termos que possuem os coeficientes $\frac{1}{pq}$ ou $\frac{1}{q}$.

Caso (iii): $i \neq 0$ e $j = 0$. De modo análogo ao caso (ii), segue que $T_0^3 = 0$ e T_u^3 é uma cópia de T_u^1, onde copiamos somente os termos que possuem os coeficientes $\frac{1}{p}$ ou $\frac{1}{pq}$.

Caso (iv): $i \neq 0$ e $j \neq 0$. De nodo análogo ao caso (ii), segue que $T_0^4 = 0$ e T_u^4 é uma cópia de T_u^1, onde copiamos somente os termos que possuem os coeficientes $\frac{1}{pq}$.

Observamos que esses casos se relacionam com os a_{ij} da seguinte forma

$$(i) \to \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}^2, \qquad (ii) \to \sum_{i=0}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{q-1} a_{ij}a_{iv}$$

$$(iii) \to \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{j=0}^{q-1} a_{ij}a_{uj}, \quad (iv) \to \sum_{\substack{i,u=0\\ i\neq u}}^{p-1}\sum_{\substack{j,v=0\\ j\neq v}}^{q-1} a_{ij}a_{uv}$$

$$(i)+(ii) \to \sum_{i=0}^{p-1}\left(\sum_{j=0}^{q-1} a_{ij}\right)^2, \quad (i)+(iii) \to \sum_{j=0}^{q-1}\left(\sum_{i=0}^{p-1} a_{ij}\right)^2,$$

$$(i)+(ii)+(iii)+(iv) \to \left(\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\right)^2.$$

Agora, analisando à soma relacionada aos coeficientes 1, segue que

$$\begin{aligned} T_1^* &= h\Bigg(\phi(n) + (-1)(-1)\sum_{k=1}^{e}\frac{\phi(n)}{f_k} \\ &\quad + (-1)^2(-1)^2\sum_{1\le k_1<k_2\le e}\frac{\phi(n)}{f_{k_1}f_{k_2}} + \cdots + (-1)^e(-1)^e\Bigg). \end{aligned}$$

Usando o fato que

$$n = (f_1+1)(f_2+1)\cdots(f_e+1) = \phi(n) + \sum_{k=1}^{e}\frac{\phi(n)}{f_k} + \cdots + 1,$$

segue que $T_1^* = hn$. Agora, analisando os termos que aparecem junto a $\frac{1}{p}$, segue que

$$\begin{aligned} T_p^* &= \frac{h}{p}\Bigg(-\binom{a}{a-1}\phi(n) + \binom{a}{a-2}\phi(n) + \cdots + (-1)^a\phi(n) \\ &\quad + \sum_{k=1}^{a}\frac{\phi(n)}{f_k}\left(-\binom{a-1}{a-2} + \binom{a-1}{a-3} + \cdots + (-1)^{a-1}\binom{a-1}{0}\right) \\ &\quad + \sum_{k=a+1}^{e}\frac{\phi(n)}{f_k}\left(-\binom{a}{a-1} + \binom{a}{a-2} + \cdots + (-1)^{a-1}\binom{a}{0}\right) \\ &\quad + \cdots + \sum_{k=1}^{a}\frac{\phi(n)f_k}{f_1\cdots f_e}(-1)\Bigg). \end{aligned}$$

Usando o fato que

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

segue que

$$\begin{aligned} T_p^* &= \frac{h}{p}\left(-\phi(n) - \sum_{k=1}^{a}\frac{\phi(n)}{f_k} - \sum_{a<k}\frac{\phi(n)}{f_k} - \cdots - \sum_{k=1}^{a}\frac{\phi(n)f_k}{f_1\cdots f_e}\right) \\ &= \frac{h}{p}\Bigg(-\phi(n) - \sum_{k=1}^{e}\frac{\phi(n)}{f_k} - \sum_{k_1<k_2}\frac{\phi(n)}{f_{k_1}f_{k_2}} - \cdots \\ &\quad - \sum_{k_1<\cdots<k_{a-1}}\frac{\phi(n)}{f_{k_1}\cdots f_{k_{a-1}}} - \sum_{\substack{k_1<\cdots<k_a \\ \{1,\ldots,a\}\not\subset\{k_i,\ldots,k_a\}}}\frac{\phi(n)}{f_{k_1}\cdots f_{k_a}} \\ &\quad - \sum_{\substack{k_1<\cdots<k_{a+1} \\ \{1,\ldots,a\}\not\subset\{k_i,\ldots,k_{a+1}\}}}\frac{\phi(n)}{f_{k_1}\cdots f_{k_{a+1}}} - \cdots - \sum_{k=1}^{a}\frac{\phi(n)f_k}{f_1\cdots f_e}\Bigg) \\ &= \frac{h}{p}\Bigg(-\phi(n) - \sum_{k=1}^{e}\frac{\phi(n)}{f_k} - \cdots - \sum_{k_1<\cdots<k_a}\frac{\phi(n)}{f_{k_1}\cdots f_{k_a}} \end{aligned}$$

$$
\begin{aligned}
& + \frac{\phi(n)}{f_1 \cdots f_a} - \sum_{k_1 < \cdots < k_{a+1}} \frac{\phi(n)}{f_{k_1} \cdots f_{k_{a+1}}} \\
& + \sum_{k=a+1}^{e} \frac{\phi(n)}{f_1 \cdots f_a f_k} - \cdots - \frac{\phi(n)}{\phi(n)} + \frac{\phi(n)}{\phi(n)} \Bigg) \\
= \; & \frac{h}{p}(-n + n_2),
\end{aligned}
$$

visto que

$$
n_2 = (f_{a+1} + 1) \cdots (f_e + 1) = \frac{\phi(n)}{f_1 \cdots f_a} + \sum_{k=a+1}^{e} \frac{\phi(n)}{f_1 \cdots f_a f_k} + \cdots + 1.
$$

De modo análogo, segue que

$$
T_q^* = \frac{h}{q}(-n + n_1).
$$

Agora, analisemos o caso T_{pq}^*. Para isso, seja $hc = T_{pq}^*$. Como $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x^2) = hTr_{\mathbb{M}/\mathbb{Q}}(x^2)$, tomando $a_{ij} = 1$, para $i = 0, \ldots, p-1$ e $j = 0, \ldots, q-1$, pela Proposição 1.37, segue que

$$
x = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \theta_1^i \circ \theta_2^j (Tr_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)) = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = \pm 1.
$$

Assim, $x^2 = 1$, e deste modo, $Tr_{\mathbb{M}/\mathbb{Q}}(x^2) = Tr_{\mathbb{M}/\mathbb{Q}}(1) = pq$. Por outro lado,

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

Deste modo,

$$
\begin{aligned}
pq &= npq - \frac{n - n_1}{q} pq^2 - \frac{n - n_2}{p} p^2 q + cp^2 q^2 \\
pq &= npq - npq + n_1 pq - npq + n_2 pq + cp^2 q^2 \\
c &= \frac{n - n_1 - n_2 + 1}{pq}.
\end{aligned}
$$

Portanto, concluímos o resultado. □

Observemos que este resultado independente da relação entre n_1 e n_2.

3.5 Caso não ramificado de grau $p_1 \cdots p_r$

Na Seção 3.4, estendemos o resultado da forma traço integral de um corpo de grau p para o grau pq. Nesta seção, vamos estender este mesmo resultado para um corpo de números de grau $p_1 \cdots p_r$ e condutor livre de quadrados. Desta forma, consideramos, para $i = 1, \ldots, r$,

$\mathbb{K}_i$ uma p_i-extensão não ramificada de condutor n_i, e $p_i \neq p_j$ se $i \neq j$, e $\mathbb{M} = \mathbb{K}_1 \cdots \mathbb{K}_r$. Consideramos $n_{i_1,\ldots,i_s} = cond(\mathbb{K}_{i_1} \cdots \mathbb{K}_{i_s})$, $n = n_{i_1,\ldots,i_r} = m_1 \cdots m_c$ e denotamos $N_{i_1,\ldots,i_s} = \{x \in \mathbb{N} \mid x | n_{i_1,\ldots,i_s}\}$. Observamos que, neste caso, p_i e n_i estão relacionados.

Lema 3.13. Se H é o subgrupo de $\mathbb{Z}_n^*$ que fixa $\mathbb{K}_1 \cdots \mathbb{K}_r$ e a projeção $\Pi : H \to \mathbb{Z}_{y_1}^* \times \cdots \times \mathbb{Z}_{y_j}^*$, onde $\Pi(\alpha_{m_1}, \ldots, \alpha_{m_c}) = (\alpha_{y_1}, \ldots, \alpha_{y_j})$, então

$$|\mathrm{Ker}\Pi| = \frac{\prod_{i=1}^{e}(m_{d_i} - 1)}{w},$$

onde $w = \prod p_i$ tal que $n_i \notin Y = \{y \in \mathbb{N} \mid y | y_1 \cdots y_j\}$ e $m_{d_1}, \ldots, m_{d_e}$ são as coordenadas de α que são distintas de $y_1, \ldots, y_j$.

Demonstração. Sejam $Z = \mathbb{Z}_{y_1}^* \times \cdots \times \mathbb{Z}_{y_j}^*$ e $Z^c = \mathbb{Z}_{m_{d_1}}^* \times \cdots \times \mathbb{Z}_{m_{d_e}}^*$, onde, Z^c é o complemento de Z em $\mathbb{Z}_n^*$. Como $H < \Pi(H) \times Z^c < \mathbb{Z}_n^*$ e $[\mathbb{Z}_n^* : H] = p_1 \cdots p_r$, segue que $[\mathbb{Z}_n^* : \Pi(H) \times Z^c] = \beta$ divide $p_1 \cdots p_r$. Seja p_i tal que $n_i \in Y$. Se $p_i \nmid \beta$, então $\Pi(H) \times Z^c$ não fixa $\mathbb{K}_i$. Se $I < \mathbb{Z}_n^*$ é o grupo que fixa $\mathbb{K}_i$, então $H < I$, e assim, estendendo a função Π para $\mathbb{Z}_n^*$, segue que $\Pi(H) \subset \Pi(I)$. Portanto,

$$[Z : \Pi(H)] = [Z : \Pi(I)][\Pi(I) : \Pi(H)].$$

Logo, $p_i | \beta$, o que é um absurdo. Agora, seja p_i tal que $n_i \notin Y$. Se $p_i \mid \beta$, então $\Pi(H) \times Z^c$ fixa um corpo acima de $\mathbb{K}_i$, e deste modo, $cond(\mathbb{K}_i) = n_i$ divide o condutor do corpo fixado por $\Pi(H) \times Z^c$, logo $n_i \in Y$, o que é um absurdo. Assim, concluímos que $\beta = \prod p_i$, onde $n_i \in Y$. Logo $|\Pi(H)| = |Z|/(Z : \Pi(H))$ e $H/\mathrm{Ker}\Pi \simeq \Pi(H)$, e deste modo,

$$|\mathrm{Ker}\Pi| = \frac{\phi(n)}{p_1 \cdots p_r} \frac{\beta}{((y_1 - 1) \cdots (y_j - 1))} = \frac{\prod_{i=1}^{e}(m_{d_i} - 1)}{w},$$

o que prova o resultado. □

Agora, seja $Gal(\mathbb{M}/\mathbb{Q}) = \{\theta_1^{j_1} \circ \cdots \circ \theta_r^{j_r}\}_{j_i=0,\ldots,p_i-1}$, onde $\theta_i|_{\mathbb{K}_i}$ é um gerador de $Gal(\mathbb{K}_i/\mathbb{Q})$ e $\theta_i|_{\mathbb{K}_j} = Id_{\mathbb{K}_j}$ se $i \neq j$. Se $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{M}}(\zeta_n)$, então qualquer $x \in \mathcal{O}_{\mathbb{M}}$ pode ser escrito como

$$x = \sum_{i=0}^{r} \sum_{j_i=0}^{p_i-1} a_{j_1,\ldots,j_r} \theta_1^{j_1} \circ \cdots \circ \theta_r^{j_r}(t).$$

Teorema 3.14. Sejam $\mathbb{K}_i$ uma p_i-extensão não ramificada de condutor n_i para $i = 1, \ldots, r$ com $p_i \neq p_j$ se $i \neq j$, $\mathbb{M} = \mathbb{K}_1 \cdots \mathbb{K}_r$ e $n_{i_1,\ldots,i_j} = cond(\mathbb{K}_{i_1} \cdots \mathbb{K}_{i_j})$. Se $x \in \mathcal{O}_{\mathbb{M}}$ com $x = \sum_{i=0}^{r} \sum_{j_i=0}^{p_i-1} a_{j_1,\ldots,j_r} \theta_1^{j_1} \circ \cdots \circ \theta_r^{j_r}(t)$, então

$$\begin{aligned} Tr_{\mathbb{M}/\mathbb{Q}}(x^2) &= n \sum_{j=1}^{r} \sum_{i_j=0}^{p_j-1} a_{1,\ldots,r}^2 + \sum_{j=1}^{r} T_{p_j} \sum_{\substack{k=0 \\ k \neq j}}^{r} \sum_{i_k=0}^{p_k-1} \left(\sum_{j=0}^{p_j-1} a_{1,\ldots,r} \right)^2 + \\ &+ \sum_{j_1<j_2} T_{p_{j_1} p_{j_2}} \sum_{\substack{k=0 \\ k \neq j_1, j_2}}^{r} \sum_{i_k=0}^{p_k-1} \left(\sum_{j_1=0}^{p_{j_1}-1} \sum_{j_2=0}^{p_{j_2}-1} a_{1,\ldots,r} \right)^2 + \end{aligned}$$

$$+\cdots+T_{p_1\cdots p_r}\left(\sum_{j=1}^{r}\sum_{i_j=0}^{p_j-1}a_{1,\ldots,r}\right)^2,$$

onde

$$T_{p_{i_1}\cdots p_{i_s}}=\frac{h}{p_{i_1}\cdots p_{i_s}}\left((-1)^s n+(-1)^{s-1}\sum_{j=1}^{s}n_{\hat{i}_j}+(-1)^{s-2}\sum_{j_1<j_2}n_{\hat{i}_{j_1}\hat{i}_{j_2}}+\cdots+n_{\hat{i}_{j_1},\ldots,\hat{i}_{j_s}}\right),$$

$n_{\hat{1},\ldots,\hat{r}}=1$ e $n_{\hat{i}}=n_{1,\ldots,i-1,i+1,\ldots,r}$.

Demonstração. Para cada $i=1,\ldots,r$, segue que $\mathbb{K}_i\subset\mathbb{M}\subset\mathbb{Q}(\zeta_n)$, e assim, existe $\varphi_i\in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que $\varphi_i|_{\mathbb{M}}=\theta_i$, onde $\varphi_i^j(\zeta_n)=\zeta_n^{s_i^j}$. Seja H o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{M}$. Deste modo,

$$t(\theta_1^{j_1}\circ\cdots\circ\theta_r^{j_r})(t)=\sum_{\alpha\in H}\zeta_n^{\alpha}(\theta_1^{j_1}\circ\cdots\circ\theta_r^{j_r})(t)\left(\sum_{\beta\in H}\zeta_n^{\beta}\right)=\sum_{\alpha,\beta\in H}\zeta^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}.$$

Escrevendo $d=\frac{n}{m_1}+\cdots+\frac{n}{m_c}$, segue que $\zeta_n^d=\zeta_{m_1}\cdots\zeta_{m_c}$. Desta forma, $\zeta^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}$ é uma raiz primitiva da unidade se, e somente se,

$$\zeta_n^{d(\alpha+\beta s_1^{j_1}\cdots s_r^{j_r})}=\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}$$

também o é. Denotando $\alpha=(\alpha_1,\ldots,\alpha_c)$, $\beta=(\beta_1,\ldots,\beta_c)$, $s_1=(s_{1_1},\ldots,s_{1_c}),\ldots,s_r=(s_{r_1},\ldots,s_{r_c})\in\mathbb{Z}_n^*\simeq\mathbb{Z}_{m_1}^*\times\ldots\times\mathbb{Z}_{m_c}^*$, segue que $\alpha+\beta s_1^{j_1}\cdots s_c^{j_r}\equiv\alpha_k+\beta_k s_{1_k}^{j_1}\cdots s_{r_k}^{j_r}\pmod{s_k}$. Portanto,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^{j_1}\circ\cdots\circ\theta_r^{j_r})(t))=\sum_{\alpha,\beta\in H}Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}).$$

Como

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}})=$$
$$Tr_{\mathbb{Q}(\zeta_{\frac{n}{m_1}})/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{\frac{n}{m_1}})}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}})),$$

segue que

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{\frac{n}{s_1}})}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}})=$$
$$\zeta_{m_2}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}\cdots\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}Tr_{\mathbb{Q}(\zeta_{s_1})/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}).$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t(\theta_1^{j_1}\circ\cdots\circ\theta_r^{j_r})(t))=$$
$$\sum_{\alpha,\beta\in H}Tr_{\mathbb{Q}(\zeta_{m_1})/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}})\cdots Tr_{\mathbb{Q}(\zeta_{m_c})/\mathbb{Q}}(\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}),\quad(3.2)$$

onde

$$Tr_{\mathbb{Q}(\zeta_{m_k})/\mathbb{Q}}(\zeta_{m_k}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}) = \begin{cases} m_k - 1, & \text{se } \alpha + \beta s_1^{j_1} \cdots s_r^{j_r} = 0 \\ -1, & \text{se } \alpha + \beta s_1^{j_1} \cdots s_r^{j_r} \neq 0, \end{cases}$$

para $k = 1, \ldots, c$. Agora, a prova será dividida em dois casos.

Caso (i): $j_1 = \cdots = j_r = 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_c) \in H$. Como $\mathbb{M}$ é totalmente real, segue que a conjugação complexa pertence a H. Logo, $(-1, \ldots, -1) \in H$, e portanto, $\beta = (-\alpha_1, \ldots, -\alpha_c) \in H$. Além disso, β é o único elemento de H tal que $\alpha + \beta = 0$. Deste modo, $\alpha_k + \beta_k = 0$, para $k = 1, \ldots, c$. Assim, denotando $m_k - 1 = f_k$, segue que

$$Tr_{\mathbb{Q}(\zeta_{m_1})/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}) \cdots Tr_{\mathbb{Q}(\zeta_{m_c})/\mathbb{Q}}(\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}) = f_1 \cdots f_e = \phi(n),$$

onde ϕ é função de Euler. Como para cada $\alpha \in H$ existe um único $\beta \in H$ tal que $\alpha + \beta = 0$, segue que existem $h = |H| = \frac{\phi(n)}{p_1 \cdots p_r}$ parcelas iguais a $\phi(n)$ quando fazemos o somatório da Equação 3.2. Deste modo, a soma desses termos é $T_0^1 = h\phi(n)$. Pelo Lema 3.13, para cada $\alpha \in H$, segue que existem $\frac{f_k}{w} - 1$ (w dependendo da coordenada) elementos de H com uma coordenada diferente e as outras iguais. Assim,

$$Tr_{\mathbb{Q}(\zeta_{m_1})/\mathbb{Q}}(\zeta_{m_1}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}) \cdots Tr_{\mathbb{Q}(\zeta_{m_c})/\mathbb{Q}}(\zeta_{m_c}^{\alpha+\beta s_1^{j_1}\cdots s_r^{j_r}}) = f_1 \cdots f_{k-1}(-1)f_{k+1} \cdots f_e = -\frac{\phi(n)}{f_k}.$$

Logo, pela Equação 3.2, segue que a soma da parcela é

$$\begin{aligned} T_1^1 &= h\left(\sum_{k=1}^{c} -\frac{\phi(n)}{f_k}\left(\frac{f_k}{w_k} - 1\right)\right) \\ &= -h\left(\sum_{k=1}^{c} \binom{z_k}{z_k - 1}\frac{\phi(n)}{w_k} - \sum_{k=1}^{c}\frac{\phi(n)}{f_k}\right), \end{aligned}$$

onde $w_k = w$ é dado no Lema 3.13 pela projeção em $\mathbb{Z}_n^*$, excluindo a coordenada k, e z_k é a quantidade de primos que aparecem no condutor do corpo $\mathbb{L}$ de grau w_k e que não aparecem no condutor dos corpos $\mathbb{K}_i$ que não estão contidos em $\mathbb{L}$. Em geral, sendo Π a projeção do Lema 3.11, segue que

$$\begin{aligned} T_u^1 &= (-1)^u \sum_{k_1 < \cdots < k_u} \frac{\phi(n)}{f_{k_1} \cdots f_{k_u}} \left(|\mathrm{Ker}\Pi_{\hat{k_1} \cdots \hat{k_u}}| - \sum_{k_1 \leq k_l \leq k_u} |\mathrm{Ker}\Pi_{\hat{k_1} \cdots \hat{k_{l-1}} \hat{k_{l+1}} \cdots \hat{k_u}}| + \cdots + \right. \\ &\quad \left. + (-1)^{u-1} \sum_{l=1}^{u} |\mathrm{Ker}\Pi_{\hat{k_l}}| + (-1)^u \right), \end{aligned}$$

onde $\Pi_{\hat{k_1} \cdots \hat{k_u}}$ é a projeção nas coordenadas de $\mathbb{Z}_n^*$, excluindo as coordenadas $k_1, \ldots, k_u$. Observemos que, neste caso, aparecem os termos 1, $\frac{1}{p_i}$, $\frac{1}{p_i p_j}$,..., $\frac{1}{p_1 \cdots p_r}$. Notamos que $\binom{z_k - i}{z_k - i - j}$ representa que temos z_k primos que determinam o mesmo w_k, onde i desses primos estão com suas coordenadas sendo excluída da projeção, e j deles fornecem a variação dos outros primos (que variam livremente).

Caso (ii): $j_i \neq 0$, para $i = 1, \cdots, e$, e $j_i = 0$ para $i = e + 1, \cdots, r$. Provamos que este

caso é similar ao caso (i), mas tomando somente os elementos onde w_k é divisível por $p_1 \cdots p_e$. Dado $\alpha \in H$, utilizando o mesmo argumento de classes laterais da demonstração do Teorema 3.12, segue que não existe $\beta \in H$ tal que $\alpha + \beta s_1^{j_1} \cdots s_e^{j_e} = 0$. Dado $\alpha \in H$, queremos saber quantos $\beta \in H$ existem tal que $\alpha + \beta s_1^{j_1} \cdots s_e^{j_e}$ é diferente de zero em l coordenadas e zero nas demais. Observamos que as l coordenadas determinam o w_k ao definir a projeção ¶ do Lema 3.13 nas l coordenadas, e assim, analisamos a existência de tal β. Seja w_k tal que $p_1 \cdots p_e \nmid w_k$. Sem perda de generalidade, suponhamos que p_1 não divide w_k, ou seja, estamos projetando em todas as coordenada de n_1. Dado α, suponhamos que existe tal β. Seja $I < \mathbb{Z}_n^*$ o grupo que fixa $\mathbb{K}_1$. Estendendo a projeção do Lema 3.13, como $H < I$, segue que, $\Pi(H) < \Pi(I)$. Temos que $\alpha, \beta \in H < I$ e $\Pi(\alpha) = \Pi(\beta s_1^{j_1} \cdots s_e^{j_e}) \in \Pi(H) < \Pi(I)$, mas $\Pi(\beta s_1^{j_1}) \notin \Pi(I)$, visto que todas as coordenadas de I estão na projeção. Logo, $\Pi(\beta s_1^{j_1} \cdots s_e^{j_e}) \notin \Pi(I)$, o que é um absurdo. Portanto, se $p_1 \cdots p_e \nmid w_k$, então não existe β. Agora, seja w_k tal que $p_1 \cdots p_e \mid w_k$, ou seja, para cada n_i, para $i = 1, \ldots, e$ existe uma coordenada na qual não estamos projetando. Se $e = r$, então a função é sobrejetora, e assim, existe tal β. Se $e \neq r$, então existe $\mathbb{K}_v = \mathbb{K}_{v_1} \cdots \mathbb{K}_{v_u}$ tal que estes são os únicos corpos de $\mathbb{K}_1, \ldots, \mathbb{K}_r$ em que a projeção está definida em todas as coordenadas do condutor de cada corpo. Seja $J < \mathbb{Z}_n^*$ o grupo que fixa $\mathbb{K}_v$. Como $H < J$ e estendendo a projeção do Lema 3.13, segue que $\Pi(H) < \Pi(J)$. Pela cardinalidade, segue que $|\Pi(H)| = |\Pi(J)|$. Logo $\Pi(H) = \Pi(J)$. Dado $\alpha \in H < J$, segue que $s_1^{-j_1} \cdots s_e^{-j_e} \alpha \in J$, e assim, $\Pi(s_1^{-j_1} \cdots s_e^{-j_e} \alpha) \in \Pi(J) = \Pi(H)$, ou seja, $\beta \in \Pi^{-1}(\Pi(s_1^{-j_1} \cdots s_e^{-j_e} \alpha))$. Concluímos assim que β existe. Portanto, provamos que o este caso é uma cópia do caso (i), mas copiando somente os elementos onde w_k é divisível por $p_1 \cdots p_e$. Desta forma, já sabemos como comportam a quantidade de elementos na Equação 3.2.

Agora, analisamos as somas desses termos. Começamos pelos termos independentes. Estes termos só aparecem quando $j_1 = \cdots = j_r = 0$. Assim,

$$T_1^* = h\left(\phi(n) + (-1)^2 \sum_{k=1}^{c} \frac{\phi(n)}{f_k} + (-1)^4 \sum_{1 \leq k_1 \leq k_2 \leq c} \frac{\phi(n)}{f_{k_1} f_{k_2}} + \cdots + (-1)^{2e}\right).$$

Usando o fato que

$$n = (f_1 + 1)(f_2 + 1) \cdots (f_e + 1) = \phi(n) + \sum_{k=1}^{c} \frac{\phi(n)}{f_k} + \cdots + 1,$$

segue que

$$T_1^* = hn.$$

Analisamos os termos que aparecem junto a $\frac{1}{p_i}$. Sem perda de generalidade, consideramos $i = 1$ e que os primeiros a termos de n são os termos que aparecem em n_1 e não aparecem nos demais n_j, com $j \neq 1$. Assim,

$$\begin{aligned} T_{p_1}^* \;=\; & \frac{h}{p_1}\left(-\binom{a}{a-1}\phi(n) + \binom{a}{a-2}\phi(n) + \cdots + (-1)^a \phi(n) + \right. \\ & + \sum_{k=1}^{a} \frac{\phi(n)}{f_k}\left(-\binom{a-1}{a-2} + \binom{a-1}{a-3} + \cdots + (-1)^{a-1}\binom{a-1}{0}\right) + \\ & + \sum_{k=a+1}^{c} \frac{\phi(n)}{f_k}\left(-\binom{a}{a-1} + \binom{a}{a-2} + \cdots + (-1)^{a-1}\binom{a}{0}\right) + \end{aligned}$$

$$+ \cdots + \sum_{k=1}^{a} \frac{\phi(n) f_k}{f_1 \cdots f_e}(-1) \Bigg).$$

Como

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

segue que

$$\begin{aligned}
T^*_{p_1} &= \frac{h}{p_1}\left(-\phi(n) - \sum_{k=1}^{a} \frac{\phi(n)}{f_k} - \sum_{a<k} \frac{\phi(n)}{f_k} - \cdots - \sum_{k=1}^{a} \frac{\phi(n) f_k}{f_1 \cdots f_c}\right) \\
&= \frac{h}{p_1}\Bigg(-\phi(n) - \sum_{k=1}^{c} \frac{\phi(n)}{f_k} - \sum_{k_1<k_2} \frac{\phi(n)}{f_{k_1} f_{k_2}} - \cdots - \sum_{k_1<\cdots<k_{a-1}} \frac{\phi(n)}{f_{k_1} \cdots f_{k_{a-1}}} - \\
&\quad - \sum_{\substack{k_1<\cdots<k_a \\ \{1,\ldots,a\} \not\subset \{k_i,\ldots,k_a\}}} \frac{\phi(n)}{f_{k_1} \cdots f_{k_a}} - \sum_{\substack{k_1<\cdots<k_{a+1} \\ \{1,\ldots,a\} \not\subset \{k_i,\ldots,k_{a+1}\}}} \frac{\phi(n)}{f_{k_1} \cdots f_{k_{a+1}}} - \cdots \\
&\quad - \sum_{k=1}^{a} \frac{\phi(n) f_k}{f_1 \cdots f_c}\Bigg) \\
&= \frac{h}{p_1}\Bigg(-\phi(n) - \sum_{k=1}^{c} \frac{\phi(n)}{f_k} - \cdots - \sum_{k_1<\cdots<k_a} \frac{\phi(n)}{f_{k_1} \cdots f_{k_a}} + \frac{\phi(n)}{f_1 \cdots f_a} \\
&\quad - \sum_{k_1<\cdots<k_{a+1}} \frac{\phi(n)}{f_{k_1} \cdots f_{k_{a+1}}} + \sum_{k=a+1}^{c} \frac{\phi(n)}{f_1 \cdots f_a f_k} - \cdots - \frac{\phi(n)}{\phi(n)} + \frac{\phi(n)}{\phi(n)}\Bigg) \\
&= \frac{h}{p_1}(-n + n_{2,\ldots,r}),
\end{aligned}$$

visto que

$$n_{2,\ldots,r} = (f_{a+1}+1)\cdots(f_c+1) = \frac{\phi(n)}{f_1 \cdots f_a} + \sum_{k=a+1}^{c} \frac{\phi(n)}{f_1 \cdots f_a f_k} + \cdots + 1.$$

Ou seja,

$$T^*_{p_i} = \frac{h}{p_i}(-n + n_{1,\ldots,i-1,i+1,\ldots,r}).$$

Agora, analisemos os termos que aparecem junto a $\frac{1}{p_i p_j}$. Sem perda de generalidade, consideramos $i = 1$, $j = 2$ e que os primeiros a termos de n são os termos que aparecem em $n_{1,2}$ e não aparecem nos demais $n_{i,j}$. Os termos variando de $a+1$ até $a+b$, e de $a+b+1$ até $a+b+d$, são os termos que estão em n_1 e n_2, respectivamente, e não aparecem em nenhum outro n_k. Observamos que em $\binom{a-u}{a-u-v}$ o elemento a representa quantos elementos que determinam o termo que queremos. Neste caso, o termo é $\frac{1}{p_1 p_2}$, onde v representa a quantidade de elementos que estão sendo utilizados para gerar o termo, e u representa a quantidade de termos livres de $\sum \frac{\phi(n)}{f_{i_1} \cdots f_{i_{u+v}}}$ que estão variando dentro dos a termos. Desta forma,

$$
\begin{aligned}
T^*_{p_1p_2} &= \frac{h}{p_1p_2}\left(-\binom{a}{a-1}\phi(n)+\binom{a}{a-2}\phi(n)+\cdots+(-1)^a\phi(n)\right.\\
&+\phi(n)\sum_{u,v,w\in W}(-1)^{u+v+w}\binom{a}{a-w}\binom{b}{b-u}\binom{d}{d-v}\\
&+\sum_{k=1}^{a}\frac{\phi(n)}{f_k}\left(-\binom{a-1}{a-2}+\binom{a-1}{a-3}+\cdots+(-1)^{a-1}\binom{a-1}{0}\right)\\
&+\sum_{k=a+1}^{c}\frac{\phi(n)}{f_k}\left(-\binom{a}{a-1}+\binom{a}{a-2}+\cdots+(-1)^{a-1}\binom{a}{0}\right)\\
&\left.+\cdots+\sum_{k=1}^{a}\frac{\phi(n)f_k}{f_1\cdots f_e}(-1)\right),
\end{aligned}
$$

onde $W=\{0\le w\le a,\ 0\le u\le b,\ 0\le v\le d \mid uvw\neq 0$ ou $(uv\neq 0$ e $w=0)$ ou $(uw\neq 0$ e $v=0)$ ou $(wv\neq 0$ e $u=0)\}$. Lembramos que

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

e assim, fixando $uv\neq 0$ no termo

$$
\sum_{\substack{2\le u+v+w\le a+b+d\\ uv\neq 0}}(-1)^{u+v+w}\binom{a}{a-w}\binom{b}{b-u}\binom{d}{d-v},
$$

segue que

$$
(-1)^{u+v}\binom{b}{b-u}\binom{d}{d-v}\sum_{0\le w\le a}(-1)^w\binom{a}{a-w}=0.
$$

Desta forma,

$$
\sum_{u,v,w\in W}(-1)^{u+v+w}\binom{a}{a-w}\binom{b}{b-u}\binom{d}{d-v}=
$$

$$
\sum_{\substack{2\le u+w\le a+b\\ uw\neq 0}}(-1)^{u+w}\binom{a}{a-w}\binom{b}{b-u}+\sum_{\substack{2\le v+w\le a+d\\ vw\neq 0}}(-1)^{v+w}\binom{a}{a-w}\binom{d}{d-v}.
$$

E desta forma,

$$
\sum_{\substack{2\le u+w\le a+b\\ uw\neq 0}}(-1)^{u+w}\binom{a}{a-w}\binom{b}{b-u}=-\binom{b}{b-0}\sum_{1\le w\le a}(-1)^w\binom{a}{a-w}=1.
$$

Portanto,

$$
T^*_{p_1p_2} = \frac{h}{p_1p_2}\left(-\phi(n)+2\phi(n)-\sum_{k=1}^{c}\frac{\phi(n)}{f_k}+2\sum_{k=1}^{c}\frac{\phi(n)}{f_k}+\cdots\right),
$$

mas esse padrão de $-\phi(y)+2\phi(y)$ não se mantém em $T^*_{p_1p_2}$, pois se colocarmos $f_{a+1}\cdots$

$f_{a+b}f_{k_1}\cdots f_{k_l}$ no denominador, o termo $\sum \binom{a}{a-w}\binom{b}{b-u}\binom{d}{d-v}$ aparecerá somente com $u = 0$. Desta forma, teremos $-\phi(y) + \phi(y)$ ao invés de $-\phi(y) + 2\phi(y)$. E o mesmo vale para $f_{a+b+1}\cdots f_{a+b+d}f_{k_1}\cdots f_{k_l}$. Como

$$\begin{aligned}
n &= \phi(n) + \sum_{k=1}^{c} \frac{\phi(n)}{f_k} + \cdots + 1,\\
n_{2,\ldots,r} &= \frac{\phi(n)}{f_{a+1}\cdots f_{a+b}} + \sum_{k=1}^{c} \frac{\phi(n)}{f_{a+1}\cdots f_{a+b}f_k} + \cdots + 1,\\
n_{1,3,\ldots,r} &= \frac{\phi(n)}{f_{a+b+1}\cdots f_{a+b+d}} + \sum_{k=1}^{c} \frac{\phi(n)}{f_{a+b+1}\cdots f_{a+b+d}f_k} + \cdots + 1,\\
n_{3,\ldots,r} &= \frac{\phi(n)}{f_1\cdots f_{a+b+d}} + \sum_{k=1}^{c} \frac{\phi(n)}{f_1\cdots f_{a+b+d}f_k} + \cdots + 1,
\end{aligned}$$

segue que

$$T^*_{p_1p_2} = \frac{h(n - n_{2,\ldots,r} - n_{1,3,\ldots,r} + n_{3,\ldots,r})}{p_1p_2}.$$

Mas isto independe do índice p_1 e p_2. Para simplificar a notação, denotamos

$$n_{\hat{i}} = n_{1,\ldots,i-1,i+1,\ldots,r}.$$

Logo,

$$T^*_{p_ip_j} = \frac{h(n - n_{\hat{i}} - n_{\hat{j}} + n_{\hat{i},\hat{j}})}{p_1p_2}.$$

Vamos analisar o caso $T^*_{p_{i_1}\cdots p_{i_v}}$. Sem perda de generalidade, consideramos $i_j = j$ e que os primeiros a termos de n são os termos que aparecem em $n_{1,\ldots,v}$ e que não aparecem nos outros $n_{k_1,\ldots,k_w}$. Assim, existem a_j termos que aparecem em n_j e que não aparecem nos outros n_k. Logo,

$$\begin{aligned}
T^*_{p_1\cdots p_v} = \frac{h}{p_1\cdots p_v}\Bigg(&-\binom{a}{a-1}\phi(n) + \binom{a}{a-2}\phi(n) + \cdots + (-1)^a\phi(n) +\\
&+\phi(n)\sum_{\{u,u_1,\ldots,u_v\}\in W}(-1)^{u+u_1+\cdots+u_s}\binom{a}{a-u}\binom{a_1}{a_1-u_1}\cdots\\
&\binom{a_v}{a_v-u_v} + \cdots\Bigg),
\end{aligned}$$

onde

$$\begin{aligned}
W = \{&\{u, u_1, \ldots, u_v\} \mid 0 \le u \le a,\ \ 0 \le u_j \le a_j,\ j = 1, \cdots, v, \text{ e } u_1\cdots u_v \neq 0\\
&\text{ou } uu_{j_1}\cdots u_{j_k} \neq 0 \text{ para algum conjunto de índices}\}.
\end{aligned}$$

Assim,

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

e com respeito aos outros elementos do conjunto W, segue que se $uu_1\cdots u_k \neq 0$. Desta forma,

$$
\begin{aligned}
& \sum_{uu_1\cdots u_k\neq 0} (-1)^{u+u_1+\cdots+u_k}\binom{a}{a-u}\binom{a_1}{a_1-u_1}\cdots\binom{a_k}{a_k-u_k} \\
= & \sum_{uu_1\cdots u_{k-1}\neq 0} (-1)^{u+u_1+\cdots+u_{k-1}}\binom{a}{a-u}\binom{a_1}{a_1-u_1}\cdots \\
& \binom{a_{k-1}}{a_{k-1}-u_{k-1}}\sum_{j=1}^{a_k}\binom{a_k}{a_k-u_k} \\
= & (-1)\sum_{uu_1\cdots u_{k-1}\neq 0} (-1)^{u+u_1+\cdots+u_{k-1}}\binom{a}{a-u}\binom{a_1}{a_1-u_1}\cdots\binom{a_{k-1}}{a_{k-1}-u_{k-1}} \\
= & (-1)^{k+1}.
\end{aligned}
$$

No entanto, para cada combinação de índices de W, segue que o somatório é igual à $(-1)^{k+1}$. Portanto,

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

e este termo é o primeiro termo que vai gerar $(-1)^v n$. Similarmente a $T_{p_1p_2}$, segue que a forma geral é dada por

$$
T^*_{p_{i_1}\cdots p_{i_s}}=\frac{h}{p_{i_1}\cdots p_{i_s}}\left((-1)^s n+(-1)^{s-1}\sum_{j=1}^{s} n_{\hat{i}_j}+(-1)^{s-2}\sum_{j_1<j_2} n_{\hat{i}_{j_1}\hat{i}_{j_2}}+\cdots+n_{\hat{i}_{j_1},\ldots,\hat{i}_{j_s}}\right)
$$

e $n_{\hat{1},\ldots,\hat{r}}=1$. Como $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(x^2)=hTr_{\mathbb{M}/\mathbb{Q}}(x^2)$, tomando $T_{p_ip_j}=\frac{1}{h}T^*_{p_ip_j}$, segue que se $x=\sum_{i=0}^{r}\sum_{j_i=0}^{p_i-1}a_{1,\ldots,r}\,(\theta_1^{j_1}\circ\cdots\circ\theta_r^{j_r})(t)$, então

$$
\begin{aligned}
Tr_{\mathbb{M}/\mathbb{Q}}(x^2) \;=\; & n\sum_{j=1}^{r}\sum_{i_j=0}^{p_j-1}a^2_{1,\ldots,r}+\sum_{j=1}^{r}T_{p_j}\sum_{\substack{k=0\\k\neq j}}^{r}\sum_{i_k=0}^{p_k-1}\left(\sum_{j=0}^{p_j-1}a_{1,\ldots,r}\right)^2 \\
& +\sum_{j_1<j_2}T_{p_{j_1}p_{j_2}}\sum_{\substack{k=0\\k\neq j_1,j_2}}^{r}\sum_{i_k=0}^{p_k-1}\left(\sum_{j_1=0}^{p_{j_1}-1}\sum_{j_2=0}^{p_{j_2}-1}a_{1,\ldots,r}\right)^2 \\
& +\cdots+T_{p_1\cdots p_r}\left(\sum_{j=1}^{r}\sum_{i_j=0}^{p_j-1}a_{1,\ldots,r}\right)^2,
\end{aligned}
$$

o que prova o resultado. □

Observemos que este resultado independe da relação entre os condutores n_i.

3.6 Considerações finais do capítulo

Neste capítulo, apresentamos a forma traço integral de um corpo com grau e condutor ímpar e livre de quadrados. O objetivo destes resultados é caracterizar a forma traço integral, para

assim, poder minimiza-la em alguns $\mathbb{Z}$-módulos. Com isto, obter o ρ da Equação 2.1, e assim, calcular a densidade de centro dos reticulados. Portanto, no próximo capítulo apresentamos um método de como minimizar a forma traço integral em certos $\mathbb{Z}$-módulos.

4 Mínimo da forma traço integral

O estudo de reticulados possui aplicações em diversas áreas, como na teoria de códigos e criptografia. Como esses tópicos vem ganhando importância devido ao desenvolvimento tecnológico, os reticulados vem chamando cada vez mais atenção dos pesquisadores. No Capítulo 2, a Equação 2.1, apresenta os parâmetros necessários para calcular a densidade de centro de um reticulado algébrico. No Capítulo 3 caracterizamos a forma traço integral que está diretamente relacionado ao raio de empacotamento do reticulado. Porém, somente com a forma traço integral não é possível calcular a densidade de centro. Desta forma, neste capítulo, nosso objetivo é minimizar a forma traço integral para assim obter o raio de empacotamento da Equação 2.1 e obtermos a densidade de centro de um reticulado em $\mathbb{R}^n$, com n livre de quadrados.

4.1 Módulos em um compósito de corpos de graus primos distintos e condutores iguais

Seja $\mathbb{M} = \mathbb{K}_1 \cdots \mathbb{K}_r$ um compósito de corpos de números com $[\mathbb{K}_i : \mathbb{Q}] = p_i \neq p_j = [\mathbb{K}_j : \mathbb{Q}]$ e condutores iguais a n. Deste modo, pelo Teorema 3.14, segue que

$$Tr_{\mathbb{M}/\mathbb{Q}}(x^2) = n \sum_{i=0}^{c-1} a_i^2 - \frac{n-1}{c} \left(\sum_{i=0}^{c-1} a_i \right)^2,$$

onde $c = p_1 \cdots p_r$. Sejam m um número natural e

$$\mathcal{M} = \left\{ x = \sum_{i=0}^{c-1} a_i \sigma^i(t) \mid \sum_{i=0}^{c-1} a_i \equiv 0 \ (mod\ m) \right\}.$$

Consideramos a órbita de x, denotado por $O(x)$, como sendo os elementos $y \in \mathcal{O}_{\mathbb{M}}$, com $y = \sum b_i \sigma^i(t)$, tal que a soma dos b_i de y seja igual a soma dos a_i de x. Observamos que na órbita $O(x)$ o segundo termo $(\sum a_i)^2$ da forma traço está fixado, e assim, para minimizar a forma traço em uma órbita é suficiente minimizar o primeiro termo $(\sum a_i^2)$, o qual podemos denotar por $|x|$. Seja $T_{i,j} : \mathcal{M} \to \mathcal{M}$ definida por

$$T_{i,j}((a_1, \ldots, a_c)) = ((a_1, \ldots, a_{i-1}, a_i + 1, a_{i+1}, \ldots, a_{j-1}, a_j - 1, a_{j+1}, \ldots, a_c)),$$

onde $x = \sum a_i \theta^i(t)$ é denotado por $(a_1, \ldots, a_c)$. Observamos que $T_{i,j}(x)$ não altera a órbita de x.

A seguir, apresentamos dois lemas essenciais para a demonstração do Teorema 4.3.

Lema 4.1. $|x| > |T_{i,j}(x)|$ se, e somente se, $a_j - a_i > 1$.

Demonstração. Note que $|x| > |T_{i,j}(x)| \Leftrightarrow a_i^2 + a_j^2 > (a_i+1)^2 + (a_j-1)^2 \Leftrightarrow 2(a_j - a_i) > 2 \Leftrightarrow a_j - a_i > 1$. □

Considerando a órbita onde à soma dos a_i é zero, segue que o mínimo da forma traço nesta órbita é

$$Tr_{\mathbb{M}/\mathbb{Q}}(x^2) = 2n, \text{ onde } x = (1, -1, 0, \ldots,). \tag{4.1}$$

Agora, analisemos as outras órbitas. Seja S a soma dos a_i's. Podemos escrever $S = cs + r$ com $0 \leq r < c$, e tomando

$$x = (s, \ldots, s, \underbrace{s+1, \ldots, s+1}_{r \text{ entradas}}),$$

pelo Lema 4.1, segue que x é o elemento mínimo da órbita cuja soma dos a_i's é S. Desta forma, a norma mínima é

$$|x| = \sum_{i=1}^{c-r} s^2 + \sum_{i=c-r+1}^{p} (s+1)^2 = (c-r)s^2 + r(s^2 + 2s + 1) = cs^2 + 2rs + r.$$

Portanto, temos os seguinte Lema.

Lema 4.2. Sejam $x = (a_1, \ldots, a_c)$ e $S = a_1 + \cdots + a_c$. Se $S = cs + r$, com $0 \leq r < c$, então

$$\min_{y \in O(x)} |y| = cs^2 + 2rs + r.$$

Assim, substituindo $z = \min_{y \in O(x)} |y|$ na forma traço, segue que

$$\begin{aligned} Tr_{\mathbb{M}/\mathbb{Q}}(z^2) &= n(cs^2 + 2rs + r) - \frac{n-1}{c}(cs+r)^2 \\ &= ncs^2 + 2nrs + nr - \frac{n-1}{c}(c^2s^2 + 2csr + r^2) \\ &= cs^2 + 2sr + nr - \frac{n-1}{c}r^2. \end{aligned} \tag{4.2}$$

Para simplificar a notação, consideramos

$$F(S) = \min_{y \in O(x)} Tr_{\mathbb{M}/\mathbb{Q}}(x^2),$$

onde $S = a_1 + \cdots + a_c$ e $x = (a_1, \ldots, a_c)$.

Teorema 4.3. Se m é um inteiro positivo, então

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

onde $d = mdc(c, m)$.

Demonstração. A Equação 4.2 é crescente quando s cresce e quando consideramos $S > 0$. Desta forma, temos que tomar o menor $s > 0$ possível, e todas as possibilidades de r, ou seja, um conjunto completo de resíduos. Observamos que o conjunto $\{m, 2m, \ldots, \frac{c}{d}m\}$ é um conjunto completo de resíduos, uma vez que

$$\left(\frac{c}{d} + 1\right) m \equiv c\frac{m}{d} + m \equiv m \ (mod\ c).$$

O caso $F(0) = 2n$, da Equação 4.1, é contemplado nos resíduos, mas deve ser acrescentado pelo comportamento diferenciado. □

Exemplo 4.4. $i)$ Se $p_1 = 3$, $n_1 = n = 397$ e $m = 40$, então $m^* = 2 \times 397$ e a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 0.1761$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^3$.

$ii)$ Se $p_1 = 3$, $p_2 = 5$, $n_1 = n_2 = n = 2371$ e $m = 49$, então $m^* = 2 \times 2371$ e a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 0.0055$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^{15}$.

$iii)$ Se $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $n_1 = n_2 = n_3 = n = 3571$ e $m = 16$, então $M^* = 2 \times 3571$ e a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 5 \cdot 10^{-16}$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^{105}$.

As melhores densidades de centro conhecidas nas dimensões 3 e 15 são $1/(4\sqrt{2}) \approx 0.17678$ e $1/(16\sqrt{2}) \approx 0.04419$ respectivamente, [19]. Na dimensão 105 não encontramos informações sobre a melhor densidade de centro conhecida.

4.2 Módulos em um compósito de dois corpos de condutores m_1 e $m_2 = rm_1$

Sejam $\mathbb{K}$ uma p-extensão não ramificada de condutor m_1, $\mathbb{L}$ uma q-extensão não ramificada de condutor $m_1 r = n$, com $p \neq q$. Assim, a forma traço de $\mathbb{KL}$ é

$$Tr_{\mathbb{KL}/\mathbb{Q}}(x^2) = n \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij}^2 - \frac{n - m_1}{q} \sum_{i=0}^{p-1} \left(\sum_{j=0}^{q-1} a_{ij} \right)^2 + \frac{-m_1 + 1}{pq} \left(\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} \right)^2 .$$

Consideramos

$$\mathcal{M} = \left\{ x = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} \theta_1^i \circ \theta_2^j(t) \text{ com } \sum_{j=0}^{q-1} a_{ij} \equiv 0 \ (mod\ m) \right\} .$$

Assim, escrevendo x como uma matriz, isto é,

$$x = \begin{pmatrix} a_{0,0} & \cdots & a_{0,q-1} \\ \vdots & \ddots & \vdots \\ a_{p-1,0} & \cdots & a_{p-1,q-1} \end{pmatrix},$$

segue que a soma de cada linha é congruente a zero módulo m, onde m é um número natural não nulo. Agora, consideremos a órbita de x, $O(x)$, como sendo os elementos de $\mathcal{M}$ tal que a soma de cada linha da matriz seja igual a soma de cada linha da matriz x. Observamos que na órbita $O(x)$ o segundo termo $\sum(\sum a_{ij})^2$ e o terceiro termo $(\sum \sum a_{ij})^2$ da forma traço estão fixado, e assim, para minimizar a forma traço em uma órbita é suficiente minimizar o primeiro

termo $\sum\sum a_{ij}^2$, o qual podemos denotar por $|x|$. Seja $T_{i,j,k} : \mathcal{M} \to \mathcal{M}$ definida como

$$T_{i,j,k}\left(\left(\begin{array}{ccccccc} a_{0,0} & \cdots & a_{0,j} & \cdots & a_{0,k} & \cdots & a_{0,q-1} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{i,0} & \cdots & a_{i,j} & \cdots & a_{i,k} & \cdots & a_{i,q-}, \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{p-1,0} & \cdots & a_{p-1,j} & \cdots & a_{p-1,k} & \cdots & a_{p-1,q-1} \end{array}\right)\right) =$$

$$\left(\begin{array}{ccccccc} a_{0,0} & \cdots & a_{0,j} & \cdots & a_{0,k} & \cdots & a_{0,q-1} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{i,0} & \cdots & a_{i,j}+1 & \cdots & a_{i,k}-1 & \cdots & a_{i,q-1} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{p-1,0} & \cdots & a_{p-1,j} & \cdots & a_{p-1,k} & \cdots & a_{p-1,q-1} \end{array}\right).$$

Observamos que $T_{i,j,k}(x)$ não altera a órbita de x.

A seguir, apresentamos dois lemas essenciais para a demonstração do Teorema 4.7.

Lema 4.5. $|x| > |T_{i,j,k}(x)|$ se, e somente se, $a_{ij} - a_{ik} > 1$.

Demonstração. Note que $|x| > |T_{i,j,k}(x)| \Leftrightarrow a_{ij}^2 + a_{ik}^2 > (a_{ij}+1)^2 + (a_{ik}-1)^2 \Leftrightarrow 2(a_{ij} - a_{ik}) > 2 \Leftrightarrow a_{ij} - a_{ik} > 1$. □

Considerando a órbita onde à soma de todas as linhas são zero, segue que o mínimo da forma traço nesta órbita é

$$Tr_{\mathbb{KL}/\mathbb{Q}}(x^2) = 2n, \text{ onde } x = \left(\begin{array}{ccccc} 1 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{array}\right).$$

Analisamos as outras órbitas. Seja β_i a soma de cada linha. Podemos escrever $\beta_i = qs_i + r_i$, com $0 \leq r_i < q$, e tomando

$$x = \left(\begin{array}{cccccc} s_1 & s_1 & \cdots & s_1+1 & \cdots & s_1+1 \\ s_2 & & \cdots & & \cdots & s_2+1 \\ \vdots & & \vdots & & \vdots & \vdots \\ s_p & & \cdots & & \cdots & s_p+1 \end{array}\right),$$

segue que $|x| = \sum qs_1^2 + 2s_ir_i + r_i$. Assim, o mínimo de $Tr_{\mathbb{KL}/\mathbb{Q}}(x^2)$ da órbita é

$$\begin{aligned} Tr_{\mathbb{KL}/\mathbb{Q}}(x^2) &= n\sum_{i=1}^{p}(qs_1^2 + 2s_ir_i + r_i) - \frac{n-m_1}{q}\sum_{i=1}^{p}\beta_i^2 + \frac{-m_1+1}{pq}(\sum \beta_i)^2 \\ &= n\sum_{i=1}^{p}(qs_1^2 + 2s_ir_i + r_i) - n\sum_{i=1}^{p}(qs_i^2 + 2s_ir_i + \frac{r_i^1}{q}) + \frac{m_1}{q}\sum_{i=1}^{p}\beta_i^2 \\ &\quad + \frac{-m_1+1}{pq}(\sum_{i=1}^{p}\beta_i)^2 \\ &= n\sum_{i=1}^{p} r_i - \frac{n}{q}\sum_{i=1}^{p} r_i^2 + \frac{m_1}{q}\sum_{i=1}^{p}\beta_i^2 + \frac{-m_1+1}{pq}(\sum_{i=1}^{p}\beta_i)^2. \end{aligned}$$

Agora, analisemos os β_i fixando os r_i. Com os r_i fixos, podemos desconsiderá-los no estudo para minimizar a forma traço, ou seja, é suficiente minimizar

$$F(x^2) = m_1 \sum_{i=1}^{p} \beta_i^2 + \frac{-m_1+1}{p} \left(\sum_{i=1}^{p} \beta_i \right)^2. \tag{4.3}$$

Esta expressão é exatamente $Tr_{\mathbb{K}/\mathbb{Q}}(x^2)$, onde $x = \sum_{i=1}^{p} \beta_i \theta_1^i(t')$. Logo, esta expressão é sempre maior que zero, conforme provado em [15]. Denotamos $x = (\beta_1, \cdots, \beta_p)$, e consideramos a órbita

$$O_1(x) = \{y = (\gamma_1, \cdots, \gamma_p), \sum_{i=1}^{p} \gamma_i = \sum_{i=1}^{p} \beta_i \text{ e } \gamma_i \equiv \beta_i \ (mod\ q),\ i = 1, \cdots, p\}.$$

Lembramos que somente estamos considerando $\beta_i \equiv 0 \ (mod\ m)$. Seja $mmc(m, q) = d$.

Lema 4.6. Seja $T_{i,j} : \mathcal{M} \to \mathcal{M}$ definida por $T_{i,j}((\beta_1, \cdots, \beta_p)) = (\beta_1, \cdots, \beta_i + d, \cdots, \beta_j - d, \cdots, \beta_p)$. Assim, $|x| > |T_{i,j}(x)| \Leftrightarrow \beta_i - \beta_j > d$.

Demonstração. Note que $|x| > |T_{i,j}(x)| \Leftrightarrow \beta_i^2 + \beta_j^2 > (\beta_i + d)^2 + (\beta_j - d)^2 \Leftrightarrow 2d(\beta_i - \beta_j) > 2d^2 \Leftrightarrow \beta_i - \beta_j > d$. □

Note que o termo d foi escolhido para não alterarmos o resto da divisão de β_i por q e para manter o fato de que β_i é divisível por m.

Teorema 4.7. Se $\mathbb{K}$ é uma p-extensão não ramificada de condutor m_1, $\mathbb{L}$ uma q-extensão não ramificada de condutor $n = m_1 r$, onde $p \neq q$ e m é um inteiro positivo, então,

$$\min_{x \in \mathcal{M}/\{0\}} Tr_{\mathbb{KL}/\mathbb{Q}}(x^2) = \min_{\substack{(\beta_1, \cdots, \beta_p) \in C_i^p/\{0\}, \\ i \in I}} \{2n, F(\beta_1, \cdots, \beta_p)\},$$

onde $F(\beta_1, \cdots, \beta_p) = n \sum r_i - \frac{n}{p} \sum r_i^2 + \frac{m_1}{q} \sum \beta_i^2 + \frac{-m_1+1}{pq} (\sum \beta_i)^2$, $0 \leq r_i < q, r_i \equiv \beta_i \ (mod\ q)$, com

i) $C_i = \{m(q(i+c)+a)\}_{c=0,1}^{a=0,\cdots,q}, I = \{-2, -1, 0\}$ se $mdc(q, m) = 1$.

ii) $C_i = \{m(i+c)\}_{c=0,1}, I = \{-1, 0\}$ se $mdc(q, m) = q$.

Demonstração. Como p_2 é um número primo, vamos dividir a prova em 2 casos, ou seja, $p_2 \mid m$ e $p_2 \nmid m$.
Caso (i): $mdc(q, m) = 1$. Escrevendo $\beta_i = m(qb_i + a_i)$, onde a_i é o menor inteiro tal que $0 \leq a_i < q$ e $ma_i \equiv r_i \ (mod\ q)$. Sem perda de generalidade, podemos permutar os β_i, deste modo, vamos reescreve-los de forma que $a_1 \geq a_2 \geq \cdots \geq a_p$. Assim, o elemento de norma mínima na órbita é

$$(m(q\alpha + a_1), m(q\alpha + a_2), \cdots, m(q(\alpha+1) + a_{p-\gamma}), \cdots, m(q(\alpha+1) + a_p)),$$

onde $\sum b_i = \alpha p + \gamma$, com $0 \leq \gamma < p$, pois considerando $i > j$, segue que

- $|m(q\alpha + a_i) - m(q\alpha + a_j)| = m|a_i - a_j| < mq$
- $|m(q\alpha + a_i) - m(q(\alpha+1) + a_j)| = m|a_i - a_j - q| \leq mq$

- $|m(q(\alpha+1)+a_i) - m(q(\alpha+1)+a_j)| = m|a_i - a_j| < mq.$

Assim, o mínimo da órbita na Equação 4.3 é

$$\begin{aligned}
F(x^2) &= m_1 \sum_{i=1}^{p} \beta_i^+ \frac{-m_1+1}{q} \left(\sum_{i=1}^{p} \beta_i \right)^2 \\
&= m_1(m^2(q+\alpha+a_1)^2 + \cdots + m^2(q(\alpha+1)+a_p)^2) \\
&\quad + \frac{-m_1+1}{p} \left(mq \sum_{i=1}^{p} b_i + m \sum_{i=1}^{p} a_i \right)^2 \\
&= m_1 m^2 \left(pq^2\alpha^2 + 2q\alpha \sum_{i=1}^{p} a_i + \sum_{i=1}^{p} a_i^2 + 2\gamma q^2 \alpha + \gamma q^2 + 2q \sum_{i=p-\gamma}^{\gamma} a_i \right) \\
&\quad + \frac{-m_1+1}{q} m^2 \left(q^2(\alpha^2 p^2 + 2\alpha p\gamma + \gamma^2) + 2q(\alpha p + \gamma) \sum_{i=1}^{p} a_i + \left(\sum_{i=1}^{p} a_i \right)^2 \right) \\
&= m_1 m^2 \left(\sum_{i=1}^{p} +\gamma q^2 (1 - \frac{\gamma}{p}) + 2q \sum_{i=p-\gamma}^{p} a_i - 2q\gamma \sum_{i=1}^{p} a_i - \frac{1}{p} \left(\sum_{i=1}^{p} a_i \right)^2 \right) \\
&\quad + \frac{m^2}{p} \left((q(\alpha p + \gamma) + \sum_{i=1}^{p} a_i \right)^2 . \qquad (4.4)
\end{aligned}$$

Se $\alpha \geq 0$, então a Equação 4.4 é crescente. Por outro lado, como $0 \leq \gamma < p$ e $0 \leq a_i < q$, segue que

$$q(\alpha p + \gamma) + \sum a_i < 0 \Leftrightarrow \alpha < \frac{\sum \frac{a_i}{q} - \gamma}{p}, \text{ e } -2 < \frac{\sum \frac{a_i}{q} - \gamma}{p}.$$

Logo, se $\alpha \leq -2$, então a Equação 4.4 é crescente. Assim, para minimizar a forma traço integral é suficiente analisar $-2 \leq \alpha \leq 0$. Portanto, $\beta_i = m(q(\alpha + \gamma_i) + a_i)$, onde $\alpha = -2, -1, 0$, $\gamma_i = 0, 1$ e $a_i = 0, 1, \cdots, q-1$.

Caso (ii): $mdc(q, m) = q$. Neste caso, q divide m e m divide β_i. Logo, $r_i = 0$, para todo i. Assim, $\beta_i = m\alpha_i$, e escrevendo $\sum \alpha_i = \alpha p + \gamma, 0 \leq \gamma < p$, segue que

$$(m\alpha, \cdots, m\alpha, m(\alpha+1), \cdots, m(\alpha+1))$$

é um elemento de norma mínima do conjunto que fixa o resto dos β_i e fixam $\sum \beta_i$, pois

$$|m\alpha - m(\alpha+1)| \leq m = mmc(q, m).$$

Assim, o mínimo da órbita na Equação 4.3 é

$$m_1 \sum_{i=1}^{p} \beta_i^2 + \frac{-m_1+1}{p} \left(\sum_{i=1}^{p} \beta_i \right)^2 = m_1 m^2(\alpha^2 + 2\alpha\gamma + \gamma) + \frac{-m_1+1}{p} m^2(\alpha^2 p^2$$

$$
\begin{aligned}
& +2\alpha p\gamma + \gamma^2) \\
= \; & m_1 m^2(\alpha^2 + 2\alpha\gamma + \gamma) - m_1 m^2 \left(\alpha^2 p + 2\alpha\gamma \right. \\
& \left. + \frac{\gamma^2}{p}\right) + m^2 \left(\alpha^2 p + 2\alpha\gamma + \frac{\gamma^2}{p}\right) \\
= \; & m_1 m^2 \left(\gamma - \frac{\gamma^2}{p}\right) + m^2 \left(\alpha^2 p + 2\alpha\gamma + \frac{\gamma^2}{p}\right) \\
= \; & m_1 m^2 \left(\gamma - \frac{\gamma^2}{p}\right) + \frac{m^2}{p}(\alpha p + \gamma)^2. \qquad (4.5)
\end{aligned}
$$

Se $\alpha \geq 0$ e α crescente, ou $\alpha \leq -1$ e α decrescente, então a Equação 4.5 é crescente. Assim, para minimizar a forma traço integral é suficiente analisar $-1 \leq \alpha \leq 0$. Portanto, $\beta_i = m(\alpha + \gamma_i)$ onde $\alpha = -1, 0$, $\gamma_i = 0, 1$. Assim, concluímos o resultado. □

Observamos que a variação de a no Teorema 4.7 se dá de 0 à q para que tenhamos um conjunto completo de resíduos módulo q.

Exemplo 4.8. $i)$ Se $p = 3$, $q = 5$, $m_1 = 31$ e $r = 11$, $m = 7$, então a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 0.0015$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^{15}$.

$i)$ Se $p = 3$, $q = 5$, $m_1 = 31$ e $r = 11$, $m = 8$, então a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 0.0021$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^{15}$.

$iii)$ Se $p = 3$, $q = 5$, $m_1 = 31$ e $r = 461$, $m = 52$, então a densidade de centro do reticulado $\sigma_{\mathbb{M}}(\mathcal{M})$ é $\delta \approx 0.00212$. Note que $\sigma_{\mathbb{M}}(\mathcal{M}) \subset \mathbb{R}^{15}$.

A melhor densidade de centro conhecida na dimensão 15 é $1/(16\sqrt{2}) \approx 0,04419$, [19].

4.3 Considerações finais do capítulo

A partir da caracterização da forma traço integral do Capítulo 3, neste capítulo construímos reticulados a partir de certos $\mathbb{Z}$-módulos e calculamos suas respectivas densidade de centro. Porém, não obtivemos reticulados com densidades de centro próximas as melhores conhecidas. No próximo capítulo damos uma perspectiva sobre a forma traço integral via o homomorfismo torcido.

5 Considerações finais do trabalho e perspectivas futuras

Neste trabalho, apresentamos inicialmente resultados básicos da teoria de Galois, extensões de corpos, reticulados e reticulados algébricos, todos estes sendo tópicos essenciais para compreender o desenvolvimento do trabalho. Tendo como objetivo o cálculo da densidade de centro de reticulados algébricos, apresentamos os parâmetros que influenciam neste cálculo. Dentre esses parâmetros, damos destaque ao raio de empacotamento, que já possui varias maneiras para ser calculado computacionalmente para casos específicos no qual os corpos estão conhecidos. No entanto, para caracterizar o raio de empacotamento de um corpo qualquer o calculo do raio de empacotamento apresenta um alto nível de dificuldade.

Alguns trabalhos, como [2] e [15], tem analisado como descrever o raio de empacotamento de um reticulado algébrico construído via o homomorfismo canônico. Dentre os trabalhos, se destacam a caracterização do raio de empacotamento de corpos ciclotômicos, dos subcorpos maximais de corpos ciclotômicos e de corpos de números abelianos de grau primo ímpar.

Este trabalho teve como objetivo estender o conjunto de corpos no qual o raio de empacotamento é caracterizado. Desta forma, caracterizamos o raio de empacotamento de corpos de números abelianos de grau ímpar e livre de quadrados e condutor livre de quadrados. Assim, o Capítulo 3, é voltado para exibir a forma traço integral, e para a caracterização da forma traço integral utilizamos um processo de contagem em um subgrupo H de $\mathbb{Z}_n^*$, uma vez que conhecemos todos os grupos entre H e $\mathbb{Z}_n^*$. A caracterização da forma traço integral de um corpo de números de grau ímpar e livre de quadrados e condutor livre de quadrados dada nos Teoremas 3.12 e 3.14 é uma expressão para o raio de empacotamento, mas não calcula o raio. Desta forma, no Capítulo 4, minimizamos a forma traço integral em certos $\mathbb{Z}$-módulos para assim calcular explicitamente o raio de empacotamento, e deste modo, a densidade de centro de alguns reticulados. Embora os reticulados obtidos não sejam os melhores em suas densidades, fica neste trabalho a contribuição teórica para o assunto. Neste caso, fica em aberto uma perspectiva futura de pesquisa a procura de reticulados com boas densidade de centro nas dimensões ímpares e livres de quadrados.

5.1 Homomorfismo torcido

Ao longo deste trabalho, apresentamos diversos assuntos, alguns destes assuntos já foram muito pesquisados, tendo diversos artigos que tratam sobre os problemas inerentes a ele. Porém, existem alguns que ainda há muito a ser pesquisado. Desta forma, apresentamos, a seguir, alguns temas que ainda necessitam serem pesquisados.

Os reticulados obtidos utilizando os Teoremas 3.12, 3.14, 4.3 e 4.7 não apresentam densidades de centro próxima a $1/(16\sqrt{2})$, que é a melhor densidade de centro conhecida na dimensão

15. Desta forma, nesta seção, damos uma perspectiva sobre o homomorfismo torcido, que podem ser uma alternativa para resolver esse problema.

Seja $\mathbb{K}$ um corpo de números e M um $\mathbb{Z}$-módulo em $\mathcal{O}_{\mathbb{K}}$. Ao analisarmos a densidade de centro de um reticulado gerado via o homomorfismo canônico

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

e a densidade de centro de um reticulado gerado via o homomorfismo torcido

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

a única diferença esta no termo $|N(\alpha)|^{\frac{1}{2}}$. Porém este termo, escolhido adequadamente, pode ajustar a densidade de centro do reticulado para assim se aproximar da melhor densidade de centro conhecida na dimensão em que o reticulado esta sendo construído. Portanto, exibimos algumas ideias sobre a forma traço integral do homomorfismo torcido.

Consideramos o homomorfismo torcido da Equação 5.1, ou seja,

$$\sigma_{\alpha,\mathbb{K}}(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \ldots, \sqrt{\sigma_{r_1}}(\alpha)\sigma_{r_1}(x), \sqrt{\sigma_{r_1+1}}(\alpha)Re(\sigma_{r_1+1}(x)), \ldots, \sqrt{\sigma_{r_1+r_2}}(\alpha)Im(\sigma_{r_1+r_2}(x))). \quad (5.1)$$

Seja $\mathbb{K}$ uma p-extensão não ramificada, com p primo ímpar e conduto n. Sejam $Gal(\mathbb{K}\mathbb{L}/\mathbb{Q}) = \{\theta^i\}_{i=0}^{p-1}$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$. Se $x \in \mathcal{O}_{\mathbb{K}}$, então $x = \sum_{i=0}^{p-1} x_i\theta^i(t)$. Se $a, x \in \mathcal{O}_{\mathbb{K}}$, então

$$Tr_{\mathbb{K}/\mathbb{Q}}(ax^2) = \sum_{i,j,k=0}^{p-1} a_i a_j a_k Tr_{\mathbb{K}/\mathbb{Q}}(t\theta^{j-i}(t)\theta^{k-i}(t)).$$

Agora, analisamos o que acontece em $Tr_{\mathbb{K}/\mathbb{Q}}(t\theta^i(t)\theta^j(t))$.

Como $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$, segue que existe $\varphi \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que $\varphi|_{\mathbb{K}} = \theta$ e $\varphi(\zeta_n) = \zeta_n^r$. Se H é o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa $\mathbb{K}$, então

$$t\theta^i(t)\theta^j(t) = \sum_{\alpha\in H} \zeta_n^{\alpha}\theta^i\left(\sum_{\beta\in H}\zeta_n^{\beta}\right)\theta^j\left(\sum_{\gamma\in H}\zeta_n^{\gamma}\right) = \sum_{\alpha,\beta,\gamma\in H}\zeta^{\alpha+\beta r^i+\gamma r^j}.$$

Escrevendo $d = \frac{n}{p_1} + \cdots + \frac{n}{p_s}$, seque que $\zeta_n^d = \zeta_{p_1}\cdots\zeta_{p_s}$. Desta forma, $\zeta_n^{\alpha+\beta r^i+\gamma r^j}$ é uma raiz primitiva da unidade se, e somente se,

$$\zeta_n^{d(\alpha+\beta r^i+\gamma r^j)} = \zeta_{p_1}^{\alpha+\beta r^i+\gamma r^j}\cdots\zeta_{p_s}^{\alpha+\beta r^i+\gamma r^j}$$

também o é. Denotando $\alpha = (\alpha_1, \ldots, \alpha_s)$, $\beta = (\beta_1, \ldots, \beta_s)$, $\gamma = (\gamma_1, \ldots, \gamma_s)$, $r = (r_1, \ldots, r_s) \in \mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1}^* \times \ldots \times \mathbb{Z}_{p_s}^*$, segue que $\alpha + \beta r^i + \gamma r^j \equiv \alpha_k + \beta_k r_k^i + \gamma_k r_k^j (\text{mod } s_k)$. Portanto,

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t\theta(t)^i\theta^j(t)) = \sum_{\alpha,\beta,\gamma\in H} Tr_{\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}}(\zeta_{p_1}^{\alpha_1+\beta_1 r_1^i+\gamma_1 r_1^j})\cdots Tr_{\mathbb{Q}(\zeta_{p_s})/\mathbb{Q}}(\zeta_{p_s}^{\alpha_s+\beta_s r_s^i+\gamma_s r_s^j})$$

onde

$$Tr_{\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}}(\zeta_{p_k}^{\alpha_k+\beta_k r_k^i+\gamma_k r_k^j}) = \begin{cases} p_k - 1, & \text{se } \alpha_k + \beta_k r_k^i + \gamma_k r_k^j = 0 \\ -1, & \text{se } \alpha_k + \beta_k r_k^i + \gamma_k r_k^j \neq 0, \end{cases}$$

para $k = 1, \ldots, s$. Seguindo os passos da demostração do Teorema 3.12, a demonstração aconteceria numa divisão de quatro casos, porém algumas diferenças começam a surgir. Para exemplificar analisamos o caso (i).

Caso (i): $i = 0$ e $j = 0$. Seja $\alpha = (\alpha_1, \ldots, \alpha_s) \in H$. O objetivo é calcular quantos $\beta, \gamma \in H$ existem tal que $\alpha + \beta + \gamma = 0$. Como $\mathbb{K}$ é totalmente real, segue que a conjugação complexa pertence a H, pela Observação 3.5. Logo, $(-1, \ldots, -1) \in H$, e portanto, $-\gamma \in H$, ou seja, $\alpha + \beta + \gamma = 0$ se reduz a $\alpha + \beta = -\gamma \in H$. Agora, analisamos um exemplo para vermos algumas possibilidades para a questão de $\alpha + \beta \in H$.

Exemplo 5.1. Em $\mathbb{Q}(\zeta_{91})$ existem dois subcorpos de grau 3 e condutor $91 = 7 \cdot 13$. Um deles é gerado pelas raízes do polinômio $p(x) = x^3 - x^2 - 30x - 27$ e o outro pelas raízes do polinômio $q(x) = x^3 - x^2 - 30x + 64$. Os grupo que fixam esses corpos em $\mathbb{Z}_7^* \times \mathbb{Z}_{13}^*$ são os grupos $H_1 =< (2,2), (3,4) >$ e $H_2 =< (3,3), (2,6) >$. Observamos que, se $\alpha, \beta \in H < \mathbb{Z}_7^* \times \mathbb{Z}_{13}^*$, então

$$\alpha + \beta \in H \Leftrightarrow (1,1) + \alpha^{-1}\beta \in H,$$

ou seja, a pergunta

"dado $\alpha \in H$, existem quantos $\beta \in H$ tal que $\alpha + \beta \in H$?"

se reduz a "existem quantos $\beta \in H$ tal que $(1,1) + \beta \in H$?". Para o grupo H_1 a resposta é 5, e os elementos β que proporcionam essa resposta são:

$$(1,1),\ (2,3),\ (4,9),\ (5,11) \text{ e } (3,6).$$

Para o grupo H_2 a resposta é 8, e os elementos β que proporcionam essa resposta são:

$$(1,8),\ (2,9),\ (4,3),\ (1,5),\ (5,4),\ (3,10),\ (3,2) \text{ e } (5,7).$$

Observamos que os corpos possuem o mesmo grau, condutor e discriminante. Assim, fica em aberta a questão sobre quais são os fatores que influenciam nestes corpos para que esses corpos tenham comportamentos diferentes.

A observação feita dentro do Exemplo 5.1 pode ser traduzida no seguinte lema.

Lema 5.2. Sejam m e n números livres de quadrados, m um número ímpar e $H < \mathbb{Z}_n^*$ um subgrupo de índice m. Assim, existem $\alpha, \beta, \gamma \in H$ tal que $\alpha + \beta + \gamma = 0$ se, e somente se, existe $\tau \in H$ tal que $\tau + (1, \ldots, 1) \in H$.

Demonstração. Pela Observação 3.5, segue que $(-1, \ldots, -1) \in H$. Assim,

$$\alpha + \beta + \gamma = 0 \Rightarrow \beta + \gamma = -\alpha \Rightarrow \alpha^{-1}\beta + \alpha^{-1}\gamma = (-1, \ldots, -1) \in H,$$

ou seja,

$$\alpha^{-1}\beta((1, \ldots, 1) + \beta^{-1}\gamma) = \alpha^{-1}\beta + \alpha^{-1}\gamma \in H.$$

Logo, $\beta^{-1}\gamma, \beta^{-1}\gamma + (1, \ldots, 1) \in H$. Reciprocamente, se $\tau, \tau + (1, \ldots, 1) \in H$, então

$$-\tau(\tau + (1, \ldots, 1)) + \tau + \tau^2 = 0,$$

o que prova o lema. □

Desta forma, para verificar em quais condições de m e n o Lema 5.2 seja verdadeiro é uma possibilidade para a demonstração da forma traço integral para o homomorfismo torcido.

5.2 Mínimo da forma traço

Outra perspectiva futura, que este trabalho fornece, é o estudo sobre minimizar a forma traço integral em ideais ou em $\mathbb{Z}$-módulos de um anel de inteiros $\mathcal{O}_{\mathbb{M}}$, onde $\mathcal{M}$ é um corpo de números com grau e condutor ímpares e livres de quadrados. Na Seção 3.4, consideramos um compósito de dois corpo $\mathbb{M} = \mathbb{K}\mathbb{L}$, onde $\mathbb{K}$ é uma p-extensão não ramificada de condutor n_1 e $\mathbb{L}$ é uma q-extensão não ramificada de condutor n_2, com $p \neq q$. Assim, a forma traço integral de $\mathbb{M}$ é

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

Na Seção 4.2, considerando $n_2 = n_1 r$, minimizamos a forma traço integral em $\mathbb{Z}$-módulos que podem ser descritos como os elementos

$$x = \begin{pmatrix} a_{00} & \cdots & a_{0\,q-1} \\ \vdots & \ddots & \vdots \\ a_{p-1\,0} & \cdots & a_{p-1\,q-1} \end{pmatrix}$$

em $\mathcal{O}_{\mathbb{M}}$ que possuem a soma de cada linha congruente a zero módulo m, onde m é um número natural, isto é,

$$\mathcal{M} = \left\{ x = \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\theta_1^i \circ \theta_2^j(t) \in \mathcal{O}_{\mathbb{M}} \;\mid\; \sum_{j=0}^{q-1} a_{ij} \equiv 0 \; (mod\; m), \text{ para todo } i \right\}.$$

Porém podemos tomar outros módulos que resultem reticulados com boas densidades de centro. Como, por exemplo, o módulo onde a soma de cada linha é congruente a zero módulo m e a soma de cada coluna é côngruo a zero módulo m, isto é,

$$\begin{aligned} \mathcal{M}_1 \;=\; & \left\{ x = \sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}\theta_1^i \circ \theta_2^j(t) \in \mathcal{O}_{\mathbb{M}} \;\mid\; \sum_{j=0}^{q-1} a_{ij} \equiv 0 \; (mod\; m), \text{ para todo } i \right. \\ & \left. \text{e } \sum_{i=0}^{p-1} a_{ij} \equiv 0 \; (mod\; m), \text{ para todo } j \right\}. \end{aligned}$$

Observamos que para minimizar a forma traço integral em $\mathcal{M}_1$, é suficiente seguir os passos da Seção 4.2, onde o desafio está em minimizar o primeiro termo da forma traço, $\sum_{i=0}^{p-1}\sum_{j=0}^{q-1} a_{ij}^2$, em uma órbita do módulo $\mathcal{M}_1$.

5.3 Condutor com termos quadráticos

Os corpos estudados, neste trabalho, possuem uma base integral descrita pelo Teorema 1.40, porém ao fazer o compósito de corpos com condutores não livre de quadrados, segue que a base integral não poderá ser descrita pelo Teorema 1.40. O Teorema de Leopoldt 3.7, constrói um conjunto de elementos baseados nos corpos intermediários e afirma que dentro desse conjunto

existe uma base integral. Porém encontrar quais elementos desse conjunto formam uma base integral se torna um desafio ao fazer um compósito de vários corpos. Para exemplificar a questão da base integral de um corpo com termo quadrático no condutor construímos o seguinte exemplo.

Exemplo 5.3. Sejam $\mathbb{K}$ o corpo de números gerado pelas raízes do polinômio $p(x) = x^3 - 93x - 217$ sobre $\mathbb{Q}$ e $\mathbb{L}$ o corpo de números gerado pelas raízes do polinômio $q(x) = x^5 - x^4 - 136x^3 + 641x^2 - 371x - 67$ sobre $\mathbb{Q}$. Como $cond(\mathbb{K}) = 3^2 \cdot 31 = 279$ e $cond(\mathbb{L}) = 31 \cdot 11 = 341$, segue que $cond(\mathbb{KL}) = 3^2 \cdot 31 \cdot 11 = 3096$. Assim, pelo Teorema de Leopoldt 3.7, segue que

$$D(3^2 \cdot 31 \cdot 11) = \{1023,\ 3096\}.$$

Se $d_1 = 1023$ e $d_2 = 3096$, então

$$\mathbb{F}_{d_1} = \mathbb{KL} \cap \mathbb{Q}(\zeta_{d_1}) = \mathbb{L} \text{ e } \mathbb{F}_{d_2} = \mathbb{KL} \cap \mathbb{Q}(\zeta_{d_2}) = \mathbb{KL}.$$

Logo, o anel de inteiros de $\mathbb{KL}$ é dado por

$$\mathcal{O}_{\mathbb{KL}} = \mathbb{Z}[Gal(\mathbb{KL}/\mathbb{Q})]\eta_{d_1} \oplus \mathbb{Z}[Gal(\mathbb{KL}/\mathbb{Q})]\eta_{d_2},$$

onde $\eta_{d_1} = Tr_{\mathbb{Q}(\zeta_{d_1})/\mathbb{L}}(\zeta_{d_1})$ e $\eta_{d_2} = Tr_{\mathbb{Q}(\zeta_{d_2})/\mathbb{KL}}(\zeta_{d_2})$. Se θ é um gerador de $Gal(\mathbb{KL}/\mathbb{Q})$, então $\theta^3|_{\mathbb{L}}$ é gerador de $Gal(\mathbb{L}/\mathbb{Q})$. Deste modo, tomando

$$B = \{\theta(\eta_{d_1}), \theta^2(\eta_{d_1}), \ldots, \theta^{15}(\eta_{d_1}), \theta(\eta_{d_2}), \theta^2(\eta_{d_2}), \ldots, \theta^{15}(\eta_{d_2})\},$$

segue que existe um subconjunto de B que é uma base integral de $\mathbb{KL}$. Note que, como d_2 não é livre de quadrados, segue que $\{\theta(\eta_{d_2}), \theta^2(\eta_{d_2}), \ldots, \theta^{15}(\eta_{d_2})\}$ não é uma base integral de $\mathbb{KL}$, pois $Tr_{\mathbb{KL}/\mathbb{Q}}(\eta_{d_2}) = 0$ [7]. Deste modo, a escolha dos elementos de B que geram uma base integral de $\mathbb{KL}$ é uma questão a ser pesquisada.

Observamos que, em [2], foi apresentado alguns resultados sobre esse assunto, deixando várias questões a serem analisadas.

Referências

[1] ARAUJO, R. R. **Reticulados algébricos e aplicações a códigos e criptografia**. 2018. 128 f. Tese (doutorado) - Instituto de Matemática Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2018.

[2] Araujo, Robson R. et al. Trace form associated to cyclic number fields of ramified odd prime degree. **Journal of Algebra and its Applications**. Disponível em: http://hdl.handle.net/11449/189068. Acesso em: 14 fev. 2020.

[3] CHAGAS, A. C. M. M. **Uma contribuição a teoria dos números e reticulados**. 2015. 78 f. Tese (doutorado) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, 2015.

[4] CONNER, P. E.; PERLIS, R. **A survey of trace forms of algebraic number fields**. Singapore: World Scientific Publiching, 1984.

[5] CONWAY J. H.; SLOANE N. J. A. **Sphere packing, lattices and groups**. 3rd. New York: Springer Verlag, 1999.

[6] ENDLER, O. **Teoria dos números algébricos**. Rio de Janeiro: IMPA, 1986. (Projeto Euclides).

[7] FLORES, A. L. **Representação geométrica de ideais de corpos de números**. 1996. 86 f. Dissertação (mestrado) - Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 1996.

[8] GRISTMAIR, K. On the trace of the ring of integers of an abelian number field. **Acta Arithmetica**, Warsaw, v. 62, p. 383-389, 1992.

[9] LAGRANGE, J. L. **Recherches d'arithmétique**. Berlim: C.F. Voss, 1775.

[10] LANG, S. **Algebraic number theory**. New York: Springer-Verlag, 1994.

[11] LETTL, G. The ring of integers of an abelian number field. **Journal fur die Reine und Angewandte Mathematik**, Berlim, v. 404, p. 162-170, 1990.

[12] MARCUS, D. A. **Number field**. New York: Springer-Verlag, 1977.

[13] NÓBREGA NETO, T. P.; LOPES, J. O. D.; INTERMELO, J. C. The discriminant of abelian number fields. **Journal of Algebra and its Application**, v. 5, p. 35-41, 2006.

[14] OLIVEIRA, E. L. **Torres de extensões abelianas de grau primo ímpar não ramificado**. 2015. 62 f. Tese (doutorado) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, 2015.

[15] OLIVEIRA E. L et al. The integral trace form of cyclic extensions of odd prime degree. **Rocky Mountain Journal of Mathematics**, Tempe, v. 47, p. 1075-1088, 2017.

[16] RIBENBOIM, P. **Classical theory of algebraic numbers**. New York: Springer-Verlag, 2001.

[17] SAMUEL, P. **Algebraic theory of numbers**. Paris: Hernann, 1970.

[18] STEWART, I. N. **Galois Theory**. London: Chapman and Hall, 2003.

[19] TABLE of densest packings presently known. **In**: NEBE, G.; RWTH Aachen University. Aachen, [s. d.]. LATTICES: a catalogue of lattices. Disponível em: http://www.math.rwth-aachen.de/∼Gabriele.Nebe/LATTICES/density.html. Acesso em: 09 dez. 2019.

Índice Remissivo

n-ésimo corpo ciclotômico, $\mathbb{Q}(\zeta_n)$, 20
n-extensão, 18

A-módulo livre, 18
Anel de inteiros, $\mathcal{O}_{\mathbb{K}}$, 18

Base integral, 18
Base integral normal, 22

Compósito de corpos, 19
Condutor, 20
Corpo de números, 18
Corpo fixo, 19

Densidade de centro, 31
Discreto, 33
Discriminante, 22
Disjuntos, 22

Extensão abeliana, 19
Extensão ciclíca, 19
Extensão de corpo, 18
Extensão de Galois, 19

Grupo de Galois, 19

Homomorfismo canônico, 31
Homomorfismo torcido, 32

Inteiro, 18

Kummer, 26

Linearmente disjuntos, 22

Módulo, 17

Norma, 21

Raiz n-ésima da unidade, ζ_n, 20
Ramificado, 25
Reticulado, 29, 33
Reticulado algébrico, 32

Teorema de Kronecker-Weber, 20
Teorema de Leopoldt, 39
Totalmente complexo, 20
Totalmente positivo, 32
Totalmente real, 20
Traço, 21