Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Uma contribuição a teoria dos números e reticulados

Ana Cláudia Machado Mendonça Chagas

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto

Agosto - 2015

Ana Cláudia Machado Mendonça Chagas

Uma contribuição a teoria dos números e reticulados

Tese apresentada 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 São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto

2015

Chagas, Ana Cláudia Machado Mendonça.
Uma contribuição a teoria dos números e reticulados / Ana Cláudia Machado Mendonça Chagas. -- São José do Rio Preto, 2015
78 f. : tabs.

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

1. Matemática. 2. Álgebra. 3. Teoria dos números algébricos. 4. Extensões de corpos (Matemática) 5. Teoria dos reticulados. 6. Anéis (Álgebra) I. Andrade, Antonio Aparecido de. II. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU – 512

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

Ana Cláudia Machado Mendonça Chagas

Uma contribuição a teoria dos números e reticulados

Tese apresentada 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 São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
Professor Doutor - IBILCE - UNESP
Orientador

Prof. Dr. Agnaldo José Ferrari
Professor Doutor- FC - UNESP

Prof. Dr. Clotilzio Moreira dos Santos
Professor Doutor - IBILCE - UNESP

Prof. Dr. José Othon Dantas Lopes
Professor Doutor- Campus Fortaleza -UFC

Prof. Dr. Trajano Pires da Nóbrega Neto
Professor Doutor - IBILCE- UNESP

São José do Rio Preto, 14 de agosto de 2015.

Agradecimentos

Ao concluir este trabalho, agradeço:

Primeiramente à Deus.

Aos meus pais, pelo incentivo ao estudo.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, pela paciência, pelos conselhos e pela confiança ao designar a mim este trabalho.

Aos meus amigos pela companhia nos momentos em que mais precisei.

Ao Prof. Dr. Trajano Pires da Nóbrega Neto pelos conselhos, os quais enriqueceram esse trabalho.

Ao Prof. Dr. Agnaldo José Ferrari, por dispor de seu tempo para me ajudar em alguns cálculos.

À banca examinadora: Prof. Dr. Agnaldo José Ferrari, Prof. Dr. Clotilzio Moreira dos Santos, Prof. Dr. José Othon Dantas Lopes e Prof. Dr. Trajano Pires da Nóbrega Neto.

À FAPESP, pelo apoio financeiro, processo 2011/19973-3.

A todos que de alguma forma contribuiram para a realização deste trabalho.

Resumo

O objetivo desse trabalho é contribuir com resultados algébricos sobre extensões abelianas de grau p, com p um primo ímpar. Mais precisamente, explicitamos o elemento primitivo e uma base integral de uma extensão abeliana de grau p e condutor p^2q, com q primo tal que $q \equiv 1(mod\ p)$. Construímos também reticulados algébricos sobre essas extensões abelianas e reticulados ideais sobre subcorpos de $\mathbb{Q}(\zeta_{p^r})$ de dimensão par e ímpar.

Palavras chave: corpos de números abelianos, reticulado, densidade de centro, diversidade e distância produto mínima.

Abstract

The aim of this work is to contribute to results algebraic on abelian extensions of degree p, with p a prime odd. More precisely, we made explicit primitive element and a integral base of an abelian extension of degree p and conductor p^2q, with q prime such that $q \equiv 1(mod\ p)$. We built also algebraic lattices of these abelian extensions and ideal lattices for subfields of $\mathbb{Q}(\zeta_{p^r})$ of even and odd dimension.

Keywords: ***abelian extension, lattices, center density, diversity and minimum product distance.***

Sumário

Introdução

Em 1948, Shannon [24] analisando um sistema de comunicação, formulou o Teorema de Codificação de Canal, o qual diz que pode-se ter a probabilidade de erro do canal tão pequena quanto se queira através de códigos corretores de erros eficientes.

Shannon propôs representar cada sinal como um ponto no espaço n-dimensional. Considerando cada ponto como o centro de uma esfera de um empacotamento esférico. Pode-se ter um empacotamento esférico reticulado, ou seja, os centros das esferas formam um reticulado n-dimensional. Neste caso, é possível melhorar a probabilidade de erro do canal melhorando alguns parâmetros dos reticulados.

Daremos novas construções de reticulados algébricos e reticulados ideais, já que reticulados algébricos densos e reticulados ideais com alta distância produto mínima e diversidade máxima diminuem a probabilidade de erro dependendo do canal utilizado.

Para esse estudo foi necessário conseguir resultados avançados em teoria dos números algébricos, mais precisamente trabalhamos com reticulados construídos através de corpos de números abelianos de grau p, com p um primo ímpar e reticulados ideais construídos através de subcorpos de $\mathbb{Q}(\zeta_{p^r})$.

Este trabalho está dividido da seguinte forma:

No Capítulo 1, apresentamos a motivação desse trabalho. Relacionando a teoria dos códigos com reticulados algébricos.

No Capítulo 2, apresentamos resultados básicos sobre módulos, teoria algébrica dos números, teoria dos corpos e de Galois, ramificação de ideais e a definição de anel de grupo.

No Capítulo 3, além de apresentar resultados recentes de extensões abelianas de

grau um número primo ímpar, também contribuímos com novos resultados sobre essas extensões abelianas (3^o Caso).

No Capítulo 4, apresentamos construções de reticulados algébricos e ideais. Estudando a densidade de centro, diversidade e distância produto mínima.

Capítulo 1

Preliminares

Neste capítulo introduzimos a relação entre reticulados com teoria da informação e códigos. Apresentamos dois canais utilizados para a transmissão de sinais, explicitando quais parâmetros dos reticulados são importantes em cada um desses canais. O controle sobre esses parâmetros é necessário para o cálculo da taxa de probabilidade de erro do canal.

1.1 Teoria da informação e códigos

Um sistema de comunicação é um conjunto de meios físicos e equipamentos responsáveis por transportar uma informação da fonte ao destinatário, usando um canal de comunicação.

Este processo segue as seguintes etapas.

- Fonte: transforma a informação a ser emitida pela fonte (pessoa ou máquina) em símbolos discretos, ou seja, símbolos pertencentes a um alfabeto $\mathcal{A}$.
- Codificador de fonte: associa às saídas da fonte as sequências de dígitos (geralmente binários) chamadas sequências de informações ou palavras códigos fonte.
- Codificador de canal: transforma a palavra código fonte em uma outra sequência chamada de palavra código de canal. O principal objetivo desta fase é minimizar os ruídos do canal.

- Modulador: gera formas de ondas as quais são apropriadas para a transmissão através do canal.
- Canal: meio físico por onde a informação é transmitida. No canal o sinal está sujeito à vários tipos de ruídos, imperfeições e interferências, as quais geram distorções modificando o sinal recebido.
- Demodulador, decodificador do canal e decodificador de fonte: faz o inverso do modulador, codificador de canal e codificador de fonte, respectivamente.

1.2 Constelação de sinais

Novos sistemas de informações propõem melhorar o desempenho na transmissão de sinais sob o critério de probabilidade de erro.

Porém, a informação transmitida estará sempre sujeita à um conjunto de interferências alocadas no canal de transmissão. Esse conjunto de interferências é denominado ruído do canal. O principal desafio é sempre controlar a ação do ruído. Pode-se controlar a ação do ruído fazendo um esquema de modulação adequada e/ou um esquema de codificação específico.

Uma constelação de sinais são palavras códigos e sinais representadas por pontos ou vértices de grafos.

1.3 Canal gaussiano

O canal gaussiano é um canal de comunicação via satélite (AWGN - Additive White Gaussian Noise). Nesse canal a interferência dar-se-á através de um ruído branco. O nome branco se dá pelo fato da cor branca ser formada pela soma de todas as outras cores.

1.4 Canal de Rayleigh com desvanecimento

O canal de Rayleigh com desvanecimento é um canal de comunicação terrestre, o qual possui como principal característica a propagação por múltiplos percursos. Isso se dá através da reflexão e/ou difração do sinal em edifícios, árvore, etc..

Desvanecimento é o nome dado a alteração de intensidade do canal. O nome Rayleigh é dado ao canal, pois este canal é modelado por uma distribuição de probabilidade de Rayleigh. Uma ferramenta muito útil para melhorar o desempenho nesse canal é rotacionar constelações de sinais, preservando a distância euclidiana entre os pontos.

1.5 Probabilidade de erro

Dada uma constelação de sinais $\mathcal{S}$, denotamos por $P_e(\mathcal{S})$ a probabilidade de erro na transmissão de um sinal do canal.

Para o canal gaussiano, segue que

$$P_e(\mathcal{S}) \leq \frac{v}{2} erfc\left(\sqrt{\frac{nS}{2}}\Delta^{\frac{1}{n}}\right),$$

onde $\leq$ significa aproximação do limite superior.

Dentre outras variáveis, segue que Δ é a densidade de empacotamento da constelação de sinal. Para minimizar a probabilidade de erro do canal é necessário maximizar a densidade de empacotamento.

Para um canal de Rayleigh com desvanecimento tem-se que

$$P_e(\mathcal{S}) \leq \sum_{l=L}^{n} \frac{1}{2} \frac{(8N_0)^l}{d_p^l(x,\widehat{x})^2},$$

onde L é a diversidade da constelação de sinais, d_p^l é a distância l-produto de x e $\widehat{x}$ é quando dois pontos diferem em l componentes.

Assim, para minimizar a probabilidade de erro no canal de Rayleigh é necessário maximizar a diversidade L e maximizar a distância produto mínima $d_{p,min} = d_p^l(x,\widehat{x})$.

1.6 Reticulados e teoria da informação

Constelações de sinais com estrutura de reticulados são eficientes por causa da estrutura linear e simétrica dos reticulados.

O problema de empacotamento esférico, o qual faz parte do 18º Problema de Hilbert, está relacionado com o problema de encontrar constelações de sinais boas para um canal gaussiano, pois o número de vizinhos de um ponto fixo é o números de vizinhos de um elemento $x \in \mathcal{S}$. Logo, para o canal gaussiano boas constelaçções de sinais com estruturas de reticulados são aquelas que apresentam alta densidade de empacotamento.

Para o canal de Rayleigh com desvanecimento, uma alternativa para maximizar a diversidade é trabalhar com constelações de reticulados obtidas através de corpos de números totalmente reais. Bons candidatos a constelações de sinais reticulados são os reticulados $\mathbb{Z}^n$-rotacionados, os quais são de fácil rotulação.

1.7 Teoria algébrica dos números e reticulados

É possível construir reticulados n-dimensionais através de homomorfismos associados a corpos de números.

Dado um corpo de números $\mathbb{K}$, definimos nesse trabalho o homomorfismo canônico e o homomorfismo torcido, que é uma pertubação do homomorfismo canônico. Esses homomorfismos nos darão reticulados que serão chamados de reticulados algébricos.

Os reticulados ideais são reticulados algébricos dotados de uma forma traço relacionada com um ideal fracionário do anel de inteiros de um corpo de números.

A facilidade de trabalhar com reticulados obtidos dessas formas é que a densidade de empacotamento, diversidade e distância produto mínima dependem parcialmente de parâmetros dos corpos de números.

A densidade de empacotamento está relacionada com $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, onde $x \in \mathcal{O}_{\mathbb{K}}$ não nulo, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros algébricos do corpo $\mathbb{K}$ e $\mathbb{K}$ é um corpo de números totalmente real. A diversidade é maximizada quando trabalhamos sobre corpos de números totalmente reais e a distância produto mínima é maximizada quando trabalhamos

sobre corpos de números com discriminante mínimo.

1.8 Considerações finais

Neste Capítulo, relacionamos a probabilidade de erro na transmissão de sinais, utilizando os canais gaussiano e de Rayleigh, com a construção de reticulados através de corpos de números. Essa relação é a motivação desse trabalho.

Capítulo 2

Resultados básicos de teoria algébrica dos números

Neste capítulo apresentamos alguns conceitos básicos da teoria algébrica dos números necessários para a compreensão e desenvolvimento dos próximos capítulos. Começamos com o conceito de módulo, depois faremos um breve resumo de resultados de teoria dos corpos, teoria de Galois e anel de inteiros, em seguida definimos norma, traço e discriminante e finalizamos com resultados sobre corpos ciclotômicos, ramificação de ideais e anéis de grupos.

2.1 Módulos

Nesta seção definimos o conceito de módulo sobre um anel. Mais precisamente, queremos estudar resultados sobre $\mathbb{Z}$-módulos livres de posto n.

Definição 2.1 *Seja A um anel. Dizemos que um conjunto não vazio M é um A-módulo se:*

i) $(M, +)$ *é um grupo abeliano;*

ii) Existe uma aplicação $\varphi : A \times M \longrightarrow M$ *dada por* $\varphi(a, x) = ax$, *que satisfaz*

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

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

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

d) $1x = x$,

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

Note que todo anel A é um A-módulo, todo espaço vetorial V sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo e todo grupo abeliano é um $\mathbb{Z}$-módulo.

Definição 2.2 *Sejam* M *um* A*-módulo e* $N \subseteq M$ *um subconjunto não vazio. Dizemos que* N *é um* A*-submódulo de* M *se* N *é um subgrupo de* $(M, +)$ *e* $an \in N$*, para todo* $a \in A$ *e* $n \in N$.

Definição 2.3 *Um* A*-módulo* M *é livre se existe um subconjunto* $\{x_i\}_{i\in I}$ *de* M *tal que cada* $x \in M$ *é escrito de forma única como* $x = \sum_{i\in I} a_i x_i$*, onde* $a_i \in A$ *para* $i \in I$*, ou seja, o conjunto* $\{x_i\}_{i\in I}$ *é um conjunto de geradores linearmente independentes de* M*. O número de elementos de* I *é chamado de posto de* M*. No caso em que* I *é finito e* $\{x_i\}_{i\in I}$ *não é necessariamente linearmente independente, ou seja,* $x = \sum_{i\in I} a_i x_i$ *mas não de forma única,* M *é dito um* A*-módulo finitamente gerado.*

Proposição 2.1 *[14] Seja* $\{x_i\}_{i\in I}$ *um conjunto gerador de um* A*-módulo livre* M *de posto* n*. Se* $\#I = n$*, então* $\{x_i\}_{i\in I}$ *é uma* A*-base de* M.

2.2 Extensões de corpos, anel de inteiros e teoria de Galois

Nesta seção, apresentamos alguns resultados de extensões de corpos, extensões de Galois e anel de inteiros de um corpo de números, necessários para compreensão das próximas seções e dos próximos capítulos.

Definição 2.4 *Dizemos que um corpo* $\mathbb{L}$ *é uma extensão de um corpo* $\mathbb{K}$ *se* $\mathbb{K} \subseteq \mathbb{L}$. *Podemos considerar* $\mathbb{L}$ *como um* $\mathbb{K}$*-espaço vetorial e assim chamamos* $dim_{\mathbb{K}}\mathbb{L} = [\mathbb{L} : \mathbb{K}]$ *de grau da extensão* $\mathbb{L}$ *sobre* $\mathbb{K}$. *Denotamos a extensão* $\mathbb{L}$ *de* $\mathbb{K}$ *por* $\mathbb{L}|\mathbb{K}$.

Definição 2.5 *Se* $\mathbb{K}$ *é uma extensão finita de* $\mathbb{Q}$, *ou seja,* $[\mathbb{K} : \mathbb{Q}]$ *é finito, dizemos que* $\mathbb{K}$ *é um corpo de números, onde* $\mathbb{Q}$ *é o conjunto dos números racionais.*

No capítulo 2, focamos nosso estudo em corpos de números de grau p, com p um primo ímpar.

Definição 2.6 *Seja* $\mathbb{K}$ *um corpo de números. Definimos o anel de inteiros* $\mathcal{O}_{\mathbb{K}}$ *de* $\mathbb{K}$ *como o conjunto dos elementos de* $\mathbb{K}$ *que são raizes de polinômios mônicos sobre* $\mathbb{Z}$. *Se* $x \in \mathcal{O}_{\mathbb{K}}$, x *será chamado de elemento inteiro de* $\mathbb{K}$.

Proposição 2.2 *([23], pág. 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 2.7 *Uma base de* $\mathcal{O}_{\mathbb{K}}$ *como* $\mathbb{Z}$*-módulo é chamada base integral de* $\mathbb{K}$.

A seguir, damos resultados de teoria de corpos e de Galois, os quais são de fundamental importância na demonstração de resultados do Capítulo 3.

Proposição 2.3 *([23], pág. 31) Se* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ *são extensões de corpos de números, então* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Definição 2.8 *Sejam* $\mathbb{K}$ *um corpo de números e* $\alpha \notin \mathbb{K}$. *O menor corpo que contém* $\mathbb{K}$ *e* α *é definido com* $\mathbb{K}(\alpha)$ *e* $[\mathbb{K}(\alpha) : \mathbb{K}] = gr(min_{\mathbb{K}}\alpha)$, *onde* $min_{\mathbb{K}}\alpha$ *é o polinômio minimal de* α *sobre o corpo* $\mathbb{K}$.

Teorema 2.1 *([23], pág. 33) Se* $\mathbb{K}$ *é um corpo de números,* $\mathbb{L}$ *uma extensão de grau* n *de* $\mathbb{K}$ *e* $\mathbb{F}$ *um corpo algebricamente fechado contendo* $\mathbb{K}$, *então existem* n $\mathbb{K}$*-monomorfismos distintos de* $\mathbb{L}$ *em* $\mathbb{F}$.

O próximo Teorema caracteriza um corpo de números $\mathbb{K}$. Esse resultado será de fundamental importância no Capítulo 3.

Teorema 2.2 *([23], pág. 34) (Teorema do elemento primitivo) Se $\mathbb{L}|\mathbb{K}$ é uma extensão finita, então existe $t \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(t)$, onde t é chamado de elemento primitivo.*

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

Definição 2.9 *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 $\{\sigma \in Aut(\mathbb{L});\ \sigma|_{\mathbb{K}} = id_{\mathbb{K}}\}$. Denotamos este grupo por $Gal(\mathbb{L}|\mathbb{K})$.*

Definição 2.10 *Uma extensão finita $\mathbb{L}$ de $\mathbb{K}$ é dita uma extensão galoisiana, ou simplesmente de Galois, se $[\mathbb{L} : \mathbb{K}] = o(Gal(\mathbb{L}|\mathbb{K}))$. Uma extensão de Galois é dita abeliana (ou ciclíca) se o grupo de Galois é abeliano (ou ciclíco).*

As extensões abelianas de grau p, com p um primo ímpar é um dos focos desse trabalho.

Definição 2.11 *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e G um subgrupo do grupo $Aut(\mathbb{L})$. O corpo*

$$\mathbb{L}^G = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha,\ \textit{para todo } \sigma \in G\}$$

é chamado corpo fixo de G.

Teorema 2.3 *[22] (Correspondência de Galois) Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de Galois e $G = Gal(\mathbb{L}|\mathbb{K})$. Considerando os seguintes diagramas,*

$$\begin{array}{ccc} \mathbb{L} & \longrightarrow & \{id\} \\ | & & \\ \mathbb{M} & \longrightarrow & Gal(\mathbb{L}|\mathbb{M}) \\ | & & \\ \mathbb{K} & \longrightarrow & Gal(\mathbb{L}|\mathbb{K}) = G \end{array} \qquad \begin{array}{ccc} \mathbb{L} & \longleftarrow & \{e\} \\ | & & \\ \mathbb{L}^H & \longleftarrow & \{H\} \\ | & & \\ \mathbb{L}^G & \longleftarrow & G \end{array}$$

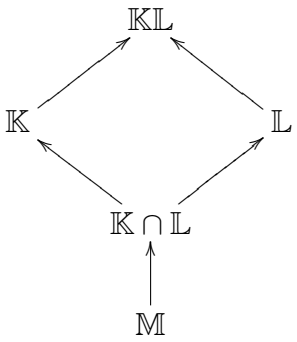
então que existe uma correspondência entre os corpos intermediários entre $\mathbb{K}$ e $\mathbb{L}$ e os subgrupos de G, ou seja,

i) $\mathbb{M} = \mathbb{L}^H \iff Gal(\mathbb{L}|\mathbb{M}) = H$

ii) $[\mathbb{L}^H : \mathbb{K}] = (G : H)$ *(índice de G sobre H).*

Definição 2.12 *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ extensões de um corpo $\mathbb{K}$. O menor corpo que contém $\mathbb{L}_1$ e $\mathbb{L}_2$ é chamado de corpo compósito de $\mathbb{L}_1$ e $\mathbb{L}_2$, e denotado por $\mathbb{L}_1\mathbb{L}_2$.*

Teorema 2.4 *[22](Irracionalidade Natural) Se $\mathbb{K}|\mathbb{M}$ é uma extensão de Galois e $\mathbb{L}|\mathbb{M}$ é uma extensão arbitrária, então $\mathbb{KL}|\mathbb{L}$ é Galois e $Gal(\mathbb{KL}|\mathbb{L}) \simeq Gal(\mathbb{K}|\mathbb{K} \cap \mathbb{L})$.*



Usamos o Teorema da Irracionalidade Natural em diversas demonstrações no Capítulo 3, para monstrarmos isomorfismos entre grupos de Galois. Também usamos para o cálculo do discriminante de certos corpos de números do Capítulo 4.

Teorema 2.5 *[22] Se $\mathbb{K}|\mathbb{M}$ e $\mathbb{L}|\mathbb{M}$ são extensões de Galois, então $\mathbb{KL}|\mathbb{M}$ é uma extensão de Galois.*

Teorema 2.6 *[22] Sejam $\mathbb{K}|\mathbb{M}$ e $\mathbb{L}|\mathbb{M}$ extensões de Galois. Se $G = Gal(\mathbb{K}|\mathbb{M})$ e $H = Gal(\mathbb{L}|\mathbb{M})$, então a aplicação*

$$\begin{aligned} \varphi : Gal(\mathbb{KL}|\mathbb{M}) &\longrightarrow G \times H \\ \rho &\longmapsto (\rho|_{\mathbb{K}}, \rho|_{\mathbb{L}}) \end{aligned}$$

é um homomorfismo injetor. Em particular, se $\mathbb{K} \cap \mathbb{L} = \mathbb{M}$, então φ é um isomorfismo.

2.3 Norma, traço e discriminante

Os conceitos de norma, traço e discriminante são necessários para obtenção de alguns parâmetros dos reticulados. Como foi colocado no Capítulo 1, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$ está relacionado com a densidade de centro de um reticulado algébrico e discriminante de um corpo de

números está relacionado com a distância produto mínima. Vamos definir esses conceitos nesta seção.

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 $\mathbb{F}$.

Definição 2.13 *Seja $\alpha \in \mathbb{L}$. Definimos a norma e o traço de α na extensão $\mathbb{L}|\mathbb{K}$ da seguinte forma:*

$$Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

$$N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Propriedades 2.1 *([23], pág. 36) Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, onde $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $x, y \in \mathbb{L}$ e $a \in \mathbb{K}$ valem as seguintes propriedades:*

a) $Tr_{\mathbb{L}|\mathbb{K}}(ax) = aTr_{\mathbb{L}|\mathbb{K}}(x)$

b) $Tr_{\mathbb{L}|\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a$

c) $N_{\mathbb{L}|\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$

d) $N_{\mathbb{L}|\mathbb{K}}(ax) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}|\mathbb{K}}(x)$

e se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, então

e) $N_{\mathbb{L}|\mathbb{K}}(x) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(x))$

f) $Tr_{\mathbb{L}|\mathbb{K}}(x) = Tr_{\mathbb{M}|\mathbb{K}}(Tr_{\mathbb{L}|\mathbb{M}}(x))$.

Proposição 2.4 *([23], pág. 36) Se $\mathbb{K}$ é um corpo de números, $\mathbb{L}$ uma extensão de grau n de $\mathbb{K}$, $\alpha \in \mathbb{L}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$ raízes do polinômio minimal de α sobre $\mathbb{K}$, então $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$.*

Proposição 2.5 *([23], pág. 38) Se $\mathbb{K} \subseteq \mathbb{L}$ são corpos de números e $\alpha \in \mathcal{O}_{\mathbb{L}}$, então o $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ pertencem a $\mathcal{O}_{\mathbb{K}}$.*

Proposição 2.6 *([23], pág. 39) Se $\mathbb{K}$ é um corpo de números, $\mathbb{L}$ uma extensão de grau n sobre $\mathbb{K}$, $\sigma_1, \ldots, \sigma_n$ $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$ e $\{x_1, x_2, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}|\mathbb{K}} = D(x_1, x_2, \ldots, x_n) = det(Tr_{\mathbb{L}|\mathbb{K}}(x_i x_j)) = det(\sigma_i(x_j))^2 \neq 0.$$

Observação 2.1 *Denotamos $D_{\mathbb{K}|\mathbb{Q}}$, simplesmente por $D_{\mathbb{K}}$.*

2.4 Ramificação de ideais

Consideramos agora $\mathbb{L}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$.

Teorema 2.7 *[22] Todo ideal J de $\mathcal{O}_{\mathbb{L}}$ é decomposto de forma única como $J = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, onde os $\mathfrak{P}_i$'s são ideais primos distintos e os e_i's são inteiros positivos.*

Assim, considerando um número primo $p \in \mathbb{Z}$, segue que $p\mathbb{Z}$ gerado por p em $\mathbb{Z}$ é um ideal primo. Desse modo, $p\mathcal{O}_{\mathbb{L}}$ é um ideal de $\mathcal{O}_{\mathbb{L}}$, e assim, é decomposto de forma única como $p\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$. Neste caso, dizemos que os ideais primos $\mathfrak{P}_i$'s estão acima do ideal primo $p\mathbb{Z}$ em $\mathcal{O}_{\mathbb{L}}$.

Proposição 2.7 *[22] Se $\mathfrak{P}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$, então*

i) $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$;

ii) $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$ *é uma extensão finita de* $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ *e* $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}} : \mathbb{F}_p\right] \leq n$.

Definição 2.14 *Seja J um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$. Chamamos de norma do ideal J o número de elementos do anel quociente $\dfrac{\mathcal{O}_{\mathbb{L}}}{J}$ e denotamos por $N_{\mathbb{L}}$, ou simplesmente, $N(J)$.*

Proposição 2.8 *[22] Se $\mathfrak{P}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ que está acima de $p\mathbb{Z}$, então $N(\mathfrak{P}) = p^f$, onde $f = \left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}} : \mathbb{F}_p\right]$.*

Definição 2.15 *Seja $p\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, onde os $\mathfrak{P}_i$'s são ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$.*

1) *O grau* $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i} : \dfrac{\mathbb{Z}}{p\mathbb{Z}}\right] = dim_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i)$ *é chamado de grau de inércia de* $\mathfrak{P}_i$ *sobre* $p\mathbb{Z}$ *e denotado por* $f_i = f(\mathfrak{P}_i|p\mathbb{Z})$.

2) *O expoente* $e_i = e(\mathfrak{P}_i|p\mathbb{Z})$ *de* $\mathfrak{P}_i$ *é chamado de índice de ramificação de* $\mathfrak{P}_i$ *sobre* $p\mathbb{Z}$.

Teorema 2.8 *[22](Igualdade Fundamental) Com as notações da Definição 2.15, tem-se que* $\sum_{i=1}^{g} e_i f_i = n$.

Definição 2.16 *Dizemos que o ideal primo* $p\mathbb{Z}$ *é:*

a) *totalmente decomposto em* $\mathcal{O}_{\mathbb{L}}$ *ou* $\mathbb{L}$, *se* $g = n$;

b) *totalmente inerte em* $\mathcal{O}_{\mathbb{L}}$ *ou* $\mathbb{L}$, *se* $f(\mathfrak{P}|p\mathbb{Z}) = n$, *para algum ideal* $\mathfrak{P}$ *acima de* $p\mathbb{Z}$;

c) *totalmente ramificado em* $\mathcal{O}_{\mathbb{L}}$ *ou* $\mathbb{L}$, *se* $e(\mathfrak{P}|p\mathbb{Z}) = n$, *para algum ideal* $\mathfrak{P}$ *acima de* $p\mathbb{Z}$;

d) *ramificado em* $\mathcal{O}_{\mathbb{L}}$ *ou em* $\mathbb{L}$, *se* $e(\mathfrak{P}|p\mathbb{Z}) > 1$ *para algum ideal* $\mathfrak{P}$ *acima de* $p\mathbb{Z}$.

Se $\mathbb{L}|\mathbb{Q}$ é uma extensão de Galois, então que $e_1 = \ldots = e_g$ e $f_1 = \ldots = f_g$. Logo, o Teorema da igualdade fundamental fica da seguinte forma $efg = n$.

Agora, consideramos $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L}$ extensões de corpos, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$.

Definição 2.17 *Chamamos de discriminante de* $\mathcal{O}_{\mathbb{L}}$ *sobre* $\mathcal{O}_{\mathbb{K}}$ *o ideal gerado pelo discriminante de uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *contida em* $\mathcal{O}_{\mathbb{L}}$ *e denotamos por* $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}}$.

Teorema 2.9 *[22] Se* $\mathfrak{p}$ *é um ideal primo de* $\mathcal{O}_{\mathbb{K}}$, *então* $\mathfrak{p}$ *se ramifica em* $\mathcal{O}_{\mathbb{L}}$ *se, e somente se,* $\mathfrak{p}$ *contém* $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}}$. *Em particular,* $p\mathcal{O}_{\mathbb{L}}$ *ramifica em* $\mathcal{O}_{\mathbb{L}}$ *se, e somente se,* p *divide o discriminante de* $\mathbb{L}$.

Lema 2.1 *([23], pág. 58)(Minkowski) Se* $\mathbb{K}$ *é uma extensão de* $\mathbb{Q}$ *tal que* $\mathbb{K} \neq \mathbb{Q}$, *então* $|D_{\mathbb{K}}| \geq 2$.

2.5 Corpos ciclotômicos

Os corpos ciclotômicos são de fundamental importância neste trabalho. Utilizando subcorpos de corpos ciclotômicos construímos reticulados algébricos e reticuados ideais. Por isso, veremos alguns resultados essenciais para compreensão dos demais capítulos.

Definição 2.18 *Sejam n um inteiro positivo.*

1) *Uma raíz do polinômio $x^n - 1$ é chamada de raíz n-ésima da unidade e denotamos por ζ_n.*

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

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

4) *O polinômio $\phi_n(x) = \prod_{j=1}^{n}(x - \zeta_n^j)$, onde $mdc(j,n) = 1$, é chamado de n-ésimo polinômio ciclotômico. O grau de $\phi_n(x)$ é dado pela Função de Euler $\varphi(n) = \#\{0 < m < n;\ mdc(m,n) = 1\}$ e $\phi_n(x)$ é mônico e irredutível sobre $\mathbb{Q}$.*

Proposição 2.9 *([27], pág. 11) Se $\zeta_n \in \mathbb{C}$ é uma raíz n-ésima primitiva da unidade e $k \in \mathbb{N}$, então ζ_n^k é uma n-ésima raíz primitiva da unidade se, e somente se, $mdc(k,n) = 1$.*

Tem-se que $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$ e se $mdc(m,n) = 1$, então vale a igualdade, pois $\varphi(mn) = \varphi(m)\varphi(n)$, com $mdc(m,n) = 1$, e assim, $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Proposição 2.10 *([27], pág. 11) Se ζ_n é uma raíz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ e $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*$.*

Tem-se que $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ é uma extensão de Galois. Além disso, $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = \{\sigma_i \in Aut(\mathbb{Q}(\zeta_n));\ mdc(i,n) = 1 \text{ e } \sigma_i(\zeta_n) = \zeta_n^i\}$. Como $\mathbb{Z}_n^*$ é abeliano, segue que $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ é abeliano. Agora, como $\mathbb{Z}_n^*$ é ciclíco para $n = 2, 4, p^r$ ou $2p^r$, onde p é primo ímpar e $r \geq 1$, segue que $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ é ciclíco para $n = 2, 4, p^r$ ou $2p^r$, onde p é primo e $r \geq 1$. Caso, $\mathbb{Z}_n^*$ não seja ciclíco, tem-se que $\mathbb{Z}_n^*$ contém pelo menos dois subgrupos ciclícos de ordem 2 [27].

Proposição 2.11 *([27], pág. 15) Se $\zeta_n \in \mathbb{C}$ é uma raíz n-ésima primitiva da unidade, com $n \in \mathbb{N}^*$, e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathbb{K} \subset \mathbb{R}$ e $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = 2$.*

Definição 2.19 *O corpo $\mathbb{K}$ da Proposição 2.11 é chamado de subcorpo real maximal de $\mathbb{Q}(\zeta_n)$.*

Teorema 2.10 *([27], pág.11) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, com $n \geq 1$, onde ζ_n é uma raíz n-ésima primitiva da unidade, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \ldots, \zeta_n^{\frac{\varphi(n)}{2}-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como um $\mathbb{Z}$-módulo.*

Teorema 2.11 *[17] Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, com $n \geq 1$, então*

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

Proposição 2.12 *([18], pág. 25) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_n) = (-1)^s$, se n é livre de quadrados, com s o número de primos que aparecem na fatoração de n;*

Proposição 2.13 *[10] Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, então*

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

Lema 2.2 *([27], pág. 10) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então um primo p ramifica em $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ se, e somente se, $p|n$.*

Demonstração. Segue diretamente dos Teoremas 2.9 e 2.11. ■

Lema 2.3 *[22] Se p é um primo e $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, então $(1-\zeta_{p^r})\mathbb{Z}[\zeta_{p^r}]$ é o único ideal primo acima de $p\mathbb{Z}$ em $\mathbb{Z}[\zeta_{p^r}]$.*

2.6 Anel de grupo

Vamos definir nesta seção o conceito de anel de grupo. Usamos este conceito para a compreensão dos Teoremas 3.2 e 3.3.

Sejam R um anel e G um grupo.

Definição 2.20 *Um anel de grupo $R[G]$ é o conjunto de todas as combinações lineares*

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

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

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

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\alpha\beta = (\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g,h \in G} (a_g b_h) gh$$

$$\lambda\alpha = \lambda(\sum_{g \in G} a_g g) = \sum_{g \in G} (\lambda a_g) g, \text{ com } \lambda \in R.$$

Tem-se que $R[G]$ com a soma e o produto definidos dessa maneira é um anel.

2.7 Considerações finais

Mencionamos nesse capítulo, resultados importantes em teoria algébrica dos números necessários para compreensão dos demais capítulos. Destacamos o Teorema do Elemento Primitivo, resultados sobre $\mathbb{Z}$-módulos livres, ramificação de um ideal primo de $\mathbb{Z}$ em $\mathcal{O}_{\mathbb{K}}$, com $\mathbb{K}$ um corpo de números, o valor do traço de ζ_n e a definição de anéis de grupos.

Capítulo 3

Extensão abelianas de grau p

Neste capítulo vamos explicitar resultados sobre um corpo de números $\mathbb{K}$ abeliano de grau p, com p um primo ímpar. Determinamos um elemento primitivo de $\mathbb{K}$, uma base integral para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, caracterizamos um elemento de $\mathcal{O}_{\mathbb{K}}$ tal que pertença à um ideal primo especicfíco de $\mathcal{O}_{\mathbb{K}}$ e encontramos o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$. Estes resultados algébricos são de fundamental importância para as construções de reticulados algébricos, construções estas que veremos com mais detalhes no Capítulo 4.

Para a obtenção desses resultados dividimos em três casos considerando o condutor do corpo de números abeliano $\mathbb{K}$.

Iniciamos relacionando alguns resultados já conhecidos sobre corpos de números abelianos.

3.1 Corpos de números abelianos

Nesta seção citamos alguns resultados sobre corpos de números abelianos, particularizando alguns resultados para extensões abelianas de grau p, com p um primo ímpar. Os principais resultados dessa seção são 3.2 e 3.3 encontrados em [15].

Como visto no Capítulo 2, um corpo de números $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$. Se $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana cujo o grupo $Gal(\mathbb{K}|\mathbb{Q})$ é abeliano (cíclico), dizemos que a extensão $\mathbb{K}|\mathbb{Q}$ é abeliana (cíclica).

Proposição 3.1 *[7] Se G é um grupo de ordem p, com p um primo, então G é um grupo cíclico.*

Logo, se $\mathbb{K}|\mathbb{Q}$ é uma extensão galoisiana de grau p, com p um primo ímpar, então $\mathbb{K}$ é uma extensão ciclíca, e consequentemente, abeliana.

Teorema 3.1 *[11](Kronecker-Weber) Se $\mathbb{K}$ é um corpo de números abeliano, então $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, para algum $n \in \mathbb{N}^*$.*

Definição 3.1 *Seja $\mathbb{K}$ um corpo de números abeliano. Chamamos o menor $n \in \mathbb{N}^*$ tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ de condutor do corpo $\mathbb{K}$ e denotamos por $cond(\mathbb{K})$.*

Assim, se $\mathbb{K}$ é um corpo de números abeliano de grau p, com p primo ímpar, então $Gal(\mathbb{K}|\mathbb{Q})$ é um subgrupo de $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*$. Lembrando que $\mathbb{Z}_n^*$ é cíclico, quando $n = 2, 4, p^r, 2p^r$, com $r \geq 1$ [27].

Observe que os possíveis primos que ramificam em $\mathcal{O}_{\mathbb{K}}$ são os primos que dividem $cond(\mathbb{K}) = n$ (Lema 2.2).

Proposição 3.2 *([18], pág. 29) Se $\mathbb{K}$ um corpo de números abeliano de grau p, com p primo ímpar, então*

i) p ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $cond(\mathbb{K}) = p^2 p_1 p_2 ... p_s$,

ii) p não ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $cond(\mathbb{K}) = p_1 p_2 ... p_s$,

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

Agora, vamos analisar os resultados sobre os corpos de números abelianos de grau p, em três casos de acordo com seus respectivos condutores.

1º Caso: $cond(\mathbb{K}) = p_1 p_2 \ldots p_s$, com os p_i's primos tais que $p_i \equiv 1 (mod\ p)$ para $i = 1, \ldots, s$.

2º Caso: $cond(\mathbb{K}) = p^2$.

3º Caso $cond(\mathbb{K}) = p^2 q$, com q um primo tal que $q \equiv 1 (mod\ p)$.

O 1º Caso foi analisado por Everton Luiz de Oliveira em sua Tese de Doutorado [18]. O 2º Caso foi analisado por Eduardo Rogério Favaro também em sua Tese de Doutorado [9].

O nosso objetivo aque é analisar o 3º Caso. Também serão abordados outros resultados dos dois primeiros casos. A generalização do 3º Caso, é um problema que ainda está em aberto.

Para encontrarmos um elemento primitivo e uma $\mathbb{Z}$-base para o anel de inteiros de um corpo de números abeliano $\mathbb{K}$, vamos usar fortemente os resultados a seguir.

Teorema 3.2 *[15](Teorema de Leopoldt) Se $\mathbb{K}$ é um corpo de números abeliano de condutor n, então $\mathbb{K} = \mathbb{Q}[G]T = \bigoplus_{d\in D} \mathbb{Q}[G]\eta_d$, onde*

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

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

Teorema 3.3 *[15][16](Teorema de Leopoldt-Lettl)Se $\mathbb{K}$ é um corpo de números abeliano de condutor n, então $\mathcal{O}_{\mathbb{K}} = \bigoplus_{d\in D} \mathbb{Z}[G]\eta_d$, onde*

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

$$\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}(\zeta_d), \eta_d = Tr_{\mathbb{Q}(\zeta_d)|\mathbb{K}_d}(\zeta_d) \text{ e } G = Gal(\mathbb{K}|\mathbb{Q})$$

Apesar de termos uma caracterização tanto para o corpo $\mathbb{K}$, quanto para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, não é fácil chegarmos a uma caracterização mais clara e compreensível desses resultados. Porém, quando $[\mathbb{K} : \mathbb{Q}] = p$, podemos simplificar os resultados acima.

A proposição a seguir fornece a quantidade de subcorpos de $\mathbb{Q}(\zeta_n)$ de grau p. Porém, estamos interessados em eliminar os subcorpos que não têm condutor n. Faremos isso, caso a caso.

Proposição 3.3 *[18] Existem $\frac{p^k-1}{p-1}$ subcorpos de $\mathbb{Q}(\zeta_n)$ de grau p, com $n = \prod_{i=1}^{r} p_i^{a_i}$ e $k = \#\{i; p|\varphi(p_i^{a_i})\}$.*

Proposição 3.4 *[17]Se $\mathbb{K}$ é um corpo de números abeliano de condutor $n = \prod_{i=1}^{r} p_i^{a_i}$, então*

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

onde $|D_{\mathbb{K}}|$ *denota o valor absoluto de* $D_{\mathbb{K}}$.

Corolário 3.1 *[17] Se* $\mathbb{K}$ *é um corpo de números abeliano de grau p e condutor n, então*

$$|D_{\mathbb{K}}| = n^{p-1}$$

A partir de agora consideramos $\mathbb{K}$ uma extensão abeliana de grau p, com p um primo ímpar.

3.2 1º Caso: $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$, com $p_i \equiv 1(mod\ p)$ e p_i's primos

Seja $\mathbb{K}$ um corpo de números abeliano de grau p, com p primo ímpar. Pelo Teorema de Kronecker-Weber 3.1, segue que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, para algum $n \in \mathbb{N}^*$. O menor n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado de condutor do corpo $\mathbb{K}$. Suponhamos nesta seção que $n = \prod_{i=1}^{s} p_i$ seja o condutor de $\mathbb{K}$, com p_i's primos distintos para $i = 1, \ldots, s$ e $p_i \equiv 1(mod\ p)$. A priori, damos o número de subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n e grau p. Logo após, explicitamos o elemento primitivo de $\mathbb{K}$. Em seguida, encontramos uma base integral de $\mathcal{O}_{\mathbb{K}}$. E finalmente, apresentamos uma família de $\mathbb{Z}$-submódulos de $\mathcal{O}_{\mathbb{K}}$, a qual fornecerá reticulados algébricos com alta densidade de centro, como veremos no Capítulo 4.

Proposição 3.5 *([18], pág. 30) Existem* $(p-1)^{s-1}$ *subcorpos de grau p e condutor n em* $\mathbb{Q}(\zeta_n)$, *com* $n = \prod_{i=1}^{s} p_i$ *e* $p_i \equiv 1(mod\ p)$.

Demonstração. Consideramos primeiramente, o caso em que $n = p_1p_2$. Neste caso, que existem 2 subcorpos de $\mathbb{Q}(\zeta_n)$ que não tem condutor n e sim condutor p_i, para $i = 1, 2$. Logo, temos dois subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. Portanto, existem $\frac{p^2-1}{p-1} - 2 = p + 1 - 2 = p - 1$ subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. Agora, consideramos $n = p_1p_2p_3$. Devemos desconsiderar os subcorpos de condutor p_i e p_ip_j, para $i \neq j$. Os subcorpos de condutor p_i's são 3 e os de condutor p_ip_j são $\frac{3!}{2!(3-2)!}(p-1)$. Logo, existem $\frac{p^3-1}{p-1} - 3 - 3(p-1) = (p-1)^2$ subcorpos de $\mathbb{Q}(\zeta_n)$ de condutor n. Aplicando o processo sucessivamente, segue que

existem $\frac{p^s-1}{p-1} - s - \frac{s!}{2!(s-2)!}(p-1) - \frac{s!}{3!(s-3)!}(p-1)^2 - \ldots - \frac{s!}{(s-1)!(s-(s-1))!}(p-1)^{s-2} = (p-1)^{s-1}$ subcorpos de grau p e condutor n em $\mathbb{Q}(\zeta_n)$. ■

Exemplo 3.1 *Se $\mathbb{Q}(\zeta_{91})$, então $n = 7.13$, com $7 \equiv 1(mod\ 3)$ e $13 \equiv 1(mod\ 3)$. Existe $\frac{3^2-1}{3-1} = 4$ extensões cúbicas de $\mathbb{Q}(\zeta_{91})$. Existem um corpo de números abeliano de condutor 7, um de condutor 13 e dois de condutor 91.*

Pelo Teorema do Elemento Primitivo, segue que $\mathbb{K} = \mathbb{Q}(t)$, para algum $t \in \mathbb{K}$. O teorema a seguir, fornece a caracterização de t neste 1º caso.

Teorema 3.4 *[12] Se $\mathbb{K}$ um corpo de números abeliano e $cond(\mathbb{K}) = n$, com n ímpar livre de quadrados, então $\mathbb{K} = \mathbb{Q}(t)$, com $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$ e $\mathbb{L} = \mathbb{Q}(\zeta_n)$.*

Exemplo 3.2 *Se $\mathbb{K}_1$ e $\mathbb{K}_2$ são os subcorpos de $\mathbb{Q}(\zeta_{91}) = \mathbb{L}$ de condutor 91, então $\mathbb{K}_1 = \mathbb{Q}(Tr_{\mathbb{L}|\mathbb{K}_1}(\zeta_{91}))$ e $\mathbb{K}_2 = \mathbb{Q}(Tr_{\mathbb{L}|\mathbb{K}_2}(\zeta_{91}))$.*

Definição 3.2 *Seja $\mathbb{K}|\mathbb{Q}$ uma extensão de Galois finita. Se os conjugados de um elemento $t \in \mathbb{K}$ formam uma $\mathbb{Q}$-base de $\mathbb{K}$, diremos que $\mathbb{K}$ tem uma base normal gerada por t. Em outras palavras, $\mathbb{K} = \mathbb{Q}[G]t$, com $G = Gal(\mathbb{K}|\mathbb{Q})$.*

Com as notações do Teorema 3.4, segue que $\mathbb{K}$ tem uma base normal com gerador $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$.

Definição 3.3 *Seja $\mathbb{K}|\mathbb{Q}$ uma extensão de Galois finita. Se os conjugados de um elemento $t \in \mathcal{O}_{\mathbb{K}}$ formam uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, dizemos que $\mathcal{O}_{\mathbb{K}}$ tem uma base integral normal gerada por t. Em outras palavras, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G]t$, com $G = Gal(\mathbb{K}|\mathbb{Q})$.*

O próximo teorema, o Teorema de Hilbert-Speiser fornece condições quando $\mathcal{O}_{\mathbb{K}}$ tem uma base integral normal.

Teorema 3.5 *[12](Hilbert-Speiser)Seja $\mathbb{K}$ um corpo de números abeliano, com $cond(\mathbb{K}) = n$. Assim, $\mathcal{O}_{\mathbb{K}}$ tem uma base integral normal se, e somente se, n é livre de quadrados.*

Observação 3.1 *Se $\mathbb{K}$ é uma extensão abeliana de grau p e condutor $n = \prod_{i=1}^{s} p_i$, com p_i's distintos e $p_i \equiv 1(mod\ p)$, então $\mathcal{O}_{\mathbb{K}}$ tem uma base integral normal gerada por t, ou seja, os conjugados de t em $\mathbb{K}|\mathbb{Q}$, $\{\theta(t), \theta^2(t), \ldots, \theta^p(t)\}$, formam uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*

3.2.1 Forma traço integral, com $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$

Vamos considerar, nesta subseção, $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar, $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$ e θ o gerador do $Gal(\mathbb{K}|\mathbb{Q})$. Seja $x = \sum_{i=1}^{p} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$, não nulo. Estamos interessados em calcular $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$. Primeiramente, notamos que $x^2 = \sum_{i,j=1}^{p} a_i a_j \theta^i(t)\theta^j(t)$.

Proposição 3.6 *([18], pág. 30)* $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)\theta^j(t) = Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t))$, *para* $i, j = 1, \ldots, p$.

Da Proposição 3.6, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = \sum_{i,j=1}^{p} a_i a_j Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{i-j}(t))$.

Proposição 3.7 *([18], pág. 32)* $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t)) = \begin{cases} n - (\frac{n-1}{p}), & \text{se } k = 0 \\ -(\frac{n-1}{p}), & \text{se } k \neq 0, \end{cases}$ *onde* $k = 1, \ldots, p-1$.

Teorema 3.6 *([18], pág. 38) Seja* $\mathbb{K}$ *um corpo de números abeliano de grau p, com p um primo ímpar, e condutor n livre de quadrados. Se* $x \in \mathcal{O}_{\mathbb{K}}$ *é não nulo, então*

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

3.2.2 Mínimo da forma traço integral, com $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$

Nesta subseção definimos uma família de $\mathbb{Z}$-submódulos M_m de $\mathcal{O}_{\mathbb{K}}$, onde é possível encontar $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);\ x \in \mathrm{M}, x \neq 0\}$. Com este minímo será possível construir reticulados algébricos com densidade de centro alta.

Definição 3.4 *Sejam* $Gal(\mathbb{K}|\mathbb{Q}) = \langle\theta\rangle$ *e* $t = Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_n)$. *Definimos o seguinte* $\mathbb{Z}$*-submódulo de* $\mathcal{O}_{\mathbb{K}}$

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

onde m é um inteiro positivo.

Claramente, se $m = 1$, então $\mathrm{M}_1 = \mathcal{O}_\mathbb{K}$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) \geq pN_{\mathbb{K}|\mathbb{Q}}(x^2)^{\frac{1}{p}} \geq p$, para todo $x \in \mathcal{O}_\mathbb{K}$ não nulo. Logo, $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);\ x \in \mathcal{O}_\mathbb{K}, x \neq 0\} = p$ e é atingido em $x = 1 \in \mathcal{O}_\mathbb{K}$.

Suponhamos agora, $m > 1$. Para cada par (i, j), com $i \neq j$ e $i, j = 0, \ldots, p-1$, definimos a seguinte aplicação:

$$\tau_{ij} : \mathbb{Z}^p \longrightarrow \mathbb{Z}^p$$

$$a = (a_0, \ldots, a_{p-1}) \longmapsto b = (b_0, \ldots, p_{p-1})$$

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

Notamos que, se $\tau_{ij}(a) = b$, então $\sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k$. Reciprocamente, se $\sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k$, então existe uma aplicação τ_{ij} tal que $\tau_{ij}(a) = b$.

Denotamos $\|a\|^2 = \sum_{i=0}^{p-1} a_i^2$, para $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$.

Proposição 3.8 *([18], pág. 40) Sejam $a, b \in \mathbb{Z}^p$ tal que $\tau_{ij}(a) = b$, onde $i, j = 1, \ldots, p-1$. Assim, $\|a\|^2 > \|b\|^2$ se, e somente se, $a_i - a_j > 1$.*

Definição 3.5 *Seja $a \in \mathbb{Z}^p$. Definimos a órbita de a como sendo o conjunto*

$$\mathrm{O}(a) = \left\{ b \in \mathbb{Z}^p;\ \sum_{k=0}^{p-1} a_k = \sum_{k=0}^{p-1} b_k \right\}.$$

Definimos também a órbita de um elemento $x \in \mathcal{O}_\mathbb{K}$ como sendo o conjunto

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

Lema 3.1 *([18], pág. 40) Sejam $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$ e $S := \sum_{k=0}^{p-1} a_k \geq 0$. Se q e r são, respectivamente, o quociente e o resto da divisão de S por p, então*

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

Além disso, o minímo é atingido exatamente nos elementos $b \in \mathbb{Z}^p$, onde r de b entradas são iguais a $q+1$ e $p-r$ entradas são iguais a q.

Teorema 3.7 *([18], pág. 40) Sejam* $x = \sum_{k=0}^{p-1} a_k\theta^k(t) \in \mathcal{O}_{\mathbb{K}}$, $S = S(x) = \sum_{k=0}^{p-1} a_k$, q *o quociente e* r *o resto da divisão de* S *por* p. *Se* $S \geq 0$, *então*

$$M(S) = \min_{y \in \mathrm{O}(x) y \neq 0} Tr_{\mathbb{K}|\mathbb{Q}}(y^2) = pq^2 + 2rq + nr - \frac{n-1}{p} r^2.$$

Concluiremos esse estudo no Capítulo 4, após termos definido densidade de centro de um reticulado algébrico.

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

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

Proposição 3.9 *Seja* $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$. *Tem-se que* $x \in \mathfrak{P}_i$ *se, e somente se,* $\sum_{i=0}^{p-1} a_i \equiv 0(mod\ p_i)$.

Demonstração. Como $t \in \mathcal{O}_{\mathbb{K}}$, então $t \equiv c(mod\ \mathfrak{P}_i)$, com $c \in \mathbb{Z}$ constante. Assim, $\theta^i(t) \equiv c(mod\ \mathfrak{P}_i)$. Logo, $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \equiv c\sum_{i=0}^{p-1} a_i(mod\ \mathfrak{P}_i)$. Desta forma, $x \in \mathfrak{P}_i$ se, e somente se, $c\sum_{i=0}^{p-1} a_i \equiv 0(mod\ \mathfrak{P}_i)$ se, e somente se, $c \in \mathfrak{P}_i$ ou $\sum_{i=0}^{p-1} a_i \in \mathfrak{P}_i$, uma vez que $\mathfrak{P}_i$ é um ideal primo. Se $c \in \mathfrak{P}_i$, então t e $\theta^i(t)$ pertencem a $\mathfrak{P}_i$. Logo, $\sum_{i=0}^{p-1} \theta^i(t) \in \mathfrak{P}_i$, ou seja, $Tr_{\mathbb{K}|\mathbb{Q}}(t) \in \mathfrak{P}_i$. Como $Tr_{\mathbb{K}|\mathbb{Q}}(t) = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n) = (-1)^s$, segue que $\pm 1 \in \mathfrak{P}_i$, o que é um absurdo. Portanto, $x \in \mathfrak{P}_i$ se, e somente se, $\sum_{i=0}^{p-1} a_i \in \mathfrak{P}_i \cap \mathbb{Z} = p_i\mathbb{Z}$, como queríamos. ■

Proposição 3.10 *Os ideias primos* $\mathfrak{P}_i$*'s de* $\mathcal{O}_{\mathbb{K}}$ *que estão acima de* $p_i\mathbb{Z}$ *são da forma* $p_i\mathbb{Z}t + \sum_{j=1}^{p-1} p_i\mathbb{Z}(\theta^j(t) - t)$, *onde* $\mathfrak{P} \cap \mathbb{Z} = p_i$.

Demonstração. Se $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$, então $x = \sum_{i=0}^{p-1} a_i\theta^i(t) + \sum_{i=0}^{p-1} a_i t - \sum_{i=1}^{p-1} a_i t = t\sum_{i=0}^{p-1} a_i + \sum_{i=0}^{p-1} a_i(\theta^i(t) - t)$. Logo, pela Proposição 3.9, segue que $x \in \mathfrak{P}_i$ se, e somente se, $x = p_i\mathbb{Z}t + p_i\mathbb{Z}(\theta^i(t) - t)$. ■

3.3 2º Caso: $cond(\mathbb{K}) = p^2$

Consideramos $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Pelo Teorema de Kronecker-Weber 3.1, segue que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ para algum $n \in \mathbb{N}$ tal que $p|\varphi(n)$, onde φ é a função de Euler. O menor n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado condutor do corpo $\mathbb{K}$. Nesta seção, vamos considerar p^2 o condutor de $\mathbb{K}$.

Nosso objetivo é explicitar o elemento primitivo de $\mathbb{K}$, uma base integral do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$, caracterizar os ideais de $\mathcal{O}_{\mathbb{K}}$ que estão acima do ideal primo $p\mathbb{Z}$ e calcular o valor $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, para $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Em [9], alguns desses resultados já foram apresentados.

Se $G = Gal(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^*$, então G é cíclico. Desta forma, consideramos θ o gerador de G. Notemos que se $\psi \in G$, então $\psi(\zeta_{p^2}) = \zeta_{p^2}^j$, com $mdc(p^2, j) = 1$ e $1 \leq j < p^2$. Sendo assim, consideramos α tal que $mdc(\alpha, p^2) = 1$, onde $1 \leq \alpha < p^2$ e $\theta(\zeta_{p^2}) = \zeta_{p^2}^{\alpha}$, com $\langle\theta\rangle = G$. Assim, $\overline{\alpha}$ gera $\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^*$. Tomando $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$, segue que

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

Primeiramente, mostramos que $\mathbb{K} = \mathbb{Q}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2}))$. Em seguida vamos encontrar uma base integral de $\mathcal{O}_{\mathbb{K}}$, a qual já sabemos pelo Teorema de Hilbert-Spieser 3.5 que não é uma base integral normal. Para isto, usaremos fortemente o Teorema de Leoplodt-Lettl 3.3.

Observação 3.2 *Como $Gal(\mathbb{Q}(\zeta_{p^2})|\mathbb{Q})$ é cíclico e $p|\varphi(p^2)$, segue que existe um único subcorpo $\mathbb{K}$ de $\mathbb{Q}(\zeta_{p^2})$ de grau p.*

Proposição 3.11 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Se $cond(\mathbb{K}) = p^2$, então $\mathbb{K} = \mathbb{Q}(t)$, com $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$.*

Demonstração. Como $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2}) \in \mathbb{K}$, segue que $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq \mathbb{K}$. Como $[\mathbb{K} : \mathbb{Q}] = p$, com p primo, segue que $\mathbb{Q} = \mathbb{Q}(t)$ ou $\mathbb{K} = \mathbb{Q}(t)$. Pelo Teorema de Leopoldt-Lettl 3.2, segue que $\mathbb{K} = \mathbb{Q}[G](t-1)$. Logo, se $\mathbb{Q} = \mathbb{Q}(t)$, então $t \in \mathbb{Q}$, e assim, $\mathbb{K} = \mathbb{Q}$ absurdo. Portanto, $\mathbb{K} = \mathbb{Q}(t)$, com $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$. ■

Proposição 3.12 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Se $cond(\mathbb{K}) = p^2$, então $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração. Pelo Teorema de Leopoldt-Lettl 3.3, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G]t \oplus \mathbb{Z}$. Logo, $\{1, \theta(t), \ldots, \theta^{p-1}(t), \theta^p(t)\}$ é um conjunto de geradores de $\mathcal{O}_{\mathbb{K}}$ como um $\mathbb{Z}$-módulo. Como o posto de $\mathcal{O}_{\mathbb{K}}$ é p, segue que $\{1, \theta(t), \ldots, \theta^{p-1}(t), \theta^p(t)\}$ não é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, uma vez que possui $p+1$ elementos. Porém, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{p^2}) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = \sum_{j=1}^{p} \theta^j(t) = 0$, e assim, podemos considerar $\theta^p(t) = t$ uma combinação linear inteira de $\{\theta(t), \ldots, \theta^{p-1}(t)\}$. Desta forma, o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é um conjunto gerador de $\mathcal{O}_{\mathbb{K}}$ como $\mathbb{Z}$-módulo e possui p elementos, e portanto, pela Proposição 2.1, segue que $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. ■

3.3.1 Forma traço integral, com $cond(\mathbb{K}) = p^2$

Estamos interessados em calcular $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Como vimos na Seção 3.2.2, $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$. Com isso, consideramos $x = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(t) \in \mathcal{O}_{\mathbb{K}}$, com $a_i \neq 0$ para algum $i = 0, 1, \ldots, p-1$. Note que

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

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

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

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

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

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

segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2 p + \sum_{i=1}^{p-1} a_i^2 Tr_{\mathbb{K}|\mathbb{Q}}(t^2) + 2 \sum_{1\leq i<j\leq p-1} a_i a_j Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$. Desta forma, é suficiente conhecermos $Tr_{\mathbb{K}|\mathbb{Q}}(t^2)$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$ para encontrarmos o valor $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$. Para isso, usaremos a seguinte proposição.

Proposição 3.13 *[9] Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$, $\mathbb{K}$ um corpo de números abeliano de grau p e condutor p^2, com p um primo ímpar. Se $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_{p^2})$ e $\langle\theta\rangle = Gal(\mathbb{L}|\mathbb{Q})$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = p(p-1)$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t)) = -p$, onde $1 \leq i < j \leq p-1$.*

Desse modo, da Proposição 3.13, segue que

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

Proposição 3.14 *[10] Consideramos a forma quadrática dada por $Q_n(a_1,\ldots,a_n) = n\sum_{i=1}^{n} a_i^2 - 2\sum_{1\leq i<j\leq n} a_i a_j$. Então o minímo de Q_n com entradas inteiras é n e esse minímo é atingido em $\pm(1,\ldots,1)$ ou $\pm e_i$, onde $\{e_i\}$ é a base canônica de $\mathbb{Z}^n$.*

Proposição 3.15 *Com as notações acima, $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2); 0 \neq x \in \mathcal{O}_{\mathbb{K}}\} = p$. Esse mínimo é atingido para $(a_0, a_1, a_2, \ldots, a_{p-1}) = (1, 0, 0, \ldots, 0)$.*

Demonstração. Segue diretamente da Proposição 3.14. ■

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

Sejam $\mathfrak{P}_{\mathbb{K}}$ o ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$ e $\mathfrak{P}_{\mathbb{L}}$ o ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$, com $\mathbb{L} = \mathbb{Q}(\zeta_{p^2})$. Assim, nosso objetivo é caracterizar o ideal $\mathfrak{P}_{\mathbb{K}} = \mathfrak{P}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$. Com esse intuito apresentamos a seguinte proposição.

Proposição 3.16 *Se $\mathfrak{P}_{\mathbb{K}}$ é o ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$ e $\zeta_{p^2} = \zeta$, então $\mathfrak{P}_{\mathbb{K}}$ é gerado por $N_{\mathbb{L}|\mathbb{K}}(1-\zeta)$.*

Demonstração. Sabemos que $p\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_{\mathbb{L}}^{p(p-1)}$, ou seja, p ramifica totalmente em $\mathcal{O}_{\mathbb{L}}$, onde $\mathfrak{P}_{\mathbb{L}} = (1-\zeta)\mathbb{Z}[\zeta]$ 2.3. Seja $\lambda = N_{\mathbb{L}|\mathbb{K}}(1-\zeta) = \prod_{j=1}^{p-1}(1-\zeta^{\alpha^{jp}})$. Como $\mathbb{K}$ é um corpo de números, segue que o ideal $\langle\lambda\rangle$ em $\mathcal{O}_{\mathbb{K}}$ se decompõe em produto de ideais primos de $\mathcal{O}_{\mathbb{K}}$. Como $1-\zeta$ é o conjugado de $1-\zeta^{\alpha^{jp}}$, segue que $(1-\zeta)\mathcal{O}_{\mathbb{L}} = (1-\zeta^{\alpha^{jp}})\mathcal{O}_{\mathbb{L}}$, o que implica que $\prod_{j=1}^{p-1}(1-\zeta^{\alpha^{jp}})\mathcal{O}_{\mathbb{L}} = (1-\zeta)^{p-1}\mathcal{O}_{\mathbb{L}}$, e assim, $\lambda\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_{\mathbb{L}}^{p-1} = \mathfrak{P}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Portanto, $\lambda\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$, isto é, $\mathfrak{P}_{\mathbb{K}} = \langle\lambda\rangle = \langle N_{\mathbb{L}|\mathbb{K}}(1-\zeta)\rangle = \mathfrak{P}_{\mathbb{K}}^{p-1}$. ■

3.4 3º Caso: $cond(\mathbb{K}) = p^2\prod_{i=1}^{s} p_i$, com p_i's primos e $p_i \equiv 1(mod\ p)$

Consideramos $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar. Pelo Teorema de Kronecker-Weber 3.1, segue que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ para algum $n \in \mathbb{N}$ tal que $p|\varphi(n)$, onde φ é a função de Euler. O menor n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ é chamado condutor do corpo $\mathbb{K}$. Nesta seção vamos considerar $n = p^2\prod_{i=1}^{s} p_i$ o condutor de $\mathbb{K}$, onde p_i's são primos distintos e $p_i \equiv 1(mod\ p)$.

Nosso objetivo inicial é explicitar o elemento primitivo de $\mathbb{K}$ e uma base integral do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Em seguida, vamos considerar $s = 1$, ou seja, $cond(\mathbb{K}) = p^2q$, com q primo e $q \equiv 1(mod\ p)$, e caracterizar o ideal primo $\mathfrak{Q}$ de $\mathcal{O}_{\mathbb{K}}$ que está acima do ideal primo $q\mathbb{Z}$, calcular o valor $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, para $x \in \mathcal{O}_{\mathbb{K}}$ não nulo e finalmente, calcular $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2); 0 \neq x \in \mathfrak{Q}\}$.

Primeiramente, encontramos o números de subcorpos de $\mathbb{Q}(\zeta_n)$ de grau p e condutor n, com $n = p^2\prod_{i=1}^{s} p_i$.

Proposição 3.17 *Existem $(p-1)^s$ subcorpos de grau p em $\mathbb{Q}(\zeta_n)$ de condutor n.*

Demonstração. Consideramos primeiramente $n = p^2p_1$. Como $\mathbb{Q}(\zeta_{p^2})$ e $\mathbb{Q}(\zeta_{p_1})$ são ciclícas de $\mathbb{Q}$ e $p|\varphi(p^2)$ e $p|\varphi(p_1)$, segue que existem apenas dois corpos de grau p contidos

em $\mathbb{Q}(\zeta_n)$ os quais não tem condutor n. Assim, existem $\frac{p^2-1}{p-1}-2 = p-1$ subcorpos de $\mathbb{Q}(\zeta_n)$ os quais tem condutor n. Agora, consideramos $n = p^2p_1p_2$. Logo, existem 3 subcorpos de $\mathbb{Q}(\zeta_n)$ os quais tem condutor p^2, p_1 e p_2. Também existem $\frac{3!}{2!(3-2)!}(p-1) = 3(p-1)$ subcorpos de condutor p^2p_i ou p_ip_j, com $i, j = 1, 2$. Portanto, existem $\frac{p^3-1}{p-1}-3-3(p-1) = (p-1)^2$ subcorpos de condutor n.

Repetindo o processo sucessivamente, segue que existem $\frac{p^{s+1}-1}{p-1}-(s+1)-\frac{(s+1)!}{2!(s+1-2)!}(p-1)-\frac{(s+1)!}{3!(s+1-3)!}(p-1)^2-\ldots-\frac{(s+1)!}{s!(s+1-s)!}(p-1)^{s-1} = (p-1)^s$ subcorpos de condutor n. ■

Proposição 3.18 *Sejam $n = p^2\prod_{i=1}^{s} p_i$, $\mathbb{L} = \mathbb{Q}(\zeta_n)$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p e p_i's primos distintos e $p_i \equiv 1(mod\ p)$. Se $cond(\mathbb{K}) = n$, então $\mathbb{K} = \mathbb{Q}(t)$, onde $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$.*

Demonstração. Seja $n = cond(\mathbb{K}) = p^2\prod_{i=1}^{s} p_i$. Aplicando o Teorema Leopoldt [15], segue que $D = \{d_1 = p\prod_{i=1}^{s} p_i, d_2 = n\}$. Assim, $\mathbb{K}_{d_1} = \mathbb{Q}$ e $\mathbb{K}_{d_2} = \mathbb{K}$. Logo, $T = Tr_{\mathbb{Q}(\zeta_{d_1})|\mathbb{Q}}(\zeta_{d_1}) + Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n) = (-1)^{s+1} + t$. Como $t \in \mathbb{K}$, segue que $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq \mathbb{K}$. Assim, $\mathbb{Q} = \mathbb{Q}(t)$ ou $\mathbb{K} = \mathbb{Q}(t)$, uma vez que $[\mathbb{K} : \mathbb{Q}] = p$. Suponhamos que $\mathbb{Q} = \mathbb{Q}(t)$, ou seja, $t \in \mathbb{Q}$. Logo, $\mathbb{K} = \mathbb{Q}[G]T = \mathbb{Q}[G](\pm 1 + t)$, com $T \in \mathbb{Q}$ o gerador da base normal de $\mathbb{K}$. Portanto, se $x \in \mathbb{K}$, então $x = \sum_{g\in G} a_g g(\pm 1 + t) = \sum_{g\in G} a_g(\pm 1 + t) \in \mathbb{Q}$, ou seja, $\mathbb{K} \subseteq \mathbb{Q}$, o que é um absurdo. Desta forma, $t \notin \mathbb{Q}$. Portanto, $\mathbb{K} = \mathbb{Q}(t)$. ■

Proposição 3.19 *Se $n = p^2\prod_{i=1}^{s} p_i$ e $\mathbb{L} = \mathbb{Q}(\zeta_n)$, então $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$.*

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

Proposição 3.20 *Sejam $n = p^2\prod_{i=1}^{s} p_i$, $\mathbb{L} = \mathbb{Q}(\zeta_n)$ e $\mathbb{K}$ um corpo de números abeliano de grau p, com p um primo ímpar e os p_i's primos distintos tais que $p_i \equiv 1(mod\ p)$. Se $cond(\mathbb{K}) = n$, então $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração. Pelo Teorema de Leopoldt-Lettl [16], segue que $\mathcal{O}_{\mathbb{K}} = \bigoplus_{d\in D} \mathbb{Z}[G]\eta_d$. Assim, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G](\pm 1) \bigoplus \mathbb{Z}[G](t)$, onde $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$. Como $\mathbb{Z}[G](\pm 1) = \sum_{g\in G} a_g g(\pm 1) = \pm \sum_{g\in G} a_g$, com $a_g \in \mathbb{Z}$, segue que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} \bigoplus \mathbb{Z}[G](t)$. Desta forma, o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ gera $\mathcal{O}_{\mathbb{K}}$. Porém, este conjunto tem $p+1$ elementos. Agora, notamos que $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = 0$, uma vez que n não é livre de quadrados. Logo, $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)) = Tr_{\mathbb{K}|\mathbb{Q}}(t) = \sum_{i=1}^{p} \sigma^i(t) = 0$, o que implica que, $-\sum_{i=1}^{p-1} \theta^i(t) = \theta^p(t)$, ou seja, $\theta^p(t)$ é uma combinação linear inteira de $\{\theta(t)), \ldots, \theta p - 1(t)\}$, e assim, $\{\theta(t), \ldots, \theta^{p-1}(t)\}$ gera $\mathbb{Z}[G](t)$. Desta forma, o conjunto $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é um conjunto com p elementos que gera $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto p, segue que por 2.1 que $\{1, \theta(t), \ldots, \theta^{p-1}(t)\}$ é $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{K}}$. ■

3.4.1 Forma traço integral, para $cond(\mathbb{K}) = p^2 \prod_{i=1}^{s} p_i$

Consideramos $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2 \prod_{i=1}^{s} p_i$, com p e os p_i's primos ímpares e $p_i \equiv 1(mod\ p)$, para $i = 1, \ldots, s$. O conjunto $\{1, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, onde $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$ e $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$. Queremos calcular o valor de $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Para isso, seja $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ não nulo, com $a_i \in \mathbb{Z}$, para $i = 0, \ldots, p-1$. Assim,

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

Notamos que $\theta^i(t)$ é um conjugado de t em $\mathbb{K}|\mathbb{Q}$, e assim, $Tr_{\mathbb{K}|\mathbb{Q}}(\theta^i(t)) = Tr_{\mathbb{K}|\mathbb{Q}}(t) =$

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

Nosso objetivo, agora, é calcular o $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$ para $s = 1$.

Proposição 3.21 *Seja $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2q$, com $q \equiv 1(mod\ p)$ e q um primo. Se $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = pq(p-1)$.*

Demonstração. Primeiramente notamos que, $t^2 \in \mathbb{K}$ e $Tr_{\mathbb{K}|\mathbb{Q}}(t^2) = \frac{p}{\varphi(n)} Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(t^2)$. Consideramos $G = Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = \{\tau_r : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n); \tau_r$ é um $\mathbb{Q}$-automorfismo, $\tau_r(\zeta_n) = \zeta_n^r, mdc(r,n) = 1\}$. Assim, $\theta = \tau_r\,|_{\mathbb{K}}$, para algum $\tau_r \in G$. Se $H = Gal(\mathbb{Q}(\zeta_n)|\mathbb{K})$, então $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n) = \sum_{\alpha\in H} \tau_\alpha(\zeta_n) = \sum_{\alpha\in H} \zeta_n^\alpha$. Assim, $t^2 = \sum_{\alpha,\beta\in H} \zeta_n^{\alpha+\beta}$. Agora, observamos que H é um subgrupo de G e $G \simeq \mathbb{Z}_{p^2}^* \times \mathbb{Z}_q^*$. Desta maneira escrevemos $\alpha, \beta \in H$ da seguite forma $\alpha = (\alpha_0, \alpha_1)$ e $\beta = (\beta_0, \beta_1)$, onde $\alpha_0, \beta_0 \in \mathbb{Z}_{p^2}^*$ e $\alpha_1, \beta_1 \in \mathbb{Z}_q^*$. Se $d = \frac{n}{p^2} + \frac{n}{q}$, então $\zeta_n^d = \zeta_{p^2}\zeta_q$, e ainda, $\zeta_n^{\alpha+\beta}$ é uma raíz primitiva da unidade se, e somente se, ζ_n^d é uma raíz primitiva da unidade. Logo,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\sum_{\alpha,\beta\in H} \zeta_n^{\alpha+\beta}) &= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n^{\alpha+\beta}) = \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n^{d(\alpha+\beta)}) \\ &= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}\zeta_q^{\alpha_1+\beta_1}) \\ &= \sum_{\alpha,\beta\in H} Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}) Tr_{\mathbb{Q}(\zeta_q)|\mathbb{Q}}(\zeta_q^{\alpha_1+\beta_1}), \end{aligned} \tag{3.1}$$

onde

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

e também,

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

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

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

1. Como $\mathbb{K}$ é um corpo de números totalmente real, segue que a conjugação complexa pertence ao grupo H. Desta forma, para $\alpha \in H$, fixo, segue que existe um único elemento $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação 3.1 correspondente a esses elementos é igual a:

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

.

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

$$\pi_2 : H \to \mathbb{Z}_{p^2}^*$$
$$\beta \mapsto \beta_0$$

Note que, π_2 é sobrejetora. Pois, caso contrário, teríamos que $H \subseteq \pi_2(H) \times \mathbb{Z}_q^* \subseteq G$, com $o(\frac{G}{H}) = p$, o que implica que $H = \pi_2(H) \times \mathbb{Z}_q^*$ ou $G = \pi_2(H) \times \mathbb{Z}_q^*$ e se tivéssemos $H = \pi_2(H) \times \mathbb{Z}_q^*$ o condutor de $\mathbb{K}$ não seria n. Assim, pelo Teorema do Núcleo e da Imagem, segue que $\frac{o(H)}{o(Ker(\pi_2))} = o(\mathbb{Z}_{p^2}^*)$, ou seja, $o(Ker(\pi_2)) = \frac{q-1}{p}$. Desconsiderando o elemento $\beta \in \pi_2^{-1}(\alpha_0)$ tal que $\beta_1 = -\alpha_1$, segue que existem $\frac{q-1}{p}$ elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação 3.1 correspondente a esses elementos é igual a:

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

3. Vamos considerar neste caso o isomorfismo ψ existente entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Desta forma, fixado $\alpha \in H$ existe um único $\beta \in H$ tal que $\beta \in \{\psi^{-1}(\overline{-\alpha_0}, -\alpha_1)\}$. Como já sabemos que $\beta = (-\alpha_0, -\alpha_1) \in H$ e $\psi(-\alpha_0, -\alpha_1) = (\overline{-\alpha_0}, -\alpha_1)$, segue que não existe elementos $\beta \in H$ diferente do conjugado complexo de α em $\{\psi^{-1}(\overline{-\alpha_0}, -\alpha_1)\}$. Assim, a parcela da Equação 3.1 correspondente a esses elementos é nula.

4. De modo análogo ao caso 2, consideramos a projeção

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

a qual é sobrejetora, uma vez que é compostas de sobrejetoras.

Fixado $\alpha \in H$, o número de elementos $\beta \in H$ tal que $\beta \in \{\pi_4^{-1}(\overline{-\alpha_0})\}$ é dado pela cardinalidade do $Ker(\pi_4)$, a qual é $q-1$. Porém, é nessário excluírmos β tal que $\beta \in \{\pi_2^1(-\alpha_0, \alpha_1)\}$. Dessa forma, segue que existem $\frac{(p-1)(q-1)}{p}$ elementos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 (mod\ p)$, $\beta_0 \not\equiv -\alpha_0 (mod\ p^2)$ e $\beta_1 \not\equiv -\alpha_1 (mod\ q)$. Assim, a parcela da Equação 3.1 correspondente a esses elementos é igual a:

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

5. e 6. Neste caso as parcelas da Equação 3.1 correspondentes são nulos, uma vez que $Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0+\beta_0}) = 0$.

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

Proposição 3.22 *Seja $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2q$, com $q \equiv 1(mod\ p)$ e q um primo. Se $t = Tr_{\mathbb{Q}(\zeta_n)|\mathbb{K}}(\zeta_n)$ e $\langle\theta\rangle = Gal(\mathbb{K}|\mathbb{Q})$, então $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t)) = -pq$.*

Demonstração. Consideramos $\theta = \tau_r$, com τ_r como na demonstração da Proposição 3.21. Como $r \in \mathbb{Z}_n^*$, segue que podemos considerar $r = (r_0, r_1) \in \mathbb{Z}_{p^2}^* \times \mathbb{Z}_q$. Vamos calcular $Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(t\theta^k(t)) = \frac{p}{\varphi(n)} Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^k(t))$. De modo análogo, segue que

$$Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q})}(t\theta^k(t)) = \sum_{\alpha,\beta \in H} Tr_{\mathbb{Q}(\zeta_{p^2})|\mathbb{Q}}(\zeta_{p^2}^{\alpha_0 + r_0^k\beta_0}) Tr_{\mathbb{Q}(\zeta_q)|\mathbb{Q}}(\zeta_q^{\alpha_1 + r_1^k\beta_1}) \tag{3.2}$$

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

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

Assim, analisando cada caso separadamente.

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

2. Consideramos a projeção π_2 dada na demonstração da Proposição 3.21. Fixado $-\alpha_0 r_0^{-k}$, segue que existem $\frac{q-1}{p}$ elementos $\beta \in H$ tal que $\pi_2(\beta) = -\alpha_0 r_0^{-k}$. Assim, a parcela da Equação 3.2 correspondente a esses elementos é igual a:

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

.

3. Utilizando o isomorfismo ψ entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$, segue que que fixado $(\overline{\alpha_0 r_0^{-k}}, -\alpha_1 r_1^{-k}) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, existe um único $\beta \in H$ tal que $\psi(\beta) = (\overline{\alpha_0 r_0^{-k}}, -\alpha_1 r_1^{-k})$, o qual é diferente de $-\alpha r^{-k}$. Assim, a parcela da Equação 3.2 correspondente a esses elementos é igual a:

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

.

4. Consideramos a projeção

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

a qual é sobejetora. Logo, existem $q-1$ elementos $\beta \in H$ tal que $\pi_4(\beta) = \overline{-\alpha_0 r_0^{-k}}$. Porém, devemos excluir o elementos β tal que $\pi_2(\beta) = -\alpha r_0 r_0^{-k}$. Assim, existem

$\frac{(p-1)(q-1)}{p}$ elemetos $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 r_0^{-k}(mod\ p)$, $\beta_0 \not\equiv -\alpha_0 r_0^{-k}(mod\ p^2)$ e $\beta \not\equiv -\alpha_1 r_1^{-k}(mod\ q)$. É necessário também excluir o elemento contado o item 3. Assim, a parcela da Equação 3.2 correspondente a esses elementos é igual a:

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

5. 6. Nestes casos as parcelas da Equação 3.2 correspondentes a esses casos são nulas.

Finalmente, $Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(t\theta_k(t)) = P_2 + P_3 + P_4 = o(H)(-(p-1)(q-1) - p(q-1) + (p-1)(q-1) - p) = o(H)(-pq)$. Portanto, $Tr_{\mathbb{K}|\mathbb{Q}}(t\theta_k(t)) = -pq$. ■

Proposição 3.23 *Seja $\mathbb{K}$ um corpo de números abeliano de grau p e condutor $n = p^2q$, com $q \equiv 1(mod\ p)$ e q um primo. Se $x \in \mathcal{O}_\mathbb{K}$ é não nulo, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = p\left(a_0^2 - 2q \sum_{1\leq i<j\leq p-1} a_i a_j + q(p-1)\sum_{i=1}^{p-1} a_j^2\right)$.*

Demonstração. Como $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) = a_0^2 p + 2\sum_{1\leq i<j\leq p-1} a_i a_j Tr_{\mathbb{K}|\mathbb{Q}}(t^2) + \sum_{i=1}^{p-1} a_j^2 Tr_{\mathbb{K}|\mathbb{Q}}(t\theta^{j-i}(t))$, segue das Proposições 3.21 e 3.22, que

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

■

3.4.2 Mínimo da forma traço integral, para $cond(\mathbb{K}) = p^2q$, com q primo e $q \equiv 1(mod\ p)$

Nesta subseção iremos definir uma família de $\mathbb{Z}$-submódulo B_m de $\mathcal{O}_\mathbb{K}$, onde é possível encontar $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);\ x \in \mathrm{M}, x \neq 0\}$. Com este minímo será possível a construção de alguns reticulados algébricos.

Vimos anteriormente que para $x \in \mathcal{O}_\mathbb{K}$ não nulo,

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

Manipulando um pouco este resultado, tem-se que

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

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

Definição 3.6 *Sejam $Gal(\mathbb{K}|\mathbb{Q}) = \langle\theta\rangle$ e $t = Tr_{\mathbb{L}|\mathbb{K}}(\zeta_n)$. Definimos o seguinte $\mathbb{Z}$-submódulo de $\mathcal{O}_\mathbb{K}$*

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

onde m é um inteiro positivo.

Claramente, se $m = 1$, então $\mathrm{B}_1 = \mathcal{O}_\mathbb{K}$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2) \geq pN_{\mathbb{K}|\mathbb{Q}}(x^2)^{\frac{1}{p}} \geq p$, para todo $x \in \mathcal{O}_\mathbb{K}$ não nulo. Logo, $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);\ x \in \mathcal{O}_\mathbb{K}, x \neq 0\} = p$ e é atingido em $(1, 0, \ldots, 0) \in \mathcal{O}_\mathbb{K}$.

Um dos objetivos futuros é fazer uma analise do $\min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2); 0 \neq x \in \mathrm{B}_m\}$. Esse processo envolve o processo feito na Seção 3.2.2.

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

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

Considere $x = a_0 + \sum_{i=1}^{p-1} a_i\theta^i(t) \in \mathcal{O}_\mathbb{K}$ não nulo. Como $t \in \mathcal{O}_\mathbb{K}$, segue que $t \equiv c(mod\ \mathfrak{P}_i)$, uma vez que $\frac{\mathcal{O}_\mathbb{K}}{\mathfrak{P}_i} \simeq \frac{\mathbb{Z}}{p_i\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{p_i - 1}\}$. Assim, $\theta^i(t) \equiv \theta^i(c) \equiv c(mod\ \mathfrak{P}_i)$, para $i = 1, \ldots, p-1$. Desse modo, para qualquer $x \in \mathcal{O}_\mathbb{K}$, segue que $x \equiv a_0 + c\sum_{i=1}^{p-1} a_i(mod\ \mathfrak{P}_i)$. Note

que $t+\theta(t)+\theta^2(t),\ldots,\theta^{p-1}(t)=0$, um vez que $Tr_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(\zeta_n)=0$. Logo, $pc\equiv 0(mod\ \mathfrak{P}_i)$, o que implica que, $pc\equiv 0(mod\ p_i)$, e assim, $c\equiv 0(mod\ p_i)$. Portanto, $x\equiv a_0(mod\ \mathfrak{P}_i)$, ou seja, $x\in\mathfrak{P}_i$ se, e somente se, $a_0\equiv 0(mod\ p_i)$.

Proposição 3.24 *Sejam $\mathbb{K}$ um corpo de números de grau p e condutor $n=p^2q$ com $q\equiv 1(mod\ p)$, p e q primos ímpares, $x=a_0+\sum_{i=1}^{p-1}a_i\theta^i(t)\in\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de $q\mathbb{Z}$. Se $x\in\mathfrak{Q}$, então $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);\ x\in\mathfrak{Q}, x\neq 0\}=pq(p-1)$.*

Demonstração. Se $x=a_0+\sum_{i=1}^{p-1}a_i\theta^i(t)\in\mathfrak{Q}$, ou seja, $a_0\equiv 0(mod\ q)$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)=p\left(a_0^2-2q\sum_{1\leq i<j\leq p-1}a_ia_j+q(p-1)\sum_{i=1}^{p-1}a_i^2\right)$. Suponhamos primeiramente que $a_0=0$. Como $x\in\mathfrak{Q}$ é não nulo, segue que $a_i\neq 0$, para algum $i=1,2,\ldots,p-1$. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)=p\left(-2q\sum_{1\leq i<j\leq p-1}a_ia_j+q(p-1)\sum_{i=1}^{p-1}a_i^2\right)=pq\left(-2\sum_{1\leq i<j\leq p-1}a_ia_j+(p-1)\sum_{i=1}^{p-1}a_i^2\right)$. Logo, pela Proposição 3.14, segue que $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);0\neq x\in\mathfrak{Q}\}=pq(p-1)$. Agora, suponhamos que $a_0=qk$, com $k\in\mathbb{Z}^*$ e $a_i=0$ para todo $i=1,\ldots,p-1$. Logo, $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)=pq^2k^2\geq pq^2>pq(p-1)$. E se, $a_i\neq 0$ para algum $i=1,\ldots,p-1$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)=p\left(a_0^2-2q\sum_{1\leq i<j\leq p-1}a_ia_j+q(p-1)\sum_{i=1}^{p-1}a_i^2\right)\geq pq^2k^2+pq(p-1)>pq(p-1)$. Assim, se $a_0=qk$, com $k\in\mathbb{Z}^*$, então $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)>pq(p-1)$. Desta forma, $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2);x\in\mathfrak{Q},\ x\neq 0\}=pq(p-1)$ e este mínimo é atingido para $a_0=0$ e $a_i=\pm e_i$, para $i=1,\ldots,p-1$. ■

3.5 Considerações finais

Neste capítulo, descrevemos diversos fatos sobre uma extensão abeliana $\mathbb{K}$ de grau p, com p um primo ímpar. Explicitamos o elemento primitivo, uma base integral para o anel de inteiros, o valor do $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x\in\mathcal{O}_{\mathbb{K}}$ não nulo. Caracterizamos os elementos de $\mathcal{O}_{\mathbb{K}}$ que pertencem aos ideais primos acima do ideal $p_i\mathcal{O}_{\mathbb{K}}$. Destacamos os resultados apresentados no 3º Caso, onde $cond(\mathbb{K})=p^2q$, com q primo e $q\equiv 1(mod\ p)$. Estes

resultados algébricos são inéditos e serão de fundamental importância no Capítulo 4, onde construíremos reticulados algébricos.

Capítulo 4

Reticulados

Neste capítulo vamos definir um reticulado contido em $\mathbb{R}^n$ n-dimensional, reticulado algébrico e reticulado ideal. Como vimos no Capítulo 1, existe uma relação entre certos parâmetros dos reticulados e o cálculo da probabilidade de erro de um canal de comunicação. Usando os resultados algébricos obtidos no Capítulo 3, vamos construir reticulados algébricos e analisar sua densidade de centro, diversidade e distância produto mínima, com o objetivo de encontrar empacotamentos reticulados que minimizem a probabilidade de erro na transmissão de sinais no canal gaussiano e no canal de Rayleigh com desvanecimento.

4.1 Definição

Nos últimos anos o estudo de reticulados está em constante evolução, pois esta teoria é fortemente aplicada em teoria da informação, como vimos no Capítulo 1.

Nesta seção vamos definidir reticulado n-dimensional e volume de um reticulado.

Definição 4.1 *Seja $\Lambda \subset \mathbb{R}^n$ um subgrupo com a operação adição. Dizemos que Λ é um subgrupo discreto do $\mathbb{R}^n$ se para qualquer $K \subset \mathbb{R}^n$ subconjunto compacto, a interseção $K \cap \Lambda$ é finita.*

Exemplo 4.1 *O subgrupo $(\mathbb{Z}^n, +)$ é um subgrupo discreto do $\mathbb{R}^n$.*

Teorema 4.1 *([23], pág. 53) Se $\Lambda \subset \mathbb{R}^n$ é um subgrupo discreto, então Λ é um $\mathbb{Z}$-módulo livre, gerado por $\{w_1, w_2, \ldots, w_m\}$, com $m \leq n$ e $\{w_i\}_{1 \leq i \leq m}$ linearmente independente.*

Definição 4.2 *Um $\mathbb{Z}$-módulo livre contido em $\mathbb{R}^n$ é chamado de reticulado em $\mathbb{R}^n$. Se $\{w_i\}_{1 \leq i \leq m}$ gera Λ como um $\mathbb{Z}$-módulo, dizemos que Λ é um reticulado m-dimensional. Mais precisamente,*

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

Teorema 4.2 *([23], pág. 54) Todo subgrupo discreto Λ do $\mathbb{R}^n$, é um reticulado em $\mathbb{R}^n$.*

Definição 4.3 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com $\mathbb{Z}$-base $B = \{w_1, w_2, \ldots, w_m\}$. Chamamos*

$$\mathcal{P}_B = \{x \in \mathbb{R}^n;\ x = \sum_{i=1}^{m} a_i w_i,\ 0 \leq a_i < 1\}$$

de região fundamental de Λ com relação a base B.

Se transladarmos a região fundamental por vetores do reticulado, segue que a união destas regiões fundamentais cobrem o $\mathbb{R}^n$ e cada região fundamental contém apenas um ponto do reticulado.

Definição 4.4 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com $\mathbb{Z}$-base $B = \{w_1, w_2, \ldots, w_m\}$. O volume de Λ é definido por*

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

O volume de Λ independe da $\mathbb{Z}$-base B escolhida para Λ.

Definição 4.5 *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado gerado por $B = \{w_1, w_2, \ldots, w_m\}$. A matriz R formada pelas colunas $w_1, w_2, \ldots, w_m$ é chamada de matriz geradora do reticulado Λ. Mais precisamente, podemos expressar $\Lambda = \{xR;\ x \in \mathbb{Z}^m\}$.*

Observação 4.1 *Duas matrizes R_1 e R_2 geram o mesmo reticulados se, e somente se, $R_1 = AR_2$, onde A é uma matriz com entradas em $\mathbb{Z}$ e $det(A) = \pm 1$.*

Definição 4.6 *A matriz $G = RR^t$ é chamada matriz de Gram do reticulado Λ, onde R é a matriz geradora do reticulado Λ e t denota a transposição.*

Definição 4.7 *Definimos o determinante do reticulado Λ com sendo o determinante da matriz de Gram G, ou seja, $det(\Lambda) = det(G)$. Desta forma, $det(\Lambda) = det(R)^2$.*

Definição 4.8 *Dado um reticulado Λ o volume de Λ é definido por $vol(\Lambda) = \sqrt{det(\Lambda)} = |det(R)|$.*

Neste trabalho, vamos sempre considerar reticulados contidos em $\mathbb{R}^n$ n-dimensionais.

4.2 Reticulado algébrico via homomorfismo canônico

Os reticulados algébricos são reticulados obtidos através de um homomorfismo e através deste homomorfismo podemos usar ferramentas algébricas para determinar a densidade de empacotamento desses reticulados.

Como vimos no Capítulo 1, a densidade de empacotamento está relacionada com a probabilidade de erro de um código. Empacotamentos reticulados densos diminuem a taxa de erro dos códigos quando usamos o canal de comunicação gaussiano. Desta forma, estamos sempre em busca de reticulados com alta densidade de empacotamento. Porém a densidade de empacotamento também depende do que é chamamos de densidade de centro do reticulado. Definimos esses parâmetros dos reticulados nesta seção.

Seja $\mathbb{K}$ um corpo de números de grau n. Existem n $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$, $\sigma_i : \mathbb{K} \to \mathbb{C}$. Como $\mathbb{K}|\mathbb{Q}$ é finita, segue que existe um elemento primitivo t tal que $\mathbb{K} = \mathbb{Q}(t)$ e $\sigma_i(t) = t_i$, onde t_i são os conjugados de t. Considerando $\alpha : \mathbb{C} \to \mathbb{C}$ a conjugação complexa, segue que $\alpha(t_i) = t_i$, para todo $i = 1, \ldots, n$, se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$ e $\alpha(t_i) = t_j$, para todo $i = 1, \ldots, n$ e $i \neq j$, se $\sigma_i(\mathbb{K}) \nsubseteq \mathbb{R}$. Denotamos por r_1 o número de σ_i's tal que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$ e $r_2 = \frac{n-r_1}{2}$ o número de σ_i's tal que $\sigma_i(\mathbb{K}) \nsubseteq \mathbb{R}$. Neste caso, segue que $n = r_1 + 2r_2$.

Definição 4.9 *Chamamos*

$$\begin{aligned} \sigma_{\mathbb{K}} : \mathbb{K} &\longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\longmapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \end{aligned}$$

de homomorfismo canônico de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (ou homomorfismo de Minkowski).

Observação 4.2 *Podemos identificar* $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ *com* $\mathbb{R}^n$*, e assim,* $\sigma_{\mathbb{K}}$ *fica definido da seguinte forma*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$$
$$x \longmapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathcal{R}(\sigma_{r_1+1}(x)), \mathcal{I}(\sigma_{r_1+1}(x)), \ldots, \mathcal{R}(\sigma_{r_1+r_2}(x)), \mathcal{I}(\sigma_{r_1+r_2}(x))),$$

onde $\mathcal{R}(y)$ *é a parte real de* $y \in \mathbb{C}$ *e* $\mathcal{I}(y)$ *é a parte imaginária de* $y \in \mathbb{C}$*.*

Teorema 4.3 *([23], pág. 56) Se* M *é um* $\mathbb{Z}$*-submódulo livre de* $\mathbb{K}$ *de posto* n *e* $\{v_1, \ldots, v_n\}$ *é uma* $\mathbb{Z}$*-base de* M*, então* $\sigma_{\mathbb{K}}(M)$ *é um reticulado em* $\mathbb{R}^n$*, cujo volume é dado por*

$$vol(\sigma_{\mathbb{K}}(M)) = 2^{-r_2}|det(\sigma_i(v_j))|_{1 \leq i < j \leq n}.$$

Corolário 4.1 *([23], pág. 57) Se* $\mathcal{O}_{\mathbb{K}}$ *é o anel de inteiros de* $\mathbb{K}$*,* A *um ideal não nulo de* $\mathcal{O}_{\mathbb{K}}$ *e* $D_{\mathbb{K}}$ *o discriminante de* $\mathbb{K}$*, então* $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ *e* $\sigma_{\mathbb{K}}(A)$ *são reticulados em* $\mathbb{R}^n$*, com respectivos volumes*

$$vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}} \text{ e } vol(\sigma_{\mathbb{K}}(A)) = 2^{-r_2}|D_{\mathbb{K}}|^{\frac{1}{2}}N(A),$$

onde $N(A) = \left|\frac{\mathcal{O}_{\mathbb{K}}}{A}\right|$ *é a norma do ideal* A*.*

Corolário 4.2 *[23] Seja* $\{x_1, \ldots, x_n\}$ *uma* $\mathbb{Z}$*-base de* $\mathcal{O}_{\mathbb{K}}$*. Se* M *é um* $\mathbb{Z}$*-submódulo livre de posto* n *de* $\mathcal{O}_{\mathbb{K}}$*, com* $\{a_1x_1, \ldots, a_nx_n\}$ *uma* $\mathbb{Z}$*-base, então*

$$vol(\sigma_{\mathbb{K}}(M)) = vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))[\mathcal{O}_{\mathbb{K}} : M],$$

onde $[\mathcal{O}_{\mathbb{K}} : M] = |a_1 \ldots a_n|$*.*

4.3 Reticulado algébrico via homomorfismo torcido

Após conhecermos o homomorfismo canônico que dá origem aos reticulados algébricos, podemos perguntar se existem outros homomorfismos que também dão origem a reticulados, os quais podem ser estudados utilizando suas propriedades algébricas. Em [3], foi definido um homomorfismo, o qual é uma pertubação do homomorfismo canônico, que também dá origem à reticulados algébricos e que se chama homomorfismo torcido.

Definição 4.10 *Seja $\alpha \in \mathbb{K}$ um elemento totalmente real e totalmente positivo, ou seja, $\sigma_i(\alpha) = \alpha_i \in \mathbb{R}^+$, para $i = 1, \ldots, n$. O homomorfismo*

$$\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$$
$$x \longmapsto (\sqrt{\alpha_1})\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{\alpha_{r_1+1}}\mathcal{R}(\sigma_{r_1+1}(x)), \ldots, \mathcal{I}(\sqrt{\alpha_{r_1+r_2}}\sigma_{r_1+r_2}(x)))$$

é chamado de homomorfismo torcido (pertubação do homomorfismo canônico).

Teorema 4.4 *[19] Se M é um $\mathbb{Z}$-submódulo livre de posto n de $\mathcal{O}_\mathbb{K}$ com $\{v_1, v_2, \ldots, v_n\}$ uma $\mathbb{Z}$-base de M, então $\sigma_\alpha(M)$ é um reticulado em $\mathbb{R}^n$ com $\{\sigma_\alpha(v_1), \sigma_\alpha(v_2), \ldots, \sigma_\alpha(v_n)\}$ como uma $\mathbb{Z}$-base.*

Neste caso, o volume dos reticulados $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ e $\sigma_\mathbb{K}(I)$ são

$$vol(\sigma_\alpha(\mathcal{O}_\mathbb{K})) = 2^{-r_2}|D_\mathbb{K}|^{\frac{1}{2}}|N(\alpha)|^{\frac{1}{2}} \text{ e } vol(\sigma_\alpha(I)) = 2^{-r_2}|D_\mathbb{K}|^{\frac{1}{2}}|N(\alpha)|^{\frac{1}{2}}N(I),$$

onde I é um ideal não nulo de $\mathcal{O}_\mathbb{K}$ e $N(\alpha) = \left|\frac{\mathcal{O}_\mathbb{K}}{\alpha\mathcal{O}_\mathbb{K}}\right|$.

4.4 Empacotamento esférico

Um empacotamento esférico no $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de tal forma que a interseção de quaisquer duas esferas tenha no máximo um ponto e que a união dessas esferas ocupe o maior espaço possível.

Se os centros das esferas de um empacotamento esférico é formado por pontos de um reticulado no $\mathbb{R}^n$, dizemos que este empacotamento é um empacotamento reticulado.

Estudar a existência de empacotamentos reticulados densos tem sido um dos grandes problemas dos últimos anos. Para dimensões de 1 à 8, 12 e 24 já temos empacotamentos reticulados densos ótimos.

Para sabermos se um reticulado é denso, vamos dar algumas definições. Por fim, definimos densidade de empacotamento e densidade de centro, que é nosso parâmetro de interesse nesta seção.

Definição 4.11 *A norma mínima η de um reticulado Λ é definida por*

$$\eta = min\{\|x\|^2;\ 0 \neq x \in \Lambda\}.$$

Definição 4.12 *O raio de empacotamento de um reticulado é igual a metade da distância mínima entre dois pontos distintos do reticulado e denotamos o raio de empacotamento por* ρ.

A densidade de empacotamento depende do que chamamos de densidade de centro do reticulado, como podemos observar através da seguinte definição.

Definição 4.13 *Seja* Λ *um reticulado no* $\mathbb{R}^n$*, com raio de empacotamento* ρ*. A densidade de empacotamento de* Λ *é definida por*

$$\Delta(\Lambda) = \frac{volume\ da\ esfera\ de\ raio\ \rho}{volume\ do\ reticulado} = \frac{vol(B(\rho))}{vol(\Lambda)} = \frac{vol(B(1))\rho^n}{vol(\Lambda)},$$

$$onde\ vol(B(1)) = \begin{cases} \frac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!},\ se\ n\ é\ par, \\ \frac{2^n\pi^{(\frac{n-1}{2})}(\frac{n-1}{2})!}{n!},\ se\ n\ é\ ímpar. \end{cases}$$

Como $vol(B(1))$ é conhecido, vamos focar nosso estudo no parâmetro que chamamos de densidade de centro do reticulado, o qual é definido como

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

Exemplo 4.2 *No reticulado* $\mathbb{Z}^n$*, tem-se que a matriz geradora é a matriz identidade* I_n*, sua norma mínima é* $\eta = 1$*, seu raio de empacotamento é* $\rho = \frac{1}{2}$*, sua densidade de centro* $\delta(\mathbb{Z}^n) = 2^{-n}$ *e por fim sua densidade de empacotamento é*

$$\Delta(\mathbb{Z}^n) = \begin{cases} \frac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!2^n},\ se\ n\ é\ par \\ \frac{2^n\pi^{(\frac{n-1}{2})}(\frac{n-1}{2})!}{n!2^n},\ se\ n\ é\ ímpar \end{cases}.$$

Considerando Λ um reticulado algébrico temos os seguintes fatos.

3) Se $\Lambda = \sigma_{\mathbb{K}}(M)$, com M um $\mathbb{Z}$-submódulo de $\mathcal{O}_{\mathbb{K}}$, então

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

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

2) Se $\Lambda = \sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, então

$$\delta(\Lambda) = \frac{2^{r_2}\rho^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}},$$

onde $\rho = \frac{1}{2}min\{\|\sigma_{\mathbb{K}}(x)\|;\ 0 \neq x \in \mathcal{O}_{\mathbb{K}}\}$.

3) Se $\Lambda = \sigma_{\mathbb{K}}(I)$, com I um ideal de $\mathcal{O}_{\mathbb{K}}$, então

$$\delta(\Lambda) = \frac{2^{r_2}\rho^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(I)},$$

onde $\rho = \frac{1}{2}min\{\|\sigma_{\mathbb{K}}(x)\|;\ 0 \neq x \in I\}$.

Proposição 4.1 *[6]Se $\mathbb{K}$ é um corpo de números, então*

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

onde $x \in \mathcal{O}_{\mathbb{K}}$ e $\overline{x}$ é o conjugado complexo de x.

Observação 4.3 *Notamos que se $\mathbb{K}$ é um corpo de números totalmente real, então $\|\sigma_{\mathbb{K}}(x)\|^2 = Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, para $x \in \mathcal{O}_{\mathbb{K}}$ não nulo. Desta forma, podemos reescrever o raio de empacotamento dos reticulados algébricos acima, como $\rho = \frac{1}{2}min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)}; x \in \mathcal{O}_{\mathbb{K}}$ ou $x \in I\}$.*

4.5 Construções de reticulados algébricos

Nesta seção, apresentamos algumas construções de reticulados algébricos e calculamos a densidade de centro desses reticulados. Trabalhamos sobre corpos de números totalmente reais, com o objetivo de maximizar também a diversidade de tais reticulados.

Vamos começar analizando a densidade de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, considerando $\mathbb{K}$ uma extensão abeliana de grau p, com p primo ímpar. Como $[\mathbb{K} : \mathbb{Q}]$ é ímpar, segue que $\mathbb{K}$ é um corpo de números totalmente real. Logo, para calcularmos a densidade de centro dos reticulados $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é necessário conhecermos $min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)}, x \in \mathcal{O}_{\mathbb{K}}$ e $x \neq 0\}$ e $|D_{\mathbb{K}}|$. Lembramos que $min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)}, x \in \mathcal{O}_{\mathbb{K}}$ e $x \neq 0\} = p$ e $|D_{\mathbb{K}}| = n^{p-1}$, onde $n = cond(\mathbb{K})$. Assim, segue a seguinte proposição.

Proposição 4.2 *Se $\mathbb{K}$ um corpo de números de grau p e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$, com p um primo ímpar, então* $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{p^{\frac{p}{2}}}{2^p|D_{\mathbb{K}}|^{\frac{1}{2}}}$.

Demonstração. Como $[\mathbb{K} : \mathbb{Q}] = p$, com p primo ímpar, segue que $\mathbb{K}$ é um corpo de números totalmente real. Logo, $\rho = \frac{1}{2}min\{\|\sigma_{\mathbb{K}}(x)\|; 0 \neq x \in \mathcal{O}_{\mathbb{K}}\} = \frac{1}{2}min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)}; 0 \neq x \in \mathcal{O}_{\mathbb{K}}\}$. Como $min\{\sqrt{Tr_{\mathbb{K}|\mathbb{Q}}(x^2)}; 0 \neq x \in \mathcal{O}_{\mathbb{K}}\} = p$, segue que $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{\rho^p}{|D_{\mathbb{K}}|^{\frac{1}{2}}} = \dfrac{p^{\frac{p}{2}}}{2^p|D_{\mathbb{K}}|^{\frac{1}{2}}}$. ■

Observação 4.4 *Como a densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, com p fixo, depende apenas do $|D_{\mathbb{K}}|$, segue que para maximizar a densidade é necessário tomar $\mathbb{K}$ com condutor menor possível. Desta forma, os reticulados algébricos $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ que possui maior densidade são construídos através dos corpos $\mathbb{K}$ de grau p e condutor o menor possível.*

Exemplo 4.3 *Se $\mathbb{K}$ é um corpo de grau 3 e condutor 7, então*

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}) = 0,0927884361.$$

Se compararmos com a densidade de centro ótima para empacotamentos de dimensão três, $0,17678$, vemos que a densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ ainda é baixa.

Agora, vamos retornar ao 1º caso do Capítulo 2, em que $cond(\mathbb{K}) = \prod_{i=1}^{s} p_i$, com os p_i's primo tais que $p_i \equiv 1(mod\ p)$. Na Seção 3.2.2, apresentamos uma família M_m de $\mathbb{Z}$-submódulos de $\mathcal{O}_{\mathbb{K}}$ definida em [18]. As proposições abaixo apresentam o mínimo $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$ para $x \in \mathrm{M}_m$ não nulo.

Proposição 4.3 *([18], pág. 41) Sejam $x = \sum_{i=1}^{s} a_i\theta^i(t) \in \mathcal{O}_{\mathbb{K}}$ e $S = \sum_{i=1}^{s} a_i$. Se $p|S$, então $M(S) = min\{2n, S^2/p\}$, onde $M(S) = min_{y\in \mathrm{O}(x), y\neq 0} Tr_{\mathbb{K}|\mathbb{Q}}(y^2)$.*

Proposição 4.4 *([18], pág 41) Sejam m um inteiro positivo e $M^* = min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2); 0 \neq x \in \mathrm{M}_m\}$. Se $p|m$, então $M^* = min\{2n, m^2/p\}$. Se $p \nmid m$, então $M^* = min\{2n, M(m), \ldots, M(pm)\}$.*

Após uma análise de M^* em cada caso, pode-se perceber que é possível encontrar $\mathbb{Z}$-submódulos M de $\mathcal{O}_{\mathbb{K}}$, com densidade próxima da recorde.

Exemplo 4.4 *Se $p = 5$, $n = 92111$ e $m = 607$, então $\delta(\sigma_{\mathbb{K}}(\mathrm{M}_{607})) = 0,08838$. Sendo 0,08839 a densidade ótima na dimensão 5, tem-se que o reticulado algébrico $\sigma_{\mathbb{K}}(\mathrm{M}_{607})$ apresenta densidade de centro muito boa.*

Finalmente, vamos analisar a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{Q})$, onde $\mathfrak{Q}$ é o ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima do ideal primo $q\mathbb{Z}$, apresentado no 3º caso do Capítulo 3.

Lembramos que $min\{Tr_{\mathbb{K}|\mathbb{Q}}(x^2); x \in \mathfrak{Q} \text{ e } x \neq 0\} = pq(p-1)$, com $q \equiv 1(mod\ p)$. Desta forma, podemos anunciar a seguinte proposição.

Proposição 4.5 *Sejam $\mathbb{K}$ um corpo de números abeliano de grau p e $cond(\mathbb{K}) = p^2q$, com p e q primos ímpares tal que $q \equiv 1(mod\ p)$. Se $\mathfrak{Q}$ é o ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima do ideal $q\mathbb{Z}$, então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{Q})) = \frac{(\sqrt{pq(p-1)})^p}{2^p q\sqrt{(p^2q)^{p-1}}}.$$

Tabela 4.1: Comparação de densidade de centro

p	q	$\delta(\sigma_{\mathbb{K}}(\mathfrak{Q})$	densidade ótima
3	7	$0,07715$	$0,17678$
3	13	$0,050208$	$0,17678$
5	11	$0,026965$	$0,08839$
7	29	0,00592073	0,06250
7	71	0,00378395	0,06250

Na tabela 4.1, consta a comparação da densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{Q})$ com a densidade ótima [6]. Podemos observar que a densidade de $\sigma_{\mathbb{K}}(\mathfrak{Q})$ é inferior a ótima.

4.6 Reticulado ideal

Nesta seção, apresentamos os conceitos de reticulado ideal sobre um corpo de números totalmente real, diversidade e distância produto mínima. Apresentamos construções cíclicas de reticulados ideais que são isomorfos à um reticulado $\mathbb{Z}^n$-rotacionado. Como

mencionamos no Capítulo 1, os reticulados $\mathbb{Z}^n$-rotacionados são eficientes na modulação e codificação do sinal.

Reticulados ideais são reticulados algébricos dotados de uma forma traço. A seguir definimos um reticulado ideal sobre um corpo de números totalmente real. Isto se faz necessário, pois estamos interessados em maximizar a diversidade de tal reticulado. Além disso, podemos definir um reticulado ideal em qualquer corpo de números [19].

Definição 4.14 *Seja $\mathbb{K}$ um corpo de números totalmente real de grau n. Um reticulado ideal é um reticulado $(\mathcal{A}, q_\alpha)$, onde $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ é um ideal e*

$$q_\alpha : \mathcal{A} \times \mathcal{A} \to \mathbb{Z}, \quad q_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha xy), \quad \forall x, y \in \mathcal{A},$$

com $\alpha \in \mathbb{K}$ é totalmente positivo, ou seja, $\sigma_i(\alpha) > 0$ para todo $i = 1, 2, \cdots, n$.

Se $\{\omega_1, \omega_2, \cdots, \omega_n\}$ é uma base de $\mathcal{A}$ sobre $\mathbb{Z}$, então a matriz geradora R do reticulado $\Lambda = \{x = \lambda R : \lambda \in \mathbb{Z}^n\}$ é dada por

$$R = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(\omega_1) & \sqrt{\sigma_2(\alpha)}\sigma_2(\omega_1) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(\omega_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\omega_n) & \sqrt{\sigma_2(\alpha)}\sigma_2(\omega_n) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(\omega_n), \end{pmatrix}.$$

Neste caso, segue que a matriz de Gram RR^t coincide com a matriz na forma traço $(Tr(\alpha\omega_i\omega_j))_{i,j=1}^n$, onde t denota a transposição.

Definição 4.15 *A diversidade L de um reticulado Λ em $\mathbb{R}^n$ é a distância mínima de Hamming entre quaisquer dois pontos distintos do reticulado, ou ainda,*

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

onde $x = (x_1, \ldots, x_n)$.

Teorema 4.5 *[19] Se $\Lambda = (\mathcal{A}, q_\alpha)$ é um reticulado ideal definido sobre um corpo de números totalmente real, então $div(\Lambda) = r_1$, onde r_1 é o números de homomorfismo de $\mathbb{K}$ em $\mathbb{C}$ totalmente reais, ou seja, Λ tem diversidade máxima n.*

Definição 4.16 *Seja Λ um reticulado n-dimensional com diversidade máxima $L = n$ e $x = (x_1, \ldots, x_n) \in \Lambda$ um elemento não nulo. A distância produto de x à origem é definida como*

$$d_p(x) = \prod_{i=1}^{n} \mid x_i \mid,$$

e a distância produto mínima de Λ é definida como

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

Teorema 4.6 *[19] Seja $\mathcal{A}$ um ideal principal de $\mathcal{O}_{\mathbb{K}}$. A distância produto mínima do reticulado ideal de determinante $D = det(\Lambda)$ definido sobre $\mathcal{A}$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{D}{D_{\mathbb{K}}}}.$$

4.7 Construções de reticulados Ideais

Lembramos do Capítulo 1, que para a construção de código reticulado eficiente, é necessário maximizar a diversidade, maximizar a distância produto mínima, garantindo assim, facilidade na decodificação. Nesta seção, apresentamos códigos reticulados que preenchem estes critérios.

A construção de reticulados $\mathbb{Z}^n$-rotacionados deste trabalho é uma extensão da construção apresentada em [4], [5], [21], [19] e [20] usando extensões cílicas de grau primo, em [8] de grau ímpar e em [1] de grau par.

Seja p um número primo ímpar. Se $\zeta = \zeta_{p^s}$ é uma p^s-ésima raíz primitiva da unidade, então $\mathbb{Q}(\zeta)$ é uma extensão cíclica de grau $p^{s-1}(p-1)$ sobre $\mathbb{Q}$ e contém o subcorpo real maximal $\mathbb{Q}(\zeta + \zeta^{-1})$ que é cíclico de grau $p^{s-1}(p-1)/2$ sobre $\mathbb{Q}$. Se $G = Gal(\mathbb{Q}(\zeta)|\mathbb{Q})$ com gerador σ, então $\sigma(\zeta) = \zeta^r$, onde r é um gerador de $\mathbb{Z}_{p^s}^*$.

Lema 4.1 *Se $m = p^{s-1}(p-1)/2$, então $r^m \equiv -1 (mod\ p^s)$, ou seja, r é um elemento primitivo módulo p^s.*

Demonstração. Como r gera $\mathbb{Z}_{p^s}^*$, segue que $o(r) = p^{s-1}(p-1) = 2m$. Além disso, $r^{2m} \equiv 1 (mod\ p^s)$ se, e somente se, $r^{2m} - 1 = p^s a$ para algum $a \in \mathbb{Z}$ se, e somente se,

$(r^m - 1)(r^m + 1) = r^{2m} - 1 = p^s a$. Assim, $p \mid (r^m - 1)(r^m + 1)$. Se $p \mid (r^m - 1)$, então $r^m - 1 = pb_1$, para algum $b_1 \in \mathbb{Z}$. Logo, $r^m = 1 + pb_1$, e portanto, $r^{2m} = (1 + pb_1)^2 = 1 + 2pb_1 + p^2 b_1^2 = 1 + p^s a$. Desta forma, $2pb_1 + p^2 b_1^2 = p^s a$, isto é, $2b_1 + pb_1^2 = p^{s-1} a$. Consequêntemente, $p \mid 2b_1$, e como $p \neq 2$, segue que $b_1 = pb_2$ para algum $b_2 \in \mathbb{Z}$. Assim, $2pb_2 + pp^2 b_2^2 = p^{s-1} a$, o que implica que, $2b_2 + p^2 b_2^2 = p^{s-2} a$. Como $p \neq 2$, segue que $b_2 = pb_3$, e assim, $2pb_3 + p^2 p^2 b_3^2 = p^{s-2} a$, ou seja, $2b_3 + p^3 b_3^2 = p^{s-3} a$. Similarmente, segue que $2b_{s-1} + p^{s-1} b_{s-1}^2 = pa$ e $b_{s-1} = pb_s$. Logo, $b_1 = pb_2 = \cdots = p^{s-1} b_s$. Desta forma, $r^m - 1 = p^s b_s$, e assim, $r^m \equiv 1 (mod\ p^s)$. Mas, isto é uma contradição pois, $o(r) = 2m$. Portanto, $p \mid (r^m + 1)$, e similarmente, segue que $p^s \mid (r^m + 1)$, isto é, $r^m \equiv -1 (mod\ p^s)$. ■

Lema 4.2 *Existe um inteiro λ tal que $\lambda(r - 1) \equiv 1 (mod\ p^s)$.*

Demonstração. Como $p^{s-1}(p - 1)$ é o menor inteiro tal que $r^{p^{s-1}(p-1)} \equiv 1 (mod\ p^s)$, segue que p^s não divide $r - 1$. Assim, $mdc(p^s, r - 1) = 1$, e portanto, $y(r - 1) \equiv 1 (mod\ p^s)$ tem uma única solução $y = \lambda$. ■

Sejam $\alpha = \prod_{k=0}^{m-1} (1 - \zeta^{r^k})$ e λ tal que $\lambda(r - 1) \equiv 1 (mod\ p^s)$.

Lema 4.3 $\sigma(\alpha) = -\zeta^{p^s - 1} \alpha$.

Demonstração. Tem-se que

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

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

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

Mas,

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

e assim,

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

Porém, como $r^m \equiv -1(mod\ p^s)$, segue que $\zeta^{r^m} = \zeta^{-1}$. Desta forma, $\sigma(\alpha) = (1-\zeta)^{-1}(1-\zeta^{-1})\alpha$ e pelo fato de $\zeta^{p^s-1} = \zeta^{-1}$, tem-se que

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

Como ζ é uma raíz do polinômio

$$\frac{x^{p^s}-1}{x-1} = x^{p^s-1} + x^{p^s-2} + \cdots + x + 1,$$

segue que $-\zeta^{p^s-1} = \zeta^{p^s-2} + \cdots + \zeta + 1$, e portanto, $\sigma(\alpha) = -\zeta^{p^s-1}\alpha$. ■

Lema 4.4 $\sigma(\zeta^\lambda\alpha) = -\zeta^\lambda\alpha$.

Demonstração. Pelo Lema 4.3, segue que

$$\sigma(\zeta^\lambda\alpha) = \sigma(\zeta^\lambda)\sigma(\alpha) = \zeta^{r\lambda}(-\zeta^{p^s-1}\alpha).$$

Mas, como $\lambda(r-1) \equiv 1(mod\ p^s)$, segue que $\lambda r \equiv (\lambda+1)(mod\ p^s)$, e assim, $\zeta^{r\lambda} = \zeta^{\lambda+1}$. Portanto, $\sigma(\zeta^\lambda\alpha) = \zeta^{\lambda+1}(-\zeta^{p^s-1}\alpha) = -\zeta^{\lambda+p^s}\alpha = -\zeta^\lambda\alpha$. ■

Lema 4.5 $(\zeta^\lambda\alpha)^2 = (-1)^m p$.

Demonstração. Considere o p^s-ésimo polinômio ciclotômico

$$\phi_{p^s}(x) = \prod_k (x-\zeta^k) = \frac{x^{p^s}-1}{x^{p^{s-1}}-1} = x^{p^{s-1}(p-1)} + x^{p^{s-1}(p-2)} + \cdots + x^{p^{s-1}} + 1,$$

onde o produto é tomado sobre todos $k = 1, 2, \cdots, p^s$ tal que $mdc(k, p^s) = 1$. Como ζ é uma raíz de $\phi_{p^s}(x)$, segue que cada elemento de

$$Gal(\mathbb{Q}(\zeta) : \mathbb{Q}) = \langle\sigma\rangle$$

aplicado em ζ é uma raíz de $\phi_{p^s}(x)$, pois $\phi_{p^s}(\sigma^k(\zeta)) = \sigma^k(\phi_{p^s}(\zeta)) = 0$, isto é, os elementos $\sigma^k(\zeta)$, com $mdc(p^s, k) = 1$ e $1 \leq k \leq p^s$, são todas as raízes distintas de $\phi_{p^s}(x)$. Assim,

$$\phi_{p^s}(x) = \prod_{k=0}^{\varphi(p^s)-1} (x - \sigma^k(\zeta)) = \prod_{k=0}^{\varphi(p^s)-1} (x - \zeta^{r^k}).$$

Portanto,

$$p = \phi_{p^s}(1) = \prod_{k=0}^{\varphi(p^s)-1} (1 - \zeta^{r^k}).$$

Por outro lado, como $r^m \equiv -1(mod\ p^s)$, segue que $r^{m+i} = r^m r^i \equiv -r^i(mod\ p^s)$, para todo $i \in \mathbb{Z}$. Logo, $\zeta^{r^{m+i}} = \zeta^{-r^i}$, para todo $i = 0, 1, \cdots, m-1$. Consequêntemente,

$$\prod_{k=m}^{\varphi(p^s)-1} (1 - \zeta^{r^k}) = \prod_{i=0}^{m-1} (1 - \zeta^{r^{m+i}}) = \prod_{i=0}^{m-1} (1 - \zeta^{-r^i})$$

e assim,

$$p = \prod_{k=0}^{\varphi(p^s)-1} (1 - \zeta^{r^k}) = \prod_{k=0}^{m-1} (1 - \zeta^{r^k}) \prod_{k=m}^{\varphi(p^s)-1} (1 - \zeta^{r^k}) = \alpha \prod_{i=0}^{m-1} (1 - \zeta^{-r^i}).$$

Mas,

$$\alpha \prod_{i=0}^{m-1} \zeta^{-r^i} = \prod_{i=0}^{m-1} (\zeta^{-r^i} - 1) = \begin{cases} \prod_{i=0}^{m-1} (1 - \zeta^{-r^i}), & \text{if } m \text{ é par} \\ -\prod_{i=0}^{m-1} (1 - \zeta^{-r^i}), & \text{if } m \text{ é ímpar} \end{cases}$$

ou seja,

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

Deste modo, tem-se que

$$p = (-1)^m \alpha^2 \prod_{i=0}^{m-1} \zeta^{-r^i}.$$

Observe que $\dfrac{1 - r^m}{r - 1} = -r^{m-1} - \cdots - r - 1$. Assim,

$$\prod_{i=0}^{m-1} \zeta^{-r^i} = \zeta^{-r^{m-1} - \cdots - r - 1} = \zeta^{\frac{1-r^m}{r-1}}.$$

Mas, $r^m \equiv -1(mod\ p^s)$, o que implica que, $1 - r^m \equiv 2(mod\ p^s)$ e do fato que $\lambda(r-1) \equiv 1(mod\ p^s)$ (e portanto $2\lambda(r-1) \equiv 2(mod\ p^s)$), segue que $2\lambda(r-1) \equiv 2(mod\ p^s)$. Logo pela transitividade, segue que $1 - r^m \equiv 2\lambda(r-1)(mod\ p^s)$. Como $\frac{r-1}{r-1} \equiv 1(mod\ p^s)$, segue que $\frac{1-r^m}{r-1}(r-1) \equiv 2\lambda(r-1)(mod\ p^s)$. Pelo fato de que $mdc(p^s, r-1) = 1$ (pois, se $p \mid r-1$, então $r \equiv 1(mod\ p)$, e assim, $r^m \equiv 1(mod\ p)$. Mas $r^m \equiv -1(mod\ p^s)$, e assim,

$p \mid p^s$, $p^s \mid r^m + 1$. Logo, $p \mid 2$, que é uma contradição), segue que $\frac{1-r^m}{r-1} \equiv 2\lambda (mod\ p^s)$. Consequêntemente, $\zeta^{\frac{1-r^m}{r-1}} = \zeta^{2\lambda}$. Assim, $p = (-1)^m \alpha^2 \zeta^{2\lambda}$, e portanto,

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

o que prova o lema. ■

4.7.1 Construção cíclica ímpar

Seja n um inteiro ímpar tal que n divide $p^{s-1}(p-1)/2$.

Lema 4.6 *Seja $\omega_{d,t} = \zeta^{r^{nd}+r^t}$, onde d e t são inteiros tais que $d \in \{0, 1, \cdots, p^{s-1}(p-1)/n\}$ e $t \in \{0, 1, \cdots, n-1\}$. Assim, $\omega_{d,t} = 1$ se, e somente se, $t = 0$ e $d = \frac{p^{s-1}(p-1)}{2n}$.*

Demonstração. Se $\omega_{d,t} = \zeta^{r^{nd}+r^t} = 1$, então $r^{nd} + r^t \equiv 0 (mod\ p^s)$, e assim, $r^{nd} \equiv -r^t (mod\ p^s)$. Como $r^{m+t} \equiv -r^t (mod\ p^s)$, segue que $r^{nd} \equiv r^{m+t} (mod\ p^s)$. Pelo fato de que $r^{m+t} = r^{nd} r^{m+t-nd}$, segue que $r^{nd} \equiv r^{nd} r^{m+t-nd} (mod\ p^s)$. Como $mdc(r^{nd}, p^s) = 1$, segue que $r^{m+t-nd} \equiv 1 (mod\ p^s)$. Do Lema 4.1, segue que $p^{s-1}(p-1) \mid (-nd + m + t)$, ou seja, existe $k_1 \in \mathbb{Z}$ tal que $-nd + m + t = k_1 p^{s-1}(p-1)$. Assim, $t = dn - m + k_1 p^{s-1}(p-1)$. Como $n \mid dn$, $n \mid m$ e $n \mid p^{s-1}(p-1)$, segue que $n \mid t$. Como $t = 0, 1, 2, \cdots, n-1$, segue que $t = 0$, e assim, $dn = m - k_1 p^{s-1}(p-1)$. Desta forma, $d = \frac{p^{s-1}(p-1)}{2n} - k_1 \frac{p^{s-1}(p-1)}{n} = \frac{p^{s-1}(p-1)}{2n}(1 - 2k_1) = k_2 \frac{p^{s-1}(p-1)}{2n}$, onde $k_2 = 1 - 2k_1$. Como $d \geq 0$, segue que $k_2 \geq 0$. Como $d \leq \frac{p^{s-1}(p-1)}{n}$, segue que $k_2 = 0, 1, 2$ pois, se $k_3 \geq 3$, então $d > \frac{p^{s-1}(p-1)}{2n}$, o que é uma contradição. Como k_2 é ímpar, segue que $k_2 = 1$. Portanto, $d = \frac{p^{s-1}(p-1)}{2n}$. Reciprocamente, como $r^m \equiv -1 (mod\ p^s)$, segue que $r^{\frac{p^{s-1}(p-1)}{2}} + 1 \equiv 0 (mod\ p^s)$. Como $t = 0$ e $d = \frac{p^{s-1}(p-1)}{2}$, segue que

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

o que prova o resultado. ■

Seja $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta)$ e $[\mathbb{K} : \mathbb{Q}] = n$. Se $z = \zeta^{\lambda}\alpha(1-\zeta) \in \mathcal{O}_{\mathbb{Q}(\zeta)}$, então $x = Tr_{\mathbb{Q}(\zeta)|\mathbb{K}}(z) = \sum_{j=1}^{p^{s-1}(p-1)/n} \sigma^{jn}(z) \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. Como $[G_n G_n^T](i,j) = Tr_{\mathbb{K}|\mathbb{Q}}(\sigma^i(x)\sigma^j(x)) = Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^{j-i}(x))$, para $i, j = 0, 1, \cdots, n-1$, segue que estamos interessados em $Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x))$, para $t = 0, 1, \cdots, n-1$.

Teorema 4.7 *Se* $z = \zeta^{\lambda}\alpha(1-\zeta)$ *e* $x = Tr_{\mathbb{Q}(\zeta)|\mathbb{K}}(z)$, *então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) = \begin{cases} p^s(p-1)+p, & se\ t=0 \\ 0, & se\ t \neq 0 \end{cases},$$

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

Demonstração. Como $Gal(\mathbb{K}|\mathbb{Q}) = \{Id_{\mathbb{K}}, \sigma|_{\mathbb{K}}, \cdots, \sigma^{n-1}|_{\mathbb{K}}\}$, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) = \sum_{a=0}^{n-1} \sigma^a(x\ \sigma^t(x)), \quad t = 0, 1, \cdots, n-1\ .$$

Como

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

segue que

$$\begin{aligned}
Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) &= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p^{s-1}(p-1)}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\
&= \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p^{s-1}(p-1)}{n}} \sigma^{a+cn}(\zeta^{\lambda}\alpha(1-\zeta))\sigma^{a+t+jn}(\zeta^{\lambda}\alpha(1-\zeta)) \\
&\overset{(1)}{=} \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^{a+cn}\zeta^{\lambda}\alpha(1-\zeta^{r^{a+cn}})(-1)^{a+t+jn}\zeta^{\lambda}\alpha(1-\zeta^{r^{a+t+jn}}) \\
&\overset{(2)}{=} \sum_{a=0}^{n-1} \sum_{c,j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^{t+c+j}(\zeta^{\lambda}\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\
&= (-1)^t \sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j(\zeta^{\lambda}\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}) \\
&\overset{(3)}{=} (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}(-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}}).
\end{aligned}$$

Pelos Lemas 4.4 e 4.5, segue a igualdade (1) e (3), respectivamente. Agora, a igualdade (2) segue do fato que $(-1)^{a+cn}(-1)^{a+t+jn} = (-1)^{2a}(-1)^t(-1)^{cn}(-1)^{jn} = (-1)^{t+c+j}$, pois n é ímpar, e assim, $(-1)^{cn} = (-1)^c$ e $(-1)^{jn} = (-1)^j$. Como

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

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

segue que $Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x))$ é igual a

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

$$\left. + \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}} \right).$$ Como $(\frac{p^{s-1}(p-1)}{n})n = p^{s-1}(p-1)$ é par e n é ímpar, segue que $\frac{p^{s-1}(p-1)}{n}$ é par. Logo,

$$\sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j(1-\zeta^{r^{a+cn}}) = 0,$$

uma vez que o termo $(1-\zeta^{r^{a+cn}})$ não depende de j. Assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x))$ é igual a

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

$$\left. \sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}} \right).$$ Como $\frac{p^{s-1}(p-1)}{n}$ é par e o termo

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

não depende de c, segue que

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) &= (-1)^{t+m}p \sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}} \\ &\overset{(*)}{=} (-1)^{t+m}p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{\frac{p^{s-1}(p-1)}{n}} \zeta^{r^{a+dn+kn}+r^{a+t+kn}} \\ &= (-1)^{t+m}p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{\frac{p^{s-1}(p-1)}{n}} \zeta^{(r^{dn}+r^t)r^{a+kn}}, \end{aligned}$$

.

A igualdade $(*)$ segue levando em conta o fato que todos os índices percorrendo todos os termos do sumatório, verificando que eles cobrem o mesmo conjunto de expoentes de $\zeta \ (mod\, p^s)$. Além disso, note que r^{a+kn} para $a = 0, 1, \ldots, n-1$ e $k = 1, 2, \ldots, p^{s-1}(p-1)/n$ toma valores $j = 1, 2, \ldots, p^s$ tal que $mdc(j, p^s) = 1$, ou seja,

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

Logo, denotando $\omega_{d,t} = \zeta^{r^{dn}+r^t}$, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) = (-1)^{t+m} p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{mdc(j,p^s)=1} (\omega_{d,t})^j,$$

onde

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

Pelo Lema 4.6, segue que

$$\omega_{d,t} = 1 \iff t = 0 \quad \text{e} \quad d = \frac{p^{s-1}(p-1)}{2n}.$$

Se $t \neq 0$, então $\omega_{d,t} \neq 1$, e assim,

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) &= (-1)^{t+m} p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{mdc(j,p^s)=1} (\omega_{d,t})^j \\ &= (-1)^{t+m} p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d (-1) = 0, \end{aligned}$$

pois $p^{s-1}(p-1)/n$ é par. Agora, suponha $t = 0$. Se $d = p^{s-1}(p-1)/2n$, então $\omega_{d,t} = 1$, e se $d \neq p^{s-1}(p-1)/2n$, então $\omega_{d,t} \neq 1$. Assim,

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) &= (-1)^{t+m} p \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{mdc(j,p^s)=1} (\omega_{d,t})^j \\ &= (-1)^m p (-1)^{\frac{p^{s-1}(p-1)}{2n}} p^{s-1}(p-1) + (-1)^m p \sum_{\substack{d=1 \\ d \neq \frac{p^{s-1}(p-1)}{2n}}}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d (-1). \end{aligned}$$

Como $m = \frac{p^{s-1}(p-1)}{2}$ e $\frac{p^{s-1}(p-1)}{2n}$ têm a mesma paridade, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\ \sigma^t(x)) = p^s(p-1) + p,$$

o que conclui a demonstração. ■

Algoritmo de construção de reticulados $\mathbb{Z}^n$-rotacionados

(1) Escolha um inteiro ímpar n.

(2) Encontre um primo ímpar p tal que n divide $\frac{p^{s-1}(p-1)}{2}$, com s o menor possível.

(3) Calcule os valores de r e λ.

(4) Calcule α e z na base de $\mathbb{Q}(\zeta_{p^s})$.

(5) Calcule x e seus conjugados na extensão $\mathbb{K}|\mathbb{Q}$.

(6) Calcule a matriz geradora M do reticulado $\mathbb{Z}^n$-rotacionado obtido.

Na Tabela 4.2, apresentamos exemplos para os parâmentros n, p, r e λ.

Tabela 4.2: Exemplos dos parâmetros

n	p	s	r	λ
3	3	2	2	10
5	5	2	18	3
11	11	2	28	9
21	7	2	3	25

Na Tabela 4.3, analisamos a distância produto mínima dos reticulados $\mathbb{Z}^n$-rotacionados que obtivemos com a construção cíclica apresentada neste trabalho. Notamos que nos corpos de números $\mathbb{K}$ de grau n ímpar, a construção apresentada aqui, considera que apenas o ideal $p\mathbb{Z}$ ramifica em $\mathcal{O}_{\mathbb{K}}$. Caso, contrário, $\mathbb{K} \nsubseteq \mathbb{Q}(\zeta_{p^s})$.

Tabela 4.3: Distância produto mínima

n	p^s	$D_{\mathbb{K}}$	$d_{p,min}$
3	9	9^2	$\frac{1}{9}$
9	27	3^{22}	$\frac{1}{3^{11}}$
5	25	25^4	$\frac{1}{25^2}$
25	125	5^{68}	$\frac{1}{5^{34}}$

4.7.2 Construção cíclicas par

Seja n um inteiro par tal que n divide $p^{s-1}(p-1)/2$.

Lema 4.7 *Se* $q = \frac{p^{s-1}(p-1)}{n}$, *então* $\sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j \zeta^{r^{a+cn}+r^{a+t+jn}}$

$= \sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{\frac{p^{s-1}(p-1)}{n}} \zeta^{r^{a+kn}(r^{nd}+r^t)}$.

Demonstração. Como q é par, segue que podemos tratar c, j, d, k como elementos de $\mathbb{Z}_q$. Assim,

$$\sum_{c=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^j \zeta^{r^{a+cn}+r^{a+t+jn}} = \sum_{c\in\mathbb{Z}_q} (-1)^c \sum_{a=0}^{n-1} \sum_{k\in\mathbb{Z}_q} (-1)^k \zeta^{r^{a+cn}+r^{a+t+kn}}$$
$$= \sum_{c\in\mathbb{Z}_q} \sum_{k\in\mathbb{Z}_q} (-1)^{c+k} \sum_{a=0}^{n-1} \zeta^{r^{a+cn}+r^{a+t+kn}}.$$

Fazendo uma mudança de variável $c = d + k(mod\ q)$ o que implica, como q é par, que $c = d + k(mod\ 2)$, e assim, $d = c - k = c + k(mod\ 2)$. Como (c, k) varia sobre todos os elementos de $\mathbb{Z}_q \times \mathbb{Z}_q$, segue que o par (d, k). Logo,

$$\sum_{c\in\mathbb{Z}_q} \sum_{k\in\mathbb{Z}_q} (-1)^{c+k} \sum_{a=0}^{n-1} \zeta^{r^{a+cn}+r^{a+t+kn}} = \sum_{d\in\mathbb{Z}_q} (-1)^d \sum_{a=0}^{n-1} \sum_{k\in\mathbb{Z}_q} \zeta^{r^{a+(d+k)n}+r^{a+t+kn}} =$$
$$\sum_{d\in\mathbb{Z}_q} (-1)^d \sum_{a=0}^{p-1} \sum_{k\in\mathbb{Z}_q} \zeta^{(r^{nd}+r^t)(r^{a+nk})} = \sum_{d=1}^{\frac{p^{s-1}(p-1)}{n}} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{\frac{p^{s-1}(p-1)}{n}} \zeta^{(r^{nd}+r^t)r^{a+nk}},$$

o que completa a demonstração. ■

Proposição 4.6 *$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{\frac{p^{s-1}(p-1)}{2n}} p^2\delta_{0,t}$, para $t = 0, 1, \cdots, n-1$.*

Demonstração. Tem-se que $Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = \sum_{a=0}^{n-1} \sigma^a(x\sigma^t(x)) =$

$= \sum_{a=0}^{n-1} \sum_{c,j=1}^{p^{s-1}(p-1)/n} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z)$. Pelo Lema 4.7, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = \sum_{a=0}^{n-1} \sum_{c,j=1}^{p^{s-1}(p-1)/n} (-1)^{a+cn}\zeta^\lambda\alpha(1-\zeta^{r^{a+cn}})(-1)^{a+t+jn}\zeta^\lambda\alpha(1-\zeta^{r^{a+t+jn}}).$$

Como n é par, segue que $(-1)^{cn} = (-1)^{jn} = 1$. Além disso, $(-1)^a(-1)^a = 1$, e $(-1)^t$ é comum nas somas anteriores. Pelo Lema 4.5, segue que podemos substituir $(\zeta^\lambda\alpha)^2$ por $(-1)^m p$. Desta forma, depois de rearranjar a soma, segue que

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) \; &= (-1)^t(-1)^m p \sum_{c=1}^{p^{s-1}(p-1)/n} (-1)^c \Big(\sum_{a=0}^{n-1} \sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j(1-\zeta^{r^{a+cn}}) \\ &\quad - \sum_{a=0}^{n-1} \sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j(\zeta^{r^{a+t+jn}} - \zeta^{r^{a+cn}+r^{a+t+jn}})\Big). \end{aligned}$$

Observe o termo $\sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j(1-\zeta^{r^{a+cn}})$, o qual podemos reescrever como $(1-\zeta^{r^{a+cn}}) \sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j$. Como $p^{s-1}(p-1)/n$ é par, segue que existem tantos termos negativos quanto termos positivos na expressão $\sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j$, e assim, a soma é nula. Similarmente, o termo

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

é nulo, uma vez que os termos em $\sum_{a=0}^{n-1}(-1) \sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j\zeta^{r^{a+t+jn}}$ são independentes de c, enquanto o termo $\sum_{c=1}^{p^{s-1}(p-1)/n} (-1)^c = 0$ como $p^{s-1}(p-1)/n$ é par e existem tantos termos positivos quantos termos negativos. Assim encontramos

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m} p \sum_{c=1}^{p^{s-1}(p-1)/n} (-1)^c \sum_{a=0}^{n-1} \sum_{j=1}^{p^{s-1}(p-1)/n} (-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}.$$

Pelo Lema 4.7, segue que $T_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m}p \sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{p^{s-1}(p-1)/n} \zeta^{r^{a+kn}(r^{nd}+r^t)}$ e podemos provar deixando todos os índices percorrer os termos do somatório para verificar que eles cobrem o mesmo conjunto de expoentes de $\zeta(mod\ p^s)$. Notamos que r^{a+kn} para $a = 0, 1, \cdots, n-1$, $k = 1, 2, \cdots, p^{s-1}(p-1)/n$ tomando valores $j = 1, 2, \cdots, p^s$ tal que $mdc(j, p^s) = 1$. Denotando $\omega_{d,t} = \zeta^{r^{nd}+r^t}$, como em [19] podemos escrever

$$\sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d \sum_{a=0}^{n-1} \sum_{k=1}^{p^{s-1}(p-1)/n} \zeta^{r^{a+kn}(r^{nd}+r^t)} = \sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d \sum_{mdc(j,p^s)=1} \omega_{d,t}^j, \qquad (4.1)$$

onde $\sum_{mdc(j,p^s)=1} \omega_{d,t}^j = \begin{cases} p^{s-1}(p-1) & \text{se } \omega_{d,t} = 1 \\ -1 & \text{caso contrário.} \end{cases}$ Para avaliar a Equação (4.1), dividimos em dois casos. O caso $\omega_{d,t} = 1$ aparece quando

$$r^{nd} + r^t \equiv 0(mod\ p^s) \ \Leftrightarrow\ r^{nd} \equiv r^{m+t}(mod\ p^s) \ \Leftrightarrow\ t = nk - m + k_1 p^{s-1}(p-1),$$

onde $k_1 \in \mathbb{Z}$. Como n divide o termo à direita, segue que t precisa ser um múltiplo de n, o qual pertence a $\{0, 1, \cdots, n-1\}$ e concluímos que devemos ter $t = 0$. Agora, se $\omega_{d,t} = 1$, então $r^{nd} \equiv -1(mod\ p^s)$, e escrevendo -1 como r^m, tem-se que $nd - m = lp^{s-1}(p-1)$ para algum l. Logo, $d = p^{s-1}(p-1)(2l+1)/2n$, o qual podemos escever como $(2l+1)$ vezes $p^{s-1}(p-1)/2n$ (note que n divide $p^{s-1}(p-1)/2$). Como d varia em $\{1, 2, \cdots, p^{s-1}(p-1)/n\}$, encontramos que l será zero, ou seja, $d = p^{s-1}(p-1)/2n$. Assim, $\omega_{d,t} = 1$, precisamente quando $t = 0$ e $d = p^{s-1}(p-1)/2n$. Logo, o segundo caso aparece quando $t \neq 0$ e obtemos

$$Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m}p \sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d \sum_{mdc(j,p^s)=1} \omega_{d,t}^j = (-1)^{t+m}p \sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d(-1).$$

Como $p^{s-1}(p-1)/n$ é par, segue que $\sum_{d=1}^{p^{s-1}(p-1)/n}(-1)^d = 0$, e assim, $Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) = 0$ para $t \neq 0$. Agora, quando $t = 0$, como m e $p^{s-1}(p-1)/n$ são pares, segue que

$$\begin{aligned}
Tr_{\mathbb{K}|\mathbb{Q}}(x\sigma^t(x)) &= (-1)^{t+m}p \sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d \sum_{mdc(j,p^s)=1} \omega_{d,t}^j \\
&= (-1)^m p \sum_{d=1, d\neq p^{s-1}(p-1)/2n}^{p^{s-1}(p-1)/n} ((-1)^d(-1)) + ((-1)^m p(-1)^{p^{s-1}(p-1)/2n} p^{s-1}(p-1)) \\
&= p(\sum_{d=1}^{p^{s-1}(p-1)/n} (-1)^d(-1)^{\frac{p^{s-1}(p-1)}{2n}})(-1) + (-1)^{\frac{p^{s-1}(p-1)}{2n}} pp^{s-1}(p-1) \\
&= p(-1)(-1)^{\frac{p^{s-1}(p-1)}{2n}} + (-1)^{\frac{p^{s-1}(p-1)}{2n}} pp^{s-1}(p-1) \\
&= (-1)^{\frac{p^{s-1}(p-1)}{2n}}(p + p^2 - p) = (-1)^{\frac{p^{s-1}(p-1)}{2n}} p^2,
\end{aligned}$$

o que completa a demonstração. ■

Algoritmo de construção de reticulados $\mathbb{Z}^n$-rotacionados

(1) Escolha um inteiro par n.

(2) Encontre um primo p tal que $n|\varphi(p^s)$, para algum $s \in \mathbb{N}^*$.

(3) Calcule os valores de r e λ.

(4) Calcule α e z na base de $\mathbb{Q}(\zeta_{p^s})$.

(5) Calcule x e seus conjugados na extensão $\mathbb{K}|\mathbb{Q}$.

(6) Calcule a matriz geradora R do reticulado $\mathbb{Z}^n$-rotacionado obtido.

4.8 Considerações finais

Neste capítulo apresentamos construções de reticulados algébricos via o homomorfismo canônico e reticulados ideais. Na busca por reticulados densos, com diversidade máxima e distância produto mínima estudamos a densidade de centro de alguns reticulados sobre corpos de números abelianos de grau p com p um primo ímpar e construímos reticulados $\mathbb{Z}^n$-rotacionados através de um subcorpo de $\mathbb{Q}(\zeta_{p^s})$. No primeiro caso, os reticulados construídos são imagens, pelo homomorfismo canônico do anel de inteiros de corpo de

números e de ideais. Apesar, de termos encontrado reticulados com densidade abaixo das ótimas, esses reticulados também apresentam diversidade máxima. No segundo caso, apresentamos a construções de reticulados ideais, via o homomorfismo torcido, de grau ímpar e par, que fornecem reticulados com diversidade máxima e é possível o cálculo da distância produto mínima.

Capítulo 5

Considerações finais e perspectivas

Neste trabalho apresentamos inicialmente resultados sobre corpos de números abeliano $\mathbb{K}$ de grau p, com p um primo ímpar. Dividimos em 3 casos de acordo com o condutor do corpo $\mathbb{K}$. Em cada caso explicitamos o elemento primitivo de $\mathbb{K}$ e uma $\mathbb{Z}$-base para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Destacamos os resultados apresentados no 3º caso do Capítulo 3. Os resultados algébricos, do Capítulo 3, foram de fundamental importância para as construções de reticulados algébricos feitas no Capítulo 4.

Como apresentamos no Capítulo 1, a relação entre empacotamentos esféricos reticulados, com certos parâmetros otimizados, e códigos tem grande importância atualmente. Em busca de reticulados densos, com deversidade máxima e distância produto mínima, fizemos algumas construções de reticulados algébricos via corpos de números.

Como para o cálculo desses parâmetros em um reticulado algébrico é necessário conhecermos propriedades algébricas do corpo em que estamos trabalhando, tivemos que aprofundar os estudos em alguns corpos de números.

O maior desafio deste trabalho foi encontrar $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$, com $x \in \mathcal{O}_{\mathbb{K}}$, quando consideramos $\mathbb{K}$ uma extensão abeliana de grau p e $cond(\mathbb{K}) = p^2q$, onde q é um primo e $q \equiv 1(mod\ p)$. Um dos objetivos futuros é considerar o $cond(\mathbb{K}) = p^2 \prod_{i=1}^{s} p_i$, com p_i's primos tais que $p_i \equiv 1(mod\ p)$ e $s > 1$.

Ainda no Capítulo 3, caracterizamos alguns ideais de $\mathcal{O}_{\mathbb{K}}$ e em certos casos encontramos o mínimo $Tr_{\mathbb{K}|\mathbb{Q}}(x^2)$ com x pertencentes à esses ideais.

A construção da família M_m de $\mathbb{Z}$-submódulos de $\mathcal{O}_{\mathbb{K}}$ feita em [18], a qual apresentou alta densidade de centro, também poderá ser estudada no caso em que o $cond(\mathbb{K}) = p^2q$. Podendo surgir futuramente como complemento a este trabalho.

As construções de reticulados ideais feitas no Capítulo 4, os quais são reticulados $\mathbb{Z}^n$-rotacionados, é de grande utilidade na transmissão de sinais usando o canal de comunicação de Rayleigh com desvanecimento, já que apresentam diversidade máxima e propriedades algébricas que facilitam o cálculo da distância produto mínima.

Referências Bibliográficas

[1] ANDRADE, A. A.; CARVALHO, E. D. **Cyclic constructions of rotated lattices with full diversity**, Journal of Advanced Research in Applied Mathematics, 3(3), 2011, 82-92.

[2] ATIYAH, M. F.; MACDONALD, I. J. **Introduction to commutative algebra**. Addison-Wesley, London, 1969.

[3] BAYER-FLUCKIGER, E., **Lattices and number fields**, Contemporany Mathematics, vol. 241,p. 69-84, 1999.

[4] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. **New algebraic construction of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel**. IEEE Trans. Inform. Theory, 2004, 50(4): 702-704.

[5] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. **Algebraic lattices constellations: bounds on performance**. IEEE Trans. Inform. Theory, 2006, 52(1): 319-327.

[6] CONWAY, J. H.; SLOANE, N. J. A. **Sphere Packings, Lattices and Groups**, Springer-Verlag, New York, 3º ed, 1999.

[7] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. Atual Editora, São Paulo, 1982.

[8] ELIA, P.; SETHURAMAN, B. A.; KUMAR, P. V. **Perfect space-time codes for any number od antennas**, IEEE Tras. Inform. Theory, 2007, 53(11), 3853-3868.

[9] FÁVARO, E. R., **Corpos cujo condutor é potência de primo: Caracterização e reticulados ideais associados**, Tese de Doutorado em Matemática, Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, São Paulo, 2012.

[10] FLORES, A. L., **Representação geométrica de ideais de corpos de números**, Dissertação de Mestrado, Imecc - Unicamp, Campinas, São Paulo, 1996.

[11] GREENBERG, M. J. **An Elementary Proof of the Kronecker-Weber Theorem**. Amer. Math. Monthly, v.81 (1974), p. 601-607; correction,v.82 (1975), p. 803.

[12] JOHNSTON, H., **Notes on Galois Modulus**, 15th March, 2011.

[13] LANG, S. **Algebraic Number Theory**. Springer-Verlag, New York, 1994.

[14] LANG, S **Algebra**. Addison-Wesley, New York, 1972.

[15] LEOPOLDT, H. W., **Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers**, J. reine angew, Math. 201 (1959), 119-149.

[16] LETTL, G., **The ring of integers of an abelian number field**. Journal für die reine und angewandte Mathematik, 162-170, New york, 1990

[17] NOBREGA NETO, T. P.; INTERLANDO, J. C.; LOPES, J. O. D. **The discriminant of abelian number fields**. Journal of Algebra and Its Applications, vol. 5 N 1, 35-41, 2006.

[18] OLIVEIRA, E. L., **Torres de Extensões Abelianas de grau primo ímpar não ramificado**, Tese de Doutorado em Matemática, Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, São Paulo, 2015.

[19] OGGIER, F., **Algebraic methodos for channel coding**, PhD, Thesis, EPFL, 2005.

[20] OGGIER, F.; VITERBO, E. **Algebraic number theory and coding desing for Rayleign fadins channel**. in Foundations and Thends in Communications an Information Theory, Yokohama, Japan, 2003.

[21] OGGIER, F.; BAYER-FLUCKIGER, E. **Best rotated cubic lattice constellation for the Raileigh fadins channel**. Proceeding of the IEEE International Symposium in Information Theory, Yokohama, Japan, 2003.

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

[23] SAMUEL, P. **Algebraic theory of numbers**. Hermann, Paris, 1970.

[24] SHANNON, C. **Mathematical Theory of Communication**. Bell Systems journal, vol. 27, pag. 379-423, 623-656, 1948.

[25] STEWAR, I.; TALL, D. **Algebraic number theory**. A K Peters, London, 1987.

[26] STEWART, I. **Galois Theory**. Chapman and Hall, 2004.

[27] WASHINGTON, L.C. **Introduction to cyclotomic fields**. Springer-Verlag, New York, 1982.

Índice Remissivo

Autorizo a reprodução xerográfica para fins de pesquisa.

São José do Rio Preto, 14/08/2015.

Ana Cláudia Machado Mendonça Chagas

Assinatura