UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

JOSÉ VALTER LOPES NUNES

p-EXTENSÕES GALOISIANAS E APLICAÇÕES

FORTALEZA
2015

JOSÉ VALTER LOPES NUNES

p-EXTENSÕES GALOISIANAS E APLICAÇÕES

Tese apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Doutor em Matemática. Área de concentração: Álgebra.

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto
Coorientador: Prof. Dr. José Othon Dantas Lopes.

FORTALEZA
2015

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

N925p Nunes, José Valter Lopes
p-extensões galoisianas e aplicações / José Valter Lopes Nunes. – 2015.
65 f. : enc. ; 31 cm

Tese (doutorado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática, Fortaleza, 2015.
Área de Concentração: Álgebra.
Orientação: Prof. Dr. Trajano Pires da Nóbrega Neto.
Coorientação: Prof. Dr. José Othon Dantas Lopes.

1. Extensões algébricas. 2. Corpos ciclotômicos. 3. Reticulados algébricos. 4. Densidade de centro. I. Título.

CDD 512

JOSÉ VALTER LOPES NUNES

P-EXTENSÕES GALOISIANAS E APLICAÇÕES

Tese apresentada ao Programa de Pós-graduação em Matemática do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Doutor em Matemática. Área de concentração: Álgebra.

Aprovoda em: 19/06/2015.

BANCA EXAMINADORA

Prof. Dr. Trajano Pires da Nóbrega Neto (Orientador)
Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP)

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará (UFC)

Prof. Dr. José Robério Rogério
Universidade Federal do Ceará (UFC)

Prof. Dr. José Carmelo Interlando
San Diego State University (SDSU)

Prof. Dr. André Luiz Flores
Universidade Federal de Alagoas (UFAL)

"No tempo favorável, Eu te responderei e no Dia da salvação, Eu mesmo te ajudarei."
Is.49.8

Dedico este trabalho a minha mulher
Maria do Carmo e as minhas três filhas,
Tercia, Tarcia e Ana Carla .

AGRADECIMENTOS

A Deus, que em sua misericórdia, me concedeu a Graça da possibilidade desse doutorado e ainda de ter a ajuda ou apoio de tantas pessoas.

A minha mulher Maria do Carmo, minha cúmplice em todos os momentos e em todas as lutas.

As minhas filhas, genros e neto: Tercia, Alexandre e Isaac; Tarcia e Kilmer; Ana Carla e Airton Junior.

Ao professor Trajano Nóbrega, meu orientador, que com sua amizade tem me ensinado muitas coisas além da matemática, por sua participação imprescindível para que este trabalho chegasse a bom termo e no tempo previsto.

Ao professor Gregório Bessa pelo apoio imprescindível e incentivo constante.

Aos professores José Othon e José Carmelo pela ajuda com valiosas sugestões e apoio constante.

Aos professores José Robério e André Flores pela participação na banca e sugestões apresentadas.

A todos os amigos que intercederam pelo êxito deste trabalho.

A todos os colegas do Departamento de Matemática: professores, funcionários e alunos, pelo apoio, amizade, e incentivo. Compreensivelmente cito apenas alguns nomes: Alexandre Fernandes, Ana Shirley, José Fábio, Renivaldo Sodré, Andréa Dantas, Antônio Caminha, Abdênago Barros, Ernani Ribeiro, Luquésio Petrola, Marcelo Melo e Gleydson Chaves.

RESUMO

Seja $K/\mathbb{Q}$ uma extensão abeliana de grau primo ímpar p e condutor n, onde p não se ramifica em $K/\mathbb{Q}$. As principais contribuicões deste trabalho são: 1) caracterização de ideais de $\mathfrak{O}_K$ em cuja fatoração constam apenas ideais primos ramificados $K/\mathbb{Q}$; 2) cálculo da densidade de centro da representação geométrica de $\mathbb{Z}$-módulos em $\mathfrak{O}_K$ caracterizados por uma equação modular (para $p = 3, 5$ e 7, parametriza-se o algorítmo que otimiza a densidade de centro destes reticulados). Além disso, os seguintes resultados são também descritos: 1) Famílias de reticulados associados a polinômios em $\mathbb{Z}[x]$ de grau dois e três; 2) uma prova alternativa da finitude do grupo das classes de um corpo números baseada somente em empacotamentos esféricos.

Palavras-chave: Extensões Abelianas. Corpos ciclotômicos. Reticulados algébricos. Densidade de centro.

ABSTRACT

Let $K/\mathbb{Q}$ be an Abelian extension of odd degree p and conductor n, where p does not ramify in $K/\mathbb{Q}$. The main contributions of this work are: 1) caracterization of ideals of $\mathfrak{O}_K$ whose factorization includes only prime ramified ideals $K/\mathbb{Q}$; 2) calculation of the center density of the geometric representation of $\mathbb{Z}$-modules in $\mathfrak{O}_K$ caracterized by a modular equation (for $p = 3, 5$, and 7, the algorithm that is used to optimize the center density of those lattices is parametrized). Besides, the following results are also described: 1) Families of lattices associated to polynomials in $\mathbb{Z}[x]$ of degree two and three; 2) an alternative proof of the finiteness of the class group of a number field based solely on sphere packings.

Keywords: Abelian extension. Cyclotomic fields. Algebraic lattices. Center density.

LISTA DE SÍMBOLOS

$\mathbb{N}$	O conjunto dos Números Naturais.
$\mathbb{Z}$	O conjunto dos Números Inteiros.
$\mathbb{Q}$	O conjunto dos Números Racionais.
$\mathbb{R}$	O conjunto dos Números Reais.
$\mathbb{C}$	O conjunto dos Números Complexos.
Σ	Somatório
$\prod$	Produtório
#(A)	Cardinalidade do conjunto A.
$M = (a_{ij})$	Matriz de entradas a_{ij}.
$(a, b) = d$	Máximo divisor comum igual a d.
$\det M$	Determinante de M.
$a \mid b$	a divide b.
$\mathfrak{a}^*$	$\mathfrak{a}$ menos o elemento nulo.
$a \equiv b \pmod{m}$	a congruente a b módulo m.
$\phi(n)$	Função de Euler aplicada à n.
$ker(f)$	Núcleo da função f.
$Im(f)$	Imagem da função f.
Rz	Parte real do número complexo z
Iz	Parte imaginária do número complexo z
H, G	Grupos
$A[x]$	Anel dos polinômios à coeficientes no anel A.
$\mathfrak{a}$	Ideal.
$A/\mathfrak{a}$	anel quociente.
G/H	Grupo quociente.
$[G : H]$	Índice do subgrupo H no grupo G.
F, K, L	corpos.
L/K	O corpo L é uma extensão do corpo K.
KL	Composito dos corpos K e L.
$Gal(K/L)$	Grupo de galois de K sobre L.
$irr(\alpha, \mathbb{Q})$	Polinômios irredutível de α sobre $\mathbb{Q}$.
$Tr_{L/K}(\alpha)$	Traço, em relação à L/K, de α.
$N_{L/K}(\alpha)$	Norma, em relação à L/K, de α.
$N(\mathfrak{a}$	Norma do ideal $\mathfrak{a}$.
$\mathfrak{O}_K$	Anel de inteiros do corpo K.
$\mathfrak{M}$	Módulo.
$D(\alpha_1, \ldots, \alpha_n)$	Discriminante de $(\alpha_1, \ldots, \alpha_n)$.
$Disc(K)$	Discriminante do corpo de números K.

$cont(x)$	Conteúdo de x.
ζ_n	Raiz primitiva n-ésima da undade.
$\mathbb{Q}(\zeta_n)$	n-ésimo corpo ciclotômico.
$H(L)$	Grupo das classes de L.
$H(L)_p$	A p-parte do grupo das classes.
Λ	Reticulado.
Λ_β	Reticulado com base β.
$vol(\Lambda)$	Volume de Λ.
$\Delta(\Lambda)$	Densidade de empacotamento.
$\delta(\Lambda)$	Densidade de centro.
σ_L	Homomorfismo de Minkowski.
$\sigma_L(\mathfrak{M})$	Reticulado algébrico.
δ^*	Cota superior para δ.

SUMÁRIO

1 INTRODUÇÃO

O empacotamento de esferas é um tema atual, principalmente pelas suas ligações com várias áreas do conhecimento, em especial com a Teoria da Informação.

Os primeiros resultados que se conhece são anteriores a Gauss, Newton e outros grandes nomes da matemática.

Em 1900 o problema do empacotamento de esferas foi destacado por Hilbert, dentre outros que seriam de grande relevância no século seguinte, pela sua importância e complexidade.

Muito tem sido feito ao longo dos últimos anos, e muito mais há por se fazer. A relação comprovada entre a densidade de um empacotamento de esferas e a eficiência de um código corretor de erros, aumentou o interêsse pelo assunto e novas técnicas para a obtenção de reticulados foram disponibilizadas.

No corpo desta tese abordamos uma técnica nova na obtenção de reticulados, deduzida das raízes reais de um polinômio. Algumas famílias de polinômios são apresentadas para mostrar a eficiência do método em dimensões 2 e 3. Estes resultados encontram-se no Capítulo 3, onde incluímos uma demonstração da finitude do Grupo das Classes de um corpo de números, utilizando reticulados algébricos como ferramenta. Os resultados acima relatados constituem a base de dois artigos publicados: (FLORES *et al.*) e (INTERLANDO, NOBREGA NETO, and NUNES).

No quarto capítulo o foco são extensões Galoisianas de grau primo ímpar p. Conhecemos dados importantes destes corpos quando o ideal $p\mathbb{Z}$ não se ramifica. Assim conseguimos caracterizar os ideais que se ramificam e explorar propriedades da forma traço, quando restrita aos ideais primos ramificados.

Na Seção 4.3 abordamos a p-parte do grupo das classes, apontando para resultados inéditos na Teoria dos Corpos de Classe e abrindo a possibilidade de novos resultados nesta direção.

Na Seção 4.4, estendemos para certos $\mathbb{Z}$-módulos o conceito dos ideais primos ramificados. Nestes módulos a forma traço foi exautivamente explorada e bons resultados foram obtidos. Conseguimos parametrizar o desempenho de um algorítmo que calcula a densidade de centro da representação geométrica destes módulos e, para as dimensões 3, 5 e 7, apresentamos ótimos resultados.

No Capítulo 5 apresentamos as conclusões e algumas propostas para pesquisas futuras.

2 PRELIMINARES

Apresentaremos neste capítulo algumas definições e resultados básicos da Teoria algébrica dos Números, diretamente relacionados com o conteúdo desta tese. O objetivo é que este material seja, na medida do possível, se não autosuficiente, uma sequência que forneça ao leitor informações sobre os principais resultados, definições e idéias básicas que contribuirão para a obtenção dos resultados.

Abordamos conceitos como elemento inteiro, norma traço, anel de inteiros, corpo de números, discriminante, decomposição de ideais, extensões galoisianas, reticulados e outros conceitos relacionados. Os resultados apresentados, em sua maioria, são dirigidos para corpos de números e especificamente para serem aplicados nos capítulos seguintes. Para cada um desses resultados a referência bibliográfica é citada.

Optamos por não incluir as demonstrações por considerá-las de domínio público. Exceção será feita a poucos resultados por entender que a demonstração aqui escrita contribuirá para uma melhor comprensão do texto.

A sequência dos resultados deste capítulo seguiu inicialmente a ordem do livro Algebraic Theory Of Numbers de Pierre Samuel e mais adiante adotamos prioritariamente o livro Number Fields de Daniel A. Marcus.

2.1 Inteiros Algébricos

Definição 2.1 *Sejam B um anel e A um subanel de B. Um elemento x de B é inteiro sobre A se x é raiz de um polinômio mônico com coeficientes em A. Se todo elemento de B é inteiro sobre A dizemos que B é inteiro sobre A.*

Exemplo 2.1 *O elemento $1+i$, de $\mathbb{Z}[i]$, é inteiro sobre $\mathbb{Z}$, pois é raiz do polinômio $m(X) = X^2 - 2X + 2$. O número racional $\frac{1}{2}$, não é inteiro sobre $\mathbb{Z}$.*

Exemplo 2.2 *O anel $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2}; a, b \in \mathbb{Z}\right\}$ é inteiro sobre $\mathbb{Z}$ pois um elemento qualquer, $a + b\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ é raiz do polinômio $f(X) = X^2 - 2aX + a^2 - 2b^2$.*

Observe que $\frac{1}{2}$ não é inteiro sobre $\mathbb{Z}$, assim $\mathbb{Z}\left[\frac{1}{2}\right]$ não é inteiro sobre $\mathbb{Z}$. De modo análogo, $\frac{\sqrt{2}}{2}$ não é inteiro sobre $\mathbb{Z}$ e $\mathbb{Z}\left[\frac{\sqrt{2}}{2}\right]$ não é inteiro sobre $\mathbb{Z}$. Ambos, $\mathbb{Z}\left[\frac{1}{2}\right]$ e $\mathbb{Z}\left[\sqrt{2}\right]$ estão contidos em $\mathbb{Z}\left[\frac{\sqrt{2}}{2}\right]$.

Proposição 2.1 *(SAMUEL, Corolário 2, p.29) Sejam B um anel e A um subanel de B. O conjunto A' dos elementos de B que são inteiros sobre A é um subanel de B que contém A.*

Definição 2.2 *Sejam B um anel e A um subanel de B. O anel A' dos elementos de B inteiros sobre A é chamado de fecho integral de A em B. Em particular, se A é um domínio de integridade e B é o corpo de frações de A, dizemos que A' é o fecho integral de A. No caso em que $A' = A$, dizemos que A é integralmente fechado.*

Exemplo 2.3 *Todo anel principal é integralmente fechado. Assim o anel $\mathbb{Z}$ dos números inteiros é integralmente fechado.*

Proposição 2.2 *(SAMUEL, Proposição 2, p.29) Sejam C um anel, B um subanel de C e A um subanel de B. Se B é inteiro sobre A e C é inteiro sobre B, então C é inteiro sobre A.*

Exemplo 2.4 *O fecho integral de um domínio de integridade A é integralmente fechado.*

Exemplo 2.5 *Como $-3 \equiv 1 \pmod 4$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ é inteiro sobre $\mathbb{Z}$, assim $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ é algébrico sobre $\mathbb{Z}\left[\sqrt{-3}\right]$, logo $\mathbb{Z}\left[\sqrt{-3}\right]$ não é integralmente fechado.*

Consideraremos agora o caso em que o subanel A de B, é um corpo K.

Definição 2.3 *Seja B um anel e K um subcorpo de B. Um elemento $x \in B$ é algébrico sobre K se x é raiz de um polinômio com coeficientes em K. Um elemento de B que não é algébrico sobre K é chamado de transcendente sobre K.*

Assim, sobre um corpo, um elemento é algébrico, se e somente se , é inteiro.

Temos também que um elemento x é algébrico sobre um corpo K, se e somente se, a dimensão do K-espaço vetorial $K[x]$ sobre K, denotada $[K[x] : K]$, é finita.

Definição 2.4 *Dizemos que um anel B que contém um corpo K é algébrico sobre K se todo elemento de B é algébrico sobre K. Neste caso, se B é um corpo dizemos que B é uma extensão algébrica de K e a dimensão do K-espaço vetorial B sobre K, denotada $[B : K]$, é chamada de grau de B sobre K.*

Com a notação acima, se x é um elemento de B algébrico sobre K, existe um homomorfismo $\varphi : K[X] \to B$ tal que $\varphi(X) = x$ e $\varphi(a) = a$ para todo $a \in K$. A imagem de φ é $K[x]$. Podemos então dizer que um elemento $x \in B$ é algébrico sobre K se, e somente se, $Ker(\varphi) \neq (0)$. Nesse caso, como $K[X]$ é um domínio principal, seja $F(X)$ o polinômio não nulo gerador do ideal $Ker(\varphi)$, o qual pode ser tomado mônico e neste caso é unicamente determinado e chamado polinômio minimal de x sobre K. O grau do polinômio minimal de x sobre K é chamado de grau de x sobre K. Podemos verificar também que, se $G(X)$ é um polinômio qualquer de $K[X]$ então $G(x) = 0 \Leftrightarrow F(X)$ divide $G(X)$ em $K[X]$. Ainda pelo fato de que $K[X]/(F(X)) \cong K[x]$, temos $K[x]$ é corpo $\Leftrightarrow K[x]$ é domínio de integridade $\Longleftrightarrow F(X)$ é irredutível. Particularmente, se B é um

corpo e um elemento x de B é algébrico sobre K, o polinômio minimal de x sobre K é irredutível.

Por outro lado, se K é um corpo e $F(X)$ um polinômio irredutível de $K[X]$, podemos ver $K[X]/(F(X))$ como um corpo que contém K. Denotando por x a classe de X nesse corpo, temos $F(x) = 0$ e assim $F(X)$ é divisível por $X - x$ em $K[x]$. Mais geralmente temos:

Proposição 2.3 *(SAMUEL, Proposição 3, p.32) Sejam K um corpo e $P(X) \in K[X]$ um polinômio não constante. Existe uma extensão algébrica K' de K tal que $P(X)$ se decompõe em fatores lineares em $K'[X]$.*

Dizemos que um corpo K é algebricamente fechado se todo polinômio não constante $P(X)$ em $K[X]$ se decompõe em fatores do primeiro grau em $K[X]$. Para que um corpo K seja algebricamente fechado é suficiente que todo polinômio não constante $P(X)$ em $K[X]$ admita uma raiz em K. O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado. Um exemplo de um corpo que não é algebricamente fechado é o corpo $\mathbb{R}$ dos números reais.

Dados dois corpos L e M contendo um corpo K, chamamos de K-isomorfismo de L sobre M a todo isomorfismo φ de L sobre M tal que $\varphi(a) = a$ para todo a em K. Nestas condições dizemos que L e M são K-isomorfos ou, se L e M são algébricos sobre K dizemos que são corpos conjugados sobre K. Se L e M são extensões de K, dizemos que dois elementos x de L e y de M são conjugados sobre K se existe um K-isomorfismo $\varphi : K(x) \to K(y)$ tal que $\varphi(x) = y$. Tal isomorfismo é único e o fato de dois elementos serem conjugados sobre K significa que ou os dois são transcendentes sobre K ou os dois são algébricos sobre K e neste caso, têm o mesmo polinômio minimal.

Como exemplo tomamos um polinômio $F(X)$, irredutivel sobre K, cujas raízes numa extensão L de K são $x_1, x_2, \ldots, x_n$. Neste caso os x_i são dois a dois conjugados sobre K, bem como os corpos $K(x_i)$ são dois a dois conjugados sobre K.

Lema 2.1 *(SAMUEL, Lema, p.33) Sejam K um corpo de característica zero, $F(X)$ um polinômio mônico irredutivel em $K[X]$ e $F(X) = \prod_{i=1}^{n}(X - x_i)$, sua decomposição em fatores lineares em uma extensão L de K. Então as n raízes $x_1, x_2, \ldots, x_n$ de $F(X)$ são distintas.*

Teorema 2.1 *(SAMUEL, Teorema 1, p.33) Sejam K um corpo de característica zero, L uma extensão de K de grau n e C um corpo algebricamente fechado contendo K. Então existem n K-monomorfismos distintos de L em C.*

Corolário 2.1 (Teorema do Elemento Primitivo) *(SAMUEL, Corolário, p.34) Sejam K um corpo de característica zero e L uma extensão de K de grau finito n. Então*

existe um elemento x em L tal que $L = K[x]$. Um tal elemento x è chamado de elemento primitivo.

Na verdade, tomando como hipótese o resultado do Corolário 2.1, podemos demonstrar o Teorema 2.1. Portanto esses dois resultados são equivalentes. Para ver isso basta verificar a demonstração do Teorema 2.1 em (SAMUEL, Teorema 1, p.33).

Definição 2.5 *Se K é uma extensão finita de $\mathbb{Q}$, de grau n, dizemos que K é um Corpo de Números de grau n.*

Pelo Corolário 2.1, vemos que todo Corpo de Números é da forma $K = \mathbb{Q}[x]$, onde x é um elemento de K. Assim $1, x, x^2, ..., x^{n-1}$ é uma base para o $\mathbb{Q}$-espaço vetorial $K = \mathbb{Q}[x]$.

Um Corpo de Números de grau 2 é chamado um Corpo Quadrático.

Exemplo 2.6 *É possível provar que todo Corpo Quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um número inteiro livre de quadrados.*

Um corpo de números K, da forma $K = \mathbb{Q}[\zeta_n]$ onde ζ_n é uma raiz primitiva n-ésima da unidade, é chamado Corpo Ciclotômico.

Definição 2.6 *Dado um Corpo de Números K, os elementos de K que são inteiros sobre $\mathbb{Z}$, são chamados inteiros algébricos de K.*

Pela Proposição 2.1, o conjunto dos inteiros algébricos de K é um anel que denotamos por $\mathfrak{O}_K$ e o chamamos de anel de inteiros de K.

Seja d um número inteiro livre de quadrados e $K = \mathbb{Q}(\sqrt{d})$.

Lema 2.2 *(SAMUEL, Teorema 1, p.35) O anel de inteiros de K é $\mathbb{Z}[w]$ onde,*

$$w = \begin{cases} \sqrt{d} & se \;\; d \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{d}}{2}, & se \;\; d \equiv 1 \pmod 4 \end{cases}$$

O anel de inteiros de um Corpo de Números K, de grau n, contém um subconjunto $\beta = \{\alpha_1, \ldots, \alpha_n\}$ de tal modo que todo elemento de $\mathfrak{O}_K$ é uma combinação linear, com coeficientes em $\mathbb{Z}$, dos elementos de β. O conjunto β é denominado uma base integral de $\mathfrak{O}_K$ (ou K) e por isso $\mathfrak{O}_K$ satisfaz a definição de $\mathbb{Z}$-módulo livre de posto n.

Proposição 2.4 *(WASHINGTON, Teorema 2.5, p.11). Se $K = \mathbb{Q}(\zeta_n)$ onde ζ_n é raiz primitiva uma n-ésima da unidade, então o grau da extensão $K/\mathbb{Q}$ é $\phi(n)$, onde ϕ é a função de Euler.*

Proposição 2.5 *(WASHINGTON, Teorema 2.6, p.11) Se* $K = \mathbb{Q}(\zeta_n)$ *onde* ζ_n *é uma raiz primitiva n-ésima da unidade, então* $\mathfrak{O}_K = \mathbb{Z}[\zeta_n]$ *e o conjunto* $\left\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}\right\}$ *é uma base integral para* $\mathbb{Q}(\zeta_n)$.

2.2 Norma e Traço

Sejam K um corpo dos números, L uma extensão finita de K de grau n, C um corpo algebricamente fechado contendo K e σ_1,... ,σ_n os n K-monomorfismos de L em C. Definimos o Traço de um elemento x de L, relativamente à extensão L de K e Norma de um elemento x de L, relativamente à extensão L de K, denotando da seguinte maneira : para um elemento x de L, $Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$ e $N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$.

Observamos imediatamente as propriedades abaixo para elementos x e y em L:

i) $Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y)$
ii) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.

Assim se x está em K,
iii) $Tr_{L/K}(x) = nx$
iv) $N_{L/K}(x) = x^n$.

Se x está em K e y está em L, do que temos podemos deduzir que
v) $Tr_{L/K}(xy) = xTr_{L/K}(y)$
vi) $N_{L/K}(xy) = x^n N_{L/K}(y)$.

Com o que vimos acima, podemos mostrar o seguinte:

Proposição 2.6 *(MARCUS, Teorema 4, p.21) Sejam* K *um Corpo de Números,* L *uma extensão finita de* K *de grau* n, x *um elemento de* L *de grau* d *sobre* K *e* σ_1,... , σ_d *os* d K*-monomorfismos de* $K[x]$. *Entã*

i) $Tr_{L/K}(x) = \frac{n}{d} \sum_{i=1}^{d} \sigma_i(x)$

ii) $N_{L/K}(x) = \left[\prod_{i=1}^{d} \sigma_i(x)\right]^{\frac{n}{d}}$.

Nas hipoteses da Proposição 1.16, podemos concluir o seguinte:

Corolário 2.2 *(MARCUS, Corolário, p.23) Sejam* K *um Corpo de Números,* L *uma extensão finita de* K *de grau* n *e* x *um elemento de* L. *Então* $Tr_{L/K}(x)$ *e* $N_{L/K}(x)$ *são elementos de* K; *além disso se o elemento* x *está em* $\mathfrak{O}_L$, *então* $Tr_{L/K}(x)$ *e* $N_{L/K}(x)$ *estão em* $\mathfrak{O}_K$.

Exemplo 2.7 *Sejam* $K = \mathbb{Q}$ *e* $L = \mathbb{Q}(\sqrt{d})$. *Então* $x \in L$ *é da forma* $x = a + b\sqrt{d}$ *e temos* $Tr_{L/\mathbb{Q}}(x) = 2a$, $N_{L/\mathbb{Q}}(x) = a^2 - db^2$.

Proposição 2.7 *(SAMUEL, Corolário, p.38) Se* K *é um corpo de números, então* $Tr_{K/\mathbb{Q}}(x)$ *e* $N_{K/\mathbb{Q}}(x)$ *são números inteiros, para todo* $x \in \mathfrak{O}_K$.

Quando temos três corpos em torre, o próximo resultado nos dá a relação entre os Traços e entre as normas, que chamamos de regra da transitividade.

Proposição 2.8 *(MARCUS, Teorema 5, p.23) Sejam* K *um corpo de números,* L *uma extensão finita de* K *e* M *uma extensão finita de* L. *Então para todo elemento* x *de* M, *temos:*

i) $Tr_{L/K}(Tr_{M/L}(x)) = Tr_{M/K}(x)$;
ii) $N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$.

Para finalizar esta seção introduzimos o conceito de norma de um ideal inteiro não nulo $\mathfrak{I}$ como sendo a cardinalidade do quociente $\mathfrak{O}_K/\mathfrak{I}$. Quando $\mathfrak{I}$ é um ideal principal, temos a

Proposição 2.9 *(SAMUEL, Proposição 1, p.52) Sejam* K *um corpo de números* x *um elemento não nulo de* $\mathfrak{O}_K$, *então* $\left|N_{K/\mathbb{Q}}(x)\right| = \#\left(\dfrac{\mathfrak{O}_K}{< x >}\right)$.

2.3 Teoria de Galois

Sejam L um corpo e G um conjunto de automorfismos de L. O conjunto dos $x \in L$ tais que $\sigma(x) = x$ para todo $\sigma \in G$ é um subcorpo de L, que é chamado de corpo dos invariantes de G. Por outro lado, dada uma extensão L de um corpo K o conjunto dos K-automorfismos de L é um grupo com a operação composição.

Proposição 2.10 *(SAMUEL, Teorema 1, p.86) Seja* L *uma extensão de grau* n *de um corpo* K *de característica* 0. *As seguintes condições são equivalentes:*

i) K *é o corpo dos invariantes do grupo* G *dos* K*-automorfismos de* L.

ii) Para todo $x \in L$ *o polinômio minimal de* x *sobre* K *tem todas as raízes em* L.

iii) L *é gerado pelas raízes de um polinômio sobre* K.

Com as condições acima, o grupo G *dos* K*-automorfismos de* L *tem ordem* n.

Definição 2.7 *Se as condições da Proposição 2.10 são satisfeitas, dizemos que L é uma extensão de Galois (ou Galoisiana) de K e que G é o grupo de Galois de L sobre K, que denotamos $G = Gal(L/K)$. Se G é abeliano (respectivamente cíclico), dizemos que L é uma extensão abeliana (respectivamente cíclica) de K.*

Exemplo 2.8 *Toda extensão quadrática é uma extensão de Galois.*

A partir da definição é fácil concluir que uma extensão ciclotômica é Galoisiana.

Corolário 2.3 *(SAMUEL, Corolário, p.87) Seja K um corpo de caracteristica 0, L uma extensão de grau finito n de K e H um grupo de automorfismos de L que admitem K como corpo de invariantes. Então L é uma extensão galoisiana de K e seu grupo de Galois é H.*

Teorema 2.2 *(SAMUEL, Teorema 2, p.87) Seja K um corpo de característica 0, L uma extensão Galoisiana de K e G seu grupo de Galois. Para cada subgrupo H de G, seja $k(H)$ o corpo dos invariantes de H e para cada subcorpo M de L que contém K, seja $g(M)$ o grupo dos M-automorfismos de L. Então:*

i) As aplicações g e k são bijeções inversas uma da outra e decrescentes pela relação de inclusão e L é uma extensão Galoisiana de todo corpo intermediário M.

ii) Para que um corpo intermediário M seja uma extensão Galoisiana de K, é necessário e suficiente que $g(M)$ seja um subgrupo normal de G. Neste caso, o grupo de Galois de M sobre K é isomorfo a $G/g(M)$.

Teorema 2.3 *(MARCUS, Teorema 7, p.263) Sejam L e M extensões galoisianas de um corpo de característica zero K tais que $L \cap M = K$. Então o compósito LM é uma extensão galoisiana de M e $Gal(LM/M)$ é isomorfo ao $Gal(L/K)$.*

Desse Teorema podemos concluir que para todo elemento, $x \in L$, teremos que $Tr_{LM/M}(x) = Tr_{L/K}(x)$ e com essa observação demonstra-se o Lema seguinte que será utilizado no Capítulo 4.

Lema 2.3 *Seja m um inteiro da forma $m = a \cdot b$, com $(a, b) = 1$. Então:*

$$Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a) \cdot Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b)$$

.

Demonstração: Como $(a, b) = 1$, existem inteiros r e s tais que $ar + bs = 1$. Com isso podemos escrever

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

Assim,

$$Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a)}(\zeta_a^s \cdot \zeta_b^r)\right) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a^s) \cdot Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^r).$$

Visto que $(s,a) = (r,b) = 1$, ζ_a e ζ_a^s são conjugados e assim têm o mesmo traço; do mesmo modo ζ_b e ζ_b^r são conjugados.

Portanto, $Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a) \cdot Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b)$.

□

O resultado a seguir é de extrema importância para a Teoria dos Números e em particular para esta Tese.

Teorema 2.4 *(RIBENBOIM, p.273) (Teorema de Kronecker-Weber) Se K é um corpo de números abeliano, então existe um inteiro positivo n tal que $K \subset \mathbb{Q}(\zeta_n)$.*

O menor inteiro positivo n tal que $K \subset \mathbb{Q}(\zeta_n)$, é definido como o condutor de K.

2.4 Discriminante

Sejam K um corpo de números, L uma extensão finita de K de grau n, C um corpo algebricamente fechado contendo K e $\sigma_1, \ldots, \sigma_n$ os n K-monomorfismos de L em C. Definimos o discriminante de uma n-upla de elementos $x_1, x_2, \ldots, x_n$, todos em L, relativamente a extensão L de K, denotando da seguinte maneira : para uma n-upla de elementos $x_1, x_2, \ldots, x_n$, todos em L, $D(x_1, x_2, \ldots, x_n) = \det(\sigma_i(x_j))^2$, isto é: o quadrado do determinante da matriz cujo elemento da i-ésima linha e j-ésima coluna é $\sigma_i(x_j)$. Dessa definição podemos deduzir que $D(x_1, x_2, \ldots, x_n) = \det(Tr_{L/K}(x_i x_j))$.

Proposição 2.11 *(SAMUEL, Proposição 1, p.38) Nas condições da definição de discriminante, sejam $x_1, x_2, \ldots, x_n$ e $y_1, y_2, \ldots, y_n$, elementos de L tais que $y_i = \sum_{j=1}^{n} a_{ij} x_j$, com $a_{ij} \in K$. Então $D(y_1, \ldots, y_n) = (det(a_{ij}))^2 \cdot D(x_1, \ldots, x_n)$.*

Corolário 2.4 *Se K é um Corpo de Números de grau n, então os discriminantes das bases do $\mathbb{Z}$-módulo $\mathfrak{O}_K$, diferem por um elemento invertível de $\mathbb{Z}$ e que é um quadrado. Portanto esses discriminantes são iguais.*

Proposição 2.12 *(SAMUEL, Proposição 3, p.39) Sejam K um corpo de característica zero, L uma extensão de K, de grau finito n e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os n K-monomorfismos distintos de L em um corpo algebricamente fechado $\mathbf{C}$ contendo K. Então se $(x_1, x_2, \ldots, x_n)$ é uma base de L sobre K, teremos $D(x_1, x_2, \ldots, x_n) \neq 0$.*

Definição 2.8 *Seja K um Corpo de Números. O discriminante, relativamente a extensão K de $\mathbb{Q}$, de uma base integral qualquer de K é chamado discriminante do corpo K e denotamos por $Disc(K)$.*

Teorema 2.5 *(NÓBREGA NETO, LOPES, and INTERLANDO) Se K é um corpo de números de grau primo e condutor n, então $|Disc(K)| = n^{p-1}$.*

Tendo em vista a demonstração do Lema 4.2 do Capítulo 4, enunciamos a seguinte

Proposição 2.13 *(WASHINGTON, Proposição 2.7, p.12)*

$$Disc(\mathbb{Q}(\zeta_n)) = (-1)^{\frac{\phi(n)}{2}} \cdot \frac{n^{\phi(n)}}{\prod\limits_{p|n} p^{\frac{\phi(n)}{(p-1)}}}.$$

Definição 2.9 *Dizemos que K_1 e K_2, Corpos de Números de graus respectivamente n_1 e n_2, são disjuntos se $[K_1K_2 : \mathbb{Q}] = n_1n_2$. Se além disso, seus discriminantes são relativamente primos, dizemos que K_1 e K_2 são linearmente disjuntos.*

Se K_1 e K_2 são extensões galoisianas, Segue do Teorema 2.2 da seção 2.3 que K_1 e K_2 são disjuntos, se e somente se, $K_1 \cap K_2 = \mathbb{Q}$.

Proposição 2.14 *(LANG, p.68) Se K_1 e K_2 são corpos linearmente disjuntos de graus n_1 e n_2, respectivamente, então*

i) $\mathfrak{O}_{K_1K_2} = \mathfrak{O}_{K_1}\mathfrak{O}_{K_2}$.

ii) $Disc(K_1K_2) = Disc(K_1)^{n_2} Disc(K_2)^{n_1}$.

2.5 Reticulado e Empacotamento Esférico

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço euclideano n-dimensional de forma que a fração do espaço recoberto pelas esferas seja a maior possível.

Um Reticulado de posto n, do $\mathbb{R}^n$ é um subgrupo discreto de $\mathbb{R}^n$, de posto n. Podemos descrevê-lo como $\Lambda = \{\sum_{i=1}^{n} a_i u_i; a_i \in \mathbb{Z}\}$, onde $\{u_i; i = 1, \ldots, n\}$ é linearmente independente sobre $\mathbb{R}$.

Um Empacotamento em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que a interseção entre duas dessas esferas, seja no máximo um ponto.

Pode-se descrever um empacotamento somente indicando o conjunto dos centros das esferas e o raio; dito raio de empacotamento.

Um Empacotamento Reticulado é um empacotamento em que o conjunto dos centros forma um reticulado Λ do $\mathbb{R}^n$. Doravante quando nos referirmos a empacotamento, estamos considerando empacotamento reticulado, que diremos empacotamento associado a Λ.

A fração do espaço $\mathbb{R}^n$ coberta pela união das esferas é chamada, Densidade de Empacotamento de Λ.

Se $\beta = \{u_i; i = 1, \ldots, n\}$ é uma $\mathbb{Z}$-base do reticulado Λ do $\mathbb{R}^n$, denominamos Região Fundamental de Λ, com relação à β, ao conjunto

$$\Lambda_\beta = \{x \in \mathbb{R}^n; x = \sum_{i=1}^{n} \lambda_i u_i, 0 \leq \lambda_i < 1\}.$$

Observemos que $\mathbb{R}^n$ é a união disjunta de translações de Λ_β por vetores de Λ e que o cálculo da densidade de empacotamento basta ser feito em Λ_β. Por outro lado, como o volume de Λ_β é dado pelo módulo do determinante da matriz cujas linhas são as coordenadas dos vetores de β, concluímos que o volume de Λ_β, independe da base β.

Assim, definimos o Volume do Reticulado como sendo o volume de uma região fundamental.

No empacotamento associado à Λ, interessa as esferas de raio máximo. Para isso observemos que existe o número $\Lambda_{min} = min\{|v|\,; v \in \Lambda, v \neq 0\}$.

Assim $\rho = \frac{1}{2}\Lambda_{min}$ é o maior raio para o qual é possivel distribuir esferas centradas nos pontos de Λ e obter um empacotamento. Com isso, quando falamos em Densidade do Reticulado, nos referimos a densidade do empacotamento associado que denotamos por $\Delta(\Lambda)$.

Se $B(\rho)$ é a esfera de centro na origem e raio ρ e $v(\Lambda)$ é o volume de Λ, então:

$$\Delta(\Lambda) = \frac{v(B(\rho))}{v(\Lambda)} = \frac{v(B(1)) \cdot \rho^n}{v(\Lambda)}.$$

Como $v(B(1))$ é constante, interessa maximizar

$$\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)},$$

que denominamos Densidade de Centro.

Exemplo 2.9 *Seja* $\Lambda = \mathbb{Z}^2$. *Toda base para* Λ *é da forma* $\{(a_1, b_1); (a_2, b_2)\}$, *onde o determinante da matriz* $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ *é* ± 1. *Consideremos a base canônica* $\{v_1, v_2\}$.

Qualquer vetor de Λ *é da forma* $v = xv_1 + yv_2 = (x, y)$ *e* $|v|^2 = x^2 + y^2$. *O mínimo que essa forma quadrática assume, com entradas inteiras e não todas nulas, é 1, nos vetores* $(\pm 1, 0)$ *e* $(0, \pm 1)$.

A região fundamental para essa base é o quadrado $\{(x, y) \in \mathbb{R}^2; 0 \leq x, y \leq 1\}$, *cujo "volume" é* 1. *Com tais informações podemos deduzir que o raio de empacotamento é* $\frac{1}{2}$ *e a densidade de centro é* $\dfrac{(\frac{1}{2})^2}{1} = \dfrac{1}{2^2}$.

Não é difícil deduzir que se $\Lambda = \mathbb{Z}^n$ *e considerarmos a base canônica, um vetor genérico de* Λ *é da forma* $v = (x_1, \ldots, x_n)$, $|v|^2 = x_1^2 + \ldots + x_n^2$, *cujo menor comprimento não nulo é* 1; *a região fundamental é o hipercubo,* $\{(x_1, \ldots, x_n) \in \mathbb{R}^n; 0 \leq x_i \leq 1, i = 1, \ldots, n\}$, *cujo volume é* 1. *Assim podemos concluir que o raio de empacotamento é* $\frac{1}{2}$ *e a densidade de centro de* $\mathbb{Z}^n$ *é* $\dfrac{1}{2^n}$.

Exemplo 2.10 *Consideremos o reticulado* Λ, *contido no* $\mathbb{R}^2$ *e gerado pelos vetores* $(1, 0)$ *e* $(\frac{1}{2}, \frac{\sqrt{3}}{2})$.

Um vetor de Λ *é sempre da forma* $v = \left(x + \frac{y}{2}, \frac{\sqrt{3}y}{2}\right)$ *e*

$$|v|^2 = \left(x + \frac{y}{2}\right)^2 + \left(\frac{\sqrt{3}y}{2}\right)^2 = x^2 + xy + \frac{y^2}{4} + \frac{3y^2}{4},$$

ou seja, $|v|^2 = x^2 + xy + y^2$, x *e* y *inteiros. É claro que, se* $v \neq 0$, $|v|^2$ *é sempre um inteiro positivo e portanto o seu menor comprimento é* 1, *quando* $x = \pm 1$ *e* $y = 0$ *ou* $x = 0$ *e* $y = \pm 1$.

O volume da região fundamental é o determinante da matriz $\begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$, *que é* $\frac{\sqrt{3}}{2}$. *Logo o raio de empacotamento deste reticulado é* $\frac{1}{2}$ *e a densidade de centro é*

$$\frac{\left(\frac{1}{2}\right)^2}{\frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}}.$$

É fácil ver que a densidade de centro deste reticulado é maior do que a densidade de centro de $\mathbb{Z}^2$. *Na verdade a densidade de centro deste reticulado é a maior possível em* $\mathbb{R}^2$ *e tal reticulado é denominado de Hexagonal e denotado por* Λ_2.

Exemplo 2.11 *Consideremos agora em* $\mathbb{R}^3$, *o reticulado* Λ *gerado pelos vetores* $v_1 = (1,1,0)$, $v_2 = (1,0,1)$ *e* $v_3 = (0,1,1)$. *Um vetor genérico de* Λ *é da forma* $v = xv_1 + yv_2 + zv_3$, $x, y, z \in \mathbb{Z}$, *ou seja,* $v = (x+y, x+z, y+z)$; *logo*

$$|v|^2 = (x+y)^2 + (x+z)^2 + (y+z)^2 = 2(x^2+y^2+z^2+xy+xz+yz).$$

É claro que o menor valor não nulo que $|v|^2$ *assume é* 2, *quando* $x = \pm 1$, $y = z = 0$; $x = y = 0$ *e* $z = \pm 1$ *ou* $y = \pm 1$ *e* $x = z = 0$. *O determinante da matriz cujas entradas são as coordenadas dos vetores* v_1, v_2 *e* v_3, *é* ± 2. *Logo o raio de empacotamento de* Λ *é* $\frac{\sqrt{2}}{2}$, *o volume da região fundamental é* 2 *e a densidade de centro de* Λ *é*

$$\frac{\left(\frac{\sqrt{2}}{2}\right)^3}{2} = \frac{1}{4\sqrt{2}}.$$

Esta densidade é a maior possível em $\mathbb{R}^3$ *e este reticulado é denotado por* Λ_3.

Para mais detalhes sobre o que expomos nesta Seção e mais informações sobre o assunto, ver (CONWAY and SLOANE)

2.6 Ideais e Grupo das Classes

Sejam K um corpo de números e L uma extensão finita de K, de grau n. Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathfrak{O}_K$, então por (SAMUEL, p.49, p.71) o ideal $\mathfrak{p}\mathfrak{O}_L$ se escreve de modo único como $\mathfrak{p}\mathfrak{O}_L = \mathfrak{b}_1^{e_1} \cdot \ldots \cdot \mathfrak{b}_r^{e_r}$, onde $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ são os ideais primos de $\mathfrak{O}_L$, tais que $\mathfrak{b}_i \cap \mathfrak{O}_K = \mathfrak{p}$ e para cada $i = 1, \ldots, r$, e_i é um inteiro positivo que chamamos índice de ramificação de $\mathfrak{b}_i$.

Sabemos que $\mathfrak{O}_K/\mathfrak{p}$ e $\mathfrak{O}_L/\mathfrak{b}_i$ são corpos e por (SAMUEL, p.49) que $\mathfrak{O}_L/\mathfrak{b}_i$ é uma extensão finita de $\mathfrak{O}_K/\mathfrak{p}$ e seu grau é chamado, grau de inércia de $\mathfrak{b}_i$, que denotamos f_i, para cada $i = 1, \ldots, r$.

Teorema 2.6 *(Igualdade Fundamental) (SAMUEL, Teorema 1, p.71) Com a notação acima,*

$$\sum_{i=1}^{r} e_i f_i = [\mathfrak{O}_L/\mathfrak{p}\mathfrak{O}_L : \mathfrak{O}_K/\mathfrak{p}] = n.$$

Proposição 2.15 *(MARCUS, p.71) Com as notações anteriores se* L *é uma extensão galoisiana de* K *e* $\mathfrak{b}_1, \mathfrak{b}_2$ *são primos de* $\mathfrak{O}_L$ *na decomposição de* $\mathfrak{p}\mathfrak{O}_L$, *então seus graus de inércia são iguais, como também seus índices de ramificação.*

Seja A um domínio com corpo quociente K. Dizemos que um A-módulo M contido em K é um ideal fracionário de K, se existe $\alpha \in A, \alpha \neq 0$ tal que αM é um ideal de A. Se $M \subset A$, então M é um ideal fracionário de A, se e somente se, M é um ideal de A (no sentido usual); a estes ideais, chamamos ideais inteiros.

Assim qualquer ideal fracionário pode ser escrito na forma $\alpha^{-1}\mathfrak{a}$, onde $\mathfrak{a}$ é um ideal inteiro de A e α é um elemento não nulo de A .

Dizemos que um ideal fracionário M é principal se é gerado por um elemento da forma $\dfrac{\alpha}{\beta}$, onde $\alpha, \beta \in \mathfrak{O}_K$, $\beta \neq 0$.

Lembrando que dado um ideal inteiro, não nulo, $\mathfrak{a}$ de $\mathfrak{O}_L$, sua norma é $N(\mathfrak{a}) = \left|\dfrac{\mathfrak{O}_L}{\mathfrak{a}}\right|$ e com esta notação temos a

Proposição 2.16 *(SAMUEL, Proposição 2, p.52) Sejam L é um Corpo de Números, $\mathfrak{a}$ e $\mathfrak{b}$ ideais inteiros não nulos de $\mathfrak{O}_L$. Então $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$.*

Se M é um ideal fracionário não nulo de K, então podemos escrever $M = \alpha^{-1} \cdot \mathfrak{a}$ onde $\alpha \in \mathfrak{O}_K$ e $\mathfrak{a}$ é um ideal inteiro de $\mathfrak{O}_K$. Definimos a norma do ideal fracionário M por $N(M) = \dfrac{N(\mathfrak{a})}{N(<\alpha>)}$, onde $N(\mathfrak{a})$ e $N(<\alpha>$ são as normas dos ideais inteiros, $\mathfrak{a}$ e $<\alpha>$.

Da demonstração do (SAMUEL, Teorema 2, p.58), obtemos o seguinte:

Proposição 2.17 *Sejam L um Corpo de Números e m um número inteiro positivo. Então existe apenas uma quantidade finita de ideais inteiros $\mathfrak{a}$ de $\mathfrak{O}_L$, tais que $N(\mathfrak{a}) = m$.*

Definimos o produto de dois ideais fracionários, M e N de um anel A, como o menor A-módulo contendo todos os produtos ab, com $a \in M$ e $b \in N$. Esse A-módulo é então o conjunto de todas as somas finitas, $\sum\limits_i a_i b_i$, $a_i \in M$, $b_i \in N$.

No caso em que A é o anel de inteiros de um Corpo de Números, podemos escrever o (MOLLIN, Lema 3.56, p.154), do seguinte modo:

Proposição 2.18 *Se L é um Corpo de Números, então o conjunto dos ideais fracionários não nulos de $\mathfrak{O}_L$ forma um grupo multiplicativo abeliano, denotado por $\mathfrak{F}(\mathfrak{O}_L)$. O conjunto $\mathfrak{P}(\mathfrak{O}_L)$, dos ideais fracionários principais de $\mathfrak{O}_L$, é um subgrupo de $\mathfrak{F}(\mathfrak{O}_L)$.*

Nesse caso o grupo quociente $\dfrac{\mathfrak{F}(\mathfrak{O}_L)}{\mathfrak{P}(\mathfrak{O}_L)}$ é chamado grupo das classes de $\mathfrak{O}_L$ e denotado por $H(L)$.

Observamos que dois ideais fracionários I e J, estão na mesma classe, se e somente se, existe $\alpha \in L$ tal que $I =< \alpha > J$.

Seja K um corpo de números de grau n. Sabemos do Teorema 2.1 que existem exatamente n monomorfismos distintos $\sigma_i : K \longrightarrow \mathbb{C}$, onde $\mathbb{C}$ é o corpo dos números complexos. Sejam $\sigma_1, \ldots, \sigma_n$ esses monomorfismos e $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ a conjugação complexa. Então, para qualquer $i = 1, \ldots, n$, $\alpha \circ \sigma_i = \sigma_j$, $1 \leq j \leq n$ e $\sigma_i = \sigma_j$ se e somente se, $\sigma_i(K) \subset \mathbb{R}$.

Se o número de monomorfismos reais é r, então escrevemos $n - r = 2s$, o número de monomorfismos complexos e enumeramos esses monomorfismos da seguinte forma: $\sigma_1, \ldots, \sigma_r$ os monomorfismos reais e $\sigma_{r+1}, \ldots, \sigma_n$, os complexos, com σ_{j+s} o complexo conjugado de σ_j, para $r + 1 \leq j \leq r + s$.

Definimos então a imersão canônica, $\sigma_K : K \longrightarrow \mathbb{R}^n$ tal que

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_r(x), R\sigma_{r+1}(x), I\sigma_{r+1}, \ldots, R\sigma_{r+s}(x), I\sigma_{r+s})$$

para todo $x \in K$, onde Rz e Iz são as partes real e imaginária de z, respectivamente.

Observamos que σ_K é um monomorfismo de módulos, também chamado de monomorfismo de Minkowski.

Proposição 2.19 *(SAMUEL, Proposição 1, p.56) Se M é um $\mathbb{Z}$-submódulo livre de K de posto n e se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_K(M)$ é um reticulado do $\mathbb{R}^n$, cujo volume é dado por:*

$$v(\sigma_K(M)) = 2^{-s} \left| \underset{1 \leq i,j \leq n}{det} (\sigma_i(x_j)) \right|. \tag{1}$$

Proposição 2.20 *(SAMUEL, Proposição 2, p.57) Sejam K um corpo de números e $\mathfrak{a}$ um ideal inteiro não nulo de $\mathfrak{O}_K$, então $\sigma_K(\mathfrak{O}_K)$ e $\sigma_K(\mathfrak{a})$ são reticulados do $\mathbb{R}^n$. Além disso,*

$$v(\sigma_K(\mathfrak{O}_K)) = 2^{-s}\sqrt{|Disc(K)|} \quad e \quad v(\sigma_K(\mathfrak{a})) = 2^{-s}\sqrt{|Disc(K)|}N(\mathfrak{a}). \tag{2}$$

Neste caso do reticulado $\sigma_K(\mathfrak{a})$, o raio de empacotamento e a densidade de centro, que definimos na Seção 2.5, são dados respectivamente por,

$$\rho = \frac{1}{2} min\{|\sigma_K(x)| \, ; x \in \mathfrak{a}^*\} \quad e \quad \delta(\sigma_K(\mathfrak{a})) = \frac{2^s \rho^n}{\sqrt{|Disc(K)|}N(\mathfrak{a})}. \tag{3}$$

3 RETICULADOS E FINITUDE DO GRUPO DAS CLASSES

A construção de reticulados cuja densidade de centro seja alta é assunto de permanente interesse. Várias técnicas são conhecidas, cada uma com suas particularidades. Apresentamos na primeira Seção deste Capítulo, uma técnica de construção a partir de um polinômio dado com certas características. Este resultado foi publicado em (FLORES *et al.*).

Na segunda Seção faremos uma demonstração do conhecido "Teorema da Finitude do Grupo das Classes de Ideais", usando uma técnica nova, baseada na representação geométrica dos ideais inteiros de um Corpo de Números. Tal resultado foi publicado em (INTERLANDO, NOBREGA NETO, and NUNES).

3.1 Famílias de Reticulados à partir de Polinômios

Existem várias formas de se construir reticulados: $\mathbb{Z}^n$, A_n, D_n, Λ_n. (Confira (CONWAY and SLOANE)).

Nesta seção apresentaremos uma técnica de construção de reticulados à partir de polinômios com coeficientes reais. Faremos isso, construindo uma matriz geradora à partir das raízes de um polinômio.

Construiremos duas famílias infinitas de reticulados densos no $\mathbb{R}^2$ e uma família infinita de reticulados densos no $\mathbb{R}^3$. Com esses exemplos, queremos sugerir que essa técnica possa ser estendida para dimensões maiores.

Inicialmente, dado $v = (\beta_1, \ldots, \beta_n)$ um ponto do $\mathbb{R}^n$, o quadrado de sua distância à origem, isto é, o produto interno usual $v \cdot v$ será denotado por $|v|^2$.

Dividiremos esta Seção em três partes.

Na primeira partimos de uma família de polinômios quadráticos cujas raízes são reais.

Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, onde $a \neq 0$ e $a^2 > 4b$.

Denotamos por α_1 e α_2 as raízes de $f(x)$.

Como $det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} = -a\sqrt{a^2 - 4b} \neq 0$, os vetores $v_1 = (\alpha_1, \alpha_2)$ e $v_2 = (\alpha_2, \alpha_1)$ formam uma base do $\mathbb{R}^2$. Assim definimos Λ_f como sendo o reticulado gerado por v_1 e v_2, isto é, $\Lambda_f = \{\ a_1 v_1 + a_2 v_2; a_i \in \mathbb{Z}\}$.

Com a notação acima, podemos provar o seguinte:

Lema 3.1 *(FLORES et al.) Se $v \in \Lambda_f$, ou seja, se $v = xv_1 + yv_2$, $x, y \in \mathbb{Z}$, então*

$$|v|^2 = (\ a^2 - 2b)(x^2 + y^2) + 4b \cdot xy.$$

Demonstração: Temos $|v|^2 = v \cdot v = x^2 v_1 \cdot v_1 + y^2 v_2 \cdot v_2 + xy(\ v_1 \cdot v_2 + v_2 \cdot v_1)$ mas $v_1 = (\alpha_1, \alpha_2)$ e $v_2 = (\alpha_2, \alpha_1)$, logo $|v_1|^2 = |v_2|^2 = \alpha_1^2 + \alpha_2^2$ e $v_1 \cdot v_2 = v_2 \cdot v_1 = 2\alpha_1 \cdot \alpha_2$. Temos ainda, $2\alpha_1 \cdot \alpha_2 = 2b$ e $(\alpha_1 + \alpha_2)^2 = a^2$, então $(\alpha_1 + \alpha_2)^2 = a^2 - 2b$. Portanto

$$|v|^2 = (\alpha_1^2 + \alpha_2^2)(x^2 + y^2) + 4\alpha_1 \cdot \alpha_2 \cdot xy = (\ a^2 - 2b)(x^2 + y^2) + 4b \cdot xy.$$

□

Para concluírmos esta primeira parte, provamos:

Teorema 3.1 *(FLORES et al.) Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, onde $a \neq 0$ e $a^2 = 6b$. Sejam α_1 e α_2 as raízes distintas de $f(x)$ e $v_1 = (\alpha_1, \alpha_2)$, $v_2 = (\alpha_2, \alpha_1)$. Nessas condições*

$$\Lambda_f = \{\ a_1 v_1 + a_2 v_2; a_i \in \mathbb{Z}\} \tag{4}$$

tem densidade de centro igual a $\frac{1}{2\sqrt{3}}$, que é a densidade máxima alcançada em dimensão 2.

Demonstração: Se $v = xv_1 + yv_2 \in \Lambda_f$, então pelo Lema 3.1, $|v|^2 = 4b(x^2 + y^2 + xy)$. Para $x, y \in \mathbb{Z}$, o menor valor dessa expressão é $4b$, que é atingido por exemplo em $x = 1$ e $y = 0$. Assim o raio de empacotamento: $\rho = \frac{1}{2} min\{|v|\,; v \in \Lambda_f, v \neq 0\} = \sqrt{b}$ e o volume da região fundamental é

$$v(\Lambda_f) = \left| det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} \right| = \left| -a\sqrt{a^2 - 4b} \right| = 2\sqrt{3}b.$$

Portanto a densidade de centro de Λ_f é

$$\delta(\Lambda_f) = \frac{(\sqrt{b})^2}{2\sqrt{3}b} = \frac{1}{2\sqrt{3}}.$$

□

Exemplo 3.1 *Seja $f(x) = x^2 + 6x + 6$. Suas raízes são $-3 \pm \sqrt{3}$. Sejam $v_1 = (-3 + \sqrt{3}, -3 - \sqrt{3})$, $v_2 = (-3 - \sqrt{3}, -3 + \sqrt{3})$ e Λ o reticulado gerado por v_1 e v_2. O volume de Λ é o valor absoluto do determinante da matriz cujas entradas são as coordenadas de v_1 e v_2, ou seja,*

$$v(\Lambda) = \left| det \begin{pmatrix} -3 + \sqrt{3} & -3 - \sqrt{3} \\ -3 - \sqrt{3} & -3 + \sqrt{3} \end{pmatrix} \right| = \left| -12\sqrt{3} \right| = 12\sqrt{3}.$$

Agora seja $v = xv_1 + yv_2$*, então*

$$|v|^2 = x^2 v_1 \cdot v_1 + y^2 v_2 \cdot v_2 + 2xy \cdot v_1 \cdot v_2 = 24(x^2 + y^2) + 24xy = 24(x^2 + y^2 + xy),$$

cujo valor mínimo é 24*, quando* $x = 1$ *e* $y = 0$*. Assim o raio de empacotamento é*

$$\rho = \frac{\sqrt{24}}{2} = \sqrt{6} \quad e \quad \textit{a densidade de centro é} \quad \delta = \frac{(\sqrt{6})^2}{12\sqrt{3}} = \frac{1}{2\sqrt{3}}.$$

No Teorema 3.1 obtivemos uma família infinita de polinômios quadráticos de modo que a densidade de centro do reticulado associado é igual a densidade de centro do Reticulado Hexagonal, que é a densidade máxima para dimensão 2.

Na segunda construimos de uma família de polinômios quadráticos com raízes complexas, ou seja, $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, onde $a \neq 0$ e $a^2 < 4b$. Sejam α_1 e α_2 as raízes de $f(x)$, $R(z)$ e $I(z)$, as partes real e imaginária de $z \in \mathbb{C}$, respectivamente e definamos $v_1 = (R(\alpha_1), I(\alpha_1))$, $v_2 = (R(\alpha_2), I(\alpha_2))$, ou seja, se $\alpha_1 = -\frac{a}{2} + \frac{\sqrt{4b-a^2}}{2}i$ e $\alpha_2 = -\frac{a}{2} - \frac{\sqrt{4b-a^2}}{2}i$, teremos

$$v_1 = \left(-\frac{a}{2}, \frac{\sqrt{4b-a^2}}{2}\right), \; v_2 = \left(-\frac{a}{2}, -\frac{\sqrt{4b-a^2}}{2}\right) \tag{5}$$

O volume da região fundamental é dado por:

$$v(\Lambda_f) = \left| det \begin{pmatrix} -\frac{a}{2} & -\frac{a}{2} \\ \frac{\sqrt{4b-a^2}}{2} & -\frac{\sqrt{4b-a^2}}{2} \end{pmatrix} \right|.$$

Portanto

$$v(\Lambda_f) = \frac{|a|\sqrt{4b-a^2}}{2}.$$

Se $v = xv_1 + yv_2 \in \Lambda_f$, $|v|^2 = x^2 v_1 \cdot v_1 + y^2 v_2 \cdot v_2 + xy(\, v_1 \cdot v_2 + v_2 \cdot v_1)$. Mas $v_1 \cdot v_1 = \frac{a^2}{4} + \frac{4b-a^2}{4}$, assim $v_1 \cdot v_1 = b = v_2 \cdot v_2$.

$v_1 \cdot v_2 = \frac{a^2}{4} - \frac{4b-a^2}{4}$, então $v_1 \cdot v_2 = \frac{a^2}{2} - b = v_2 \cdot v_1$, logo

$$|v|^2 = b(x^2 + y^2) + (a^2 - 2b)xy = b(x-y)^2 + a^2 xy \tag{6}$$

Agora apresentaremos uma nova família infinita de polinômios quadráticos de modo que a densidade de centro do reticulado associado seja igual a densidade máxima alcançada em dimensão 2.

Teorema 3.2 *(FLORES et al.) Seja* $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, *onde* $a \neq 0$ *e* $a^2 = 3b$. *Sejam* α_1 *e* α_2 *as raízes complexas distintas de* $f(x)$ *e* v_1 , v_2, *definidos como em (2). Nessas condições*

$$\Lambda_f = \{\ a_1v_1 + a_2v_2; a_i \in \mathbb{Z}\} \tag{7}$$

tem densidade de centro igual a $\frac{1}{2\sqrt{3}}$, *que é a densidade máxima alcançada em dimensão* 2.

Demonstração: Da expressão (3), com $a^2 = 3b$, obtemos:

$$|v|^2 = bx^2 - by^2 - 2bxy + 3bxy = b(x^2 + y^2 + xy).$$

O menor valor dessa expressão é b, obtido em $x = 1$ e $y = 0$, por exemplo. Assim o raio de empacotamento é $\rho = \frac{\sqrt{b}}{2}$. O volume da região fundamental é

$$v(\Lambda_f) = \left| det \begin{pmatrix} -\frac{\sqrt{3b}}{2} & -\frac{\sqrt{3b}}{2} \\ \frac{\sqrt{b}}{2} & -\frac{\sqrt{b}}{2} \end{pmatrix} \right| = \frac{b\sqrt{3}}{2}.$$

Portanto a densidade de centro de Λ_f é $\delta(\Lambda_f) = \frac{\frac{b}{4}}{\frac{b\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}}$, a máxima alcançada em dimensão 2.

□

Exemplo 3.2 *Seja* $f(x) = x^2 + 3x + 3$. *Suas raízes são* $\frac{-3}{2} \pm \frac{\sqrt{3}}{2}$. *Sejam* $v_1 = \left(\frac{-3}{2}, \frac{\sqrt{3}}{2}\right)$, $v_2 = \left(\frac{-3}{2}, -\frac{\sqrt{3}}{2}\right)$ *e* Λ *o reticulado gerado por* v_1 *e* v_2. *O volume de* Λ *é dado por*

$$v(\Lambda) = \left| det \begin{pmatrix} -\frac{3}{2} & -\frac{3}{2} \\ \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix} \right| = \frac{3\sqrt{3}}{2}.$$

Se $v = xv_1 + yv_2 \in \Lambda$, $|v|^2 = 3x^2 + 3y^2 + 3xy = 3(x^2 + y^2 + xy)$, *pois* $v_1 \cdot v_1 = v_2 \cdot v_2 = 3$. *O menor valor de* $|v|^2$ *é* 3, *quando* $x = 1$ *e* $y = 0$. *Assim o raio de empacotamento é* $\rho = \frac{\sqrt{3}}{2}$ *e a densidade de centro é* $\delta = \frac{\frac{3}{4}}{\frac{3\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}}$, *a máxima alcançada em dimensão* 2.

Finalmente na terceira parte, partimos de uma família infinita de polinômios cúbicos cujas raízes são reais e construiremos reticulados associados com densidade de centro recorde em dimensão 3.

Lema 3.2 *(FLORES et al.) Seja* $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$*, com raízes reais* α_1*,* α_2 *e* α_3*.*

Se $M = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_3 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_3 & \alpha_1 \end{pmatrix}$*, então* $detM = -a(a^2 - 3b)$*.*

Demonstração: Temos que $detM = \alpha_1^3+\alpha_2^3+\alpha_3^3-3\alpha_1\alpha_2\alpha_3$. Das relações Newton-Girard, $\alpha_1 + \alpha_2 + \alpha_3 = -a$, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b$ e $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = a^2 - 2b$. Multiplicando a primeira pela última dessas igualdades, obtemos:

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_1\alpha_2^2 + \alpha_1\alpha_3^2 + \alpha_2\alpha_1^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_3\alpha_2^2 = -a(a^2 - 2b).$$

Daí, $\alpha_1^3+\alpha_2^3+\alpha_3^3+\alpha_1\alpha_2(\alpha_1+\alpha_2)+\alpha_1\alpha_3(\alpha_3+\alpha_1)+\alpha_2\alpha_3(\alpha_3+\alpha_2) = -a(a^2-2b)$. Usando as relações Newton-Girard: $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 - ab - 3\alpha_1\alpha_2\alpha_3 = -a(a^2 - 2b)$ e finalmente, $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3\alpha_1\alpha_2\alpha_3 = -a(a^2 - 3b)$

□

Lema 3.3 *(FLORES et al.) Seja* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$*, com raízes reais* α_1*,* α_2 *e* α_3*. Defina* $v_1 = (\alpha_1, \alpha_2, \alpha_3)$*,* $v_2 = (\alpha_3, \alpha_1, \alpha_2)$*,* $v_3 = (\alpha_2, \alpha_3, \alpha_1)$*. Se* x *,* y*,* z *são inteiros e* $v = xv_1 + yv_2 + zv_3$*, então*

$$|v|^2 = (a^2 - 2b)(x^2 + y^2 + z^2) + 2b(xy + xz + yz).$$

Demonstração: Temos $v = (\alpha_1x + \alpha_3y + \alpha_2z, \alpha_2x + \alpha_1y + \alpha_3z, \alpha_3x + \alpha_2y + \alpha_1z)$, então,

$$|v|^2 = (\alpha_1x + \alpha_3y + \alpha_2z)^2 + (\alpha_2x + \alpha_1y + \alpha_3z)^2 + (\alpha_3x + \alpha_2y + \alpha_1z)^2.$$

Daí,

$$|v|^2 = (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)(x^2 + y^2 + z^2) + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)(xy + xz + yz).$$

Portanto, usando novamente as relações Newton-Girard,

$$|v|^2 = (a^2 - 2b)(x^2 + y^2 + z^2) + 2b(xy + xz + yz).$$

□

Observação: Dado $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, em (Dickson, p48) temos que uma condição necessária e suficiente para que suas raízes, α_1, α_2 e α_3, sejam reais e distintas é que o discriminante de $f(x)$ seja estritamente maior do que zero. Isto é equivalente à condição: $c(27c + 4a^3 - 18ab) < b^2(a^2 - 4b)$.

Teorema 3.3 *(FLORES et al.) Seja* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$*, onde* $a \neq 0$*,* $a^2 = 4b$ *e* $b \geq 9$*. Sejam* α_1*,* α_2 *e* α_3 *as raízes reais de* $f(x)$ *e defina* $v_1 = (\alpha_1, \alpha_2, \alpha_3)$*,*

$v_2 = (\alpha_3, \alpha_1, \alpha_2)$, $v_3 = (\alpha_2, \alpha_3, \alpha_1)$. *Então* $\Lambda_f = \{\ a_1v_1 + a_2v_2 + a_3v^3; a_i \in \mathbb{Z}\}$ *tem densidade de centro igual a* $\frac{\sqrt{2}}{8}$*, que é o máximo alcançado em dimensão* 3.

Demonstração: Temos $v = (\alpha_1 x + \alpha_3 y + \alpha_2 z, \alpha_2 x + \alpha_1 y + \alpha_3 z, \alpha_3 x + \alpha_2 y + \alpha_1 z)$, então pelo Lema 3, $|v|^2 = (a^2 - 2b)(x^2 + y^2 + z^2) + 2b(xy + xz + yz)$ e como por hipotese $a^2 = 4b$, obtemos:

$$|v|^2 = 2b(x^2 + y^2 + z^2 + xy + xz + yz).$$

O valor mínimo dessa expressão é $2b$, atingido em $x = 1$, $y = 0$, por exemplo. Então o raio de empacotamento é $\rho = \sqrt{\frac{b}{2}}$ e o volume da região fundamental é dado pelo Lema 2, ou seja, $v(\Lambda_f) = |detM| = |-a(a^2 - 3b)|$, mas por hipotese $a^2 = 4b$, então $v(\Lambda_f) = 2b\sqrt{b}$.

Portanto a densidade de centro de Λ_f é

$$\delta(\Lambda_f) = \frac{(\frac{b}{2})^{\frac{3}{2}}}{2b\sqrt{b}} = \frac{\sqrt{2}}{8},$$

a máxima alcançada em dimensão 3.

□

Com o exemplo abaixo vemos que é possível, fora das condições do Teorema 3.3, construir um reticulado de posto 3 e densidade de centro recorde.

Exemplo 3.3 *Seja* $f(x) = x^3 + 6x^2 + 9x + 4$.

Suas raízes são $\alpha_1 = \alpha_2 = -1$ *e* $\alpha_3 = -4$.

Tomamos Λ *o reticulado gerado por* $v_1 = (-1, -1, -4)$*;* $v_2 = (-4, -1, -1)$*;* $v_3 = (-1, -4, -1)$. *Temos* $M = \begin{pmatrix} -1 & -1 & -4 \\ -4 & -1 & -1 \\ -1 & -4 & -1 \end{pmatrix}$ *e* $detM = -54$*, logo o volume do reticulado é* $v(\Lambda) = 54$. *Um vetor* v *do reticulado, é da forma* $v = xv_1 + yv_2 + zv_3$ *e calculando a norma, obtemos:*

$$|v|^2 = 18(x^2 + y^2 + z^2 + xy + xz + yz).$$

Assim o menor valor para $|v|^2$ *é* 18 *e* $\rho = \frac{\sqrt{18}}{2} = \frac{3\sqrt{2}}{2}$. *Portanto* $\delta = \frac{\left(\frac{3\sqrt{2}}{2}\right)^3}{54} = \frac{\sqrt{2}}{8}$.

Nota: A técnica de construção de reticulados acima descrita, se inspira na Teoria de Galois sob a seguinte lógica:

Dada uma extensão cúbica real K, digamos $K = \mathbb{Q}(\alpha)$ e $Gal(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3\}$. Sejam α_1, α_2 e α_3 os conjugados de α e $v = (\alpha_1, \alpha_2, \alpha_3)$. Considere $\sigma_i(v) = (\sigma_i(\alpha_1), \sigma_i(\alpha_2), \sigma_i(\alpha_3)) = v_i$ e tratamos do reticulado gerado por $\{v_1, v_2, v_3\}$.

3.2 Finitude do Grupo das Classes

Sejam K um Corpo de Números de grau n e $\mathfrak{O}_K$ seu anel de inteiros.

A prova que é bem conhecida da finitude do grupo das classes de K (MOLLIN, p.155), envolve o Critério de Minkowski para um conjunto convexo conter um ponto de um reticulado (MOLLIN, Teorema 2.50, p.97) e a existencia de um ideal inteiro de $\mathfrak{O}_K$ cuja norma não exceda M_K, a cota de Minkowski (MOLLIN, Teorema 2.56, p.100).

Nesta Seção apresentaremos uma prova alternativa para esse problema clássico da Teoria dos Números, por meio de resultados de empacotamento esférico.

Uma consequência dessa nova prova é a obtenção de uma cota inferior para a densidade de centro do empacotamento reticulado associado a ideais inteiros de $\mathfrak{O}_K$.

Consideremos a imersão canônica $\sigma_K : K \longrightarrow \mathbb{R}^n$, como na Seção 2.6, definida por:

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_r(x), R\sigma_{r+1}(x), I\sigma_{r+1}, \ldots, R\sigma_{r+s}(x), I\sigma_{r+s})$$

para todo $x \in K$, onde Rz e Iz são as partes real e imaginária de z, respectivamente. Daí,

$$|\sigma_K(x)|^2 = \sigma_1(x)^2 + \cdots + \sigma_r(x)^2 + |\sigma_{r+1}(x)|^2 + \cdots + |\sigma_{r+s}(x)|^2 .$$

Como $\sigma_{r+s+j} = \overline{\sigma}_{r+j}, j = 1, \ldots, s$, então $2\,|\sigma_K(x)|^2 = 2(\sigma_1(x)^2 + \cdots + \sigma_r(x)^2) + |\sigma_{r+1}(x)|^2 \cdot \cdots + |\sigma_{r+2s}(x)|^2$.

Assim, usando o Teorema das Médias, obtemos:

$$2\,|\sigma_K(x)|^2 \geq \sum_{i=0}^{n} |\sigma_i(x)|^2 \geq n \sqrt[n]{\left|\prod_{i=1}^{n} \sigma_i(x)\right|^2} = n \sqrt[n]{\left|N_{K/\mathbb{Q}}(x)\right|^2}. \tag{8}$$

Daí $|\sigma_K(x)|^2 \geq \frac{n}{2} \sqrt[n]{\left|N_{K/\mathbb{Q}}(x)\right|^2}$, então

$$|\sigma_K(x)| \geq \frac{\sqrt{2n}}{2} \sqrt[n]{\left|N_{K/\mathbb{Q}}(x)\right|^2} \tag{9}$$

Seja $\mathfrak{a}$ um ideal inteiro de $\mathfrak{O}_K$, então $N(\mathfrak{a}) = \left|\frac{\mathfrak{O}_K}{\mathfrak{a}}\right|$. O conjunto $\Lambda(\mathfrak{a}) = \{\sigma_K(x); x \in \mathfrak{a}\}$ é um reticulado de dimensão n no espaço euclideano $\mathbb{R}^n$ (Proposição 2.21, Seção 2.6). Dizemos que $\Lambda(\mathfrak{a})$ é o reticulado associado a $\mathfrak{a}$.

Como definimos na Seção 2.5, a densidade de centro de $\Lambda(\mathfrak{a})$ é $\delta(\Lambda) = \dfrac{\rho^n}{v(\Lambda(\mathfrak{a}))}$, onde ρ é o raio de empacotamento e $\rho = \frac{1}{2}min\{|\sigma_K(x)|\,; x \in \mathfrak{a}^*\}$, onde $\mathfrak{a}^* = \mathfrak{a} - \{0\}$ (Seção 2.5). Temos também que o volume $v(\Lambda(\mathfrak{a}))$ é dado por $v(\sigma_K(\mathfrak{a})) = 2^{-s}\sqrt{|Disc(K)|}N(\mathfrak{a})$ (Proposição 2.21, Seção 2.6).

Assim,

$$\delta(\Lambda(\mathfrak{a})) = \frac{2^s\rho^n}{\sqrt{|Disc(K)|}N(\mathfrak{a})}$$

Observemos que $\rho^n = \frac{1}{2^n}min\{|\sigma_K(x)|^n\,; x \in \mathfrak{a}^*\}$, então substituindo obtemos:

$$\delta(\Lambda(\mathfrak{a})) = \frac{1}{2^{r+s}\sqrt{|Disc(K)|}} \cdot \frac{\underset{x\in\mathfrak{a}^*}{min}|\sigma_K(x)|^n}{N(\mathfrak{a})}. \tag{10}$$

De (8) e (9), concluímos:

$$\delta(\Lambda(\mathfrak{a})) \geq \frac{1}{2^{r+s}\sqrt{|Disc(K)|}} \cdot \frac{[2n]^{\frac{n}{2}} \cdot \left[\underset{x\in\mathfrak{a}^*}{min}\left|N_{K/\mathbb{Q}}(x)\right|\right]^n}{2^n N(\mathfrak{a})}.$$

Portanto,

$$\delta(\Lambda(\mathfrak{a})) \geq \frac{n^{\frac{n}{2}}}{2^{\frac{3r}{2}+2s}\sqrt{|Disc(K)|}} \cdot \frac{\underset{x\in\mathfrak{a}^*}{min}\left|N_{K/\mathbb{Q}}(x)\right|}{N(\mathfrak{a})} \tag{11}$$

Sejam $c_{\mathfrak{a}} \in H(K)$ a classe de ideal contendo $\mathfrak{a}$ e $\overline{c}_{\mathfrak{a}}$ o conjunto dos ideais inteiros de $\mathfrak{O}_K$ contidos em $c_{\mathfrak{a}}$. Para $x \in \mathfrak{a}$, podemos escrever: $< x >= \mathfrak{a} \cdot \mathfrak{b}_x$, onde $\mathfrak{b}_x$ é um ideal inteiro de $\mathfrak{O}_K$, pois como $< x > \subset \mathfrak{a}$, então $\mathfrak{a}$ divide $< x >$, além disso $\mathfrak{b}_x = \mathfrak{a}^{-1} \cdot < x >$.

Agora pela Proposição 2.17, Seção 2.6, $\left|N_{K/\mathbb{Q}}(x)\right| = N(< x >) = N(\mathfrak{a}) \cdot N(\mathfrak{b}_x)$. Além disso, a aplicação

$$\Phi : \mathfrak{a} \longrightarrow \overline{c_{\mathfrak{a}}^{-1}}$$

$$\Phi(x) =< x > \cdot \mathfrak{a}^{-1},$$

é bijetiva. Como $\mathfrak{b}_x = \mathfrak{a}^{-1} \cdot < x >$, então a classe de $\mathfrak{b}_x$ é a mesma classe de $\mathfrak{a}^{-1}$, isto é, $c_{\mathfrak{a}}^{-1}$.

Assim.

$$\frac{\underset{x\in\mathfrak{a}^*}{min}\left|N_{K/\mathbb{Q}}(x)\right|}{N(\mathfrak{a})} = \underset{\mathfrak{b}\in c_{\mathfrak{a}}^{-1}}{min}\frac{N(\mathfrak{a})N(\mathfrak{b})}{N(\mathfrak{a})} = \underset{\mathfrak{b}\in c_{\mathfrak{a}}^{-1}}{min}N(\mathfrak{b}). \tag{12}$$

De (11) e (12) temos:

$$\delta(\Lambda(\mathfrak{a})) \geq \frac{n^{\frac{n}{2}}}{2^{\frac{3r}{2}+2s}\sqrt{|Disc(K)|}} \cdot \min_{\mathfrak{b}\in c_{\mathfrak{a}}^{-1}} N(\mathfrak{b}) \tag{13}$$

Com a notação desta seção, podemos escrever a demonstração do seguinte:

Teorema 3.4 *(INTERLANDO, NOBREGA NETO, and NUNES) O grupo das classes de ideais $H(K)$ é finito.*

Demonstração: Provaremos por contradição.

Suponha que $H(K)$ possui uma infinidade de classes de ideais. Para um inteiro positivo i, definamos $\mathfrak{C}_i = \{c \in H(K); \min_{\mathfrak{b}\in\overline{c}} N(\mathfrak{b}) = i\}$.

Provaremos inicialmente que para cada $i \in \mathbb{N}$, $\mathfrak{C}_i$ é finito. Supondo que existe $i \in \mathbb{N}$ tal que $\mathfrak{C}_i$ tem cardinalidade infinita, então existe um ideal $\mathfrak{b}_j$ para cada classe c_j de $\mathfrak{C}_i$ tal que $N(\mathfrak{b}_j) = i$, ou seja, existe uma quantidade infinita de ideais com norma igual i, o que contradiz a Proposição 2.18 da Seção 2.6.

Agora provaremos que os $\mathfrak{C}_i$ são disjuntos. Suponha que $\mathfrak{C}_i \cap \mathfrak{C}_j \neq \emptyset$ para algum $i \neq j$. Então existe $c \in \mathfrak{C}_i \cap \mathfrak{C}_j$. Podemos supor $i < j$.

Como $c \in \mathfrak{C}_j$, então para todo $\mathfrak{a} \in \overline{c}, N(\mathfrak{a}) \geq j$. Por outro lado como $c \in \mathfrak{C}_i$ existe $\mathfrak{b} \in \overline{c}$ tal que $N(\mathfrak{b}) = i < j$, o que é uma contradição.

Assim $H(K) = \bigcup_{i=1}^{\infty} \mathfrak{C}_i$, onde os $\mathfrak{C}_i$ são disjuntos.

Finalmente, voltando a hipótese inicial de que $H(K)$ tem cardinalidade infinita. Então como cada $\mathfrak{C}_i$ é finito, para todo $M > 0$ existe $i \geq M$ tal que $\mathfrak{C}_i \neq \emptyset$, ou seja, existe $c \in H(K)$ tal que $\min_{\mathfrak{b}\in\overline{c}} N(\mathfrak{b}) \geq M$. Escolha $c \in \overline{c}^{-1}$. Da igualdade (10) segue:

$$\delta(\Lambda(\mathfrak{a})) \geq \frac{n^{\frac{n}{2}}}{2^{\frac{3r}{2}+2s}\sqrt{|Disc(K)|}} \cdot M.$$

Assim a densidade de centro do reticulado associado ao ideal inteiro pode ser arbitrariamente grande, o que é uma contradição. Portanto o grupo das classes $H(K)$ é finito.

□

4 IDEAIS, GRUPO DAS CLASSES E FORMA QUADRÁTICA

Dado um número primo ímpar p, aqui estudaremos as extensões abelianas de grau p dos racionais, as quais nos referimos por p-EG.

O que abordamos aqui são, em grande parte, um estímulo à busca de resultados mais profundos, mais abrangentes; mesmo que com as técnicas aqui desenvolvidas.

Iniciamos com uma seção destinada à descrição das p-EG e seu anel de inteiros algébricos. Por uma questão técnica consideramos apenas as p-EG em que o ideal $p\mathbb{Z}$ não se ramifica, isto é, as p-EG "suavemente ramificadas". Com esta restrição podemos explicitar uma base integral normal para o anel dos inteiros algébricos da p-EG, e isso será de grande importância nas seções seguintes.

Na Seção 2, abordaremos os ideais ramificados das p-EG. Para tais ideais daremos duas caracterizações, cada uma delas essencial para as seções seguintes. Ainda será dada uma caracterização dos ideais livres de quadrados que contém na sua fatoração apenas os ideais ramificados, o que também será de importância para as seções que se seguem.

A Seção 3 aborda o grupo das classes das p-EG. Será dada ênfase à p-parte do grupo das classes das p-EG e os resultados obtidos sugerem que muito mais ainda poderá ser obtido, em continuidade a este trabalho.

Ligações com o Corpo de Classes de Hilbert de L, ou até mesmo com o Corpo de Gênero de L não foram aqui tratados, mas os resultados aqui mostrados certamente servem de estímulo ao tema.

A Seção 4 é a parte mais destacada desta tese. Inicialmente aproveitamos um resultado recente que explicita a forma traço das p-EG. Os resultados aqui obtidos consistem em mostrar algumas propriedades da forma traço das p-EG e calcular a densidade de centro da representação geométrica de alguns ideais ordinários das p-EG e de alguns $\mathbb{Z}$-módulos determinados por equações modulares.

As ferramentas aqui apresentadas serão úteis no estudo da representação geométrica de outros $\mathbb{Z}-$módulos aqui não considerados e certamente terão valiosas contribuições para a Geometria de Números.

4.1 Descrição das p-extensões Galoisianas

Devido ao Teorema de Kronecker-Weber (Teorema 2.4, Seção 2.3), as p-EG estão contidas em corpos ciclotômicos, ou seja, dada uma extensão galoisiana L de $\mathbb{Q}$, de grau p, existe um número natural n de modo que L está contida em $\mathbb{Q}(\zeta_n)$.

É claro que existem infinitos inteiros n tais que L está contida em $\mathbb{Q}(\zeta_n)$, o menor deles é denominado o condutor de L. Na maioria das vezes, quando dizemos que L está contida em $\mathbb{Q}(\zeta_n)$, estamos admitindo que n é o condutor de L.

Desse modo podemos colocar um problema da seguinte forma: para quais inteiros n, existe uma p-EG contida em $\mathbb{Q}(\zeta_n)$?

A resposta para essa questão pode ser dada usando (BIRKHOFF, Teorema 7.2) e assegura que esses números são os inteiros n, para os quais p divide $\phi(n)$; ϕ a função de Euler.

A questão seguinte é sobre a quantidade de p-EG contidas em $\mathbb{Q}(\zeta_n)$. A referida quantidade é dada pela fórmula $\dfrac{p^s-1}{p-1}$, onde $n=\prod_{i=1}^{r} p_i^{a_i}$ é a decomposição de n como produto de primos e s é o número de primos p_i, para os quais p divide $\phi(p_i^{a_i})$. Tal resultado pode ser encontrado em (OLIVEIRA). Em relação a quantidade de p-EG, podemos perguntar: Qual é o menor divisor m, de n tal que $\mathbb{Q}(\zeta_m)$ contenha todas as p-EG que estão contidas em $\mathbb{Q}(\zeta_n)$?

A resposta a essa questão é dada por: $m=\prod_{i=1}^{s} p_i$, p_i primo tal que $p_i \equiv 1 \pmod p$, se p^2 não divide n, ou $m = p^2\prod_{i=1}^{s} p_i$, p_i primo tal que $p_i \equiv 1 \pmod p$, se p^2 divide n.

Queremos trabalhar com as extensões ciclotômicas que contenham p-EG. Assim, pelo que expomos acima, podemos sempre supor que

$$n=\prod_{i=1}^{r} p_i,\ \ p_i \equiv 1 \pmod p \ \text{ ou } \ n=p^2\prod_{i=1}^{r-1} p_i\ ,\ \ p_i \equiv 1 \pmod p.$$

Nosso interesse neste trabalho limita-se as p-EG contidas em $\mathbb{Q}(\zeta_n)$, onde p^2 não divide n.

Agora vamos caracterizar as p-EG e seus anéis de inteiros algébricos.

Inicialmente precisamos do seguinte resultado:

Lema 4.1 *Sejam $m>1$ um número inteiro, $m=\prod_{i=1}^{v} q_i^{b_i}$, sua fatoração em números primos e ζ_m uma raiz primitiva m-ésima da unidade. Então:*

$$Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m)=\begin{cases}(-1)^v, & \textit{se } m \textit{ é livre de quadrados;}\\ 0, & \textit{nos outros casos.}\end{cases}$$

Demonstração: Usaremos indução sobre v.

Inicialmente observamos (SAMUEL, Proposição 1, p.36) que se α é algébrico, então

$$irr(\alpha,\mathbb{Q})=x^n+(-1)Tr_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)x^{n-1}+\ldots+x+a_0,$$

onde $n=[\mathbb{Q}(\alpha):\mathbb{Q}]$.

Então se $v = 1$ temos $m = q^b$ e $irr(\zeta_m, \mathbb{Q})$ é o q^b-ésimo polinômio ciclotônico, ou seja, $irr(\zeta_m, \mathbb{Q}) = x^{(q-1)q^{b-1}} + x^{(q-2)q^{b-1}} + \ldots + x^{q^{b-1}} + 1$.

Assim, da observação acima, $Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = 0$ se $b > 1$ e $Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = -1$ se $b = 1$. Desse modo mostramos o lema para $v = 1$.

Finalmente, para provarmos o "passo de indução" usamos o Lema 2.2 da Seção 2.3, o qual diz: se $m = a \cdot b$, com $(a, b) = 1$, então:

$$Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = Tr_{\mathbb{Q}(\zeta_a)/\mathbb{Q}}(\zeta_a) \cdot Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b)$$

.

Assim, fazendo $a = q_1^{b_1}$ e $b = \frac{m}{a}$, conseguimos completar a demonstrção do lema.

□

Teorema 4.1 *Seja m um inteiro livre de quadrados. Se L é um subcorpo de $\mathbb{Q}(\zeta_m)$, então $L = \mathbb{Q}(t)$, onde $t = Tr_{\mathbb{Q}(\zeta_m)/L}(\zeta_m)$.*

Demonstração: Sabemos que se $t = Tr_{\mathbb{Q}(\zeta_m)/L}(\zeta_m)$, então

$$\mathbb{Q} \subset \mathbb{Q}(t) \subset L \subset \mathbb{Q}(\zeta_m).$$

Temos ainda, pelo Lema anterior, que: $Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = \pm 1$; então podemos escrever, usando a regra da transitividade do traço (Proposição 2.8, Seção 2.3):

$$\pm 1 = Tr_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\zeta_m) = Tr_{L/\mathbb{Q}}(t) = [L : \mathbb{Q}(t)] \cdot Tr_{\mathbb{Q}(t)/\mathbb{Q}}(t).$$

Como $Tr_{\mathbb{Q}(t)/\mathbb{Q}}(t) \in \mathbb{Z}$, concluímos que $[L : \mathbb{Q}(t)] = 1$, ou seja, $L = \mathbb{Q}(t)$.

□

Tendo em vista o interêsse desse texto no estudo da representação geométrica de ideais dos corpos que estamos considerando, se faz necessário o cálculo do seu discriminante.

Observamos que (WASHINGTON, Lema 2.2, p.10) nos afirma que o sinal do discriminante de um corpo de números K é $(-1)^s$, onde s é o número de pares de imersões complexas de K em $\mathbb{C}$. Quando K é uma extensão galoisiana, as imersões são todas reais ou todas complexas. Assim quando K é uma extensão galoisiana de $\mathbb{Q}$ de grau ímpar, então todas as imersões são reais e consequentemente o sinal do seu discriminante é positivo.

O resultado a seguir está registrado no Teorema 2.5, Seção 2.4.

Teorema 4.2 *Seja L uma p-EG de condutor n, então:*

$$|Disc(L)| = n^{p-1}.$$

Como consequência do Teorema acima, deduzimos que a $p-$EG de discriminante absoluto mínimo é o único subcorpo $\mathbb{Q}(\zeta_q)$ de grau p, onde q é o menor primo congruente à 1 módulo p e o discriminante de tal corpo é q^{p-1}.

Exemplo 4.1 *Para $p = 3$, a extensão galoisiana de $\mathbb{Q}$ de grau 3 com menor discriminante absoluto está contida em $\mathbb{Q}(\zeta_7)$ e seu discriminante é 7^2.*

Exemplo 4.2 *Para $p = 5$, a extensão galoisiana de $\mathbb{Q}$ de grau 5 com menor discriminante absoluto está contida em $\mathbb{Q}(\zeta_{11})$ e seu discriminante é 11^4.*

Exemplo 4.3 *Para $p = 7$, a extensão galoisiana de $\mathbb{Q}$ de grau 7 com menor discriminante absoluto está contida em $\mathbb{Q}(\zeta_{29})$ e seu discriminante é 29^6.*

A Proposição 2.5 da Seção 2.1, prova que $\left\{1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}\right\}$ é uma base integral para $\mathbb{Q}(\zeta_n)$. Nem sempre a base integral acima é mais adequada para uma determinada finalidade.

Lema 4.2 *Se n é um inteiro livre de quadrados então*
$\beta = \{\zeta_n^i, i = 1, \ldots, n; (i, n) = 1\}$ *é uma base integral de $\mathbb{Q}(\zeta_n)$.*

Demonstração: Consideremos $n = \prod_{i=1}^{s} p_i$. A demonstração será feita por indução sobre s. Se $s = 1$, o anel dos inteiros de $\mathbb{Q}(\zeta_{p_1})$ é $\mathbb{Z}[\zeta_{p_1}]$ (Proposição 2.5 da Seção 2.1), ou seja, $\left\{1, \zeta_{p_1}, \ldots, \zeta_{p_1}^{p_1-2}\right\}$ é uma base integral de $\mathbb{Q}(\zeta_{p_1})$. Mostremos que $\left\{\zeta_{p_1}, \ldots, \zeta_{p_1}^{p_1-1}\right\}$ é também uma base integral de $\mathbb{Q}(\zeta_{p_1})$.

Ora, $1 = -\zeta_{p_1} - \ldots - \zeta_{p_1}^{p_1-1}$, então $\{\zeta_{p_1}, \ldots, \zeta_{p_1}^{p_1-1}\}$ é base integral de $\mathbb{Q}(\zeta_{p_1})$, isto é, o lema vale para $s = 1$.

Suponhamos que $s > 1$ e escrevamos $n = p_1 \cdot \frac{n}{p_1}$.

Façamos, $K = \mathbb{Q}(\zeta_{p_1})$ e $E = \mathbb{Q}(\zeta_{\frac{n}{p_1}})$, podemos ver que $K \cdot E = \mathbb{Q}(\zeta_n)$.

De fato, $\zeta_n^{p_1} = \zeta_{\frac{n}{p_1}}$ e $\zeta_n^{\frac{n}{p_1}} = \zeta_{p_1}$, o que implica que E e K estão contidos em $\mathbb{Q}(\zeta_n)$ e assim $K \cdot E$ está contido em $\mathbb{Q}(\zeta_n)$.

Por outro lado, como $(p_1, \frac{n}{p_1}) = 1$, existem inteiros a e b tais que $a \cdot p_1 + b \cdot \frac{n}{p_1} = 1$. Assim $\zeta_n = \zeta_n^{a \cdot p_1 + b \cdot \frac{n}{p_1}} = \zeta_{\frac{n}{p_1}}^{a} \cdot \zeta_{p_1}^{b} \in K \cdot E$, o que nos dá que $\mathbb{Q}(\zeta_n)$ está contido em $K \cdot E$.

Pela Proposição 2.14 da Seção 2.4, temos

$$Disc(\mathbb{Q}(\zeta_n) = (-1)^{\frac{\phi(n)}{2}} \cdot \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{(p-1)}}}.$$

Usando a fórmula do discriminante, acima, vemos que $Disc(K)$ e $Disc(E)$ são relativamente primos pois na fatoração de $Disc(\mathbb{Q}(\zeta_n))$ só aparecem os primos que dividem n.

Temos ainda: $[K \cdot E : \mathbb{Q}] = \phi(p_1) \cdot \phi(\frac{n}{p_1}) = [K : \mathbb{Q}] \cdot [E : \mathbb{Q}]$.

Agora, pela Proposição 2.15 da Seção 2.4, o anel dos inteiros de $K \cdot E$ é o produto $\mathfrak{O}_K \cdot \mathfrak{O}_E$, ou seja, uma $\mathbb{Z}$-base de $\mathfrak{O}_{KE}$ é o produto de uma $\mathbb{Z}$-base de $\mathfrak{O}_K$ por uma $\mathbb{Z}$-base de $\mathfrak{O}_E$.

Para o nosso propósito as bases consideradas serão $\left\{\zeta_{p_1}^i, i = 1, \ldots, p_1 - 1\right\}$ e $\left\{\zeta_{\frac{n}{p_1}}^j, j = 1 \ldots, \frac{n}{p_1}; (j, \frac{n}{p_1}) = 1\right\}$, respectivamente $\mathbb{Z}$-base de $\mathfrak{O}_K$ e $\mathbb{Z}$-base de $\mathfrak{O}_E$. Então o produto dessas bases forma o conjunto

$$A = \left\{\zeta_{p_1}^i \cdot \zeta_{\frac{n}{p_1}}^j; i = 1, \ldots, p_1 - 1 \text{ e } j = 1, \ldots, \frac{n}{p_1}; (j, \frac{n}{p_1}) = 1\right\}.$$

Agora, $\zeta_{p_1}^i \cdot \zeta_{\frac{n}{p_1}}^j = \zeta_n^{i \cdot \frac{n}{p_1} + j \cdot p_1}$. Como i é primo com p_1 e j é primo com $\frac{n}{p_1}$, então $i \cdot \frac{n}{p_1} + j \cdot p_1$ é primo com n.

Por outro lado os $i \cdot \frac{n}{p_1} + j \cdot p_1$ são dois a dois distintos módulo n, o que nos permite concluir que

$$\left\{i \cdot \frac{n}{p_1} + j \cdot p_1; i = 1 \ldots, p_1 - 1 \text{ e } j = 1 \ldots, \frac{n}{p_1}; (j, \frac{n}{p_1}) = 1\right\}$$

é um sistema reduzido de restos módulo n, ou seja, $A = \{\zeta_n^k; (k, n) = 1\}$ e a demonstração está concluída.

□

Seja L uma extensão galoisiana finita de um corpo de números K. Dizemos que L/K possui uma base integral normal se existe um elemento $\alpha \in \mathfrak{O}_L$, de modo que o conjunto dos conjugados de α forma uma $\mathfrak{O}_K$-base de $\mathfrak{O}_L$.

Consideremos L uma extensão de grau primo contida em $\mathbb{Q}(\zeta_n)$. A existência de uma base integral normal para o seu anel de inteiros $\mathfrak{O}_L$ é garantida pelo seguinte:

Teorema 4.3 (Hilbert-Speiser) *(HILBERT, Teorema 132) Seja L uma extensão abeliana finita de $\mathbb{Q}$. Então $\mathfrak{O}_L$ possui uma base integral normal, se somente se, o condutor de L é livre de quadrados.*

O teorema acima contempla também o resultado a seguir.

Teorema 4.4 *Sejam n um inteiro livre de quadrados, $L \subset \mathbb{Q}(\zeta_n)$ e $t = Tr_{\mathbb{Q}(\zeta_m)/L}(\zeta_m)$. Então, $\{\sigma(t); \sigma \in Gal(L/\mathbb{Q})\}$ é uma base integral normal de $\mathfrak{O}_L$.*

Demonstração: Consideremos a seguinte notação, $K = \mathbb{Q}(\zeta_n)$, $G = Gal(K/\mathbb{Q}) = \{\sigma_k; k \in \{1, \ldots, n\}, (k, n) = 1\}$ $H = Gal(K/L) = \{\sigma_{i_1}, \ldots, \sigma_{i_u}\}$ e $Gal(L/\mathbb{Q}) = \{\sigma_{j_1}/L, \ldots, \sigma_{j_v}/L\}$.

Escreveremos esta demonstração por partes.

1. Mostraremos que $\{\zeta_n^{j_r i_s}; r \in \{1, \ldots, v\}, s \in \{1, \ldots, u\}\}$ é uma base integral de $\mathfrak{O}_K$.

Observemos que $\sigma_{j_r} \cdot \sigma_{i_s}$, $r = 1, \ldots, v$ e $s = 1, \ldots, u$, são dois a dois distintos.

Assim,

$$\{\sigma_{j_r} \cdot \sigma_{i_s}; r = 1, \ldots, v; s = 1, \ldots, u\} = \{\sigma_{j_r \cdot i_s}; r = 1, \ldots, v; s = 1, \ldots, u\} = \{\sigma_k; k \in \{1, \ldots, n\}, (k, n) =$$

Então $\{\zeta_n^{j_r i_s}; r \in \{1, \ldots, v\}, s \in \{1, \ldots, u\}\} = \{\zeta_n^i; i = 1, \ldots, n; (i, n) = 1\}$.

Portanto pelo Lema 4.2, segue que $\{\zeta_n^{j_r i_s}; r \in \{1, \ldots, v\}, s \in \{1, \ldots, u\}\}$ é uma base integral de $\mathfrak{O}_K$.

2. Consideremos os $\mathbb{Z}$-módulos $A_1, \ldots, A_v$, onde A_l é o $\mathbb{Z}$-módulo gerado por: $\{\zeta_n^{j_l i_1}, \zeta_n^{j_l i_2}, \ldots, \zeta_n^{j_l i_u}\}$.

Então teremos: $A_1 = (\zeta_n^{j_1 i_1}, \zeta_n^{j_1 i_2}, \ldots, \zeta_n^{j_1 i_u}); \ldots; A_v = (\zeta_n^{j_v i_1}, \zeta_n^{j_v i_2}, \ldots, \zeta_n^{j_v i_u})$.

Pelo modo como definimos A_l, $l = 1, \ldots, v$ e como $\{\zeta_n^{j_r i_s}; r \in \{1, \ldots, v\}, s \in \{1, \ldots, u\}\}$ é uma base integral de $\mathfrak{O}_K = \mathbb{Z}[\zeta_n]$, então todo elemento $x \in \mathfrak{O}_K$, pode ser escrito como $x = x_1 + \ldots + x_v$, $x_i \in A_i$.

3. O grupo H age transitivamente na base que apresentamos para A_l, para cada $l = 1, \ldots, v$, isto é:

I. A imagem dessa base por um elemento de H, nos dá a mesma base.

II. Dados dois elementos dessa base de A_l, existe um elemento de H, que leva um no outro.

Para mostrar I e II, podemos supor, sem perda de generalidade, que $A_l = A_1$. Para mostrar I, podemos supor também que um elemento $\sigma \in H$, seja $\sigma = \sigma_{i_1}$. Escolhemos $\{\zeta_n^{j_1 i_1}, \zeta_n^{j_1 i_2}, \ldots, \zeta_n^{j_1 i_u}\}$ como base para A_1. Denotemos por A o conjunto das imagens, por σ_{i_1}, dos elementos dessa base, ou seja,

$$A = \{\sigma_{i_1}(\zeta_n^{j_1 i_1}), \sigma_{i_1}(\zeta_n^{j_1 i_2}), \ldots, \sigma_{i_1}(\zeta_n^{j_1 i_u})\}.$$

Vemos facilmente que podemos escrever:

$$A = \{\sigma_{i_1} \cdot \sigma_{i_1}(\zeta_n^{j_1}), \sigma_{i_1} \cdot \sigma_{i_2}(\zeta_n^{j_1}), \ldots, \sigma_{i_1} \cdot \sigma_{i_u}(\zeta_n^{j_1})\}$$

.

Como $\{\sigma_{i_1} \cdot \sigma_{i_1}, \sigma_{i_1} \cdot \sigma_{i_2}, \ldots, \sigma_{i_1} \cdot \sigma_{i_u}\} = H$, segue que

$$A = \{\sigma_{i_1}(\zeta_n^{j_1}), \sigma_{i_2}(\zeta_n^{j_1}), \ldots, \sigma_{i_u}(\zeta_n^{j_1})\} = \{\zeta_n^{j_1 i_1}, \zeta_n^{j_1 i_2}, \ldots, \zeta_n^{j_1 i_u}\}.$$

Para mostrar II, podemos considerar, sem perda de generalidade, $\zeta_n^{j_1 i_1}$ e $\zeta_n^{j_1 i_2}$, dois elementos dessa base de A_1.

É fácil ver que $\sigma_{i_1}^{-1} \cdot \sigma_{i_2}$ é um elemento de H tal que $\sigma_{i_1}^{-1} \cdot \sigma_{i_2}(\zeta_n^{j_1 i_1}) = \zeta_n^{j_1 i_2}$. Assim terminamos a demonstração de 3.

4. Para concluirmos a demonstração do Teorema, provaremos que dado $x \in \mathfrak{O}_L$, podemos escrever: $x = b_1\sigma_{j_1}(t) + \ldots + b_v\sigma_{j_v}(t)$ e assim $\{\sigma_{j_1}(t), \ldots, \sigma_{j_v}(t)\}$ é uma base integral normal de $\mathfrak{O}_L$, ou seja, $\{\sigma(t); \sigma \in Gal(L/\mathbb{Q})\}$ é uma base integral normal de $\mathfrak{O}_L$.

Para começar escrevemos $x \in \mathfrak{O}_L$ como em 2, $x = x_1 + \ldots + x_v$, $x_i \in A_i$ e $x_1 = a_1\zeta_n^{j_1 i_1} + a_2\zeta_n^{j_1 i_2} + \ldots + a_u\zeta_n^{j_1 i_u}$. Vamos provar que $a_1 = a_2 = \ldots = a_u$. Para isso, sem perda de generalidade, podemos provar que $a_1 = a_2$ e as demais igualdades seguem o mesmo tratamento.

Sabemos que $\sigma = \sigma_{i_1}^{-1} \cdot \sigma_{i_2} \in H$ e que $x_1 = \sigma(x_1)$.

Assim,

$$a_1\zeta_n^{j_1 i_1} + a_2\zeta_n^{j_1 i_2} + \ldots + a_u\zeta_n^{j_1 i_u} = a_1\zeta_n^{j_1 i_2} + a_2\zeta_n^{j_1 i_2 i_1^{-1} i_2} + \ldots + a_u\zeta_n^{j_1 i_u i_1^{-1} i_2}.$$

Pela unicidade da representação, concluímos que $a_1 = a_2$. Portanto

$$x_1 = a_1(\zeta_n^{j_1 i_1} + \zeta_n^{j_1 i_2} + \ldots + \zeta_n^{j_1 i_u}).$$

De modo análogo, tal conclusão se aplica à $x_2, \ldots, x_v$, ou seja, podemos escrever

$$x = b_1(\zeta_n^{j_1 i_1} + \ldots + \zeta_n^{j_1 i_u}) + \ldots + b_v(\zeta_n^{j_v i_1} + \ldots + \zeta_n^{j_v i_u}).$$

Daí podemos escrever: $x = b_1\sigma_{j_1}(\zeta_n^{i_1} + \ldots + \zeta_n^{i_u}) + \ldots + b_v\sigma_{j_v}(\zeta_n^{i_1} + \ldots + \zeta_n^{i_u})$.

Mas, $t = \zeta_n^{i_1} + \ldots + \zeta_n^{i_u}$, logo

$$x = b_1\sigma_{j_1}(t) + \ldots + b_v\sigma_{j_v}(t).$$

□

No nosso caso a extensão é de grau primo e assim temos:

Corolário 4.1 *Sejam L uma p-EG de condutor n, $H = Gal(L/\mathbb{Q})$ e θ um gerador de H. Então $\beta = \{t, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$ é uma base integral normal de $\mathfrak{O}_L$.*

4.2 Extensões de Ideais nas p-Extensões Galoisianas

Nesta seção estudaremos os ideais ramificados em $\mathfrak{O}_L$. Começamos enumerando e identificando esses ideais. Em seguida daremos uma caracterização dos elementos desses ideais e apresentaremos uma $\mathbb{Z}$-base para cada ideal ramificado.

Consideremos L uma p-EG e q um número primo. Sejam $Q_1, \ldots, Q_g$ os ideais primos de $\mathfrak{O}_L$ que estão acima de $q\mathbb{Z}$, de modo que $q\mathfrak{O}_L = Q_1^{l_1} \ldots Q_g^{l_g}$.

Como vimos na Proposição 2.15 Seção 2.6, os índices de ramificação são todos iguais, e o chamamos e, bem como os graus de inércia são todos iguais e o chamamos de f.

Então a igualdade fundamental se expressa como $p = e \cdot f \cdot g$.

Isso nos dá três possibilidades. Em cada uma delas temos e, f ou g é igual a p e as outras iguais a 1. Isto é:

Se $g = p$, então $e = f = 1$, assim $q\mathfrak{O}_L = Q_1 \ldots Q_p$; dizemos que $q\mathbb{Z}$ se decompõe completamente.

Se $f = p$, então $e = g = 1$, assim $q\mathfrak{O}_L = Q_1$; dizemos que $q\mathbb{Z}$ é inerte.

Finalmente, se $e = p$, então $f = g = 1$, assim $q\mathfrak{O}_L = Q_1^p$, dizemos que $q\mathbb{Z}$ se ramifica totalmente ou que Q_1 é totalmente ramificado.

No nosso caso L é uma extensão galoisiana de grau primo, logo os ideais primos de $\mathfrak{O}_L$ ou são inertes, ou se decompõem completamente, ou são totalmente ramificados.

No nosso estudo estamos interessados nos primos que se ramificam completamente em $\mathfrak{O}_L$, ou seja, nos ideais primos de $\mathfrak{O}_L$ totalmente ramificados.

O resultado seguinte nos diz quais os primos que se ramificam em $\mathfrak{O}_L$.

Teorema 4.5 *(SAMUEL, Teorema 1, p.74) Sejam L um corpo de números e $q \in \mathbb{Z}$ um primo, então $q\mathbb{Z}$ se ramifica em $\mathfrak{O}_L$, se e somente se, q divide* $\mathrm{Disc}(L)$.

Observemos que o nosso interesse é o caso em que o condutor de L é $n = p_1 \ldots p_s$, onde $p_1, \ldots, p_s$ são primos distintos. Logo deduzimos que os únicos primos que se ramificam em $\mathfrak{O}_L$ são $p_1, \ldots, p_s$.

Consideremos então $p_i \cdot \mathfrak{O}_L = \mathfrak{p}_i^p$.

Sabemos que $\left[\dfrac{\mathfrak{O}_L}{\mathfrak{p}_i} : \dfrac{\mathbb{Z}}{p_i\mathbb{Z}}\right] = 1$. Assim identificamos $\dfrac{\mathfrak{O}_L}{\mathfrak{p}_i}$ com $\dfrac{\mathbb{Z}}{p_i\mathbb{Z}}$. Visto que $\{\ 0, 1, \ldots, p_i - 1\}$ é um sistema completo de resíduos módulo $p_i\mathbb{Z}$, então $\{\ 0, 1, \ldots, p_i - 1\}$ também é um sistema completo de resíduos módulo $\mathfrak{p}_i$, ou seja, dado $x \in \mathfrak{O}_L$, existe um inteiro $k \in \{\ 0, 1, \ldots, p_i - 1\}$ tal que $x \in k + \mathfrak{p}_i$.

Além disso, pelo (MARCUS, Teorema 23, p.70) como $\mathfrak{p}_i$ é totalmente ramificado, dado qualquer elemento $\sigma \in Gal(L/\mathbb{Q})$, $\sigma(\mathfrak{p}_i) = \mathfrak{p}_i$; assim se $x \in k + \mathfrak{p}_i$, então $\sigma(x) \in \sigma(k + \mathfrak{p}_i) = k + \mathfrak{p}_i$. Isso nos mostra que se $x \in k + \mathfrak{p}_i$ então todos os conjugados de x estão na mesma classe lateral de $\mathfrak{p}_i$. Aplicando este princípio para t, digamos $t \in c_i + \mathfrak{p}_i$, isto é, se $t \equiv c_i \pmod{\mathfrak{p}_i}$, então usando a notação do Corolário 4.1 da Seção 4.1, $\theta^j(t) \equiv c_i \pmod{\mathfrak{p}_i}$, θ o gerador de $Gal(L/\mathbb{Q})$. Pelo mesmo Corolário 4.1 podemos escrever $x = \sum_{j=0}^{p-1} a_j\theta^j(t)$, assim $x \equiv c_i \sum_{j=0}^{p-1} a_j \pmod{\mathfrak{p}_i}$ e então $x \in \mathfrak{p}_i$ se e somente se,

$c_i \sum_{j=0}^{p-1} a_j \in \mathfrak{p}_i$. Visto que $\mathfrak{p}_i$ é um ideal primo, $c_i \in \mathfrak{p}_i$ ou $\sum_{j=0}^{p-1} a_j \in \mathfrak{p}_i$. Mas se $c_i \in \mathfrak{p}_i$ então todo $x \in \mathfrak{O}_L$ está em $\mathfrak{p}_i$, o que não é verdade. Portanto temos provado o seguinte:

Proposição 4.1 *Sejam L uma p-EG de condutor $n = p_1 \cdot \ldots \cdot p_s$, onde $p_1, \ldots, p_s$ são números primos distintos e $\mathfrak{p}_i$ é o ideal primo de $\mathfrak{O}_L$ de modo que $p_i\mathfrak{O}_L = \mathfrak{p}_i^p$. Se $x = \sum_{j=0}^{p-1} a_j\theta^j(t) \in \mathfrak{O}_L$, então $x \in \mathfrak{p}_i$, se e somente se, $\sum_{j=0}^{p-1} a_j \equiv 0 \pmod{p_i}$.*

Observação: Como na demonstração acima, $t \equiv c_i \pmod{\mathfrak{p}_i}$, para algum $c_i \in \{0, 1, \ldots, p_i - 1\}$. Daí $\theta^j(t) \equiv c_i \pmod{\mathfrak{p}_i}$, para todo $j \in \{0, \ldots, p-1\}$. Assim $t + \theta(t) + \ldots + \theta^{p-1}(t) \equiv pc_i \pmod{\mathfrak{p}_i}$. Mas pela Lema 4.1, para o caso em que $n = p_1 \cdot \ldots \cdot p_s$,

$$t + \theta(t) + \ldots + \theta^{p-1}(t) = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/Q}(\zeta_n) = (-1)^s.$$

Logo,

$$pc_i \equiv (-1)^s \pmod{\mathfrak{p}_i} \Leftrightarrow [(-1)^s p] \cdot c_i \equiv 1 \pmod{\mathfrak{p}_i}.$$

Dessa observação podemos calcular c_i.

Exemplo 4.4 *Tomamos $p = 3$, $n = 7 \cdot 13$, $p_1 = 7$ e $p_2 = 13$. Então, como $s = 2$, temos: $3c_1 \equiv 1 \pmod 7$, então $c_1 = 5$ e $3c_2 \equiv 1 \pmod{13}$, daqui $c_2 = 9$. Assim, $t \equiv 5 \pmod{\mathfrak{p}_1}$ e $t \equiv 9 \pmod{\mathfrak{p}_2}$.*

Nas mesmas condições da Proposição anterior, exibiremos agora uma $\mathbb{Z}$-base para $\mathfrak{p}_i$, no seguinte:

Teorema 4.6 *Considere as hipóteses da Proposição 4.1. Então*

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

é uma $\mathbb{Z}$-base de $\mathfrak{p}_i$.

Demonstração:

Vamos mostrar que o $\mathbb{Z}$-módulo gerado por γ_i é o ideal $\mathfrak{p}_i$. Inicialmente, cada elemento de γ_i, escrito como combinação linear dos elementos de $\beta = \{t, \theta(t), \ldots, \theta^{p-1}(t)\}$, tem a soma dos coeficientes igual a zero ou p_i, logo cada elemento de γ_i, pertence a $\mathfrak{p}_i$.

Assim, qualquer combinação linear dos elementos de γ_i, pertence a $\mathfrak{p}_i$. Portanto o $\mathbb{Z}$-módulo gerado por γ_i está contido em $\mathfrak{p}_i$.

Reciprocamente, dado $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathfrak{p}_i$, devemos mostrar que x é uma combinação linear dos elementos de γ_i.

Podemos escrever:

$$x = \sum_{i=0}^{p-1} a_i\theta^i(t) = \sum_{i=0}^{p-1} a_i(\theta^i(t) - t) + (\sum_{i=0}^{p-1} a_i) \cdot t.$$

Assim x pertence ao $\mathbb{Z}$-módulo gerado por γ_i, pois da Proposição 4.1 $\sum_{i=0}^{p-1} a_i \equiv 0 \pmod{p_i}$. Portanto γ_i é uma $\mathbb{Z}$-base de $\mathfrak{p}_i$.

□

Obteremos agora uma $\mathbb{Z}$-base para um produto de ideais ramificados de $\mathfrak{O}_L$: $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$.

Para isso usaremos o seguinte:

Lema 4.3 *(SAMUEL, Lema 1, p.18) Sejam A um anel comutativo, $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A tais que $\mathfrak{a} + \mathfrak{b} = A$, então*

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$

Corolário 4.2 *Sejam $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ ideais primos não nulos de $\mathfrak{O}_L$, $r > 1$. Então*

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r.$$

Demonstração: Será feita por indução sobre r. Como em $\mathfrak{O}_L$, todo ideal primo não nulo é maximal, para $r = 2$ segue que $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{O}_L$, logo o Lema 4.3 nos dá $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2$. Assim se $r = 2$, o Corolário está provado.

Se $r > 2$, suponha que o resultado do Corolário vale para $s = 2, \ldots, r-1$. Então fazendo $\mathfrak{a} = \mathfrak{p}_1 \cdot, \ldots, \cdot\mathfrak{p}_{r-1}$ e $\mathfrak{b} = \mathfrak{p}_r$, obtemos pelo Lema 4.3 e pela hipótese de indução que

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r.$$

Portanto, por indução, o resultado é válido para todo $r > 1$.

□

Corolário 4.3 *Sejam $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ ideais primos ramificados de $\mathfrak{O}_L$ e $x = \sum_{i=0}^{p-1} a_i\theta^i(t)$. Então $x \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, se e somente se, $\sum_{i=0}^{p-1} a_i \in p_1 \cdot \ldots \cdot p_r\mathbb{Z}$.*

Demonstração:

Pelo Corolário 4.2, $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$, logo $x \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, se e somente se, $x \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$. Pela Proposição 4.1, $x \in \mathfrak{p}_j$, se e somente se, $\sum_{i=0}^{p-1} a_i \in p_j\mathbb{Z}$. Finalmente, $p_1\mathbb{Z} \cap \ldots \cap p_r\mathbb{Z} = p_1 \cdot \ldots \cdot p_r\mathbb{Z}$ e o resultado está provado.

□

Corolário 4.4 *Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideais primos ramificados de $\mathfrak{O}_L$. Então*

$$\gamma = \{t - \theta(t), t - \theta^2(t), \ldots, t - \theta^{p-1}(t), p_1 \cdot \ldots \cdot p_r t\}$$

é uma $\mathbb{Z}$-base para $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$.

Demonstração: Pelo Teorema 4.6, $t - \theta^i(t) \in \mathfrak{p}_j$, para quaisquer $j = 1, \ldots, r$ e $i = 1, \ldots, p-1$; logo pelo Corolário 4.2,

$$t - \theta^i(t) \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

e portanto o $\mathbb{Z}$-módulo gerado por γ está contido em $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$. Agora seja $x = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$.

Podemos escrever,

$$x = \sum_{i=0}^{p-1} a_i \theta^i(t) = \sum_{i=0}^{p-1} a_i (\theta^i(t) - t) + (\sum_{i=0}^{p-1} a_i) \cdot t.$$

Visto que $\theta^i(t) - t \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, então

$$\left(\sum_{i=0}^{p-1} a_i \right) \cdot t \in \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r,$$

ou seja, $\left(\sum_{i=0}^{p-1} a_i \right) \cdot t \in \mathfrak{p}_j$ para $j = 1, \ldots, r$, mas $t \notin \mathfrak{p}_j$, para $j = 1, \ldots, r$, pois se $t \in \mathfrak{p}_j$ então $\theta^i(t) \in \mathfrak{p}_j$ e $\mathfrak{O}_L$ está contido em $\mathfrak{p}_j$, o que não pode acontecer. Portanto $\sum_{i=0}^{p-1} a_i \in \mathfrak{p}_j \cap \mathbb{Z} = p_j \mathbb{Z}$.

Logo $\sum_{i=0}^{p-1} a_i \in p_1 \cdot \ldots \cdot p_r \mathbb{Z}$, ou seja, x está no $\mathbb{Z}$-módulo gerado por γ.

□

Sabemos que $p_i\mathbb{Z}$ se ramifica completamente, isto é, existe $\mathfrak{p}_i$, ideal primo de $\mathfrak{O}_L$, tal que $p_i \mathfrak{O}_L = \mathfrak{p}_i^p$.

Se $\mathfrak{p}_i$ é principal, digamos $\mathfrak{p}_i = (\alpha_i)$, então

$$p_i = \left| \frac{\mathfrak{O}_L}{\mathfrak{p}_i} \right| = N(\mathfrak{p}_i) = \left| N_{L/\mathbb{Q}}(\alpha_i) \right|.$$

Sem perda de generalidade, podemos supor $N_{L/\mathbb{Q}}(\alpha_i) = p_i$, pois se $N_{L/\mathbb{Q}}(\alpha_i) = -p_i$, podemos trocar α_i por $-\alpha_i$.

Mas $\alpha_i \notin \mathfrak{p}_j$, para $j \neq i$ pois caso contrário todos os múltiplos de α_i estariam em $\mathfrak{p}_j$, isto é, $\mathfrak{p}_i$ estaria contido em $\mathfrak{p}_j$, o que não é verdade.

Assim $\alpha_i \equiv c_j \pmod{\mathfrak{p}_j}$, onde $c_j \in \{1, \ldots, p_j - 1\}$.

Portanto,

$$p_i = N_{L/\mathbb{Q}}(\alpha_i) = \prod_{k=0}^{p-1} \theta^k(\alpha_i) \equiv c_j^p \pmod{\mathfrak{p}_j}.$$

Então teremos $p_i \equiv c_j^p \pmod{p_j}$ para $j \neq i$, ou seja, $x^p \equiv p_i \pmod{p_j}$ possui solução para $j \in \{1, \ldots, s\}, j \neq i$. Com isso temos demonstrado a seguinte:

Proposição 4.2 *Sejam L uma p-EG de condutor $n = p_1 \cdot \ldots \cdot p_s$, onde $p_1, \ldots, p_s$ são primos distintos e $\mathfrak{p}_i$ o ideal primo de $\mathfrak{O}_L$ tal que $p_i\mathfrak{O}_L = \mathfrak{p}_i^p$. Se $\mathfrak{p}_i$ é principal, então existe solução para cada uma das congruências $x^p \equiv p_i \pmod{p_j}$, $j \in \{1, \ldots, s\}, j \neq i$.*

Exemplo 4.5 *Considere $p = 3$ e $n = 7 \cdot 13$. Denotando $\mathfrak{p}_1$ o ideal primo de $\mathfrak{O}_L$ tal que $7\mathfrak{O}_L = \mathfrak{p}_1^3$. Pela Proposição 4.2 como $x^3 \equiv 7 \pmod{13}$ não possui solução, então $\mathfrak{p}_1$ não é principal.*

Por outro lado, nada podemos afirmar sobre a principalidade do ideal primo que está acima de $13\mathbb{Z}$, pois $x^3 \equiv 13 \pmod{7}$ possui solução.

Exemplo 4.6 *Considere ainda $p = 3$ e $n = 7 \cdot 13 \cdot 19$. Seja $\mathfrak{p}_1$ o ideal primo de $\mathfrak{O}_L$ tal que $7\mathfrak{O}_L = \mathfrak{p}_1^3$. Como $x^3 \equiv 7 \pmod{13}$ não possui solução, então pela Proposição 4.2, $\mathfrak{p}_1$ não é principal.*

Considere o primo $\mathfrak{p}_2$ tal que $13\mathfrak{O}_L = \mathfrak{p}_2^3$. Como $x^3 \equiv 13 \pmod{19}$ não possui solução, então pela Proposição 4.2, $\mathfrak{p}_2$ não é principal.

Agora seja $\mathfrak{p}_3$ o primo tal que $19\mathfrak{O}_L = \mathfrak{p}_3^3$. Como $x^3 \equiv 19 \pmod{7}$ não possui solução, pela Proposição 4.2, $\mathfrak{p}_3$ não é principal.

□

4.3 A p-parte do grupo das classes

O grupo das classes de um corpo de números, desempenha papel central na Teoria dos Corpos de Classes, através das suas ligações com o grupo das unidades, extensões não ramificadas e outros tópicos da Teoria dos Números. A determinação da estrutura do grupo das classes $H(F)$ de um corpo de números F pode ser uma grande tarefa nesse que é um dos problemas importantes na Teoria dos Números Computacional.

A p-parte, ou o subgrupo p-Sylow, de $H(F)$ é importante por exemplo na Teoria de Iwasawa, curvas elíticas e também por muito tempo foi de grande interêsse para o Último Teorema de Fermat, visto o famoso critério de Kummer que diz: se $p \nmid |H(\mathbb{Q}(\zeta_p))|$ então $x^p + y^p = z^p$ não tem solução inteira não trivial, conforme (WASHINGTON, Teorema 1.1, p.1).

Nesta Seção focaremos o grupo das classes $H(L)$ de uma p-EG. Podemos escrever, $H(L) = H(L)_p \oplus H(L)_{\neq p}$, onde $H(L)_p$ é a p-parte de $H(L)$ e $H(L)_{\neq p}$ a parte prima com p de $H(L)$. A cardinalidade de $H(L)$, isto é, o número de classes de L, é denotado por $h(L)$. Aqui nos propomos a apresentar um método aritmético para caracterizar $H(L)_p$.

Conhecemos por (LEOPOLDT) que $p \nmid h(L)$, se e somente se, exatamente um número primo se ramifica em L. Conner e Hurrelbrink (CONNER and HURRELBRINK) provaram que se $p \mid\mid h(L)$, então exatamente dois números primos se ramificam em L. Reciprocamente, por (CONNER and HURRELBRINK, Teorema 2.69) se exatamente dois primos p_1 e p_2 se ramificam e $p \neq p_1, p_2$ então $p \mid\mid H(L)$, se e somente se, ou p_1 não é uma p-ésima potência módulo p_2 ou p_2 não é uma p-ésima potência módulo p_1. Recordamos que um número inteiro a é um p-ésimo resído módulo um número primo q, se a não é divisível por q e a congruência $x^p \equiv a \pmod{q}$ possui solução (GAUSS). Pelo critério de Euler, (USPENSKY and HEASLET) a é um p-ésimo resíduo módulo q, se e somente se, $a^{\frac{(q-1)}{p}} \equiv 1 \pmod{q}$. Denotamos $(a|q)_p = 1$, se a é um p-ésimo resíduo módulo q, caso contrário denotamos $(a|q)_p = -1$. Se $\mathfrak{a}$ é um ideal fracionário de $\mathfrak{O}_L$, $[\mathfrak{a}]$ denota a classe de equivalência de $\mathfrak{a}$ em $\mathfrak{O}_L$. Recordamos que L é uma p-EG de condutor $n = p_1 \dots p_s$, onde $p_1, \dots, p_s$ são primos distintos, $p_i \equiv 1 \pmod{p}$, $i = 1, \dots, s$.

Observamos que, com o conceito de p-ésimo resíduo módulo q, a Proposição 4.2 da Seção 4.2 pode ser reescrita da seguinte forma:

Sejam L uma p-EG de condutor $n = p_1 \cdot \ldots \cdot p_s$, onde $p_1, \dots, p_s$ são primos distintos e $\mathfrak{p}_i$ o ideal primo de $\mathfrak{O}_L$ tal que $p_i \mathfrak{O}_L = \mathfrak{p}_i^p$, $i \in \{1, \dots, s\}$. Se $\mathfrak{p}_i$ é principal, então p_i é um p-ésimo resíduo módulo p_j, para $j \in \{1, \dots, s\}, j \neq i$.

Corolário 4.5 *Com a notação acima, se $(p_i|p_j)_p = -1$ para $i, j \in \{1, \dots, s\}$ com $i \neq j$, então $\langle [\mathfrak{p}_i] \rangle \cong (\mathbb{Z}/p\mathbb{Z})$ e consequentemente, $H(L)_p$ é não trivial.*

Exemplo 4.7 *Sejam $p = 3$, $p_1 = 7$, $p_2 = 13$, e L uma p-EG de condutor $n = 91$. Por (CONNER and HURRELBRINK, Teorema 2.69) citado no início desta Seção, como $3 || h(L)$ então $|H(L)_3| = 3$. Do Corolário 4.5, $\mathfrak{p}_7$ é não principal pois $(7|13)_3 = -1$. Assim, $H(L)_3 = \langle [\mathfrak{p}_7] \rangle$.*

A Tabela 1 lista $H(L)_3$, onde L é uma p-EG de condutor $n = p_1 p_2$, $p_1, p_2 \in \{7, 13, 19, 31, 37, 43\}$, $p_1 \neq p_2$, $p = 3$. Em todos os casos em que $|H(L)_3| = 3$.

n	p_1	p_2	$(p_1\|p_2)_3$	$(p_2\|p_1)_3$	$H(L)_3$
91	7	13	-1	1	$\langle[\mathfrak{p}_7]\rangle$
133	7	19	1	-1	$\langle[\mathfrak{p}_{19}]\rangle$
217	7	31	-1	-1	$\langle[\mathfrak{p}_7]\rangle$
259	7	37	-1	-1	$\langle[\mathfrak{p}_7]\rangle$
301	7	43	-1	1	$\langle[\mathfrak{p}_7]\rangle$
247	13	19	-1	-1	$\langle[\mathfrak{p}_{13}]\rangle$
403	13	31	-1	1	$\langle[\mathfrak{p}_{13}]\rangle$
481	13	37	-1	-1	$\langle[\mathfrak{p}_{13}]\rangle$
559	13	43	-1	-1	$\langle[\mathfrak{p}_{13}]\rangle$
589	19	31	-1	1	$\langle[\mathfrak{p}_{19}]\rangle$
703	19	37	-1	1	$\langle[\mathfrak{p}_{19}]\rangle$
817	19	43	-1	-1	$\langle[\mathfrak{p}_{19}]\rangle$
1147	31	37	1	-1	$\langle[\mathfrak{p}_{37}]\rangle$
1333	31	43	-1	-1	$\langle[\mathfrak{p}_{31}]\rangle$
1591	37	43	-1	1	$\langle[\mathfrak{p}_{37}]\rangle$

Tabela 1: $H(L)_p$ Para certos corpos cúbicos de condutor p_1p_2

Exemplo 4.8 *Sejam $p = 3$, $p_1 = 7$, $p_2 = 13$, $p_3 = 19$, $n = p_1p_2p_3 = 1729$ e L uma p-EG de condutor n. Como $(7|13)_3 = (13|19)_3 = (19|7)_3 = -1$, então $\mathfrak{p}_7$, $\mathfrak{p}_{13}$ e $\mathfrak{p}_{19}$, são todos não principais. Assim 3 divide $h(L)$.*

No Exemplo 4.8, se nós pudermos provar que $\langle[\mathfrak{p}_7]\rangle \neq \langle[\mathfrak{p}_{13}]\rangle$, poderemos concluir que $H(L)_3$ tem um subgrupo isomorfo a $(\mathbb{Z}/3\mathbb{Z})^2$ e então que $h(L)$ é um múltiplo de 3^2. Isto será dado depois da prova do Corolário 4.6.

Teorema 4.7 *(WAERDEN, p.184) Sejam $\mathfrak{I}$ um ideal fracionário principal de $\mathfrak{O}_L$ e $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ ideais primos de $\mathfrak{O}_L$. Então $\mathfrak{I}$ pode ser escrito como o quociente $\dfrac{(\alpha)}{(\beta)}$ de dois ideais inteiros principais, tais que nenhum dos ideais $\mathfrak{q}_i$, $i = 1, \ldots, r$ divide (α) e divide (β).*

Corolário 4.6 *Sejam $\mathfrak{a} = \mathfrak{p}_{i_1}^{a_1}, \ldots, \mathfrak{p}_{i_u}^{a_u}$ e $\mathfrak{b} = \mathfrak{p}_{j_1}^{b_1}, \ldots, \mathfrak{p}_{j_v}^{b_v}$, onde $1 \leq r < i_1 < \ldots < i_u \leq s$ e $1 \leq r < j_1 < \ldots < j_v \leq s$. Se $[\mathfrak{a}] = [\mathfrak{b}]$ então*

$$\left(\frac{\prod_{\ell=1}^{u} p_{i_\ell}^{a_\ell}}{\prod_{\ell=1}^{v} p_{j_\ell}^{b_\ell}} \,\middle|\, p_k\right)_p = 1 \quad \text{for } k = 1, \ldots, r.$$

Demonstração: Considere o ideal $\mathfrak{I} = \left(\prod_{\ell=1}^{u} \mathfrak{p}_{i_\ell}^{a_\ell}\right)\left(\prod_{\ell=1}^{v} \mathfrak{p}_{j_\ell}^{b_\ell}\right)^{-1}$. Como $[\mathfrak{a}] = [\mathfrak{b}]$ então $\mathfrak{I}$ é principal e $\mathfrak{I} = ((a)/(b))$, onde $a, b \in \mathfrak{O}_L$ e $b \neq 0$. Pelo Teorema 4.7 podemos supor que nem a nem b pertence algum dos ideais em $\{\mathfrak{p}_k | k = 1, \ldots, r\}$. Por outro lado,

aplicando a norma a ambos os lados de

$$\prod_{\ell=1}^{u} \mathfrak{p}_{i_\ell}^{a_\ell} = ((a)/(b)) \cdot \prod_{\ell=1}^{v} \mathfrak{p}_{j_\ell}^{b_\ell},$$

obtemos

$$\prod_{\ell=1}^{u} p_{i_\ell}^{a_\ell} = N_{L/\mathbb{Q}}\,(a/b) \cdot \prod_{\ell=1}^{v} p_{j_\ell}^{b_\ell},$$

Para cada $1 \leq k \leq r$, existe $c_k \in \{1, \ldots, p_k - 1\}$ tal que $a/b \equiv c_k \pmod{p_k}$ e assim $\theta^j(a/b) \equiv c_k \pmod{\mathfrak{p}_k}$ para $j = 1, \ldots, p-1$. Como $N_{L/\mathbb{Q}}\,(a/b) = N_{L/\mathbb{Q}}(a/b)$, segue que

$$N_{L/\mathbb{Q}}(a/b) = \prod_{j=1}^{p-1} \theta^j(a/b) \equiv c_k^p \pmod{\mathfrak{p}},$$

isto é,

$$\prod_{\ell=1}^{u} p_{i_\ell}^{a_\ell} \equiv c_k^p \cdot \prod_{\ell=1}^{v} p_{j_\ell}^{b_\ell} \pmod{p_k}.$$

Com isso, o corolário está provado.

□

Exemplo 4.9 *(continuação do Exemplo 4.8) Vimos no Exemplo 4.8 que* $\mathfrak{p}_7$, $\mathfrak{p}_{13}$ *e* $\mathfrak{p}_{19}$, *não são principais, então*

(i) $\left(\frac{13}{7} \mid 19\right)_3 = (10 \mid 19)_3 = -1$, *assim pelo Corolário 4.6, concluímos que* $[\mathfrak{p}_7] \neq [\mathfrak{p}_{13}]$.

(ii) $\left(\frac{13^2}{7} \;\middle|\; 19\right)_3 = (16 \mid 19)_3 = -1$, *assim pelo Corolário 4.6, concluímos que* $[\mathfrak{p}_7] \neq [\mathfrak{p}_{13}]^2$.

Usando (i) e (ii) concluímos que $3^2 \mid h(L)$. Ademais, $\langle [\mathfrak{p}_7] \rangle \times \langle [\mathfrak{p}_{13}] \rangle$ é um subgrupo de $H(L)_p$ isomorfo à $(\mathbb{Z}/3\mathbb{Z})^2$.

O próximo teorema é o principal resultado desta seção. Satisfeitas as hipóteses, ele nos dá um método para determinar subgrupos de $H(L)_p$.

Teorema 4.8 *Com a notação acima, sejam* $p_1, \ldots, p_r$, $r \leq s$, *tais que*

$$(p_i|p_k)_p = 1 \quad e \quad (p_{k-1}|p_k)_p = -1$$

para $k = 2, \ldots, r$ *e* $i = 1, \ldots, k-2$. *Então*

$$\langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_{r-1}] \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{r-1}.$$

Demonstração: Usaremos indução sobre r. O caso $r = 2$ está no Corolário 4.5, assim consideraremos agora $2 < r < s$. Supondo que

$$(p_i \mid p_k)_p = 1 \quad \text{e } (p_{k-1} \mid p_k)_p = -1 \quad \text{para } k = 2, \ldots, r+1,\ i = 1, \ldots, k-2$$

mostraremos que

$$\langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_{r-1}], [\mathfrak{p}_r] \rangle \cong (\mathbb{Z}/p\mathbb{Z})^r.$$

Para justificar esse isomorfismo, basta mostrar que $[\mathfrak{p}_r] \notin \langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_{r-1}] \rangle$, uma vez que pelo Corolário 4.5, $\langle [\mathfrak{p}_r] \rangle \cong (\mathbb{Z}/p\mathbb{Z})$. Supondo, por contradição, que $[\mathfrak{p}_r] = [\mathfrak{p}_1]^{e_1} \cdot \ldots \cdot [\mathfrak{p}_{r-1}]^{e_{r-1}}$, para alguma escolha de inteiros $e_1, \ldots, e_{r-1}$, isto é, $[\mathfrak{p}_r] = [\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{r-1}^{e_{r-1}}]$. Pelo Corolário 4.6,

$$N\left(\frac{\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_{r-1}^{e_{r-1}}}{\mathfrak{p}_r}\right) \equiv c_{r+1}^p \pmod{\mathfrak{p}_{r+1}},$$

isto é,

$$\prod_{i=1}^{r-1} p_i^{e_i} \equiv c_{r+1}^p \cdot p_{k-1} \pmod{p_{r+1}},$$

para algum $c_{r+1} \in \{1, \ldots, p_{r+1} - 1\}$. Como $(p_i \mid p_k)_3 = 1$ para $i = 1, \ldots, r+1$, essa última congruência implica que $(p_r \mid p_{r+1})_p = 1$, o que é uma contradição. Assim, $[\mathfrak{p}_r] \notin \langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_{r-1}] \rangle$, como queríamos.

□

Exemplo 4.10 *Sejam* $p = 3$, $p_1 = 7$, $p_2 = 13$, $p_3 = 19$, $p_4 = 223$, $p_5 = 373$, $n = p_1 \cdot \ldots \cdot p_5 = 143816491$ *e* L *uma* p*-EG de condutor* n*. Temos o seguinte:*

(i) $(p_1 \mid p_2)_3 = -1$*;*

(ii) $(p_1 \mid p_3)_3 = 1$, $(p_2 \mid p_3)_3 = -1$*;*

(iii) $(p_1 \mid p_4)_3 = (p_2 \mid p_4)_3 = 1$, $(p_3 \mid p_4)_3 = -1$*;*

(iv) $(p_1 \mid p_5)_3 = (p_2 \mid p_5)_3 = (p_3 \mid p_5)_3 = 1$, $(p_4 \mid p_5)_3 = -1$

Pelo Teorema 4.8, $H(L)_3$ possui um subgrupo gerado por $[\mathfrak{p}_7]$, $[\mathfrak{p}_{13}]$, $[\mathfrak{p}_{19}]$ e $[\mathfrak{p}_{223}]$. Assim, $h(L)$ é um múltiplo de 3^4.

Exemplo 4.11 *Sejam* $p = 5$, $p_1 = 11$, $p_2 = 31$, $p_3 = 61$, $p_4 = 191$, $p_5 = 541$, $n = p_1 \cdot \ldots \cdot p_5 = 2149388131$ *e* L *uma* p*-EG de condutor* n*. Temos o seguinte:*

(i) $(p_1 \mid p_2)_5 = -1$*;*

(ii) $(p_1 \mid p_3)_5 = 1$, $(p_2 \mid p_3)_5 = -1$*;*

(iii) $(p_1 \mid p_4)_5 = (p_2 \mid p_4)_5 = 1$, $(p_3 \mid p_4)_5 = -1$;

(iv) $(p_1 \mid p_5)_5 = (p_2 \mid p_5)_5 = (p_3 \mid p_5)_5 = 1$, $(p_4 \mid p_5)_5 = -1$

Pelo Teorema 4.8, $H(L)_5$ possui um subgrupo gerado por $[\mathfrak{p}_{11}]$, $[\mathfrak{p}_{31}]$, $[\mathfrak{p}_{61}]$ e $[\mathfrak{p}_{191}]$. Assim, $h(L)$ é um múltiplo de 5^4.

Concluímos dizendo que apresentamos nesta Seção, um método para determinar subgrupos da p-parte do grupo das classes de uma p-EG de condutor $n = p_1 \cdot \ldots \cdot p_s$, p_i primo, $p_i \equiv 1 \pmod{p}$, $i = 1, \ldots, s$. Sua eficácia depende da suposição de p_i ser um p-ésimo resíduo módulo p_j para $j = 1, \ldots, i-2$, mas não ser um p-ésimo resíduo módulo p_{i-1} para $i = 2, \ldots, r$. Apesar desta limitação o método nos permitiu resolver vários casos, que de outra forma, poderia ser computacionalmente trabalhoso. Portanto a técnica aqui apresentada poderia ser aplicada antes desses algorítmos, reduzindo assim seus 'custos' operacionais. As limitações da técnica apresentada nos é desconhecida e será assunto para futuras pesquisas. Finalmente, no caso em que dois primos se ramificam, nenhum dos quais igual à p, o (CONNER and HURRELBRINK, Teorema 2.69), ao qual nós nos referimos no início desta Seção, estabelece que $p \mid\mid h(L)$, contanto que um dos dois, $(p_1 \mid p_2)_p$ ou $(p_2 \mid p_1)_p$, não seja 1. Nossos exemplos mostraram que quando $r \geq 3$, ou seja, quando três ou mais primos se ramificam, e certas condições de 'residualidade' se verificam, então uma potência de p, maior do que 1, divide $h(L)$. Determinar exatamente essa potência é um assunto a ser estudado.

4.4 A Forma Traço

Assim como em todo este capítulo, p é um número primo ímpar, n é um produto de primos congruentes a 1 módulo p e L é uma p-EG de condutor n.

Dados σ_L o homomorfismo de Minkowski e $x \in \mathfrak{O}_L$, o quadrado do comprimento de $\sigma_L(x)$ é dado por

$$|\sigma_L(x)|^2 = \sum_{i=0}^{p-1} \sigma_i(x)^2 = \sum_{i=0}^{p-1} \sigma_i(x^2) = \mathrm{Tr}_{L/\mathbb{Q}}(x^2).$$

Tendo em vista o cálculo do raio de empacotamento associado à representação geométrica de um $\mathbb{Z}$-módulo contido em $\mathfrak{O}_L$, precisamos encontrar o menor valor não nulo que a forma quadrática $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$ assume, na condição de x pertencer a tal $\mathbb{Z}$-módulo.

Usando o Teorema das Médias, obtemos:

$$\frac{|\sigma_L(x)|^2}{p} = \frac{|\sigma_1(x)|^2 + \cdots + |\sigma_p(x)|^2}{p} \geq \sqrt[p]{\prod_{i=1}^{p} \sigma_i(x^2)} = \sqrt[p]{N_{L/\mathbb{Q}}(x)^2}.$$

Assim, $|\sigma_L(x)|^2 \geq p\sqrt[p]{N_{L/\mathbb{Q}}(x)^2} \geq p$, ou seja, a norma de qualquer vetor não nulo $\sigma_L(x), x \in \mathfrak{O}_L$, é pelo menos $\sqrt{p}$.

Observamos que em $\mathfrak{O}_L$, temos um elemento para o qual essa forma quadrática assume o valor p. Por exemplo, em $x = 1$, pois $\mathrm{Tr}_{L/\mathbb{Q}}(1^2) = p$. Assim concluimos que o menor valor da forma quadrática, $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$, x em $\mathfrak{O}_L$, x diferente de zero, é p e assim o raio de empacotamento da representação geométrica de $\mathfrak{O}_L$ é

$$\rho = \frac{1}{2}\min\left\{|\sigma_L(x)|, x \in \mathfrak{O}_L, x \neq 0\right\} = \frac{\sqrt{p}}{2}.$$

Por outro lado, sabemos do Teorema 4.4 que $\beta = \{t, \theta(t), \theta^2(t), \ldots, \theta^{p-1}(t)\}$ é uma base de $\mathfrak{O}_L$, onde θ é um gerador do grupo $Gal(L/\mathbb{Q})$. Então um elemento x de $\mathfrak{O}_L$ se escreve da forma,

$$x = \sum_{i=0}^{p-1} a_i\theta^i(t), a_i \in \mathbb{Z}. \tag{14}$$

Escrevendo x como em (14), veremos em seguida um resultado que se revelará de grande importância para o nosso propósito de minimizar a forma quadrática a que nos referimos.

Teorema 4.9 *(OLIVEIRA) Sejam θ um gerador do grupo $Gal(L/\mathbb{Q})$ e $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/L}(\zeta_n)$. Considere $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathfrak{O}_L$, então*

$$\mathrm{Tr}_{L/\mathbb{Q}}(x^2) = n\left(\sum_{i=0}^{p-1} a_i^2\right) + \frac{1-n}{p}\left(\sum_{i=0}^{p-1} a_i\right)^2. \tag{15}$$

Com o objetivo de obter os principais resultados desta Secção, enunciaremos e demonstraremos alguns resultados auxiliares:

Dado $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$, definimos o conteúdo de a e denotamos por $cont(a)$, o número: $cont(a) = \sum_{i=0}^{p-1} a_i$ e definimos o quadrado da norma de a, denotada por $\|a\|^2$ como o número $\sum_{i=0}^{p-1} a_i^2$.

De modo análogo, dado $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathfrak{O}_L$, definimos conteúdo de x e denotamos $cont(x)$, o número: $cont(x) = \sum_{i=0}^{p-1} a_i$.

Ainda com o objetivo de simplificar, dado um inteiro S, seja

$$E_S = \{x \in \mathfrak{O}_L, cont(x) = S\}.$$

De modo análogo, seja

$$G_S = \{a \in \mathbb{Z}^p, cont(a) = S\}.$$

Podemos ver que para $x = \sum_{i=0}^{p-1} a_i \theta^i(t) \in \mathfrak{O}_L$,

$$\mathrm{Tr}_{L/\mathbb{Q}}(x^2) = n\left(\sum_{i=0}^{p-1} a_i^2\right) + \frac{1-n}{p} S^2 \tag{16}$$

e portanto o menor valor para $\mathrm{Tr}_{L/\mathbb{Q}}(x^2)$, $x \in E_S$, é atingido quando a expressão $\sum_{i=0}^{p-1} a_i^2$ atingir o menor valor.

Com o objetivo de encontrar esse mínimo, definimos as funções τ_{ij}, para $i, j \in \{0, \ldots, p-1\}$:

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

Dessa definição observamos que se $a, b \in \mathbb{Z}^p$, são tais que $\tau_{ij}(a) = b$, então $cont(a) = cont(b)$. Por outro lado, dados $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$ e $b = (b_0, \ldots, b_{p-1}) \in \mathbb{Z}^p$, tais que $cont(a) = cont(b)$, podemos obter uma composição de funções τ_{ij}, que leva a em b. De fato se a e b têm as coordenadas correspondentes iguais, isto é, se $a_i = b_i$ para cada $i \in \{0, 1, 2, \ldots, p-1\}$, basta tomar a composta de τ_{ij} com τ_{ji} que nos dá a identidade.

Suponha então que $a \neq b$ e seja r o menor índice tal que $a_r \neq b_r$. Podemos supor $a_r > b_r$. É claro que $r < p-1$ pois se $r = p-1$, como $cont(a) = cont(b)$, teríamos $a_r = b_r$.

Aplicando $\tau_{r,r+1}$, $(a_r - b_r)$ vêzes na p-upla a, obtemos uma p-upla com o mesmo conteúdo de a mas com as r primeiras coordenadas coincidindo com as r primeiras coordenadas da p-upla b.

Desse modo, podemos repetir o processo até obter uma p-upla tal que as $(p-1)$ primeiras coordenadas coincidam com as $(p-1)$ primeiras coordenadas da p-upla b.

Agora, como essa última p-upla tem o mesmo conteúdo que a p-upla a, concluímos que a p-ésima coordenada dessa p-upla também coincide com a p-ésima coorde-

nada da p-upla b.

O seguinte lema contribuirá para o resultado que buscamos:

Lema 4.4 *Sejam $a = (a_0, \ldots, a_{p-1})$ e $b = (b_0, \cdots, b_{p-1})$ dois elementos de $\mathbb{Z}^p$ tais que $\tau_{ij}(a) = b$. Então: $\|a\|^2 > \|b\|^2$, se e somente se, $a_i - a_j > 1$.*

Demonstração:

Nas condições acima,

$$\|a\|^2 > \|b\|^2, \qquad \text{se e somente se,} \quad a_i^2 + a_j^2 > (a_i - 1)^2 + (a_j - 1)^2.$$

Assim,

$$\|a\|^2 > \|b\|^2, \qquad \text{se e somente se,} \quad a_i - a_j > 1.$$

□

A relação em $\mathbb{Z}^p$: "Ter o mesmo conteúdo" é de equivalência e a classe de equivalência é dada por

$$O(a) = \{b \in \mathbb{Z}^p; cont(a) = cont(b)\}. \tag{17}$$

e chamamos de órbita de a.

De modo semelhante ao que fizemos em (4), definimos para $x = \sum_{i=0}^{p-1} a_i \theta^i(t)$, $a_i \in \mathbb{Z}$,

$$O(x) = \{y \in \mathfrak{O}_L, cont(y) = cont(x)\}.$$

Portanto, pelo Lema 4.4 e pelo que expusemos acima, provamos o seguinte:

Lema 4.5 *Se $a \in \mathbb{Z}^p$, $b \in O(a)$ é tal que $\|b\|^2$ é mínimo, então duas entradas de b, não podem diferir em mais que uma unidade.*

Esse Lema nos permite obter o seguinte resultado:

Lema 4.6 *Sejam $a = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}^p$ tal que $S = cont(a)$, seja um inteiro não negativo. Então dentre todas as p-uplas pertencentes à $O(a)$, as que têm menor norma possuem r entradas iguais à $q + 1$, $0 \leq r < p$, e as demais iguais à q, onde q e r são, respectivamente, o quociente e o resto na divisão de S por p. Essa norma mínima é dada por: $\sqrt{pq^2 + 2rq + r}$ e a unicidade de q e r se deve ao algorítmo da divisão.*

Demonstração:

A demonstração da primeira parte decorre do Lema 4.5. Para finalizar, observamos que uma p-upla nessas condições é uma p-upla cujas coordenadas são uma

permutação das coordenadas da p-upla

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

Como $cont(a) = S$ então $pq + r = S$, $0 \leq r < p$, ou seja, q e r são o quociente e o resto da divisão de S por p.

Agora, para terminar

$$\|(q+1,\ldots,q+1,q,\ldots,q)\|^2 = r\,(q+1)^2 + (p-r)\,q^2 = pq^2 + 2rq + r.$$

□

O Lema 4.6, acima demonstrado e a expressão (16) nos permitem deduzir o seguinte:

Teorema 4.10 *Dado um inteiro $m > 0$, $m = pq + r$, $0 \leq r < p$, o mínimo da forma quadrática em (2) para $x \in E_m$, é dado por*

$$F(q,r) = \min\left\{\mathrm{Tr}_{L/\mathbb{Q}}(y^2), cont(y) = pq + r\right\} = pq^2 + 2rq + nr + \frac{1-n}{p}r^2.$$

Podemos escrever: $F(q,r) = \dfrac{1}{p}\{(pq+r)^2 + nr(p-r)\}$, ou seja,

$$F(m) = \frac{1}{p}\{m^2 + nr(p-r)\}. \tag{18}$$

Considere o $\mathbb{Z}$-módulo de posto p, definido por:

$$\mathfrak{M}_m = \{x \in \mathfrak{O}_L; \mathrm{cont}(x) \equiv 0 \pmod{m}\}.$$

Podemos ver que $\mathfrak{M}_m = \bigcup_{i\in\mathbb{N}} E_{im}$.

O resultado seguinte nos mostra o menor valor da Forma Traço em $\mathfrak{M}_m$.

Teorema 4.11 *Com a notação anterior, dado $m > 0$, então*

$$\min\left\{\mathrm{Tr}_{L/\mathbb{Q}}(x^2); x \in \mathfrak{M}_n, x \neq 0\right\} = \min\left\{2n, F(m), F(2m), \ldots, F(pm)\right\}. \tag{19}$$

Demonstração: Seja $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathfrak{M}_n$. Se $x \in E_0$, então

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

e para $x \neq 0$ tal expressão atinge mínimo em $x = (1,-1,0,\ldots,0)$, ou uma permutação dessa p-upla. Assim, o menor valor da Forma

Traço é $2n$.

Para $x \in E_{im}, i > 0$, a expressão do menor valor da Forma Traço é dada por $F(im)$.

Se $m \equiv 0 \pmod{p}$, isto é, se $r = 0$, então $F(im) = \dfrac{(im)^2}{p}$, que é uma função crescente e seu mínimo é atingido em $i = 1$, ou seja,

$$\min\left\{\mathrm{Tr}_{L/\mathbb{Q}}(x^2); x \in \mathfrak{M}_m, x \neq 0\right\} = \min\left\{2n, \frac{m^2}{p}\right\}\right\}.$$

Por outro lado, se $m \not\equiv 0 \pmod{p}$, podemos ver que $F((p+i)m) > F(im)$, logo

$$\min\left\{2n, F(im); i \in \mathbb{N}\right\}\} = \min\left\{2n, F(im); i = 1, \ldots, p\right\}\}.$$

□

Para a representação geométrica do $\mathbb{Z}$-módulo $\mathfrak{M}_m$, como vimos na Proposição 2.20 da Seção 2.6, o raio de empacotamento e o volume são respectivamente:

$$\rho = \frac{1}{2}\min\left\{\sqrt{\mathrm{Tr}_{L/Q}(x^2)}; x \in \mathfrak{M}_m, x \neq 0\right\} \tag{20}$$

$$v(\sigma_L(\mathfrak{M}_m)) = |Disc(K)|^{\frac{1}{2}}\,[\mathfrak{O}_L : \mathfrak{M}_m]. \tag{21}$$

Lema 4.7 *Com as notações anteriores temos que* $[\mathfrak{O}_L : \mathfrak{M}_m] = m$.

Demonstração: Sejam $t = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/L}(\zeta_n) \in \mathfrak{O}_L$ e $\overline{x}$ a classe de x em $\mathfrak{O}_L$ módulo $\mathfrak{M}_m$.

Vamos mostrar que as classes $\overline{0}, \overline{t}, \overline{2t}, \ldots, \overline{(m-1)t}$, são distintas e em seguida que dado $x = \sum_{i=0}^{p-1} a_i\theta^i(t) \in \mathfrak{O}_L$, então x está em uma dessas classes.

Suponhamos que $\overline{it} = \overline{jt}$ para $0 \leq i, j \leq (m-1)$. Isso é equivalente à $\overline{(i-j)t} = \overline{0}$, ou seja, $i - j \equiv 0 \pmod{m}$ e assim, como $0 \leq i, j \leq (m-1)$, $i = j$; portanto as classes $\overline{0}, \overline{t}, \overline{2t}, \ldots, \overline{(m-1)t}$ são distintas.

Para concluir, podemos escrever

$$x = \sum_{i=0}^{p-1} a_i\theta^i(t) = \sum_{i=0}^{p-1} a_i t + \sum_{i=1}^{p-1} a_i(\theta^i(t) - t),$$

como $\sum_{i=0}^{p-1} a_i(\theta^i(t) - t) \in \mathfrak{M}_m$, então $x \equiv \sum_{i=0}^{p-1} a_i t \pmod{\mathfrak{M}_m}$, ou seja, $x \equiv \left(\sum_{i=0}^{p-1} a_i\right) t \pmod{\mathfrak{M}_m}$. Como podemos escrever $\sum_{i=0}^{p-1} a_i = ms + r$, $0 \leq r \leq (m-1)$, então $\overline{x} = \overline{rt}$, ou seja, $x \in \overline{rt}$ e a demonstração está concluída.

□

Do Teorema 4.2 da Seção 4.1, temos que $Disc(L) = n^{p-1}$ e por (3) na Seção

2.6, temos que a densidade de centro é:

$$\delta = \delta(\sigma_L(\mathfrak{M}_m)) = \frac{\rho^p}{n^{\frac{p-1}{2}} \cdot m} \tag{22}$$

Com essa fórmula da densidade de centro analisaremos o caso em que $m \equiv 0 \pmod{p}$, para ver que avaliação podemos fazer da densidade de centro nesse caso e em seguida analisaremos $m \not\equiv 0 \pmod{p}$.

Supondo que $m \equiv 0 \pmod{p}$; $m = pq$, então $\rho = \min\left\{\frac{\sqrt{2n}}{2}, \frac{\sqrt{pq^2}}{2}\right\}$.

Se $\frac{\sqrt{pq^2}}{2} \geq \frac{\sqrt{2n}}{2}$ então $\rho = \frac{\sqrt{2n}}{2}$, ou seja, $m^2 \geq 2pn$ e a densidade é

$$\delta = \frac{\left(\frac{\sqrt{2n}}{2}\right)^p}{n^{\frac{p-1}{2}} \cdot m}.$$

Simplificando essa fração obtemos:

$$\delta = \frac{n^{\frac{1}{2}}}{2^{\frac{p}{2}} \cdot m}.$$

O valor de m que maximiza δ é o menor inteiro múltiplo de p e maior que $\sqrt{2pn}$. Assim deduzimos que

$$\delta^* = \frac{n^{\frac{1}{2}}}{2^{\frac{p}{2}} \cdot \sqrt{2pn}} = \frac{1}{2^{\frac{p+1}{2}} \cdot \sqrt{p}}$$

é um limite superior para δ.

Usando os resultados obtidos, ver Tabela 2, a cota superior que obtemos para os primos, 3, 5 e 7.

p	cota	recorde	%
3	$\frac{1}{4\sqrt{3}}$	$\frac{1}{4\sqrt{2}}$	81
5	$\frac{1}{8\sqrt{5}}$	$\frac{1}{8\sqrt{2}}$	63
7	$\frac{1}{16\sqrt{7}}$	$\frac{1}{16}$	38

Tabela 2: Cota superior para δ - dimensões 3, 5 e 7

Suponhamos ainda, $m \equiv 0 \pmod{p}$ mas $\rho = \frac{\sqrt{pq^2}}{2}$, então $m^2 \leq 2pn$ e

$$\delta = \frac{\left(\frac{\sqrt{pq^2}}{2}\right)^p}{n^{\frac{p-1}{2}} \cdot m} = \frac{m^{p-1}}{2^p \cdot p^{\frac{p}{2}} \cdot n^{\frac{p-1}{2}}}.$$

Tendo em vista essa expressão para δ, concluímos que o valor de m que maximiza δ, é o maior inteiro múltiplo de p e menor do que $\sqrt{2pn}$.

Assim um limite superior para δ é

$$\delta^* = \frac{\left(\sqrt{2pn}\right)^{p-1}}{2^p \cdot p^{\frac{p}{2}} \cdot n^{\frac{p-1}{2}}} = \frac{1}{2^{\frac{p+1}{2}} \cdot \sqrt{p}}.$$

Verificamos que é o mesmo resultado obtido quando supomos $\delta = \frac{\sqrt{2n}}{2}$.

Com as considerações acima, concluímos que quando $m \equiv 0 \pmod{p}$ os reticulados obtidos não são densos.

Doravante, suponhamos que $m \not\equiv 0 \pmod{p}$, $m > p$.

Do Teorema 4.11, temos:

$$\rho = \min\left\{\frac{\sqrt{2n}}{2}, \frac{\sqrt{F(m)}}{2}, \frac{\sqrt{F(2m)}}{2}, \ldots, \frac{\sqrt{F(pm)}}{2}\right\} \tag{23}$$

Recordamos aqui a expressão que foi dada em (5):

$$F(m) = \frac{1}{p}\{m^2 + nr(p-r)\}.$$

Para que ρ seja $\frac{\sqrt{2n}}{2}$, devemos ter $2n < F(im)$, onde $i = 1, \ldots, p$; isso significa que

$$\frac{m^2}{n} > \frac{2p - r_i(p-r_i)}{i^2}$$

onde r_i é o resto da divisão de im por p.

Lema 4.8 *Seja* $w = max\left\{\frac{2p - r_i(p-r_i)}{i^2}, i = 1, \ldots, p\right\}$ *e suponhamos* $\frac{m^2}{n} \geq w$.

Então $\rho = \frac{\sqrt{2n}}{2}$ *e* $\delta^* = \frac{1}{2^{\frac{p}{2}}\sqrt{w}}$, *onde* δ^* *é a cota superior para* δ.

A demonstração desse Lema decorre da substituição dos parâmetros na expressão da densidade de centro.

Supondo $p = 3$, temos para $m \equiv 1 \pmod{3}$,

$$w = \max\left\{\frac{6-2}{1}, \frac{6-2}{4}, \frac{6}{9}\right\} = 4.$$

Observamos que para $m \equiv 2 \pmod{3}$ obtemos o mesmo valor para w. Assim $\frac{m^2}{n} > 4$, ou seja, $\left(\frac{m}{2}\right)^2 > n$.

Consideramos então $m \equiv 1 \pmod 3$ e convém tomar m da forma, $m = 6\lambda + 1$, logo

$$\left(\frac{6\lambda+1}{2}\right)^2 = 9\lambda^2 + 3\lambda + 0,25.$$

O inteiro congruente a 1 módulo 3 e mais próximo de $\left(\frac{6\lambda+1}{2}\right)^2$ é $9\lambda^2 + 3\lambda + 1$. Se tal número for primo estaremos otimizando o nosso problema para $p = 3$.

Na tabela 3, a seguir, mostramos os resultados obtidos para densidade de centro de $\sigma_L(\mathfrak{M}_m)$. Podemos comparar com o valor recorde para a dimensão 3.

λ	$2n$	m	$F(m)$	raio	δ	record	%
1	26	7	25	2,50	0,17170330	0,17677670	97,1301%
2	86	13	85	4,61	0,17523732	0,17677670	99,1292%
3	182	19	181	6,73	0,17604872	0,17677670	99,5882%
4	314	25	313	8,85	0,17635463	0,17677670	99,7612%
5	482	31	481	10,97	0,17650170	0,17677670	99,8444%
7	926	43	925	15,21	0,17663354	0,17677670	99,9190%
8	1202	49	1201	17,33	0,17666641	0,17677670	99,9376%
30	16382	181	16381	63,99	0,17676860	0,17677670	99,9954%
63	71822	379	71821	134,00	0,17677485	0,17677670	99,9990%

Tabela 3: Densidade de centro de $\sigma_L(\mathfrak{M}_m)$, em dimensão 3

Agora consideremos $p = 5$. Se $m \equiv 1 \pmod 5$ teremos

$$w = \max\left\{\frac{10-4}{1}, \frac{10-6}{4}, \frac{10-6}{9}\right\} = 6.$$

Se $m \equiv 2 \pmod 5$ teremos $w = 4$. Assim convém considerar $m \equiv 2 \pmod 5$, m da forma $m = 10\lambda + 7$ e portanto

$$\left(\frac{m}{2}\right)^2 = \left(\frac{10\lambda+7}{2}\right)^2 = 25\lambda^2 + 35\lambda + 12 + 0,25.$$

Então consideramos o inteiro mais próximo de $25\lambda^2 + 35\lambda + 12 + 0,25$ que seja congruente a 1, módulo 5. Se $25\lambda^2 + 35\lambda + 11$ for primo, teremos um reticulado denso.

Na Tabela 4 a seguir, mostramos os resultados obtidos para densidade de centro de $\sigma_L(\mathfrak{M}_m)$ podemos comparar com o valor recorde para a dimensão 5.

λ	$2n$	m	$F(m)$	raio	δ	record	%
1	142	17	143	5,96	0,08762041	0,08838835	99,1312%
2	362	27	363	9,51	0,08808471	0,08838835	99,6565%
3	682	37	683	13,06	0,08822679	0,08838835	99,8172%
4	1102	47	1103	16,60	0,08828826	0,08838835	99,8868%
5	1622	57	1623	20,14	0,08832031	0,08838835	99,9230%
20	21422	207	21423	73,18	0,08838319	0,08838835	99,9942%
60	184222	607	184223	214,61	0,08838775	0,08838835	99,9993%
78	309682	787	309683	278,25	0,08838799	0,08838835	99,9996%

Tabela 4: Densidade de centro de $\sigma_L(\mathfrak{M}_m)$, em dimensão 5

Por fim, consideremos $p = 7$. Se $m \equiv 1 \pmod 7$, teremos $w = 8$; se $m \equiv 2 \pmod 7$, $w = 4$; se $m \equiv 3 \pmod 7$ então $w = 2$. Assim, convém considerar $m \equiv 3 \pmod 7$, m ímpar. Neste caso tomamos $m = 14\lambda + 3$. Então tomamos o inteiro mais próximo de $98\lambda^2 + 42\lambda + 4 + 0,5$, que seja congruente a 1, módulo 7. Se $n = 98\lambda^2 + 42\lambda + 1$ for primo, estaremos otimizando o problema para $p = 7$.

Na Tabela 5 a seguir, mostramos os resultados obtidos para densidade de centro de $\sigma_L(\mathfrak{M}_m)$ podemos comparar com o valor recorde para a dimensão 7.

λ	$2n$	m	$F(m)$	raio	δ	record	%
1	282	17	283	8,40	0,06173844	0,06250000	98,7815%
3	2018	45	2019	22,46	0,06239188	0,06250000	99,8270%
4	3474	59	3475	29,47	0,06243713	0,06250000	99,8994%
9	16634	129	16635	64,49	0,06248685	0,06250000	99,9790%
21	88202	297	88203	148,49	0,06249752	0,06250000	99,9960%
72	1022114	1011	1022115	505,50	0,06249979	0,06250000	99,9997%

Tabela 5: Densidade de centro de $\sigma_L(\mathfrak{M}_m)$ em dimensão 7

5 CONCLUSÃO

Neste trabalho apresentamos valiosas contribuições nas aplicações da Geometria de Números.

A relação natural entre o grupo das classes de um corpo de números e as representações geométricas de certos $\mathbb{Z}$-módulos contidos no anel de inteiros, nos direcionaram à resultados originais na estrutura do grupo das classes. A Seção 3.2 é dedicada à uma demonstração original sobre a finitude do grupo das classes. Na Seção 4.3 apresentamos resultados inéditos sobre a p-parte do grupo das classes, conhecendo uma caracterização dos ideais primos ramificados. Um desafio que parece viável, seria caracterizar a p-parte do grupo das classes nas hipóteses da Seção 4.3.

Os resultados mais significativos desta tese, encontram-se na Seção 4.4.

Os corpos de números considerados são p Extensões Galoisianas e a forma e a forma traço já é conhecida. O desafio deste trabalho foi caracterizar módulos do anel dos inteiros, de modo à otimizar as informações da forma traço.

Um resumo dos resultados obtidos e das expectativas de trabalhos futuros estão no quadro abaixo:

1. Reticulados a partir de polinômios: No Capítulo 3, obtivemos reticulados ótimos em dimensões $n = 2, 3$ a partir das raízes de polinômios de grau n. Um próximo desafio seria generalizar tal resultado para $n > 3$.
2. Na Seção 4.2 descrevemos uma $\mathbb{Z}$-base para os ideais ramificados em extensões cíclicas de grau p. Como seria a descrição das potências desses ideais?
3. Na Seção 4.3 apresentamos um método para se determinar subgrupos da p-parte de $H(L)$ onde $L/\mathbb{Q}$ é uma extensão cíclica de grau p. Tal método se mostrou mais eficiente do que softwares especializados (Magma).
4. Derivamos um limitante superior para a densidade de centro de reticulados associados a certos sub-módulos de $\mathfrak{O}_L$ onde $L/\mathbb{Q}$ é uma extensão cíclica de grau p. Com efeito, alguns desses reticulados se mostraram serem ótimos nas dimensões $p = 3, 5$ e 7. Qual a escolha apropriada para sub-módulos de $\mathfrak{O}_L$ em outras dimensões a fim de se obter reticulados com densidades recordes nas mesmas?

REFERÊNCIAS

BIRKHOFF, G. Subgroups of Abelian Groups. **Proc. London Math. Soc.** , v. 01, n. 01, p. 385–401, 1935.

CONNER, P.E.; HURRELBRINK, J. **Classs Number Parity**. Singapore: World Scientific Publishing, 1988.

CONWAY, J.H.; SLOANE, N.J.A. **Sphere Packings, Lattices and Groups**. New York: Springer Verlag, 1999.

FLORES, A. L.; ; INTERLANDO, J. C.; LOPES, J. V. N.; NOBREGA NETO, T. P. Optimal Families of Two and Three - Dimensional Lattice Pachings From polynomials with Interger Coefficients. **Journal of Álgebra, Number Theory and Applications** , v. 15, n. 01, p. 45–51, 2009.

GAUSS, C. F. Disquisitiones Arithmeticae. **Yale University Press** , v. 01, n. 01, p. 01–05, 1966.

HILBERT, D. **The Theory of Algebraic Number Fields** . Berlin Heidelberg: Springer Verlag, 1998.

INTERLANDO, J. C.; NOBREGA NETO, T. P.; NUNES, J. V. L. Finiteness of the class group of a number field via lattice pachings. **Journal of Álgebra, Number Theory and Applications** , v. 13, n. 01, p. 01–05, 2009.

LANG, S. **Algebric Number Theory**. New York:Addison-Wesley, 1970.

LEOPOLDT, H. W. Zur Geschlechtertheorie in Abelschen Zahlkorpern. **Math. Nachr.**, v. 09, n. 01, p. 351–362, 1953.

MARCUS, D. A. **Number Fields** . New York: Springer Verlag, 1977.

MOLLIN, R.A. **Algebraic Number Theory,** . New York: Chapman e Hall/ CRC, 1999.

NÓBREGA NETO, T. P.; LOPES, J.O. D.; INTERLANDO, J. C. The discriminant of Abeliam Number Fields. **Journal of Álgebra and its Applications** , v. 05, n. 05, p. 35–41, 2006.

OLIVEIRA, Everton L. **Torres de Extensões Abelianas de grau primo ímpar não ramificado.** 2015. 63 f. Tese (Doutorado em Matemática) – UNESP, S. J. do Rio Preto, 2015.

RIBENBOIM, P. **Classical Theory of Algebric Number** . New York: Springer Verlag, 2001.

SAMUEL, Pierre. **Algebraic Theory of Numbers**. New York: Dover Publications, INC, 2008.

USPENSKY, J.V.; HEASLET, M.A. **Elementary Number Theory**. New York: McGraw-Hill, 1939.

WAERDEN, VAN DER B.L. **Álgebra, 5th edition, vol 2**. New York: Springer Verlag, 1970.

WASHINGTON, L. C. **Introduction to Cyelotomic Fields** . New York: Springer Verlag, 1982.