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

Uma Forma Quadrática no Corpo de Condutor Primo

Fernanda Diniz de Melo

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

São José do Rio Preto, SP

Dezembro/2005

Comissão julgadora

Titulares

Prof. Dr. Trajano Pires da Nóbrega Neto - Orientador

Prof. Dr. José Othon Dantas Lopes

Prof. Dr. André Luíz Flores

Suplentes

Prof. Dr. Antonio Aparecido de Andrade

Prof. Dr. Osvaldo Germano do Rocio

"O mundo está nas mãos
daqueles que têm coragem de
sonhar, e correr o risco de
viver seus sonhos."
(Paulo Coelho)

Dedico com amor e carinho

aos meus pais, Renato e

Nilza e ao meu irmão

Eduardo.

Agradecimentos

A Deus.

Ao Prof. Dr. Trajano Pires da Nóbrega Neto, pela orientação e importantes sugestões dadas, baseadas no seu conhecimento técnico. Ainda pela paciência e amizade, desde a graduação.

À banca examinadora: Prof. Dr. Trajano Pires da Nóbrega Neto, Prof. Dr. José Othon Dantas Lopes e Prof. Dr. André Luíz Flores.

Aos professores do Departamento de Matemática da UNESP - S. José do Rio Preto, em especial as professores Aparecida Francisco da Silva e Neuza Kazuko Kakuto, que durante o tempo em que estive no PET-Programa Especial de Treinamento, colaboraram pela minha formação acadêmica.

À minha família, pelo apoio, carinho e estímulo.

À minha amiga Giovana, que desde a graduação tem trabalhado comigo, pelo companherismo e apoio.

À todos os amigos do mestrado, em especial aqueles que me acompanham desde a graduação, pelo companherismo e pelos momentos de distração.

Às minhas amigas de república, Carolina e Thais, pela paciência, pelos conselhos e pelos momentos de descontração.

À todos que de alguma forma contribuíram para a realização deste trabalho.

Sumário

Índice 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

∂f: grau do polinômio f

$[L : K]$: grau de L sobre K

$\prod$: produtório

$\sum$: somatório

$det\ A$: determinante de A

(a_{ij}): matriz

$\Delta[\alpha_1, \ldots, \alpha_n]$: discriminante de uma n-upla

$\mathcal{O}_{\mathbb{K}}$: anel dos inteiros algébricos do corpo de números K

$\#X$: cardinalidade do conjunto X

$\mathfrak{a}, \mathfrak{b}, \mathfrak{p}, \mathfrak{q}, \ldots$: ideais

$\mathfrak{a}^{-1}$: inverso de um ideal fracionário

$N(\mathfrak{a})$: norma de $\mathfrak{a}$

(r, s): máximo divisor comum de r e s

$\phi(n)$: função de Euler

$A[X]$: anel dos polinômios sobre A em X

$\mathbb{K}(\alpha_1, \ldots, \alpha_n)$: o corpo obtido pela adjunção de $\alpha_1, \ldots, \alpha_n$ a $\mathbb{K}$

$\frac{R}{I}$: anel quociente

$\forall$: para todo

$\exists$: existe

ζ_n: $e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, uma raiz n-ésima primitiva da unidade

$\overline{x}$: conjugado complexo do elemento x

$D_{\mathbb{K}}$: discriminante absoluto do corpo $\mathbb{K}$

$Tr_{\mathbb{L}/\mathbb{K}}$: traço em relação à extensão $\mathbb{L}/\mathbb{K}$

$N_{\mathbb{L}/\mathbb{K}}$: norma em relação à extensão $\mathbb{L}/\mathbb{K}$

$irr(\alpha, \mathbb{K})$: polinômio irredutível de α sobre $\mathbb{K}$

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

$Gal(\mathbb{L} : \mathbb{K})$: grupo de Galois de $\mathbb{L}/\mathbb{K}$

Resumo

O principal objetivo deste trabalho é calcular a densidade de centro da representação geométrica do ideal totalmente ramificado em corpos de condutor primo. Primeiro, fazemos a caracterização dos subcorpos do p-ésimo corpo ciclotômico e dos elementos do ideal, também calculamos a norma desse ideal. Em seguida, é apresentada uma forma quadrática e explicitado o seu mínimo para o cálculo do raio de empacotamento dessa representação geométrica. Finalizamos com o cálculo da densidade de centro.

Palavras-chave: corpos ciclotômicos, condutor, reticulados, densidade de centro, forma quadrática.

Abstract

The main aim of this work is to calculate density of the center from the geometric representation of the totally ramified ideal in prime conductor fields. First of all, we make the characterization of the elements from subfields of the p-th cyclotomic field and from the ideal of the elements, we also calculate the norm of this ideal. After that, a quadratic form is presented and exhibit its minimun for the radius of packing calculation this geometric representation. Concluding with the center density calculation.

Keywords: cyclotomic fields, conductor, lattices, center density, quadratic form.

Introdução

O desafio de se determinar empacotamentos esféricos com a maior densidade tem despertado a curiosidade de matemáticos desde 1900, quando esse foi citado por Hilbert como sendo o 18º problema de uma seleta lista de vinte e três problemas. Em particular, os empacotamentos esféricos cujo conjunto de centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ foram estudados com maior interesse e denominados empacotamentos reticulados.

Em 1948 Shannon publica um artigo [11] mostrando a estreita relação entre a eficiência de códigos corretores de erro e a densidade de empacotamentos reticulados, com isso o problema proposto por Hilbert ganha um espaço na Teoria da Informação.

São várias as técnicas para se obter reticulados; neste texto utilizamos a técnica descrita por Minkowski, que se baseia na Teoria Algébrica dos Números e consiste na representação geométrica de $\mathbb{Z}$-módulos livres de um corpo de números.

Na década de 90 Joseph Boutros juntamente com outros especialistas publicaram alguns resultados onde mostram que versões particulares de empacotamentos reticulados construídos de corpos ciclotômicos, coincidiam com os reticulados mais densos conhecidos. Dessa forma começam a surgir vários trabalhos em corpos ciclotômicos.

Nesta dissertação optamos por trabalhar em corpos abelianos de condutor primo, pois o grupo de Galois do p-ésimo corpo ciclotômico $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é cíclico, o que garante que para cada d divisor do grau de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ existe um único subcorpo $\mathbb{K}$ de $\mathbb{Q}(\zeta_p)$, de grau d. Ainda é possível caracterizar esse corpo e seu anel dos inteiros algébricos, $\mathcal{O}_{\mathbb{K}}$ (cf. Teorema 2.2.2). Obtemos os reticulados a partir da representação geométrica de ideais $\mathfrak{a}$

do anel dos inteiros algébricos de $\mathbb{K}$.

Dentre os vários parâmetros de um reticulado, damos ênfase à densidade de centro, que é dada pela expressão:

$$\frac{2^t \rho^n}{|D_{\mathbb{K}}|^{1/2} N(\mathfrak{a})}$$

onde t é a metade do número de imersões complexas de $\mathbb{K}$ em $\mathbb{C}$, ρ é o chamado raio de empacotamento do reticulado, n é o grau do corpo $\mathbb{K}$, $D_{\mathbb{K}}$ é o discriminante do corpo e $N(\mathfrak{a})$ é a norma do ideal.

O discriminante do corpo, nestes casos, é obtido de forma direta, aplicando o Teorema 2.2.2. Para calcular a norma de um ideal, devido às dificuldades, optamos por tomar ideais primos que se ramificam completamente em $\mathcal{O}_{\mathbb{K}}$, onde a determinação do raio de empacotamento requer a minimização de uma forma quadrática que é obtida da função traço como veremos no último capítulo.

Dessa forma percebemos que a maior dificuldade para obtermos a densidade de centro do reticulado, no nosso caso, está na determinação do raio de empacotamento. Assim o objetivo central deste trabalho é compreender a forma quadrática da função traço do corpo $\mathbb{Q}(\zeta_p)$ e dos seus subcorpos, obtendo as informações necessárias para o cálculo da densidade de centro.

Esta dissertação destina-se ao leitor que tem conhecimento básico de Teoria Algébrica dos Números, ou seja, que tenha uma familiarização dos conceitos introduzidos no primeiro capítulo, que está descrito abaixo. Os principais resultados de cada capítulo são mencionados no início de cada um, como também é dito o critério usado para a escolha de quais resultados são demonstrados. Dividimos este trabalho em três capítulos.

No primeiro Capítulo introduzimos e exemplificamos os conceitos básicos necessários para o entendimento desta dissertação tais como a definição de corpos de números, elementos algébricos, discriminante, inteiro algébrico, base integral, norma e traço de um elemento. Também apresentamos a fatoração de um ideal primo, usando o Lema de Kummer e estudamos norma de um ideal.

No segundo Capítulo encontra-se os resultados utilizados para a melhor compreensão

do Capítulo seguinte. Iniciamos com o conceito de corpo ciclotômico e polinômio ciclotômico, descrevemos o anel dos inteiros algébricos desse corpo, enunciamos e exemplificamos alguns resultados para o cálculo do seu discriminante. Na seção seguinte caracterizamos os subcorpos do p-ésimo corpo ciclotômico, o seu anel dos inteiros algébricos e o seu discriminante; nessa seção utilizamos alguns resultados da Teoria de Galois. Também apresentamos os conceitos de reticulados, empacotamento esférico e densidade de centro. Por último é apresentado o método de Minkowski e explicitada uma fórmula geral para o cálculo da densidade de centro dos reticulados obtidos a partir desse método.

No terceiro Capítulo encontra-se o principal objetivo deste trabalho. Aqui abordamos especificamente o corpo $\mathbb{Q}(\zeta_p)$ e seus subcorpos $\mathbb{K}$. A Proposição 1.6.1, sobre a decomposição de ideais em um corpo de extensão; o Teorema 1.6.6, fornecendo uma condição necessária e suficiente para que um ideal se ramifique completamente em um corpo de números; o Lema de Kummer e o Teorema da Evidência são resultados da seção 1.6 fortemente utilizados neste capítulo, assim como o Teorema 2.2.2, que caracteriza os subcorpos $\mathbb{K}$, da subseção 2.2.1.

Primeiramente estudamos o ideal $p\mathbb{Z}$ que é o único ideal primo que se ramifica completamente em $\mathcal{O}_{\mathbb{L}}$, o anel dos inteiros algébricos de $\mathbb{L} = \mathbb{Q}(\zeta_p)$; descrevemos sua decomposição em $\mathcal{O}_{\mathbb{L}}$ e no anel dos inteiros algébricos de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$. Em seguida fazemos a caracterização dos elementos dos ideais $\mathfrak{p}_{\mathbb{L}} = (1-\zeta_p)\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$.

Na seção seguinte apresentamos uma forma quadrática para a função traço no corpo $\mathbb{Q}(\zeta_p)$ e para seus subcorpos $\mathbb{K}$, que será utilizada no cálculo da densidade de centro. Depois estudamos a minimização da forma quadrática para o subcorpo $\mathbb{K}$ restrita ao ideal $\mathfrak{p}_{\mathbb{K}}$ e determinamos o mínimo dessa, consideramos esse o tópico mais difícil desse Capítulo. Finalizamos com exemplos explicitando o cálculo da densidade de centro da representação geométrica do ideal $\mathfrak{p}_{\mathbb{K}}$.

Capítulo 1

Corpos de Números

Neste capítulo, apresentamos os conceitos básicos da Teoria Algébrica dos Números afim de proporcionar um melhor entendimento dos próximos capítulos e também fixar a notação aqui adotada. Admitimos que o leitor tenha conhecimentos elementares de estruturas algébricas, que podem ser encontrados nas referências [4], [5] e [6].

Introduzimos os conceitos e as propriedades de extensões de corpos, elementos algébricos e inteiros algébricos. Também definimos corpo de números, tratamos de discriminante, anel dos inteiros algébricos, base integral e de norma e traço de um elemento.

Ainda descrevemos a decomposição de ideais em ideias primos usando o Lema de Kummer e também a decomposição de ideais em uma extensão qualquer e ainda, mais especificamente, em uma extensão galoisiana. Por último calculamos a norma de um ideal não nulo do anel dos inteiros algébricos.

Dentre os resultados centrais do capítulo destacamos o Teorema 1.4.1, que garante a existência da base integral para todo corpo de números; o Teorema 1.6.3, mostrando a unicidade da fatoração de um ideal em ideais primos, a Proposição 1.6.1, sobre a decomposição de ideais em uma extensão e também o Teorema 1.7.2, que prova que a norma de ideais é multiplicativa.

Aqui optamos por apenas citar as fontes onde se encontram as demonstrações dos resultados apresentados.

1.1 Elementos Algébricos sobre um Corpo

Sejam $\mathbb{L}$ um corpo e $\mathbb{K}$ seu subcorpo, dessa forma $\mathbb{L}$ é dito o *corpo de extensão* de $\mathbb{K}$ e denota-se $\mathbb{L}/\mathbb{K}$. A dimensão de $\mathbb{L}$, visto como $\mathbb{K}$-espaço vetorial é chamada de *grau* de $\mathbb{L}$ sobre $\mathbb{K}$ e denotada por $[\mathbb{L} : \mathbb{K}]$. A extensão $\mathbb{L}/\mathbb{K}$ é uma *extensão finita* se $[\mathbb{L} : \mathbb{K}]$ é finito. É possível mostrar que se $\mathbb{K}$ é um corpo, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e $\mathbb{F}$ uma extensão finita de $\mathbb{L}$, então $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}].[\mathbb{L} : \mathbb{K}]$

Tomando α um elemento de $\mathbb{L}$, definimos $\mathbb{K}[\alpha]$ o conjunto de todas as expressões polinomiais em α com coeficientes em $\mathbb{K}$.

Um elemento α de $\mathbb{L}$ é dito *algébrico* sobre $\mathbb{K}$ se esse é raiz de um polinômio não nulo com coeficientes em $\mathbb{K}$; caso contrário o elemento é dito *transcedente* sobre $\mathbb{K}$.

Por exemplo $\alpha = \sqrt{2} + \sqrt{-3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^4 + 18x + 25 \in \mathbb{Q}[x]$.

Se todo elemento de $\mathbb{L}$ é algébrico sobre $\mathbb{K}$ a extensão $\mathbb{L}/\mathbb{K}$ é dita *extensão algébrica*. Uma extensão $\mathbb{L}/\mathbb{K}$ é simples quando existe $\alpha \in \mathbb{L}$ tal que:

$$\mathbb{L} = \mathbb{K}(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in \mathbb{K}[x] \text{ e } g(\alpha) \neq 0\}$$

O polinômio mônico não nulo $p(x) \in \mathbb{K}[x]$ de grau mínimo tal que α é raiz chama-se *polinômio minimal* de α sobre $\mathbb{K}$, esse polinômio é irredutível sobre $\mathbb{K}$ e será denotado por $irr(\alpha, \mathbb{K})$.

Para α algébrico, temos o seguinte resultado:

Teorema 1.1.1 ([*13*], pag. 23) *Sejam $\mathbb{L}/\mathbb{K}$ e $\alpha \in \mathbb{L}$, então α é algébrico sobre $\mathbb{K}$ se, e somente se, $\mathbb{K}(\alpha)$ é uma extensão finita de $\mathbb{K}$. Neste caso $[\mathbb{K}(\alpha) : \mathbb{K}] = \partial p$, onde $p = irr(\alpha, \mathbb{K})$ e $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$.*

O conjunto de todos os números algébricos sobre $\mathbb{K}$ é um subcorpo de $\mathbb{C}$ (cf. [13], pag. 39).

Um corpo $\mathbb{K}$ é dito *corpo de números* se esse é uma extensão finita dos racionais, o que implica que $\mathbb{K}$ é uma extensão algébrica sobre $\mathbb{Q}$.

Teorema 1.1.2 ([*13*], pag. 40) *Se* $\mathbb{K}$ *é um corpo de números então* $\mathbb{K} = \mathbb{Q}(\theta)$*, para algum* θ *algébrico.*

Exemplo 1.1.1 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*, temos que* $f(x) = x^2 - 2$ *e* $g(x) = x^2 - 3$ *são respectivamente os polinômios minimais de* $\sqrt{2}$ *e* $\sqrt{3}$ *sobre* $\mathbb{Q}$*. As raízes de* f *são* $\alpha_1 = \sqrt{2}$ *e* $\alpha_2 = -\sqrt{2}$ *e de* g *são* $\beta_1 = \sqrt{3}$ *e* $\beta_2 = -\sqrt{3}$*. No Teorema acima prova-se que basta tomarmos*

$$\theta = \alpha_1 + c\beta_1, \text{ tal que } \mathrm{c} \neq \frac{\alpha_\mathrm{i} - \alpha_1}{\beta_1 - \beta_\mathrm{j}} \ \mathrm{i} = 1, 2 \text{ e } \mathrm{j} = 2.$$

Dessa forma podemos fazer $\theta = \sqrt{2} + \sqrt{3}$ *e então* $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$*.*

1.2 Conjugados e Discriminantes

O conjunto dos monomorfismos de um corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$ em $\mathbb{C}$ forma uma parte fundamental da teoria utilizada neste trabalho. Tais monomorfismos são dados pelo Teorema abaixo:

Teorema 1.2.1 ([*13*], pag. 41) *Seja* $\mathbb{K} = \mathbb{Q}(\theta)$ *um corpo de números de grau* n*. Então existem exatamente* n *monomorfismos* σ_i *de* $\mathbb{K}$ *em* $\mathbb{C}$*. Os elementos* $\sigma_i(\theta) = \theta_i$ *são as raízes distintas em* $\mathbb{C}$ *do polinômio minimal de* θ *sobre* $\mathbb{Q}$*.*

Para $\alpha \in \mathbb{K}$, os elementos $\sigma_i(\alpha)$, com $i = 1, ..., n$ são chamados $\mathbb{K}$-conjugados de α. Apesar dos θ_i (os $\mathbb{K}$-conjugados de θ) serem distintos, nem sempre os $\mathbb{K}$-conjugados de α são distintos, por exemplo $\sigma_i(1) = 1$ para todo $i = 1, ..., n$.

Exemplo 1.2.1 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2})$*, temos que* $irr(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$*. As raízes desse polinômio são:* $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$*, onde* $i = \sqrt{-1}$*. Logo para* $\alpha = 1 + 2\sqrt[4]{2}$ *temos que os* $\mathbb{K}$*-conjugados de* α *são:*

$$\sigma_1(1 + 2\sqrt[4]{2}) = 1 + 2\sqrt[4]{2} \qquad \sigma_2(1 + 2\sqrt[4]{2}) = 1 - 2\sqrt[4]{2}$$

$$\sigma_3(1 + 2\sqrt[4]{2}) = 1 + 2i\sqrt[4]{2} \qquad \sigma_4(1 + 2\sqrt[4]{2}) = 1 - 2i\sqrt[4]{2}.$$

Pelo exemplo acima notamos que os $\mathbb{K}$-conjugados de α não são necessariamente elementos de $\mathbb{K}$, como também os $\theta_i's$ não necessariamente pertencem a $\mathbb{K}$.

Ainda com $K = \mathbb{Q}(\theta)$, um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, para cada $\alpha \in \mathbb{K}$, o *polinômio característico* de α sobre $\mathbb{Q}$ é definido como sendo:

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = x^n - \left(\sum_{i=1}^{n}\sigma_i(\alpha)\right)x^{n-1} + \cdots + (-1)^n\prod_{i=1}^{n}\sigma_i(\alpha).$$

Em ([13], pag. 42), mostra-se que os coeficientes do polinômio característico são números racionais. Assim, podemos concluir que $\sum_{i=1}^{n}\sigma_i(\alpha)$ e $\prod_{i=1}^{n}\sigma_i(\alpha)$ são números racionais.

Também em ([13], pag. 43) prova-se que o polinômio característico f_α é uma potência do polinômio minimal p e os $\mathbb{K}$-conjugados de α são as raízes de p em $\mathbb{C}$, cada uma repetida n/m vezes, onde $m = \partial p$.

Tome agora, $\{\alpha_1, ..., \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, definimos o *discrimante* dessa base como sendo:

$$\Delta[\alpha_1, ..., \alpha_n] = (\det[\sigma_i(\alpha_j)])^2.$$

Exemplo 1.2.2 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\left\{1, \sqrt{7}\right\} \subset \mathbb{K}$. Então:*

$$\Delta[1, \sqrt{7}] = \left(\det\begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix}\right)^2 = (-2\sqrt{7})^2 = 28$$

Se tomarmos outra base $\{\beta_1, ..., \beta_n\}$, então $\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$, com $c_{ik} \in \mathbb{Q}$, $k = 1, ..., n$. É possível verificar que:

$$\Delta[\beta_1, ..., \beta_n] = (\det(c_{ik}))^2.\Delta[\alpha_1, ...\alpha_n].$$

Teorema 1.2.2 ([*13*], pag. 44) *O discriminante de qualquer base para $\mathbb{K} = \mathbb{Q}(\theta)$ é racional e não nulo. Se todos os $\mathbb{K}$-monomorfismos de θ são reais então o discriminante de qualquer base é positivo.*

1.3 Inteiros Algébricos

Um número complexo θ é um *inteiro algébrico* se esse é raiz de um polinômio mônico não nulo com coeficientes em $\mathbb{Z}$, por exemplo, $\sqrt{-3}$ é um inteiro algébrico pois é raiz do polinômio x^2+3. O conjunto dos inteiros algébricos constituem um anel que denotaremos por $\overline{\mathbb{Z}}$.

Teorema 1.3.1 ([*13*], pag. 47) *Seja θ um número complexo satisfazendo um polinômio mônico não nulo cujos coeficientes são inteiros algébricos. Então θ é um inteiro algébrico.*

Sabendo que $\overline{\mathbb{Z}}$ é um anel e utilizando o Teorema acima é possível construirmos novos inteiros algébricos. Por exemplo, sendo $\sqrt{7}$ e $\sqrt{8}$ inteiros algébricos então $2\sqrt{7}+5(\sqrt{8})^6$ é um inteiro algébrico e também os zeros do polinômio $x^{10}+\sqrt{7}x^8-[2\sqrt{7}+5(\sqrt{8})^6]x^3-15\sqrt{8}$ são inteiros algébricos.

A intersecção de $\overline{\mathbb{Z}}$ com um corpo de números $\mathbb{K}$ é o que chamamos de *Anel dos Inteiros Algébricos* de $\mathbb{K}$ e denotamos por $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{K}$ e $\overline{\mathbb{Z}}$ são subanéis de $\mathbb{C}$ segue que $\mathcal{O}_{\mathbb{K}}$ é um subanel de $\mathbb{K}$.

Tomando α um elemento não nulo de $\mathbb{K}$, prova-se em ([13], pag. 49) que para algum $c \in \mathbb{Z}$ não nulo $c\alpha \in \mathcal{O}_{\mathbb{K}}$, ou seja, $c\alpha$ é um inteiro algébrico. Logo podemos concluir que $\mathbb{K} = \mathbb{Q}(\theta)$, para algum θ inteiro algébrico.

Observação 1.3.1 *Se $\mathbb{K} = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, então certamente $\mathcal{O}_{\mathbb{K}}$ contém $\mathbb{Z}[\theta]$, já que $\mathcal{O}_{\mathbb{K}}$ é um anel contendo θ, mas não é necessariamente igual a $\mathbb{Z}[\theta]$. Por exemplo, $\mathbb{Q}(\sqrt{28})$ é um corpo de números e $\sqrt{28}$ é um inteiro algébrico. Mas, $\frac{1+\sqrt{28}}{2}$ é um zero de $p(x) = x^2 - 2x - 6$, logo um inteiro algébrico contido em $\mathbb{Q}(\sqrt{28})$, então pertence a $\mathcal{O}_{\mathbb{K}}$ e não pertence a $\mathbb{Z}[\sqrt{28}]$.*

O próximo lema é útil, em termos de polinômio minimal, para vereficarmos se um número é um inteiro algébrico.

Lema 1.3.1 ([*13*], pag. 49) *Um número algébrico α é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Lema 1.3.2 ([13], pag. 50) *Um inteiro algébrico é um número racional se, e somente se, é um inteiro. Equivalentemente,* $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

1.4 Base Integral

Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n e θ um inteiro algébrico. O anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um grupo abeliano sobre a adição. Uma $\mathbb{Z}$-base para $(\mathcal{O}_{\mathbb{K}}, +)$ é chamada *base integral* para $\mathbb{K}$.

Assim $\{\alpha_1, ..., \alpha_s\}$ é uma base integral se, e somente se, todos $\alpha_i \in \mathcal{O}_{\mathbb{K}}$ e todo elemento de $\mathcal{O}_{\mathbb{K}}$ é unicamente determinado como:

$$a_1\alpha_1 + \cdots a_s\alpha_s; \;\; a_i \in \mathbb{Z}.$$

Os dois próximos resultados garantem a existência da base integral para todo $\mathbb{K}$ corpo de números, ou seja, que $(\mathcal{O}_{\mathbb{K}}, +)$ é um grupo abeliano livre de posto n.

Lema 1.4.1 ([13], pag. 51) *Se* $\{\alpha_1, ..., \alpha_n\}$ *é uma base de* $\mathbb{K}$ *consistindo de inteiros algébricos, então o discriminante* $\Delta[\alpha_1, ..., \alpha_n]$ *é um inteiro não nulo.*

Teorema 1.4.1 ([13], pag. 51) *Todo corpo de números* $\mathbb{K}$ *possui uma base integral, ou seja, o grupo aditivo* $\mathcal{O}_{\mathbb{K}}$ *é abeliano livre de posto n igual ao grau de* $\mathbb{K}$.

Dada uma $\mathbb{Q}$-base de $\mathbb{K}$ consistindo de inteiros algébricos, calculamos seu discriminante e então temos o seguinte teorema:

Teorema 1.4.2 ([13], pag. 53) *Sejam* $\alpha_1, ..., \alpha_n$ *elementos de* $\mathcal{O}_{\mathbb{K}}$ *formando uma* $\mathbb{Q}$*-base para* $\mathbb{K}$. *Se* $\Delta[\alpha_1, ..., \alpha_n]$ *é um inteiro livre de quadrados então* $\{\alpha_1, ..., \alpha_n\}$ *é uma base integral.*

O discriminante de duas bases integrais são iguais (cf. [13], pag. 53), este valor comum é denominado *discriminante do corpo* $\mathbb{K}$ que denotamos por $D_{\mathbb{K}}$ e também esse é sempre um número inteiro não nulo.

1.5 Norma e Traço

Sejam $\mathbb{K} \subset \mathbb{L} = \mathbb{K}(\theta)$ corpos de números, com o grau de $\mathbb{L}$ sobre $\mathbb{K}$ igual a n e $\sigma_1, ..., \sigma_n$ os $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Para qualquer $x \in \mathbb{L}$ definimos a *norma* e o *traço* de x sobre $\mathbb{K}$ como sendo:

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

No contexto em que estiver explícito a extensão de corpos, a norma e o traço de x serão abreviados por $N(x)$ e $Tr(x)$, respecitvamente. E ainda, é possível verificar que se x é um inteiro algébrico, então a norma e o traço de x são inteiros.

Exemplo 1.5.1 *Sejam $\mathbb{K}$ e α como no exemplo 1.2.1 então temos que:*

$$Tr(x) = 1 + 2\sqrt[4]{2} + 1 - 2\sqrt[4]{2} + 1 + 2i\sqrt[4]{2} + 1 - 2i\sqrt[4]{2} = 4$$

$$N(x) = (1 + 2\sqrt[4]{2})(1 - 2\sqrt[4]{2})(1 + 2i\sqrt[4]{2})(1 - 2i\sqrt[4]{2}) = -31$$

Para a um elemento de $\mathbb{K}$ e x, y de $\mathbb{L}$, seguem como consequência da definição as seguintes propriedades:

1. $Tr_{\mathbb{L}/\mathbb{K}}(x + y) = Tr_{\mathbb{L}/\mathbb{K}}(x) + Tr_{\mathbb{L}/\mathbb{K}}(y)$
2. $Tr_{\mathbb{L}/\mathbb{K}}(ax) = aTr_{\mathbb{L}/\mathbb{K}}(x)$
3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$
4. $N_{\mathbb{L}/\mathbb{K}}(xy) = N_{\mathbb{L}/\mathbb{K}}(x)N_{\mathbb{L}/\mathbb{K}}(y)$
5. $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$

Agora sejam $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ corpos de números, dado $\alpha \in \mathbb{M}$ temos:

1. $Tr_{\mathbb{M}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\alpha))$
2. $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$

Em particular, se $x \in \mathbb{L}$, então:

1. $Tr_{\mathbb{M}/\mathbb{K}}(x) = [\mathbb{M} : \mathbb{L}]Tr_{\mathbb{L}/\mathbb{K}}(x)$

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

Proposição 1.5.1 ([*13*], pag. 53) *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números onde θ tem polinômio minimal p de grau n. A $\mathbb{Q}$-base $\{1, \theta, ..., \theta^{n-1}\}$ tem discriminante*

$$\Delta[1, \theta, ..., \theta^{n-1}] = (-1)^{n(n-1)/2} \cdot N_{\mathbb{K}/\mathbb{Q}}(p'(\theta))$$

onde p' é a derivada formal de p.

Exemplo 1.5.2 *Sejam $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[4]{5}$ e $p(x) = x^4 - 5 = irr(\theta, \mathbb{Q})$. Então:*

$$\Delta[1, \theta, \theta^2, \theta^3] = (-1)^6 N_{\mathbb{K}/\mathbb{Q}}(4\theta^3) = (4\theta^3)^4 = 256.125.$$

1.6 Fatoração de Ideais

Um domínio é dito *domínio Noetheriano* quando todos seus ideais são finitamente gerado. Temos duas condições que são equivalentes a essa definição:

1. **A condição de cadeia ascendente:** Dada uma cadeia ascendente de ideais

   $$\mathcal{I}_0 \subseteq \mathcal{I}_1 ... \subseteq \mathcal{I}_n \subseteq ...$$

   então existe algum N tal que $\mathcal{I}_n = \mathcal{I}_N$, para todo $n \neq N$, ou seja, toda cadeia ascendente é estacionária.

2. **A condição maximal:** Todo conjunto não vazio de ideais de um anel tem um elemento maximal, isto é, um elemento que não está propriamente contido em qualquer outro elemento.

Agora um domínio é definido como *domínio de Dedekind* se for integralmente fechado, Noetheriano e se todo ideal primo não nulo for maximal.

O próximo teorema garante que o anel dos inteiros algébricos é um domínio de Dedekind.

Teorema 1.6.1 ([*13*], pag. 115) *O anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$ tem as seguintes propriedades:*

(a) *$\mathcal{O}_{\mathbb{K}}$ é um domínio, com corpo de frações $\mathbb{K}$,*

(b) *$\mathcal{O}_{\mathbb{K}}$ é Noetheriano,*

(c) *Se $\alpha \in \mathbb{K}$ satisfaz um polinômio mônico com coeficientes em $\mathcal{O}_{\mathbb{K}}$, então $\alpha \in \mathcal{O}_{\mathbb{K}}$,*

(d) *Todo ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ é maximal.*

Notemos que um ideal pode ser descrito como um $\mathcal{O}_{\mathbb{K}}$-submódulo de $\mathcal{O}_{\mathbb{K}}$, dessa forma restringimos ao estudo de $\mathcal{O}_{\mathbb{K}}$-submódulos de $\mathbb{K}$.

Em particular estamos interessados nos submódulos que tem uma estrutura de grupo sobre a multiplicação; esses são caracterizados pela seguinte propriedade: um $\mathcal{O}_{\mathbb{K}}$-submódulo $\mathfrak{a}$ de $\mathbb{K}$ é dito *ideal fracionário* de $\mathcal{O}_{\mathbb{K}}$ de existe algum $c \in \mathcal{O}_{\mathbb{K}}$ não nulo tal que $c\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{K}}$. Em outras palavras, o conjunto $\mathfrak{b} = c\mathfrak{a}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{a} = c^{-1}\mathfrak{b}$; assim os ideais fracionários de $\mathcal{O}_{\mathbb{K}}$ são um subconjunto de $\mathbb{K}$ da forma $c^{-1}\mathfrak{b}$, onde $\mathfrak{b}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e c é um elemento não-nulo de $\mathcal{O}_{\mathbb{K}}$.

A seguir enunciaremos os dois principais teoremas desta seção.

Teorema 1.6.2 ([*13*], pag. 117) *Os ideais fracionários não nulos de $\mathcal{O}_{\mathbb{K}}$ formam um grupo abeliano multiplicativo.*

Teorema 1.6.3 ([*13*], pag. 117) *Todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ pode ser escrito como o produto de ideais primos unicamente determinados a menos da ordem dos fatores.*

De um modo geral, esse último teorema vale para A um anel de Dedekind; assim se $\mathfrak{a}$ é um ideal não nulo de A, então existem $\mathfrak{p}_1, ..., \mathfrak{p}_n$ ideais primos de A e $e_1, ..., e_n$ inteiros positivos tais que:

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

e esta expressão é única, a menos da ordem dos fatores (cf. [10], pag. 50).

Veremos agora a decomposição de um ideal em uma extensão.

Proposição 1.6.1 ([*10*], pag. 71) *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos de números, com $[\mathbb{L} : \mathbb{K}] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ e*

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{1.1}$$

a decomposição de $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ em ideais primos de $\mathcal{O}_{\mathbb{L}}$. Então os ideais $\mathfrak{p}_{i's}$ são precisamente os ideais primos $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$.

Nas condições da proposição anterior, diremos que os ideais $\mathfrak{p}_{i's}$ estão acima do ideal $\mathfrak{p}$. Ainda g é denominado *número de decomposição* de $\mathfrak{p}$ na extensão $\mathbb{L}/\mathbb{K}$ e os expoentes $e_{i's}$ são chamados de *índices de ramificação* que denotaremos por $e(\mathfrak{q}|\mathfrak{p})$. Dizemos que um ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ é ramificado em $\mathcal{O}_{\mathbb{L}}$ (ou em $\mathbb{L}$) se, $e(\mathfrak{q}|\mathfrak{p}) > 1$ para algum ideal primo $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$.

Teorema 1.6.4 ([*7*], pag. 63) *Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$, $\mathfrak{q}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$, então as seguintes condições são equivalentes:*

(a) $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_{\mathbb{L}}$,

(b) $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}_{\mathbb{L}}$,

(c) $\mathfrak{q} \supset \mathfrak{p}$,

(d) $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$,

(e) $\mathfrak{q} \cap \mathbb{K} = \mathfrak{p}$.

Quando ocorre uma das condições acima, dizemos que $\mathfrak{q}$ está acima de $\mathfrak{p}$, ou $\mathfrak{p}$ está abaixo de $\mathfrak{q}$. Mostra-se, em ([7], pag. 63) que todo ideal primo $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ está acima de um único ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ e todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ está abaixo de no mínimo um ideal primo $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$.

Há outro número importante associado ao par de ideais primos $\mathfrak{p}$ e $\mathfrak{q}$, com $\mathfrak{q}$ acima de $\mathfrak{p}$. Sabemos que os anéis quocientes $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ e $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$ são corpos já que $\mathfrak{p}$ e $\mathfrak{q}$ são ideais maximais e ainda existe uma maneira em que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ pode ser visto como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$, temos que $\mathcal{O}_{\mathbb{K}}$ em $\mathcal{O}_{\mathbb{L}}$, induz um homomorfismo de anéis $\mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{q}$, e o núcleo é $\mathcal{O}_{\mathbb{K}} \cap \mathfrak{q}$. Sabemos que $\mathcal{O}_{\mathbb{K}} \cap \mathfrak{q} = \mathfrak{p}$ (pelo Teorema 1.6.4 item

(d)), então obtemos a imersão $\mathcal{O}_{\mathbb{K}}/\mathfrak{p} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{q}$. Esses são chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$. Esses corpos são finitos e assim, $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ e seja f este grau. Então, f é chamado de *grau de inércia* ou *grau residual* de $\mathfrak{q}$ sobre $\mathfrak{p}$ e denoteremos por $f(\mathfrak{q}|\mathfrak{p})$.

Notemos que se $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{u}$ são ideais primos nos respectivos anéis dos inteiros algébricos $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{U}}$, então

$$\begin{aligned} e(\mathfrak{u} \mid \mathfrak{p}) &= e(\mathfrak{u} \mid \mathfrak{q})e(\mathfrak{q} \mid \mathfrak{p}), \\ f(\mathfrak{u} \mid \mathfrak{p}) &= f(\mathfrak{u} \mid \mathfrak{q})f(\mathfrak{q} \mid \mathfrak{p}). \end{aligned}$$

Teorema 1.6.5 *(Igualdade Fundamental)* ([7], pag. 65) *Sejam n o grau de $\mathbb{L}$ sobre $\mathbb{K}$ e $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ os ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$. Denotamos por $e_1, \ldots, e_g$ e $f_1, \ldots, f_g$ os correspondentes índices de ramificação e graus residuais. Então:*

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

O próximo Teorema apresenta uma condição necessária e suficiente para que um ideal primo se ramifique em $\mathcal{O}_{\mathbb{K}}$.

Teorema 1.6.6 ([10], pag. 74) *Seja $\mathbb{K}$ um corpo de números. Uma condição necessária e suficiente para que um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifique em $\mathcal{O}_{\mathbb{K}}$ é que p divida $D_{\mathbb{K}}$.*

Como consequência desse Teorema, pode-se concluir que existe apenas um número finito de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathcal{O}_{\mathbb{K}}$.

Lema 1.6.1 *(Lema de Kummer)*([1], pag. 39) *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o seu anel dos inteiros algébricos e $\theta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Dados um número primo p tal que p não divide $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]$ e $f(x)$ o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem $p_1(x), \ldots, p_g(x) \in \mathbb{Z}[X]$, polinômios irredutíveis, $e_1, \ldots, e_g \in \mathbb{N}^*$, tais que,*

$$f(x) \equiv p_1(x)^{e_1} \ldots p_g(x)^{e_g} \pmod{p\mathbb{Z}[X]} \quad e$$

(i) *$\mathfrak{p}_i = (p, p_i(\theta)) = p\mathcal{O}_{\mathbb{K}} + p_i(\theta)\mathcal{O}_{\mathbb{K}}$ são ideais primos de $\mathcal{O}_{\mathbb{K}}$ acima de $p\mathbb{Z}$, $i = 1, \ldots, g$;*

(ii) $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$;

(iii) $\left[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_i} : \dfrac{\mathbb{Z}}{p\mathbb{Z}}\right] = \partial p_i(x) = f_i$.

Exemplo 1.6.1 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{-6})$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-6}]$ *o seu anel dos inteiros algébricos e* $p = irr(\sqrt{-6}, \mathbb{Q}) = x^2 + 6$. *Considerando o ideal* $7\mathbb{Z} \subset \mathbb{Z}$, *o polinômio* p *é fatorado como:*

$$p(x) \equiv p_1(x)p_2(x) \pmod 7$$

onde $p_1(x) = x + 1$ *e* $p_2(x) = x + 6$, *logo pelo Lema de Kummer temos:*

(a) $\mathfrak{p}_1 =< 7, p_1(\sqrt{-6}) >$ *e* $\mathfrak{p}_2 =< 7, p_2(\sqrt{-6}) >$ *são os ideais primos de* $\mathcal{O}_{\mathbb{K}}$ *acima de* $7\mathbb{Z}$,

(b) $7\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1.\mathfrak{p}_2$,

(c) $[\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_1} : \frac{\mathbb{Z}}{7\mathbb{Z}}] = [\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_2} : \frac{\mathbb{Z}}{7\mathbb{Z}}] = \partial p_1 = \partial p_2 = 1$.

Pelo Teorema da Igualdade Fundamental temos que os graus residuais são $f_1 = f_2 = 1$ *e os índices de ramificação são* $e_1 = e_2 = 1$.

Considerando agora o ideal $3\mathbb{Z} \subset \mathbb{Z}$ *o polinômio* p *é fatorado da seguinte maneira:*

$$p(x) \equiv p_1(x) \pmod 3$$

onde $p_1(x) = x^2$, *logo pelo Lema de Kummer temos:*

(a) $\mathfrak{p}_1 =< 7, p_1(\sqrt{-6}) >$ *é o ideal primo de* $\mathcal{O}_{\mathbb{K}}$ *acima de* $3\mathbb{Z}$,

(b) $3\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1$,

(c) $[\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_1} : \frac{\mathbb{Z}}{3\mathbb{Z}}] = \partial p_1 = 2$.

Pelo Teorema da Igualdade Fundamental temos que o grau residual é $f_1 = 2$ *e o índice de ramificação é* $e_1 = 1$.

1.6.1 Decomposição de ideais em extensões galoisianas

Sejam $\mathbb{L}$ uma extensão galoisiana sobre $\mathbb{K}$ e $\mathfrak{q}$, $\mathfrak{q}'$ ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$. Aqui veremos como se comporta o grau de inércia e o índice de ramificação dos ideais $\mathfrak{q}$ e $\mathfrak{q}'$ sobre o ideal $\mathfrak{p}$.

Teorema 1.6.7 *(Da Evidência)*([7], pag. 70) *Dados* $\mathbb{L}/\mathbb{K}$ *uma extensão galoisiana com grupo de Galois* G *e,* $\mathfrak{q}$ *e* $\mathfrak{q}'$ *tais que* $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{q}' \cap \mathcal{O}_{\mathbb{K}}$. *Então existe* $\sigma \in G$, *tal que* $\sigma(\mathfrak{q}) = \mathfrak{q}'$.

Corolário 1.6.1 ([7], pag. 71) *Sejam* $\mathbb{L}$ *uma extensão galoisiana sobre* $\mathbb{K}$ *e* $\mathfrak{q}$, $\mathfrak{q}'$ *são dois ideais primos acima de* $\mathfrak{p}$, *então* $e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}'|\mathfrak{p})$ *e* $f(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p})$.

Pelo corolário acima temos que para a extensão galoisiana $\mathbb{L}/\mathbb{K}$, o ideal primo $\mathfrak{p}$ fatora-se em $(\mathfrak{q}_1\mathfrak{q}_2...\mathfrak{q}_g)^e$ em $\mathcal{O}_{\mathbb{L}}$, onde os $\mathfrak{q}_{i's}$ são os ideais primos distintos acima de $\mathfrak{p}$, todos tendo o mesmo grau residual f sobre $\mathfrak{p}$. Dessa forma, pelo Teorema da Igualdade Fundamental, $n = [\mathbb{L} : \mathbb{K}] = g.e.f$.

Conhecendo o índice de ramificação e o grau de inércia podemos classificar os ideais primos, $\mathfrak{p}_{i's}, i = 1, ..., g$, de $\mathcal{O}_{\mathbb{L}}$ em:

(a) Totalmente ramificado se $g = f_i = 1$ e $e_i = n$.

(b) Totalmente inerte se $f_i = n$ e $g = e_i = 1$.

(c) Totalmente decomposto se $g = n$ e $e_i = f_i = 1$.

Exemplo 1.6.2 *Sejam* $\mathbb{K} = \mathbb{Q}(i)$, *onde* $i = \sqrt{-1}$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$ *o anel dos inteiros algébricos de* $\mathbb{K}$ *e* $p(x) = x^2 + 1$ *o polinômio minimal de* i. *Este polinômio é fatorado em* $5\mathbb{Z}$ *da seguinte forma:*

$$x^2 + 1 \equiv p_1(x).p_2(x) \pmod{5\mathbb{Z}[x]}$$

onde $p_1(x) = x + 2$ *e* $p_2(x) = x + 3$, *logo pelo Lema de Kummer temos:*

(a) $\mathfrak{p}_1 =< 5, p_1(i) >$ *e* $\mathfrak{p}_2 =< 5, p_2(i) >$ *são os ideais primos de* $\mathcal{O}_{\mathbb{K}}$ *acima de* $5\mathbb{Z}$,

(b) $5\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1.\mathfrak{p}_2$,

(c) $[\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_1} : \frac{\mathbb{Z}}{5\mathbb{Z}}] = [\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}_2} : \frac{\mathbb{Z}}{5\mathbb{Z}}] = \partial p_1 = \partial p_2 = 1$.

Assim temos $g = 2$, $e = 1$, $f = 1$ *e* $2 = g.e.f = 2.1.1$.

1.7 Norma de um Ideal

Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o seu snel dos inteiros algébricos e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. A norma de $\mathfrak{a}$ é definida como sendo a cardinalidade do quociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$ e

denotada por $N(\mathfrak{a})$,ou seja,

$$N(\mathfrak{a}) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right).$$

Assim, $N(\mathfrak{a})$ é um número inteiro positivo.

Teorema 1.7.1 ([*13*], pag. 126) *Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o seu anel dos inteiros algébricos. Então,*

(a) *Todo ideal $\mathfrak{a} \subset \mathcal{O}_{\mathbb{K}}$ com $\mathfrak{a} \neq 0$ tem uma $\mathbb{Z}$-base $\{\alpha_1, \ldots, \alpha_n\}$;*

(b) *A norma de um ideal não nulo $\mathfrak{a}$ de $\mathcal{O}_{\mathbb{K}}$ satisfaz:*

$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha_1, \ldots, \alpha_n]}{D_{\mathbb{K}}}\right|^{1/2},$$

onde $D_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$.

Corolário 1.7.1 ([*13*], pag. 126) *Seja $\mathfrak{a} =< a >$ um ideal principal, então*

$$N(\mathfrak{a}) =\mid N(a) \mid .$$

Exemplo 1.7.1 *Considere o ideal $\mathfrak{a} =< 2 - i >$, com $i = \sqrt{-1}$, de $\mathbb{Z}[i]$. Pelo corolário acima temos:*

$$N(\mathfrak{a}) = |N(2 - i)| = (2 - i)(2 + i) = 5.$$

Veremos agora que a norma de ideais é multiplicativa.

Teorema 1.7.2 ([*13*], pag. 127) *Sejam $\mathbb{K}$ um corpo de números e $\mathfrak{a}$, $\mathfrak{b}$ ideais não nulos de $\mathcal{O}_{\mathbb{K}}$. Então*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Para o próximo Teorema é conveniente introduzir outro uso para a palavra “divide ”. Se $\mathfrak{a}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e b um elemento de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathfrak{a} \mid< b >$, então escrevemos também $\mathfrak{a} \mid b$ e dizemos que $\mathfrak{a}$ divide b. É claro que $\mathfrak{a} \mid b$ se, e somente se, $b \in \mathfrak{a}$.

Teorema 1.7.3 ([*13*], pag. 129) *Seja $\mathfrak{a}$ um ideal de $\mathcal{O}_{\mathbb{K}}$, $\mathfrak{a} \neq 0$.*

(a) *Se $N(\mathfrak{a})$ é um primo, então $\mathfrak{a}$ é um ideal primo,*

(b) $N(\mathfrak{a})$ *é um elemento de* $\mathfrak{a}$*, ou equivalentemente,* $\mathfrak{a} \mid N(\mathfrak{a})$*,*

(c) *Se* $\mathfrak{a}$ *é um ideal primo que divide um primo* p*, então,*

$$N(\mathfrak{a}) = p^m,$$

onde $m \leq n$*, o grau de* $\mathbb{K}$*.*

Em particular, o item (c) do Teorema 1.7.3, pode ser escrito do seguinte modo: para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$, temos que, $N(\mathfrak{p}) = p^f$, onde f é o grau residual de $\mathfrak{p}$ e p é o único número primo de $\mathfrak{p}$. De fato, como $\left[\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{p\mathbb{Z}}\right] = f$, então resulta que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ tem p^f elementos.

Exemplo 1.7.2 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$*,* $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$*, o seu anel dos inteiros algébricos,* $\mathfrak{p}_1 =< 2, 1+\sqrt{-5} >$ *ideal primo de* $\mathcal{O}_{\mathbb{K}}$*. Então* $N(\mathfrak{p}_1) = 2$ *e podemos imediatamente dizer que* $\mathfrak{p}_1$ *é primo. Notemos que* $N(\mathfrak{p}_1) = 2 \in \mathfrak{p}_1$*, como garante o Teorema 1.7.3(item (b)).*

Capítulo 2

Corpos Ciclotômicos e Representação Geométrica

Aqui descrevemos os corpos ciclotômicos e os polinômios ciclotômicos; apresentamos uma base integral para esses corpos e alguns resultados para o cálculo do seu discriminante. Também caracterizamos os subcorpos de $\mathbb{Q}(\zeta_p)$, o p-ésimo corpo ciclotômico e o seu anel dos inteiros algébricos.

Na seção seguinte, são dadas as definições de empacotamento esférico, empacotamento reticulado, densidade de empacotamento e densidade de centro. Por último, introduzimos o método algébrico para a obtenção de reticulados, bem como a fórmula para o cálculo da sua densidade de centro.

Como os principais resultados citamos o Teorema 2.1.2 que caracteriza o anel dos inteiros algébricos do corpo ciclotômico, o Teorema 2.2.2 caracterizando os subcorpos de $\mathbb{Q}(\zeta_p)$ e ainda o Teorema 2.4.1 com o método algébrico para a obtenção de reticulados.

Neste capítulo demonstramos apenas os resultados das seções 2.2 e 2.4 pois nessas encontram-se, respectivamente, a caracterização dos subcorpos de $\mathbb{Q}(\zeta_p)$ que formam o nosso ambiente de trabalho e o método de Minkowski para a obtenção de reticulados.

2.1 Corpos Ciclotômicos

O *n-ésimo corpo ciclotômico* é da forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é a n-ésima raiz primitiva da unidade. O polinômio $\Phi_n(x) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (x - \zeta_n^i)$ é chamado o *n-ésimo polinômio ciclotômico*, esse é um polinômio mônico em $\mathbb{Z}[X]$ (cf. [8], pag. 114) de grau $\phi(n)$, onde ϕ é a função de Euler.

Lema 2.1.1 ([*8*], pag. 110) *Seja n um inteiro positivo, então:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Em particular para p um número primo segue que:

$$x^p - 1 = \Phi_1(x) \cdot \Phi_p(x),$$

assim

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Mais geralmente, para as potências de p, temos:

$$x^{p^r} - 1 = \Phi_1(x) \cdot \Phi_p(x) \cdots \Phi_{p^{r-1}} \cdot \Phi_{p^r} = (x^{p^{r-1}} - 1) \cdot \Phi_{p^r},$$

e portanto

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

O próximo Teorema nos garante a irredutibilidade de Φ_n sobre $\mathbb{Q}$.

Teorema 2.1.1 ([*8*], pag. 115) *Seja n um inteiro positivo. Então o n-ésimo polinômio ciclotômico Φ_n é irredutível sobre $\mathbb{Q}$.*

Sobre o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_n)$ e o seu discriminante temos os seguintes teoremas:

Teorema 2.1.2 ([*16*], pag. 11) *Seja n um inteiro positivo. Então o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$.*

Teorema 2.1.3 ([16], pag. 12) *O discriminante do corpo* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *é:*

$$D_{\mathbb{K}} = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}$$

Exemplo 2.1.1 *Seja* $\mathbb{K} = \mathbb{Q}(\zeta_{42})$*, então pelos dois Teoremas anteriores que:*

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{42}] \qquad \text{e} \qquad D_{\mathbb{K}} = \pm \frac{42^{12}}{2^{12}.3^6.7^2} = 3^2.7^6.$$

Um outro resultado sobre discriminante, que utilizamos é:

Teorema 2.1.4 ([9], pag. 64) *Sejam* p *um número primo ímpar,* r *um inteiro positivo e* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p^r})$*,* $[\mathbb{K} : \mathbb{Q}] = up^j$*,* p *não divide* u*. Então,*

$$D_{\mathbb{K}} = \pm p^v$$

onde $v = u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$

2.2 O p-ésimo Corpo Ciclotômico

Veremos aqui, a irredutibilidade de Φ_p , o traço, a norma e o discriminante de $\mathbb{Q}(\zeta_p)$ para qualquer p : primo ímpar.

Lema 2.2.1 ([13], pag. 69) *Seja* p : *primo ímpar. Então o* p*-ésimo polinômio ciclotômico* Φ_p *é irredutível sobre* $\mathbb{Q}$*.*

Demonstração:

Temos que $\Phi_p(x) = \frac{x^p-1}{x-1}$, como $\zeta_p - 1 \neq 0$ e $\zeta_p^p = 1$ segue que $\Phi_p(\zeta_p) = 0$. Precisamos mostrar agora que $\Phi_p(x)$ é irredutível, para isso mostraremos que $\Phi_p(x+1)$ é irredutível.

Sabemos que:

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{r=1}^{p} \binom{p}{r} x^{r-1}.$$

Agora o binômio $\binom{p}{r}$ é divisível por p se $1 \leq r \leq p-1$, e $\binom{p}{1} = p$ não é divisível por p^2. Daí pelo Critério de Eisenstein's $\Phi_p(x+1)$ é irredutível. Portanto $\Phi_p(x)$ é irredutível sobre $\mathbb{Q}$ e ainda como o grau de Φ_p é $p-1$, então $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.

■

As potências $\zeta_p^2, ..., \zeta_p^{p-1}$ também são raízes p-ésimas da unidade, distintas de 1. Logo, temos que:

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x - \zeta_p) \cdot (x - \zeta_p^2) \cdots (x - \zeta_p{}^{p-1}) \tag{2.1}$$

e então os conjugados de ζ_p são $\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}$. Isso significa que os monomofismos de $\mathbb{Q}(\zeta_p)$ em $\mathbb{C}$ são dados por:

$$\sigma_i(\zeta_p) = \zeta_p^i\,, \;\; 1 \leq i \leq p-1,$$

para um elemento geral

$$\alpha = a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}, \;\; a_i \in \mathbb{Q}$$

temos que:

$$\sigma_i(\alpha) = a_1\zeta_p^i + a_2\zeta_p^{2i} + \cdots + a_{p-1}\zeta_p^{i(p-1)}$$

Agora podemos calcular a norma e o traço de ζ_p.

Sendo a $N(\zeta_p) = \zeta_p\zeta_p^2 \ldots \zeta_p^{p-1}$, basta fazer $x = 0$ na equação 2.1 e então teremos que $N(\zeta_p) = (-1)^{p-1} = 1$, como ζ_p e ζ_p^i $(1 \leq i \leq p-1)$ são conjugados temos que:

$$N(\zeta_p^i) = N(\zeta_p) = 1, \tag{2.2}$$

já para o $Tr(\zeta_p) = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1}$ fazemos $x = \zeta_p$ na mesma equação e daí $Tr(\zeta_p) = -1$ e então para ζ_p^i $(1 \leq i \leq p-1)$ temos que:

$$Tr(\zeta_p^i) = Tr(\zeta_p) = -1. \tag{2.3}$$

Sabendo que para $a \in \mathbb{Q}$ a $N(a) = a^{p-1}$ e o $Tr(a) = (p-1)a$ segue que:

$$N(1) = 1 \qquad \text{e} \qquad \text{Tr(1)} = \text{p} - 1. \tag{2.4}$$

Usando que $\zeta_p^p = 1$ e a equação 2.4, podemos estender as equações 2.2 e 2.3 para:

$$N(\zeta_p^s) = 1, \ \forall s \in \mathbb{Z} \tag{2.5}$$

e

$$Tr({\zeta_p}^s) \ = \ \begin{cases} -1, & \text{se} \quad s \not\equiv 0 \ (mod \ p); \\ p-1, & \text{se} \quad s \equiv 0 \ (mod \ p). \end{cases} \tag{2.6}$$

Ainda é possível generalizar o traço para qualquer elemento de $\mathbb{Q}(\zeta_p)$ da seguinte maneira:

$$Tr(\sum_{i=1}^{p-1} a_i\zeta_p^i) = \sum_{i=1}^{p-1} Tr(a_i\zeta_p^i) = -\sum_{i=1}^{p-1} a_i$$

Para a norma, o caso geral é mais complicado, mas um resultado útil é:

$$N(1-\zeta_p) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = p, \tag{2.7}$$

esse fato é verificado fazendo $x = 1$ na equação (2.1).

As duas próximas observações serão necessárias na demonstração do Teorema 2.1.4

Observação 2.2.1 $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z} =< p >$.

De fato: De (2.7) segue que : $p = (1-\zeta_p)\cdot(1-{\zeta_p}^2)\cdots(1-{\zeta_p}^{p-1})$. *Assim temos que* $p \in (1-\zeta_p)\mathcal{O}_K$. *Portanto* $< p > \subset (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$, *(pois* $< p >$ *é um ideal em* $\mathbb{Z}$*). Para mostrarmos a outra inclusão vamos supor que* $p\mathbb{Z} \subsetneq (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} \subseteq \mathbb{Z}$. *Como* $p\mathbb{Z}$ *é maximal* ([5], pag. 24), *então* $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$. *Como* $1 \in \mathbb{Z}$, *então* $1 = (1-\zeta_p)a$, $a \in \mathcal{O}_K$. *Então* $N(1) = N(1-\zeta_p)\cdot N(a)$, *donde segue que* $1 = p.N(a)$, *com* $N(a) \in \mathbb{Z}$, *o que é um absurdo.*

Observação 2.2.2 $Tr(y(1-\zeta_p)) \in p\mathbb{Z}$, *para todo* $y \in \mathcal{O}_K$.

De fato: Cada conjugado $y_i(1-{\zeta_p}^i)$ *de* $y(1-\zeta_p)$ *é um múltiplo em* $\mathcal{O}_K$ *de* $(1-\zeta_p)$. *Sendo o traço a soma dos conjugados, segue que*

$$Tr(y(1-\zeta_p)) = y_1(1-\zeta_p)+y_2(1-{\zeta_p}^2)+\cdots+y_{p-1}(1-{\zeta_p}^{p-1}) = \alpha(1-\zeta_p), \ \text{ com } \ \alpha \in \mathcal{O}_K.$$

Portanto $Tr(y(1-\zeta_p)) \in \mathcal{O}_K(1-\zeta_p)$ *e daí segue que* $Tr(y(1-\zeta_p)) \in \mathbb{Z}$. *Assim,* $Tr(y(1-\zeta_p)) \in \mathbb{Z} \cap (1-\zeta_p)\mathcal{O}_K$. *Ainda pela observação 2.2.1 temos que* $Tr(y(1-\zeta_p)) \in p\mathbb{Z}$.

Teorema 2.2.1 ([*13*], pag. 74) **(a)** *O anel dos inteiros algébricos de* $K = \mathbb{Q}(\zeta_p)$ *é* $\mathbb{Z}[\zeta_p]$. **(b)** *O discriminante de* $\mathbb{Q}(\zeta_p)$*, com* p *um primo ímpar é*

$$(-1)^{(p-1)/2}p^{p-2}.$$

Demonstração:

(a) Seja $\mathcal{O}_K$, o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_p)$, então é claro que $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K$. Seja $\alpha \in \mathcal{O}_K$. Então $\alpha \in \mathbb{Q}(\zeta_p)$, logo

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}{\zeta_p}^{p-2},$$

com $a_i \in \mathbb{Q}$. Multiplicando ambos os lados por $(1 - \zeta_p)$ temos:

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - {\zeta_p}^2) + \cdots + a_{p-2}({\zeta_p}^{p-2} - {\zeta_p}^{p-1}).$$

Assim,

$$Tr(\alpha(1-\zeta_p)) = a_0Tr(1-\zeta_p) + a_1Tr(\zeta_p - {\zeta_p}^2) + \cdots + a_{p-2}Tr({\zeta_p}^{p-2} - {\zeta_p}^{p-1}),$$

e pela observação (2.2.2), $Tr(\alpha(1-\zeta_p)) \in p\mathbb{Z}$. Mas, pela observação (2.2.1),

$$a_0Tr(1-\zeta_p) = a_0p \in p\mathbb{Z},$$

donde segue que $a_0 \in \mathbb{Z}$. Analogamente mostramos que $a_i \in \mathbb{Z}$, para todo i. Portanto $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

(b) Vimos que uma base integral para $\mathbb{Q}(\zeta_p)$ é $1, \zeta_p, \ldots, {\zeta_p}^{p-2}$. Assim, pela Proposição (1.5.1) o discriminante é igual a

$$(-1)^{\frac{(p-1)(p-2)}{2}}N(\Phi_p'(\zeta_p))$$

com $\Phi_p(x)$ como na equação (2.1). Sendo p um primo ímpar, o primeiro fator se reduz a $(-1)^{\frac{(p-1)}{2}}$, pois

$$(-1)^{\frac{(p-1)(p-2)}{2}} = ((-1)^{p-2})^{\frac{(p-1)}{2}} = (-1)^{\frac{(p-1)}{2}}.$$

Para desenvolver o segundo fator tomemos

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} \Longrightarrow \Phi_p^{'}(x) = \frac{(x-1)px^{p-1} - (x^p - 1)}{(x-1)^2}.$$

Assim,

$$\Phi_p^{'}(\zeta_p) = \frac{(\zeta_p - 1)p{\zeta_p}^{p-1} - ({\zeta_p}^p - 1)}{(\zeta_p - 1)^2} = \frac{-(1-\zeta_p)p{\zeta_p}^{p-1}}{(1-\zeta_p)^2} = \frac{-p{\zeta_p}^{p-1}}{1-\zeta_p}.$$

Logo,

$$N(\Phi_p^{'}(\zeta_p)) = N(\frac{-p{\zeta_p}^{p-1}}{1-\zeta_p}) = \frac{N(-p).N(\zeta_p)^{p-1}}{N(1-\zeta_p)} = \frac{(-p)^{p-1}(1)^{p-1}}{p} = p^{p-2}.$$

Portanto o discriminante é $(-1)^{\frac{(p-1)}{2}}.p^{p-2}$.

■

2.2.1 Os subcorpos de $\mathbb{Q}(\zeta_p)$

O corpo $\mathbb{Q}(\zeta_p)$ é uma extensão galoisiana, pois contém todas as raízes do polinômio $x^p - 1$. O seu grupo de Galois sobre $\mathbb{Q}$, que aqui denotaremos por $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, é isomorfo ao grupo multiplicativo $\mathbb{Z}_p^*$ (cf. [7], pag. 18) que é cíclico.

Sabendo que o grau de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$ é $p-1$ e ainda que o seu grupo de Galois é cíclico temos, pelo Teorema Fundamental da Teoria de Galois, que: dado d um divisor de $p-1$ existe um único subcorpo $\mathbb{K}$ de $\mathbb{Q}(\zeta_p)$ cujo grau é $(p-1)/d$.

Um corpo $\mathbb{K}$ é dito corpo de condutor f se esse está contido em $\mathbb{Q}(\zeta_f)$ e f é o menor número natural com essa propriedade, logo os subcorpos de $\mathbb{Q}(\zeta_p)$ também são dito *corpos abelianos de condutor primo.* Esses subcorpos e o seu discrimante são caracterizados pelo seguinte Teorema:

Teorema 2.2.2 ([*15*], pag. 57) *Sejam $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, p: primo ímpar, $d = [\mathbb{Q}(\zeta_p) : \mathbb{K}]$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ e $g \in \mathbb{Z}$ tal que σ_g gera $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Então $\mathbb{K} = \mathbb{Q}(\theta)$ e $\mathcal{O}_\mathbb{K} = \mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_g^{(p-1)/d}(\theta)$. Além disso, $D_\mathbb{K} = \pm p^{[\mathbb{K}:\mathbb{Q}]-1}$.*

Demonstração:

- Primeiro mostramos que $\mathbb{K} = \mathbb{Q}(\theta)$.

  Como $\theta \in \mathbb{K}$, segue que $\mathbb{Q}(\theta) \subset \mathbb{K}$.

  Agora seja $G' = Gal(\mathbb{Q}(\zeta_p) : \mathbb{K})$, então G' tem ordem d. Como, por hipótese, $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q}) =< \sigma_g >$ segue que a ordem do σ_g é $p-1$ e daí temos que $\sigma_{g^{(p-1)/d}}$ gera um grupo de ordem d. Portanto $G' = \{\sigma_{g^{(p-1)/d}}, \sigma_{g^{2(p-1)/d}}, ..., \sigma_{g^{(p-1)}}\}$, logo $\theta = \zeta_p^{g^{(p-1)/d}} + \zeta_p^{g^{2(p-1)/d}} + \cdots + \zeta_p^{g^{(p-1)}}$.

  Temos que $\mathbb{Q}(\theta)$ é uma extensão galoisiana pois, sendo G um grupo abeliano então todos subgrupos de G são normais logo, pelo Teorema Fundamental da Teoria de Galois, os subcorpos correspondentes a esses subgrupos são extensões galoisiana. Daí podemos garantir que $\sigma_g(\theta), ..., \sigma_{g^{(p-1)/d}}(\theta) \in \mathbb{Q}(\theta)$.

  Sejam $b_1, ..., b_{(p-1)/d} \in \mathbb{Q}$ tais que:

$$b_1\sigma_g(\theta) + \cdots + b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta) = 0, \tag{2.8}$$

  onde

$$\begin{aligned} \sigma_{g^i}(\theta) &= \sigma_{g^i}(\zeta_p^{g^{(p-1)/d}}) + \sigma_{g^i}(\zeta_p^{g^{2(p-1)/d}}) + \cdots + \sigma_{g^i}(\zeta_p^{(p-1)}) \\ &= \zeta_p^{g^{(p-1)/d+i}} + \zeta_p^{g^{2(p-1)/d+i}} + \cdots + \zeta_p^{g^{(p-1)+i}}. \end{aligned}$$

  Se $\zeta_p^{g^{t_1(p-1)/d+i_1}} = \zeta_p^{g^{t_2(p-1)/d+i_2}}$, com $1 \leq t_1, t_2 \leq d$ e $1 \leq i_1, i_2 \leq (p-1)/d$, teremos que: $g^{t_1(p-1)/d+i_1} \equiv g^{t_2(p-1)/d+i_2} \pmod{p}$, isto é, $g^{t_1(p-1)/d+i_1} - g^{t_2(p-1)/d+i_2} = pv$. Supondo que $t_1(p-1)/d + i_1 < t_2(p-1)/d + i_2$, temos:

$$g^{t_1(p-1)/d+i_1}(1 - g^{(t_2-t_1)(p-1)/d+(i_2-i_1)}) = pv.$$

  Como g é gerador então $g^a \equiv 1 \pmod{p}$, deste modo:

$$g^{(t_2-t_1)(p-1)/d+(i_2-i_1)} \equiv 1 \pmod{p},$$

  ou seja,

$$(p-1) \mid (t_2-t_1)(p-1)/d + (i_2-i_1).$$

  Daí

$$(t_2-t_1)\frac{(p-1)}{d} + (i_2-i_1) = d\frac{(p-1)}{d}u.$$

Como $1-(p-1)/d \leq i_2 - i_1 \leq (p-1)/d - 1$, segue que $i_2 = i_1$; analogamente temos que $t_2 = t_1$. Assim temos

$$b_1(\zeta_p^{g^{(p-1)/d+1}} + \cdots + \zeta_p^{g^{d(p-1)/d+1}}) + \cdots + b_{(p-1)/d}(\zeta_p^{g^{2(p-1)/d}} + \cdots + \zeta_p^{g^{d(p-1)/d+(p-1)/d}}).$$

Como $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ e todos os $\zeta_p^{g^{t(p-1)/d+i}}$ são distintos dois a dois, temos que ζ_p^i, $i = 1, ..., p-1$ são todos distintos. Deste modo podemos reescrever a equação (2.8) da seguinte maneira:

$$a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} = 0,$$

onde $\{a_i; i = 1, ..., p-1\} = \{b_i; i = 1, ..., (p-1)/d\}$.

Por outro lado, $\{\zeta_p^i, i = 1, ..., p-1\}$ é um conjunto linearmente independente sobre $\mathbb{Q}$, logo $a_i = 0$, $i = 1, ..., p-1$ e, portanto, $b_i = 0$, $i = 1, ..., (p-1)/d$, ou seja, $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq (p-1)/d$.

Sabendo que $\mathbb{Q}(\theta) \subset \mathbb{K}$ e $[\mathbb{K} : \mathbb{Q}] = (p-1)/d$, segue que $[\mathbb{Q}(\theta) : \mathbb{Q}] = (p-1)/d$ e então $\mathbb{K} = \mathbb{Q}(\theta)$.

- Agora verificaremos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_g^{(p-1)/d}(\theta)$.

  Como $\sigma_{g^i}(\theta) \in \mathbb{Z}[\zeta_p] \cap \mathbb{K}$, temos que $\mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_g^{(p-1)/d}(\theta) \subset \mathcal{O}_{\mathbb{K}}$.

  Para provarmos a outra inclusão tomemos $\alpha \in \mathcal{O}_{\mathbb{K}}$, então existem $b_1, ..., b_{(p-1)/d} \in \mathbb{Q}$ tais que $\alpha = \sum_{i=1}^{(p-1)/d} b_i\sigma_i(\theta)$, uma vez que $\{\sigma_g(\theta), ..., \sigma_{g^{(p-1)/d}}\}$ é base de $\mathbb{K}$ sobre $\mathbb{Q}$. Então como $\alpha \in \mathbb{Z}[\zeta_p]$, temos que:

  $$\alpha = \sum_{i=1}^{(p-1)/d} b_i\sigma_(g^i)(\theta) = \sum_{i=1}^{(p-1)/d} b_i\zeta_p^{g^{(p-1)/d+1}},$$

  pode ser expresso por:

  $$\alpha = \sum_{i=1}^{p-1} a_i\zeta_p^i, \quad a_i \in \mathbb{Z}, \quad i = 1, ..., p-1.$$

  Como $\{a_i; i = 1, ..., p-1\} = \{b_i; i = 1, ..., (p-1)/d\}$, concluímos que $a_i \in \mathbb{Z}$, $i = 1, ..., (p-1)/d$, donde segue o resultado.

- Por último temos que o valor do discriminante decorre do Teorema 2.1.4

■

2.3 Reticulados

Sejam V um espaço vetorial de dimensão n sobre um corpo $\mathbb{K}$, A um subanel de $\mathbb{K}$ e $v_1, ..., v_r$, $r \leq n$, vetores linearmente independentes de V. Denominamos *A-reticulado* (ou simplesmente reticulado) com base $\{v_1, ..., v_r\}$ ao conjunto de elementos da forma:

$$x = \sum_{i=1}^{r} a_i v_i, \ a_i \in A.$$

O nosso interesse é pelos casos em que $\mathbb{K} = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $r = n$, dessa forma quando citarmos um reticulado Λ estaremos nos referindo à um reticulado nas condições acima.

Definimos *empacotamento esférico* como sendo a forma de distribuir esferas de mesmo raio em $\mathbb{R}^n$ de modo que essas tenham no máximo um ponto em comum. Pode-se descrever um empacotamento esférico apenas indicando os centros e os raios destas esferas. Ainda dizemos *empacotamento reticulado* quando o conjunto de centros forma um reticulado Λ de $\mathbb{R}^n$. A partir de agora só consideraremos empacotamentos reticulados, dizemos neste caso que o empacotamento é associado a Λ.

A *densidade de empacotamento* é a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas. O nosso objetivo agora é obter uma expressão para a densidade de empacotamento.

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\beta = \{v_1, ..., v_n\}$, então o conjunto:

$$R_\beta = \{x \in \mathbb{R}^n / \ x = \sum_{i=1}^{n} \lambda_i v_i, \ 0 \leq \lambda_i < 1, \ \lambda_i \in \mathbb{R}\}$$

é chamado *região fundamental* de Λ associada a base β.

Observe que para calcular a densidade de um empacotamento associado a Λ, basta calcular a densidade em uma região fundamental R_β; é isso que faremos agora.

Fazendo $v_i = (v_{i1}, ..., v_{in}) \in \mathbb{R}^n$, $i = 1, ..., n$, o *volume* $v(R_\beta)$ de R_β é o módulo do determinante da matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{12} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}$$

a qual é denominada *matriz geradora* do reticulado Λ.

O volume da região fundamental independe da base, pois a matriz mudança de base é invertível, com entradas inteiras, ou seja, tem determinante ± 1. Assim, podemos definir o volume de Λ como sendo o volume da região fundamental de uma base qualquer e denotaremos por $v(\Lambda)$.

Interessa-nos o empacotamento associado a Λ tal que as esferas tenham raio máximo; para determinar este raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n / \ |x| \leq k\}$ com o reticulado Λ é um conjunto finito, ou seja, Λ é discreto, logo o número:

$$\lambda_{min} = \min\{|v|; \ v \in \Lambda, \ v \neq 0\}$$

está bem definido.

Assim $\rho = \frac{\lambda_{min}}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. E então quando falamos de densidade do reticulado Λ, é o mesmo que dizermos densidade do empacotamento com esferas de raio ρ associado a este reticulado que será denotada por $\Delta(\Lambda)$ e expressa por:

$$\Delta(\Lambda) = \frac{\text{volume da região fundamental coberta pelas esferas de raio } \rho}{\text{volume da região fndamental}}.$$

Seja $B(\rho)$ a esfera com centro na origem e raio ρ; temos que $v(B(\rho)) = v(B(1)).\rho^n$. Deste modo

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

dessa maneira fica conveniente introduzir um outro parâmetro, a *densidade de centro*:

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

2.4 O Homomorfismo Canônico

Nesta seção descrevemos o homomorfismo canônico de um corpo de números $\mathbb{K}$, com o qual é possível obter reticulados de posto n em $\mathbb{R}^n$ a partir de ideais de $\mathbb{K}$.

Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Se $\sigma_i(\mathbb{K}) \in \mathbb{R}$, dizemos que σ_i é real; caso contrário dizemos complexo. O corpo $\mathbb{K}$ é dito *totalmente real* quando todos seus monomorfismos são reais, senão $\mathbb{K}$ é dito *totalmente imaginário.*

Temos que $n = s_1 + 2s_2$, onde s_1 é o número de monomorfismos reais e $2s_2$ o número de imaginários. Podemos supor os monomorfismos ordenados da seguinte maneira:

$$\sigma_1, ..., \sigma_{s_1}, \sigma_{s_1+1}, \overline{\sigma_{s_1+1}}, ..., \sigma_{s_1+s_2}, \overline{\sigma_{s_1+s_2}}$$

onde $\sigma_1, ..., \sigma_{s_1}$ são os monomorfismos reais e os demais imaginários. Assim definimos *homomorfismo canônico* como sendo:

$$\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$$

por

$$\sigma_{\mathbb{K}}(\alpha) = (\sigma_1(\alpha), ..., \sigma_{s_1}(\alpha), Re\sigma_{s_1+1}(\alpha), Im\sigma_{s_1+1}(\alpha), ..., Re\sigma_{s_1+s_2}(\alpha), Im\sigma_{s_1+s_2}(\alpha)).$$

Este homomorfismo é importante pois gera reticulados em $\mathbb{R}^n$ dos quais os principais parâmetros podem ser obtidos via Teoria Algébrica dos Números, como veremos a seguir.

Teorema 2.4.1 ([*10*], pag. 56) *Sejam $\mathbb{K}$ um corpo de números de grau n, $\sigma_1, ..., \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ e $M \subset \mathbb{K}$ um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{x_1, ..., x_n\}$. Então*

(a) *$\sigma_{\mathbb{K}}(M)$ é um reticulado,*

(b) *$v(\sigma_{\mathbb{K}}(M)) = 2^{-s_2} |\det(\sigma_i(x_j))|$.*

Demonstração:

(a) Sendo $\{x_1, ..., x_n\}$ uma base de M, mostramos que $\{\sigma_{\mathbb{K}}(x_1), ..., \sigma_{\mathbb{K}}(x_n)\}$ é uma base de $\sigma_{\mathbb{K}}(M)$. No caso em que $\mathbb{K}$ é totalmente real,

$$\sigma_{\mathbb{K}}(x_i) = (\sigma_1(x_i), ..., \sigma_n(x_i)),\ i = 1, ..., n$$

Seja

$$D = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_n(x_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \cdots & \sigma_n(x_n) \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} . \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} = (\sigma_i(x_j)).$$

Assim, $\det(D) = \det(\sigma_i(x_j))$, por outro lado, sabemos que:

$$\Delta[x_1, ..., x_n] = (\det(\sigma_i(x_j)))^2,$$

logo

$$(\det(D))^2 = (\det(\sigma_i(x_j)))^2 = \Delta[x_1, ..., x_n].$$

Pelo Teorema 1.2.2 $\Delta[x_1, ..., x_n]$ é não nulo, daí segue que $\sigma_{\mathbb{K}}(x_1), ..., \sigma_{\mathbb{K}}(x_n)$ são vetores linearmente independentes sobre $\mathbb{R}$. Por construção $\sigma_{\mathbb{K}}(x_1), ..., \sigma_{\mathbb{K}}(x_n)$ geram $\sigma_{\mathbb{K}}(M)$ logo $\{\sigma_{\mathbb{K}}(x_1), ..., \sigma_{\mathbb{K}}(x_n)\}$ é uma base de $\sigma_{\mathbb{K}}(M)$ e, portanto, $\sigma_{\mathbb{K}}(M)$ é um reticulado.

Para o caso em que $\mathbb{K}$ é totalmente imaginário, provamos com argumentos similares que $\sigma_{\mathbb{K}}(M)$ é um reticulado.

(b) Mostremos que $v(\sigma_{\mathbb{K}}(M)) = 2^{-s_2}|\det(\sigma_i(x_j))|$, quando $\mathbb{K}$ é totalmente imaginário. Neste caso

$$\sigma_{\mathbb{K}}(x_i) = (Re\sigma_1(x_i), Im\sigma_1(x_i), ..., Re\sigma_{s_2}(x_i), Im\sigma_{s_2}(x_i)),\ i = 1, ..., n.$$

Seja

$$D = \begin{pmatrix} Re\sigma_1(x_1) & Im\sigma_1(x_1) & \cdots & Re\sigma_{s_2}(x_1) & Im\sigma_{s_2}(x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re\sigma_1(x_n) & Im\sigma_1(x_n) & \cdots & Re\sigma_{s_2}(x_n) & Im\sigma_{s_2}(x_n) \end{pmatrix}$$

Sabemos que $Rez = \frac{1}{2}(z+\bar{z})$ e $Imz = \frac{1}{2i}(z-\bar{z})$, deste modo somando à cada coluna de ordem ímpar a coluna seguinte previamente multiplicada por i, e multiplicando colunas par por $-2i$ e a cada uma delas adicionando a coluna anterior, obtemos a matriz

$$D_1 = \begin{pmatrix} \sigma_1(x_1) & \overline{\sigma_1(x_1)} & \cdots & \sigma_{s_2}(x_1) & \overline{\sigma_{s_2}(x_1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(x_n) & \overline{\sigma_1(x_n)} & \cdots & \sigma_{s_2}(x_n) & \overline{\sigma_{s_2}(x_n)} \end{pmatrix}.$$

Como $\det(D) = (2i)^{-s_2}.\det(D_1)$ e $\overline{\sigma_i} = \sigma_{s_2+i}$, então

$$v(\sigma_{\mathbb{K}}(M)) = |\det(D)| = |(2i)^{-s_2}|.|\det(D_1)| = 2^{-s_2}.|\det(\sigma_i(x_j))|.$$

■

Exemplo 2.4.1 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ e $M = \mathbb{Z}[\sqrt{7}]$ um $\mathbb{Z}$-módulo livre com base $\{1, \sqrt{7}\}$. Pelo Teorema acima temos que $\sigma_{\mathbb{K}}(M)$ é um reticulado e ainda sendo $s_2 = 0$, temos:*

$$v(\sigma_{\mathbb{K}}(M)) = \left|\det \begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix}\right| = |-2\sqrt{7}| = 2\sqrt{7}.$$

Exemplo 2.4.2 *Tome $\mathbb{K} = \mathbb{Q}(\sqrt{-20})$ e $M = \mathbb{Z}[\sqrt{-20}]$ um $\mathbb{Z}$-módulo livre com base $\{1, \sqrt{-20}\}$. Então $\sigma_{\mathbb{K}}(M)$ é um reticulado e como $s_2 = 1$, temos:*

$$v(\sigma_{\mathbb{K}}(M)) = 2^{-1}\left|\det \begin{pmatrix} 1 & \sqrt{-20} \\ 1 & -\sqrt{-20} \end{pmatrix}\right| = \frac{1}{2}|-2\sqrt{-20}| = |\sqrt{-20}| = |i\sqrt{20}| = \sqrt{20}.$$

Sendo $\mathcal{O}_{\mathbb{K}}$ um $\mathbb{Z}$-módulo livre de posto n; então um ideal não nulo $\mathfrak{a}$ de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto menor ou igual a n. Como o índice de $\mathfrak{a}$ sobre $\mathcal{O}_{\mathbb{K}}$ é finito, temos que $\mathfrak{a}$ é um $\mathbb{Z}$-módulo livre de posto n. Logo pelo Teorema 2.4.1 $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um reticulado. E ainda dizemos que a *representação geométrica* do ideal $\mathfrak{a}$ é o reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$.

Teorema 2.4.2 ([*10*], pag. 57) *Sejam $\mathbb{K}$ um corpo de números de grau n, com discriminante $D_{\mathbb{K}}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Então,*

$$v(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-s_2}.|D_{\mathbb{K}}|.N(\mathfrak{a}).$$

Demonstração:

Seja $\{x_1, ..., x_n\}$ uma base do ideal $\mathfrak{a}$ e como $\mathcal{O}_{\mathbb{K}} \subset \mathbb{K}$, segue do Teorema 2.4.1, $v(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-s_2}.|\det(\sigma_i(x_j))|$. Por outro lado, temos pelo Teorema 1.7.1 que:

$$|\Delta[x_1, ..., x_n]|^{1/2} = |D_{\mathbb{K}}|^{1/2}.N(\mathfrak{a})$$

e $\Delta[x_1, ..., x_n] = (\det(\sigma_i(x_j)))^2$, logo

$$v(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-s_2}.|D_{\mathbb{K}}|.N(\mathfrak{a}).$$

■

Pelo resultado acima, temos que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{a})$ é dada pela expressão:

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{s_2}.\rho^n}{|D_{\mathbb{K}}|^{1/2}.N(\mathfrak{a})}.$$

A determinação do parâmetro ρ será o objetivo central do próximo capítulo.

Capítulo 3

Corpos Abelianos de Condutor Primo

Vimos que um dos parâmetros para o cálculo da densidade de centro de um reticulado é a distância mínima entre seus pontos. Aqui veremos que essa distância é medida pela função traço e ainda obteremos uma forma quadrática dessa função em corpos de condutor primo.

Estaremos interessados na minimização desta forma quadrática, a qual será feita em ideais que se ramificam completamente em $\mathcal{O}_{\mathbb{L}}$, o anel dos inteiros algébricos de $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Então, primeiramente, veremos a caracterização desses ideais e sua norma, depois a forma quadrática e sua minimização. Com esses parâmetros será possível calcular a densidade de centro do reticulado, atingindo assim o objetivo central deste trabalho.

Podemos citar como principais resultados a Proposição 3.1.1, que caracteriza o ideal gerado por $(1 - \zeta_p)$, o Teorema 3.1.1 mostrando a forma traço de $\mathbb{Q}(\zeta_p)$ e o Lema 3.1.1 onde se obtem a forma traço em corpos de condutor primo.

Como neste capítulo encontra-se o principal objetivo deste trabalho, optamos por demonstrar todos os resultados, exceto o Teorema 3.2.1 pois sua demonstração não faz parte do nosso objetivo.

3.1 A forma quadrática nos subcorpos de $\mathbb{Q}(\zeta_p)$

Como já foi dito o nosso interesse está em ideais que se ramificam completamente em $\mathcal{O}_{\mathbb{L}}$. Do Teorema 1.6.6, temos que tal ideal é $p\mathbb{Z}$ e pelo Lema de Kummer sua decomposição é:

$$p\mathcal{O}_{\mathbb{L}} = \mathfrak{p}_{\mathbb{L}}^{p-1},$$

onde $\mathfrak{p}_{\mathbb{L}} = (1-\zeta_p)\mathcal{O}_{\mathbb{L}}$.

No restante deste Capítulo, $\mathbb{K}$ será um subcorpo de $\mathbb{L}$ de grau $(p-1)/d$ e pelo Teorema 2.2.2 temos que $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = T_{\mathbb{L}/\mathbb{K}}(\zeta_p)$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_{g^{(p-1)/d}}(\theta)$, onde σ_g é um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.

Denotando por $\mathfrak{p}_{\mathbb{K}}$ o ideal $\mathfrak{p}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$, temos pela Proposição 1.6.1 que a decomposição de $p\mathcal{O}_{\mathbb{K}}$ é:

$$p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_{\mathbb{K}}^{(p-1)/d}.$$

Com relação a norma dos ideias $\mathfrak{p}_{\mathbb{K}}$ e $\mathfrak{p}_{\mathbb{L}}$ temos, pela teoria desenvolvida na seção 1.7, que:

$$N(\mathfrak{p}_{\mathbb{K}}) = N(\mathfrak{p}_{\mathbb{L}}) = N_{\mathbb{L}/\mathbb{Q}}(1-\zeta_p) = p.$$

A próxima Proposição caracteriza os elementos de $\mathfrak{p}_{\mathbb{L}}$ e de $\mathfrak{p}_{\mathbb{K}}$.

Proposição 3.1.1 *Com a notação acima seja $y \in \mathcal{O}_{\mathbb{K}}$ onde $y = b_1\sigma_g(\theta) + b_2\sigma_{g^2}(\theta) + \cdots + b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta)$ logo*

$$y \in p_{\mathbb{K}} \iff \sum_{k=1}^{(p-1)/d} b_k \equiv 0 \pmod{p}$$

Demonstração:

- Primeiro consideremos o caso $\mathbb{K} = \mathbb{L}$

Logo temos $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p]$, daí se $y \in \mathcal{O}_{\mathbb{L}}$, temos que $y = b_1\zeta_p + b_2\zeta_p^2 + \cdots + b_{p-1}\zeta_p^{p-1}$, onde $b_k \in \mathbb{Z}$. E ainda $\mathfrak{p}_{\mathbb{L}} = (1-\zeta_p)\mathcal{O}_{\mathbb{L}}$, dessa forma $\zeta_p \equiv 1 \pmod{\mathfrak{p}_{\mathbb{L}}}$, portanto

$$y \equiv \sum_{k=1}^{p-1} b_k \pmod{\mathfrak{p}_{\mathbb{L}}},$$

dessa forma,

$$y \in \mathfrak{p}_{\mathbb{L}} \Longleftrightarrow \sum_{k=1}^{p-1} b_k \in \mathfrak{p}_{\mathbb{L}}.$$

Por outro lado, $\sum_{i=1}^{p-1} b_k \in \mathbb{Z}$ logo,

$$y \in \mathfrak{p}_{\mathbb{L}} \Longleftrightarrow \sum_{k=1}^{p-1} b_k \in \mathfrak{p}_{\mathbb{L}} \cap \mathbb{Z} = p\mathbb{Z},$$

assim,

$$y \in \mathfrak{p}_{\mathbb{L}} \Longleftrightarrow \sum_{k=1}^{p-1} b_k \equiv 0 \pmod{p}.$$

- Agora seja $\mathbb{K} = \mathbb{Q}(\theta)$

Temos $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\sigma_g(\theta) + \mathbb{Z}\sigma_{g^2}(\theta) + \cdots + \mathbb{Z}\sigma_{g^{(p-1)/d}}(\theta)$, logo se $y \in \mathcal{O}_{\mathbb{K}}$ temos

$$y = b_1 \sum_{i=1}^{d} \zeta_p^{i(p-1)/d+1} + b_2 \sum_{i=1}^{d} \zeta_p^{i(p-1)/d+2} + \cdots + b_{(p-1)/d} \sum_{i=1}^{d} \zeta_p^{i(p-1)/d+(p-1)/d}$$

e ainda $y \in \mathfrak{p}_{\mathbb{K}}$ se, e somente se, $y \in \mathfrak{p}_{\mathbb{L}}$.

Por outro lado,

$$y = \sum_{j=1}^{p-1} c_j \zeta_p^j$$

onde, $\{c_j, j = i(p-1)/d + k,\ i = 1, ..., d\} = \{b_k,\ k = 1, ..., (p-1)/d\}$, isto é, cada c_j repete d vezes e pelo caso anterior

$$y \in \mathfrak{p}_{\mathbb{L}} \Longleftrightarrow \sum_{j=1}^{p-1} c_j = d \sum_{k=1}^{(p-1)/d} b_k \equiv 0 \pmod{p},$$

mas d é um divisor de $p-1$, e portanto, p não divide d. Consequentemente $\sum_{k=1}^{(p-1)/d} b_k \equiv 0 \pmod{p}$, logo

$$y \in \mathfrak{p}_{\mathbb{K}} \Longleftrightarrow \sum_{k=1}^{(p-1)/d} b_k \equiv 0 \pmod{p}.$$

■

Exemplo 3.1.1 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{19})$, $\mathfrak{p}_{\mathbb{L}} = (1-\zeta_{19})\mathcal{O}_{\mathbb{L}}$ *e* $x \in \mathcal{O}_{\mathbb{L}}$ *onde*

$$x = 2\zeta_{19} + 3\zeta_{19}^2 + 10\zeta_{19}^5 + \zeta_{19}^{18}.$$

Pela Proposição 3.1.1 $x \notin \mathfrak{p}_{\mathbb{L}}$ *pois,* $2 + 3 + 10 + 1 = 16 \neq 0 \pmod{19}$.

Agora mostramos que, nos reticulados $\sigma_{\mathbb{K}}(\mathfrak{a})$, onde $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, a distância entre seus pontos é medida pela função traço.

Proposição 3.1.2 ([*12*], pag. 225) *Sejam $\mathbb{K}$ um corpo de números e $x \in \mathbb{K}$. Então:*

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}}.Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}),$$

sendo

$$c_{\mathbb{K}} = \begin{cases} 1, & se \quad s_2 = 0; \\ 1/2, & se \quad s_1 = 0, \end{cases}$$

onde s_1 é o número de monomorfismos reais e s_2 é a metade do número de monomorfismos imaginários.

Demonstração:

No caso em que $s_2 = 0$, isto é, $\mathbb{K}$ totalmente real, para $x \in \mathbb{K}$ e $\sigma_{\mathbb{K}} = (\sigma_1(x), ..., \sigma_n(x))$, segue que:

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

Agora, suponhamos $s_1 = 0$, ou seja, $\mathbb{K}$ totalmente imaginário. Então para $x \in \mathbb{K}$, $n = 2s_2$ e $\sigma_{\mathbb{K}}(x) = (Re\sigma_1(x), Im\sigma_1(x), ..., Re\sigma_{s_2}(x), Im\sigma_{s_2}(x))$, temos:

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

Sendo

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \sigma_1(x\overline{x}) + \cdots + \sigma_{n/2}(x\overline{x}) + \overline{\sigma}_1(x\overline{x}) + \cdots + \overline{\sigma}_{n/2}(x\overline{x}),$$

e

$$\overline{\sigma}_i(x\overline{x}) = \sigma_i(x\overline{x}), \quad \forall i = 1, ..., s_2/2,$$

segue que

$$Tr(x\overline{x}) = 2(\sigma_1(x\overline{x}) + \cdots + \sigma_{n/2}(x\overline{x})).$$

Portanto

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}Tr(x\overline{x}).$$

■

Tomando $\mathbb{L} = \mathbb{Q}(\zeta_p)$ a expressão $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ assume a seguinte forma quadrática:

Teorema 3.1.1 *Sejam p um número primo, $\mathbb{L} = \mathbb{Q}(\zeta_p)$ e x um elemento de $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p]$,*

$$x = a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}.$$

Então

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = (p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_i a_j. \tag{3.1}$$

Demonstração:

Seja $x = a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}$, assim $\overline{x} = a_1\zeta_p^{-1} + a_2\zeta_p^{-2} + \cdots + a_{p-1}\zeta_p^{-(p-1)}$, logo

$$x\overline{x} = (a_1^2 + \cdots + a_{p-1}^2) + (a_1a_2 + a_2a_3 + \cdots + a_{p-2}a_{p-1})(\zeta_p + \zeta_p^{-1}) +$$

$$+(a_1a_3 + a_2a_4 + \cdots + a_{p-3}a_{p-1})(\zeta_p^2 + \zeta_p^{-2}) + \cdots + a_1a_{p-1}(\zeta_p^{(p-2)} + \zeta_p^{-(p-2)}).$$

Fazendo $A_i = a_1a_{1+i} + \cdots + a_{p-1-i}a_{p-1}$ e $\alpha_i = \zeta_p^i + \zeta_p^{-i}$, para $i = 1, ..., p-2$ temos que $x\overline{x} = \sum_{i=1}^{p-1} a_i^2 + \sum_{i=1}^{p-2} A_i\alpha_i$, daí

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=1}^{p-1} a_i^2\right) + Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=1}^{p-2} A_i\alpha_i\right).$$

Usando as propriedades da função traço temos que:

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = (p-1)\sum_{i=1}^{p-1} a_i^2 + \sum_{i=1}^{p-2} A_i Tr_{\mathbb{L}/\mathbb{Q}}(\alpha_i),$$

e ainda

$$Tr_{\mathbb{L}/\mathbb{Q}}(\alpha_i) = Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i + \zeta_p^{-i}) = 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i),$$

como $i = 1, ...p-2$ então $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i) = -1$.

Também observemos que $\sum_{i=1}^{p-2} A_i = \sum_{1\leq i<j\leq p-1} a_i a_j$, assim

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = (p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_i a_j.$$

■

Exemplo 3.1.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{23})$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_{23}]$. *Tomemos*

$$x = 2\zeta_{23} + \zeta_{23}^2 + 5\zeta_{23}^4 - 3\zeta_{23}^6 + 7\zeta_{23}^{10} - \zeta_{23}^{13} + 2\zeta_{23}^{22},$$

então

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = (p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_i a_j = 1972.$$

Para cada r, s inteiros, seja $Q_{r,s}$ a forma quadrática dada por

$$Q_{r,s}(x_1, ..., x_r) = \sum_{i=1}^{r} x_i^2 + s\sum_{1\leq i<j\leq r} (x_i - x_j)^2.$$

Associando $x = a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}$, um elemento em $\mathcal{O}_{\mathbb{L}}$, à $(p-1)$-upla $\underline{x} = (a_1, a_2, ..., a_{p-1})$, verifica-se que:

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Q_{p-1,1}(\underline{x}).$$

Agora seja $\mathbb{K}$ um subcorpo de $\mathbb{L}$, com $[\mathbb{L} : \mathbb{K}] = d$; assim temos

Lema 3.1.1 *Dado* $y \in \mathcal{O}_{\mathbb{K}}$ *com*

$$y = b_1\sigma_g(\theta) + \cdots + b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta),$$

então

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{(p-1)/d} b_i^2 + d\sum_{1\leq i<j\leq p-1/d} (b_i - b_j)^2. \tag{3.2}$$

Demonstração:

Seja $y = b_1\sigma_g(\theta) + \cdots + b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta)$, como $\theta = Tr_{\mathbb{L}/\mathbb{K}}(\zeta_p)$, então

$$y = b_1\sum_{i=1}^{d}\zeta_p^{g^{i(p-1)/d+1}} + b_2\sum_{i=1}^{d}\zeta_p^{g^{i(p-1)/d+2}} + \cdots + b_{(p-1)/d}\sum_{i=1}^{d}\zeta_p^{g^{is+(p-1)/d}}.$$

Pelo o exposto na demonstração da Proposição 3.1.1 associamos a y a $(p-1)$-upla $\underline{y} = (\underbrace{b_1, ..., b_1}_{d \text{ vezes}}, \underbrace{b_2, ..., b_2}_{d \text{ vezes}}, ..., \underbrace{b_{(p-1)/d}, ..., b_{(p-1)/d}}_{d \text{ vezes}})$, assim temos que:

$$Tr_{\mathbb{L}/\mathbb{Q}}(y\overline{y}) = Q_{p-1}(\underline{y}),$$

logo

$$Tr_{\mathbb{L}/\mathbb{Q}}(y\overline{y}) = d\sum_{i=1}^{(p-1)/d} b_i^2 + d^2 \sum_{1\leq i<j\leq (p-1)/d} (b_i - b_j)^2.$$

Usando as propriedades da função traço temos que:

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \frac{1}{d}Tr_{\mathbb{L}/\mathbb{Q}}(y\overline{y}),$$

ou seja

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{(p-1)/d} b_i^2 + d \sum_{1\leq i<j\leq (p-1)/d} (b_i - b_j)^2.$$

■

Associando $y = b_1\sigma_g(\theta)+\cdots+b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta)$, um elemento em $\mathcal{O}_{\mathbb{K}}$, à $(p-1)/d$-upla $\underline{y} = (b_1, ..., b_{(p-1)/d})$, verifica-se que:

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = Q_{\frac{p-1}{d},d}(\underline{y}).$$

Exemplo 3.1.3 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{17})$ e $\mathbb{K} \subset \mathbb{L}$, com $[\mathbb{L} : \mathbb{K}] = 4$. Dado $y \in \mathcal{O}_{\mathbb{K}}$, associando a esse $\underline{y} = (1, 5, -3, 7)$, temos:*

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = Q_{\frac{p-1}{d},d}(\underline{y}) = 1028.$$

Observe que a forma quadrática (3.2) pode ser escrita como:

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = (p-d)\sum_{i=1}^{(p-1)/d} b_i^2 - 2d \sum_{1\leq i<j\leq (p-1)/d} (b_i b_j).$$

Vimos no Capítulo 2 que a expressão para a densidade de centro dos reticulados $\sigma_{\mathbb{K}}(\mathfrak{a})$, onde $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ é dada por:

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{s_2}\rho^n}{|D_{\mathbb{K}}|^{1/2}.N(\mathfrak{a})}. \tag{3.3}$$

Sabemos que $\rho = \frac{1}{2}\min\{|\sigma_{\mathbb{K}}(x)|;\ 0 \neq x \in \mathfrak{a}\}$ e da Proposição 3.1.2 segue que:

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}} Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Logo, tomando

$$t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x});\ 0 \neq x \in \mathfrak{a}\},$$

temos

$$\rho^n = \frac{c_{\mathbb{K}}^{n/2}}{2^n} t^{n/2}.$$

Substituindo a expressão encontrada para ρ^n na equação 3.3, obtemos

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{2^{s_2} c_{\mathbb{K}}^{n/2} t^{n/2}}{2^n |D_{\mathbb{K}}|^{1/2} N(\mathfrak{a})}.$$

Note que $2^{s_2} c_{\mathbb{K}}^{n/2} = 1$, assim

$$\sigma_{\mathbb{K}}(\mathfrak{a}) = \frac{1}{2^n |D_{\mathbb{K}}|^{1/2}}\ \frac{t^{n/2}}{N(\mathfrak{a})}.$$

3.2 Minimização da forma quadrática em $\mathbb{K}$

Estudaremos a minimização, tomando os elementos no ideal $\mathfrak{p}_{\mathbb{K}}$. Dois resultados úteis são:

Teorema 3.2.1 ([2] pag. 81) *Dados os números inteiros $a_1, ..., a_r$, com $r < p-1$, seja*

$$F(x_{r+1}, ..., x_{p-1}) = Q_{p-1,1}(a_1, ..., a_r, x_{r+1}, ..., x_{p-1}).$$

Então F atinge seu mínimo com entradas inteiras no ponto

$$(y, y, ..., y), \quad \text{com} \quad y = \left\lfloor \frac{a_1 + \cdots + a_r}{r+1} \right\rceil,$$

onde $\lfloor z \rceil$ denota o inteiro mais próximo de z.

Corolário 3.2.1 *Dado os números inteiros $a_1, ..., a_r$, com $r < (p-1)/d$, seja*

$$F(x_{r+1}, ..., x_{(p-1)/d}) = Q_{\frac{p-1}{d},d}(a_1, ..., a_r, x_{r+1}, ..., x_{(p-1)/d})$$

Então F atinge seu mínimo com entradas inteiras no ponto

$$(y, y, ..., y) \text{ com } y = \left\lfloor \frac{a_1 + \cdots + a_r}{r + 1/d} \right\rfloor.$$

Demonstração:

Tomando cada a_i, $i = 1, ..., r$ repetindo d vezes, então pelo Teorema 3.2.1 minimizamos a forma quadrática

$$Q_{p-1,1}(a_1, ..., a_1, ..., a_r, ..., a_r, x_1, ..., x_{(p-1)/d}),$$

fazendo

$$x_1 = \cdots = x_{(p-1)/d} = \left\lfloor \frac{d(a_1 + a_2 + \cdots + a_r)}{dr + 1} \right\rfloor,$$

e cada x_i, $i = 1, ..., (p-1)/d$ está repetindo d vezes. Assim a forma quadrática $Q_{\frac{p-1}{d},d}$ é minimizada no ponto

$$(y, y, ..., y) \text{ com } y = \left\lfloor \frac{a_1 + \cdots + a_r}{r + 1/d} \right\rfloor.$$

■

Observação 3.2.1 *Sejam $y, y' \in \mathcal{O}_{\mathbb{K}}$, como feito anteriormente, associamos a y e y', respectivamente, as $(p-1)/d$-uplas $\underline{y} = (a, m, ..., m)$ e $\underline{y'} = (b, m', ..., m')$. Tomando $a > b > 0$, $m = \left\lfloor \frac{a}{1+1/d} \right\rfloor$ e $m' = \left\lfloor \frac{b}{1+1/d} \right\rfloor$, então*

$$Q_{\frac{p-1}{d},d}(\underline{y}) > Q_{\frac{p-1}{d},d}(\underline{y'}).$$

De fato: Sendo $b > 0$ tomemos $a = b + 1$. Assim temos $\underline{y} = (b+1, m, ..., m)$ e $\underline{y'} = (b, m', ..., m)$', onde $m = \left\lfloor \frac{b}{1+1/d} + \frac{1}{1+1/d} \right\rfloor$ e $m' = \left\lfloor \frac{b}{1+1/d} \right\rfloor$, logo:

$$\begin{aligned} Q_{\frac{p-1}{d},d}(\underline{y}) &= (b+1)^2 + (\tfrac{p-1}{d} - 1)(m^2 + d(b+1-m)^2) \\ Q_{\frac{p-1}{d},d}(\underline{y'}) &= b^2 + (\tfrac{p-1}{d} - 1)(m'^2 + d(b-m')^2). \end{aligned}$$

Comparemos cada paracela

- *Sendo $b > 0$, então $(b+1)^2 > b^2$.*

- *Também temos que $m \geq m'$, pois $\frac{b+1}{1+1/d} > \frac{b}{1+1/d}$, logo $\left\lfloor \frac{b+1}{1+1/d} \right\rfloor \geq \left\lfloor \frac{b}{1+1/d} \right\rfloor$. Portanto $m \geq m' \geq 0$ e daí $m^2 \geq m'^2$.*

- *Agora temos*

$$(b+1) - m \geq b - m' \Leftrightarrow m - m' \leq 1,$$

para provarmos essa última desigualdade observe que $\frac{1}{2} \leq \frac{1}{1+1/d} < 1$, logo $\frac{b}{1+1/d} + \frac{1}{2} \leq \frac{b}{1+1/d} + \frac{1}{1+1/d} < \frac{b}{1+1/d} + 1$.

E ainda temos

$$\begin{array}{ccccc} \frac{b}{1+1/d} + \frac{1}{1+1/d} - \frac{1}{2} & \leq & m & \leq & \frac{b}{1+1/d} + \frac{1}{1+1/d} + \frac{1}{2} \\ \frac{b}{1+1/d} - \frac{1}{2} & \leq & m' & \leq & \frac{b}{1+1/d} + \frac{1}{2} \end{array}$$

Tomando os casos extremos em que $m' = \frac{b}{1+1/d} - \frac{1}{2}$ e $m = \frac{b}{1+1/d} + \frac{1}{1+1/d} + \frac{1}{2}$, temos que:

$$\begin{array}{rcl} m - m' & = & \frac{b}{1+1/d} + \frac{1}{1+1/d} + \frac{1}{2} - \frac{b}{1+1/d} + \frac{1}{2} \\ & = & \frac{1}{1+1/d} + 1 \end{array}.$$

Logo $m - m' < 2$, mas como m e m' são números inteiros segue que $m - m' = 1$ ou $m - m' = 0$, portanto $m - m' \leq 1$, então $(b + 1 - m) \geq b - m'$ e daí $(b + 1 - m)^2 \geq (b - m')^2$

Portanto $Q_{\frac{p-1}{d},d}(\underline{y}) > Q_{\frac{p-1}{d},d}(\underline{y'})$.

■

Observação 3.2.2 *Com a notação da seção anterior, dado y no ideal $\mathfrak{p}_{\mathbb{K}}$ então $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) \in p\mathbb{Z}$*

De fato: Pelo Teorema da Evidência 1.6.7 temos que $\sigma_i(\mathfrak{p}_{\mathbb{K}}) = \mathfrak{p}_{\mathbb{K}}$, para todo $\sigma_i \in Gal(\mathbb{K} : \mathbb{Q})$, $i = 1, ..., (p-1)/d$, logo para todo $y \in \mathfrak{p}_{\mathbb{K}}$ temos que $\sigma(y) \in \mathfrak{p}_{\mathbb{K}}$, portanto

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = \sum_{i=1}^{(p-1)/d} \sigma_i(y\overline{y}) \in \mathfrak{p}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}.$$

■

Usando esses fatos e tomando $y = b_1\sigma_g(\theta) + b_2\sigma_{g^2}(\theta) + \cdots + b_{(p-1)/d}\sigma_{g^{(p-1)/d}}(\theta)$, um elemento de $\mathfrak{p}_{\mathbb{K}}$, vamos agora minimizar a forma quadrática

$$Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = (p-d)\sum_{i=1}^{(p-1)/d} b_i^2 - 2d \sum_{1\leq i<j\leq (p-1)/d} (b_i b_j),$$

como na seção anterior associaremos a y, $\underline{y} = (b_1, b_2, ..., b_{(p-1)/d})$.

1. No caso em que d é ímpar temos que $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$ é par pois, $(p-d)$ é par; logo pela Observação 3.2.2 $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) \geq 2p$.

   O valor $2p$ é atingido para $y = 1\sigma_g(\theta) - 1\sigma_{g^2}(\theta)$, de fato:

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) &= (p-d)\sum_{i=1}^{(p-1)/d} b_i^2 - 2d \sum_{1\leq i<j\leq p-1/d} (b_i b_j) \\ &= (p-d)(1+1) - 2d(-1) \\ &= 2p - 2d + 2d \\ &= 2p \end{aligned}$$

   Assim quando d é ímpar temos que $\min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}),\ y \in \mathfrak{p}_{\mathbb{K}}\} = 2p$.

2. Veremos agora o caso em que d é par.

   Se $\underline{y}$ tem uma coordenada igual a d minimizamos a forma quadrática, completando as demais entradas com $\left\lfloor \frac{d}{1+1/d} \right\rfloor = d-1$, de fato:

   É fácil ver que:

$$-1 \ < \ 0 \ < \ \tfrac{d-1}{2},$$

   somando d^2, em cada parcela, temos:

$$d^2 - 1 \ < d^2 \ < \ d^2 + \tfrac{d}{2} - \tfrac{1}{2},$$

   finalmente dividindo por $d+1$,

$$d - 1 \ < \ \tfrac{d^2}{d+1} \ < \ d - \tfrac{1}{2},$$

   isto é,

$$d - 1 \ < \ \tfrac{d}{1+1/d} \ < \ d - \tfrac{1}{2}.$$

Portanto $\left\lfloor \frac{d}{1+1/d} \right\rfloor = d-1$

E ainda temos que para todo p primo ímpar e $\underline{y} = (d, d-1, ..., d-1)$,

$$Q_{\frac{p-1}{d},d}(\underline{y}) \geq 2p$$

pois:

$$\begin{array}{rcl} d^2 + (\frac{p-1}{d} - 1)(d-1)^2 + d((\frac{p-1}{d} - 1)1^2) & \geq & 2p \quad \Leftrightarrow \\ d^2 + dp - d - d^2 - 2p + 2 + 2d + \frac{p-1-d}{d} + p - 1 - d & \geq & 2p \quad \Leftrightarrow \\ -dp + d^2p + p - 1 - d + d & \geq & 2pd \quad \Leftrightarrow \\ p(d^2 - d + 1 - 2d) & \geq & 1, \end{array}$$

logo,

$$p \geq \frac{1}{d^2 - 3d + 1}, \tag{3.4}$$

e essa desigualdade é sempre satisfeita pois:

- Se $d = 2$, então 3.4 equivale a $p \geq -1$ o que sempre ocorre.
- Agora se $d > 3$, então $d^2 - 3d + 1 > 1$ e daí $\frac{1}{d^2-3d+1} < 1$, logo todo $p \geq \frac{1}{d^2-3d+1}$.

Portanto $Q_{\frac{p-1}{d},d}(\underline{y}) \geq 2p$, para todo p primo ímpar.

Pela Observação 3.2.1 para minimizarmos a forma quadrática teremos que tomar as entradas b_i, da seguinte forma: $-(d-1) \leq b_i \leq (d-1)$. E ainda queremos que $y \in \mathfrak{p}_{\mathbb{K}}$, logo

$$\sum_{i=1}^{(p-1)/d} b_i \equiv 0 \pmod{p},$$

nesse caso isso só ocorre quando

$$\sum_{i=1}^{(p-1)/d} b_i = 0,$$

pois $\sum_{i=1}^{(p-1)/d} b_i \leq (d-1)\frac{(p-1)}{d} < p-1.$

Dentro dessas condições podemos verificar que a forma quadrática não atinge o valor p. De fato, suponhamos que:

$$(p-d)\sum_{i=1}^{(p-1)/d} b_i^2 - 2d \sum_{1\leq i<j\leq (p-1)/d} b_i b_j = p. \tag{3.5}$$

Observa-se que sendo

$$\sum_{i=1}^{(p-1)/d} b_i = 0,$$

então,

$$\left(\sum_{i=1}^{(p-1)/d} b_i\right)^2 = 0,$$

isto é,

$$\sum_{i=1}^{(p-1)/d} b_i^2 + 2 \sum_{1\leq i<j\leq (p-1)/d} b_i b_j = 0,$$

assim,

$$\sum_{i=1}^{(p-1)/d} b_i^2 = -2 \sum_{1\leq i<j\leq (p-1)/d} b_i b_j.$$

substituindo em (3.5) temos:

$$(p-d)\sum_{i=1}^{(p-1)/d} b_i^2 + d\sum_{i=1}^{(p-1)/d} b_i^2 = p,$$

logo,

$$p\sum_{i=1}^{(p-1)/d} b_i^2 = p$$

e portanto

$$\sum_{i=1}^{(p-1)/d} b_i^2 = 1,$$

mas isso só ocorre quando temos uma entrada igual a ± 1 e as demais nulas, o que contraria o fato $\displaystyle\sum_{i=1}^{(p-1)/d} b_i = 0$.

Dessa maneira concluímos que no ideal $\mathfrak{p}_{\mathbb{K}}$

$$\sum_{i=1}^{(p-1)/d} b_i^2 + d \sum_{1\leq i<j\leq p-1/d} (b_i - b_j)^2 \geq 2p,$$

atingindo o mínimo em $2p$ para $y = 1\sigma_g(\theta) - 1\sigma_{g^2}(\theta)$.

3.2.1 Cálculo da densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}})$

Exemplo 3.2.1 *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{19})$, $\mathbb{K} \subset \mathbb{L}$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 3$, $\mathfrak{p}_{\mathbb{L}} = (1 - \zeta_{19})\mathcal{O}_{\mathbb{L}}$ *e* $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$.

Sabemos que $D_{\mathbb{K}} = \pm 19^2$, *que* $N(\mathfrak{p}_{\mathbb{K}}) = 19$ *e que* $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y});\ 0 \neq x \in \mathfrak{p}_{\mathbb{K}}\} = 38$. *Logo*

$$\begin{aligned} \delta(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}})) &= \frac{1}{2^n |D_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(\mathfrak{p}_{\mathbb{K}})} \\ &= \frac{1}{2^3 |19^2|^{1/2}} \frac{38^{3/2}}{19} \\ &\approx 0.08 \end{aligned}$$

Exemplo 3.2.2 *Agora sejam* $\mathbb{L} = \mathbb{Q}(\zeta_7)$, $\mathbb{K} \subset \mathbb{L}$ *tal que* $[\mathbb{K} : \mathbb{Q}] = 3$, $\mathfrak{p}_{\mathbb{L}} = (1 - \zeta_7)\mathcal{O}_{\mathbb{L}}$ *e* $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}}$.

Sabemos que $D_{\mathbb{K}} = \pm 7^2$, *que* $N(\mathfrak{p}_{\mathbb{K}}) = 7$ *e que* $t = \min\{Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y});\ 0 \neq x \in \mathfrak{p}_{\mathbb{K}}\} = 14$. *Logo*

$$\begin{aligned} \sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}) &= \frac{1}{2^n |D_{\mathbb{K}}|^{1/2}} \frac{t^{n/2}}{N(\mathfrak{p}_{\mathbb{K}})} \\ &= \frac{1}{2^3 |7^2|^{1/2}} \frac{14^{3/2}}{7} \\ &\approx 0.134 \end{aligned}$$

Referências Bibliográficas

[1] Boutros, J.; Viterbo, E.;*Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel*. IEEE Trans. Inform. Theory, V.44, n.4, 1988.

[2] Flores, A.L.; *Representação Geométrica de Ideais de Corpos de Números*. Dissertação de Mestrado, IMECC/UNICAMP, 1996.

[3] Flores, A.L.; *Reticulados em Corpos Abelianos*. Tese de Doutorado, FEEC/UNICAMP, 2000.

[4] Garcia, A.; Lequain, Y.; *Elementos de Álgebra*. Projeto Euclides, 2002.

[5] Gonçalves, A.; *Introdução à Álgebra*. Projeto Euclides, 1979.

[6] Herstein, I.N.; *Topics in Algebra*. John Wiley and Sons, 1975.

[7] Marcus, D.A.; *Number Fields*. Springer-Verlag, 1977.

[8] Monteiro, L.H.J.; *Elementos de Álgebra*. Impa, 1969.

[9] Nóbrega, T.P.; *Cúbicas Reais, Algumas Aplicações*. Anais do VI Encontro de Álgebra USP-UNICAMP,1997.

[10] Samuel, P.; *Algebric Theory of Numbers*. Hermann, 1970.

[11] Shannon, C.E.; *A Mathematical Theory of Communications*. BSTJ 27 (1948), 379 - 423 and 623 - 656.

[12] Sloane, N.J.A.; Conway, J.H.; *Sphere Packing, Lattices and Groups*. Springer-Verlag, 1999.

[13] Stewart, I.; Tall, D.; *Algebric Number Theory*. Chapman & Hall, 1987.

[14] Stewart, I.; *Galois Theory*. Chapman & Hall, 1989.

[15] Vicente, J.P.G.; *Reticulados de Posto 3 em Corpos de Números*. Dissertação de Mestrado,IBILCE-UNESP, 2000.

[16] Washington, L.; *Introduction to Cyclotomic Fields*. Spring-Verlag, 1982.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo