

Mariene de Fátima Oliveira Carvalho

Representação Geométrica de Ideais



1910001365





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

Representação Geométrica de Ideais

Mariene de Fátima Oliveira Carvalho

Orientador: Prof. Dr. Trajano P. da Nóbrega Neto



T. 1.365/05

Dissertação apresentada ao Departamento de
Matemática - IBILCE - UNESP, como parte dos
requisitos para a obtenção do Título de Mestre
em Ciências Matemáticas - Área de Concen-
tração: Matemática.

São José do Rio Preto - SP

Dezembro - 2004

512.91

C331r

04/03/2005

Doação

R\$ 25,00

Autor(a)

076/2005

79/05

10101004

Carvalho, Mariene de Fátima Oliveira.

Representação geométrica de ideais / Mariene de Fátima Oliveira Carvalho – São José do Rio Preto : [s.n.], 2004
110 f. ; 30 cm.

Orientador: Trajano Pires da Nóbrega Neto

Dissertação (mestrado) – Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra. 2. Teoria dos números algébricos. 3. Teoria dos reticulados. I. Nóbrega Neto, Trajano Pires da. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 512

"Feliz aquele que transfere o
que sabe e aprende o que
ensina."

(Cora Coralina)



Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus

Ao Prof. Dr. Trajano Pires da Nóbrega Neto, pela orientação, paciência e amizade;

A banca examinadora: Prof. Dr. Trajano Pires da Nóbrega Neto, Prof. Dr. Antônio Aparecido de Andrade e Prof. Dr. André Luís Flamin.

Aos professores do Departamento de Matemática da UNESP-S.José do Rio Preto, em especial aos professores Aparecida Franchesca da Silva e Waldemar Donizete Pastos pela acolhida e orientação.

Aos professores do Departamento de Matemática da UFMT-Rondonópolis, pela formação acadêmica e estímulo.

A minha família, pelo carinho e estímulo.

Ao Alípio Porciano de Carvalho, pela dedicação e cuidados dispensados à minha filha,

Durvalina(in memorian)

Aos amigos Teciara, Anderson e Rodrigo, pelo companheirismo e pelas lembranças de

e Odílio(in memorian)

dissonância.

A todos os amigos que de alguma forma contribuíram para a conclusão deste trabalho.

Marilene

A CAPES, pelo apoio financeiro.

E à minha filha,

Etiane

dedico.

Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus.

Ao Prof. Dr. Trajano Pires da Nóbrega Neto, pela orientação, paciência e amizade.

À banca examinadora: Prof. Dr. Trajano Pires da Nóbrega Neto, Prof. Dr. Antônio Aparecido de Andrade e Prof. Dr. André Luíz Flores.

Aos professores do Departamento de Matemática da UNESP-S.José do Rio Preto, em especial aos professores Aparecida Francisco da Silva e Waldemar Donizete Bastos pela acolhida e orientação.

Aos professores do Departamento de Matemática da UFMT-Rondonópolis, pela formação acadêmica e estímulo.

À minha família, pelo carinho e estímulo.

Ao Alfredo Ponciano de Carvalho, pela dedicação e cuidados dispensados à nossa filha.

Aos amigos Taciana, Anderson e Rodrigo, pelo companherismo e pelos momentos de descontração.

À todos os amigos que de alguma forma contribuíram para a conclusão deste trabalho.

À CAPES, pelo apoio financeiro.



Resumo

O principal objetivo deste trabalho é estudar a representação geométrica de ideais em corpos de números abelianos, isto será feito de dois modos. No primeiro, estudamos os reticulados gerados através de ideais ordinários do anel dos inteiros algébricos de $\mathbb{Q}(\xi_{p^r})$ com p primo. No segundo, estudamos os reticulados gerados por ideais ordinários contidos no anel dos inteiros algébricos de $\mathbb{Q}(\xi_{pq})$ com p, q primos ímpares distintos e $o_q(p) \equiv o_p(q) \equiv 1 \pmod{2}$.

Em ambos os casos calculamos a densidade de centro de tais reticulados, obtidos via representação geométrica de ideais. Este cálculo é feito a partir do discriminante do corpo, da norma do ideal e da minimização da função traço.

Palavras-chave: Corpos Ciclotômicos, Reticulados, Densidade de Centro.

Abstract

The main aim of this work is study the geometric representation of the ideals in abelian number fields. We are going to do this in two ways. First, we study the algebraic lattices generated by ordinary ideals of the algebraic integer ring of $\mathbb{Q}(\xi_{p^r})$, where p is a prime number and $r > 1$. Second, we study the algebraic lattices generated by ordinary ideals of the algebraic integer ring of $\mathbb{Q}(\xi_{pq})$, where p, q are prime number and $o_q(p) \equiv o_p(q) \equiv 1 \pmod{2}$.

From these lattices, generated from geometric representation of ideals, we calculate the center density. These calculations were made using the discriminant of the field, the norm of the ideal and the minimization of trace form.

Keywords: Cyclotomic Fields, Lattices, Center Density.

Sumário

Introdução	11
1 Corpos de Números	15
1.1 Elementos Algébricos sobre um Corpo	15
1.2 Conjugados e Discriminantes	19
1.3 Inteiros Algébricos	24
1.4 Base Integral	28
1.5 Norma e Traço	32
1.6 Decomposição em Irredutíveis	34
1.7 Fatoração de Ideais	39
1.8 Norma de um Ideal	48
2 Corpos Quadráticos e Ciclotômicos	52
2.1 Corpos Quadráticos	53
2.2 Corpos Ciclotômicos	58
2.2.1 O p -ésimo corpo ciclotômico.	62
2.3 Corpos de Números Abelianos	69
2.4 Reticulados	82

2.5 O Homomorfismo Canônico 85

3 Corpos Abelianos 91

3.1 A forma quadrática no corpo ciclotômico $\mathbb{Q}(\xi_n)$ 92

3.2 Os Reticulados Algébricos 97

3.3 Subcorpos de $\mathbb{Q}(\xi_{p^r})$ 101

3.4 Subcorpos de $\mathbb{Q}(\xi_{pq})$ 104

Bibliografia 110

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

$f_\alpha(X)$: polinômio característico de α

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

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

$\#X$: cardinalidade do conjunto X

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p}, \dots$: ideais

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

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



$A \times B$: produto cartesiano de A por B

(r, s) : máximo divisor comum de r e s

$\phi(n)$: número de elementos de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ ou ϕ de Euler

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

$K(\alpha_1, \dots, \alpha_n)$: o corpo obtido pela adjunção de $\alpha_1, \dots, \alpha_n$ a K

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

$\forall$: para todo

$\exists$: existe

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

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

D_K : discriminante absoluto do corpo K

$\text{Tr}_{L/K}$: traço em relação à extensão L/K

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

A : conjunto dos números algébricos

B : conjunto dos inteiros algébricos

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

$\text{Ker}(f)$: núcleo do homomorfismo f

$\langle \alpha_1, \dots, \alpha_n \rangle$: ideal gerado por $\alpha_1, \dots, \alpha_n$

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

$G \triangleleft H$: G é um subgrupo normal de H



Introdução

A forma de dispor esferas de mesmo raio no espaço euclidiano $\mathbb{R}^n$ de modo a cobrir a maior parte do espaço e que a intersecção entre duas dessas esferas tenha no máximo um ponto foi um desafio e mereceu citação de Hilbert, que em 1900 relacionou-o como sendo o 18º numa lista de 23 problemas matemáticos mais relevantes do século.

À distribuição de esferas de mesmo raio no espaço euclidiano de tal modo que a intersecção entre duas delas tenha no máximo um ponto denominou-se Empacotamento Esférico. E a partir da data acima citada, muitas teorias evoluíram em torno do 18º problema de Hilbert. Vários modelos matemáticos foram descritos com a finalidade de se obter empacotamentos esféricos com alta densidade; muitas cotas foram estabelecidas.

Os empacotamentos esféricos cujo conjunto de centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ começaram a ser estudados com maior interesse e receberam a denominação de Empacotamentos Reticulados.

Com o artigo de Shannon, publicado em 1948, onde foi demonstrada a estreita relação existente entre códigos corretores de erro eficientes e empacotamentos reticulados densos, o problema do empacotamento esférico proposto por Hilbert ganhou posição privilegiada na Teoria das Comunicações.

Várias técnicas foram desenvolvidas a fim de se obter reticulados, dentre essas técnicas algumas são baseadas em códigos corretores de erro e uma em especial, baseada na Teoria

Algébrica dos Números, foi descrito por Minkowski, quando este estudava a Teoria dos Corpos de Classe num período entre o final do século *XIX* e início do século *XX*. O método de Minkowski despertou o interesse em um número maior de matemáticos e os avanços foram surgindo naturalmente, dentre esses avanços destaca-se os trabalhos desenvolvidos por Maurice Craig. Outras colaborações foram surgindo a medida que o modelo se mostrava mais promissor.

Nos anos de 1994 e 1995, Joseph Boutros juntamente com a participação de outros três especialistas em Telecomunicações publicaram alguns resultados onde mostram que versões particulares de empacotamentos reticulados já conhecidos, construídos de corpos ciclotômicos coincidam com os reticulados mais densos conhecidos e até assumam novos recordes.

Isso limita o estudo às dimensões da forma $\phi(n)$, ϕ a função de Euler. Tal restrição se justifica pela complexidade do problema quando este é tratado em outros corpos, mesmo nos corpos abelianos.

Para a situação citada anteriormente, começam a surgir resultados promissores em corpos abelianos, cujo objetivo é fornecer contribuições do modelo de Minkowski em todas as dimensões cujas respectivas densidades estejam entre as maiores conhecidas.

Este trabalho tem como objetivo descrever alguns desses empacotamentos reticulados em corpos abelianos, cujo método consiste na representação geométrica de ideais do anel dos inteiros algébricos de um corpo de números abeliano.

No primeiro capítulo introduzimos os conceitos de corpos de números, elemento algébrico, discriminante, inteiro algébrico, base integral, norma e traço de um elemento, fatoração de um ideal primo e norma de um ideal, tais conceitos visam atender aos leitores com pouco conhecimento em Teoria Algébrica dos Números.



Os resultados considerados de maior relevância foram todos demonstrados, com exceção do Lema de Kummer, pois sua demonstração é muito complexa e envolve conceitos que destoam de nossos objetivos.

No Capítulo 2, apresentamos resultados básicos para a melhor compreensão do próximo capítulo, como os conceitos de corpos quadráticos, ciclotômicos e abelianos, bem como a caracterização do anel dos inteiros algébrico de um corpo quadrático e do polinômio ciclotômico. Na seção Corpos Abelianos destacam-se os Teoremas 2.3.2 e 2.3.3 para o cálculo do discriminante de um corpo, os quais serão aplicados no próximo capítulo.

Ainda no segundo Capítulo são apresentadas as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e o método de Minkowski, o qual consiste na obtenção de reticulados via representação geométrica de ideais ordinários não nulos do anel dos inteiros algébricos de um corpo de números. Destaca-se o Teorema 2.5.1 na seção "O Homomorfismo Canônico", por mostrar que a representação geométrica de um ideal é um reticulado e por apresentar uma fórmula geral para o cálculo da densidade de centro.

O Capítulo 3 é dedicado aos reticulados algébricos e suas aplicações, o principal objetivo deste capítulo é calcular a densidade de centro dos reticulados obtidos a partir de famílias de ideais em subcorpos de $\mathbb{Q}(\xi_{p^r})$ e de $\mathbb{Q}(\xi_{pq})$.

Neste capítulo introduzimos uma expressão para a forma quadrática do corpo ciclotômico $\mathbb{Q}(\xi_n)$ e caracterizamos os ideais ordinários não nulos cuja realização geométrica é nosso objeto de estudo. Na seção "Subcorpos de $\mathbb{Q}(\xi_{p^r})$ " apresentamos uma fórmula específica para o cálculo da densidade de centro de reticulados gerados através de ideais no anel dos inteiros algébricos de $\mathbb{Q}(\xi_{p^r})$ com p primo.

Na seção "Subcorpos de $\mathbb{Q}(\xi_{pq})$ " com p, q primos ímpares distintos e $o_q(p) \equiv o_q(p) \equiv$



1 (mod 2), demonstramos alguns resultados que auxiliam na melhor caracterização dos ideais no anel dos inteiros de $\mathbb{Q}(\xi_{pq})$ e também apresentamos uma fórmula para o cálculo da densidade de centro dos reticulados gerado por tais ideais.

Capítulo 1

Corpos de Números

O objetivo deste capítulo é introduzir conceitos básicos da Teoria dos Números, tendo em vista fornecer pré-requisitos para um melhor entendimento dos capítulos posteriores. Também é familiarizado com a notação aqui adotada. A presente seção visa os leitores que tenham conhecimentos elementares de Álgebra, que pode ser encontrada nas referências [24] e [25].

Neste capítulo introduziremos conceitos importantes da Teoria Algébrica dos Números, tais como elementos algébricos sobre um corpo, inteiros sobre um anel e observaremos as relações entre eles. Em seguida definiremos Corpo de Números e alguns de seus principais parâmetros, como: Anel dos Inteiros Algébricos, Discriminante, Base Integral, Norma e Traço de um elemento.

1.1 Elementos Algébricos sobre um Corpo

Quando K é um subcampo do corpo L , dizemos que L é uma extensão do corpo K e denotamos por L/K uma extensão de corpos. Denominamos a dimensão de L visto

Capítulo 1

Corpos de Números

O objetivo deste capítulo é introduzir conceitos básicos da Teoria dos Números, tendo em vista fornecer pré-requisitos para um melhor entendimento dos capítulos posteriores e também a familiarização com a notação aqui adotada. A presente redação visa os leitores que tenham conhecimentos elementares de Álgebra, que pode ser encontrado nas referências ([4]) e ([6]).

Neste capítulo introduziremos conceitos importantes da Teoria Algébrica do Números, tais como elementos algébricos sobre um corpo, inteiros sobre um anel e observaremos as relações entre eles. Em seguida definiremos Corpo de Números e alguns de seus principais parâmetros, como: Anel dos Inteiros Algébricos, Discriminante, Base Integral, Norma e Traço de um elemento.

1.1 Elementos Algébricos sobre um Corpo

Quando K é um subcorpo do corpo L , dizemos que L é uma extensão do corpo K e denotamos por L/K uma extensão de corpos. Denominamos a dimensão de L visto



como espaço vetorial sobre K como sendo o grau de L sobre K e denotamos por $[L : K]$. Dizemos que L/K é uma extensão finita se $[L : K]$ é finito. Dados $K \subset L$ corpos e α um elemento de L , denotaremos por $K[\alpha]$ o conjunto de todas as expressões polinomiais em α com coeficientes em K .

Sejam R um anel e K um subcorpo de R . Dizemos que um elemento $\alpha \in R$ é algébrico sobre K , se é raiz de um polinômio não nulo, com coeficientes em K . Caso contrário, dizemos que α é transcendente sobre K .

Exemplo 1.1.1 O elemento $\alpha = \sqrt{2} + \sqrt{-3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio

$$X^4 + 18X^2 + 25 \in \mathbb{Q}[X]$$

Dizemos que uma extensão L/K é algébrica se todo elemento de L é algébrico sobre K e uma extensão L/K é simples quando existe $\alpha \in L$ tal que:

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

Sejam $\alpha \in L$ algébrico sobre K e $J = \{p \in K[X] : p(\alpha) = 0\}$. O conjunto J contém um único polinômio mônico $p_\alpha = X^n + a_{n-1}X^{n-1} + \dots + a_0$ de grau mínimo; p_α é irredutível sobre K e se $\alpha \neq 0$, então $a_0 \neq 0$. O polinômio p_α que definimos acima é chamado polinômio minimal de α sobre K , e seu grau é chamado de grau de α sobre K .

Para α algébrico temos o seguinte resultado:

Sejam L sobre K uma extensão e $\alpha \in L$, então α é algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K . Neste caso, $[K(\alpha) : K] = \deg p$, onde p é o polinômio minimal de α sobre K e $K(\alpha) = K[\alpha]$.

Uma extensão L de um corpo K é um fêcho algébrico de K se, L é uma extensão algébrica de K e L é um corpo algebricamente fechado.

Outro resultado muito útil de extensões algébricas é que sendo K um corpo, L uma extensão algébrica de K e F uma extensão algébrica de L , temos que F é uma extensão algébrica de K e vale $[F : K] = [F : L][L : K]$.

Denotamos por A o conjunto de todos os números algébricos sobre K , o qual é corpo devido ao seguinte teorema.

Teorema 1.1.1 ([13], pag. 39) *O conjunto A dos números algébricos é um subcorpo de $\mathbb{C}$.*

Definimos um corpo de números como sendo um subcorpo K de $\mathbb{C}$ tal que $[K : \mathbb{Q}]$ é finito. Isto implica que todo elemento de K é algébrico sobre $\mathbb{Q}$ e assim $K \subseteq A$.

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

Demonstração:

Como K é um corpo de números, K é infinito e visto que K é obtido de $\mathbb{Q}$ pela adjunção de um número finito de elementos, suponhamos $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Faremos a demonstração por indução sobre n . Se $n = 1$, $K = \mathbb{Q}(\alpha_1)$ e tomemos $\theta = \alpha_1$. Provando que $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\theta)$ então, por hipótese de indução sobre s , $s \leq n - 1$, temos que:

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = \mathbb{Q}(\beta)\mathbb{Q}(\alpha_n) = \mathbb{Q}(\beta, \alpha_n) = \mathbb{Q}(\theta).$$

Assim, é suficiente provarmos para $n = 2$. Consideremos $K = \mathbb{Q}(\alpha, \beta)$ e sejam $p(X)$ e $q(X)$ os polinômios minimais de α e β sobre K , respectivamente, e suponhamos que sobre $\mathbb{C}$ tenham a seguinte fatoração:

$$p(X) = (X - \alpha_1) \dots (X - \alpha_n), \quad q(X) = (X - \beta_1) \dots (X - \beta_n),$$

e tomemos $\alpha_1 = \alpha$ e $\beta_1 = \beta$. Como os α_i 's e β_j 's são distintos. Assim, para cada i e cada $k \neq 1$, existe no mínimo um elemento $x \in K$, tal que

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1.$$

Se existem somente algumas destas equações, tomemos $c \neq 0$ em $\mathbb{Q}$, diferente de qualquer um destes x 's, e então:

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1 \implies c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_k},$$

para $1 \leq i \leq n$, $2 \leq k \leq m$. Seja $\theta = \alpha + c\beta$.

Afirmção: $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$. Com efeito, observemos que θ é uma combinação linear de α e β com coeficientes em $\mathbb{Q}$, logo $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$. Devemos mostrar que α e β estão em $\mathbb{Q}(\theta)$, para isto é suficiente mostrar que $\beta \in \mathbb{Q}(\theta)$ se $\alpha = \theta - c\beta$. Agora $p(\theta - c\beta) = p(\alpha) = 0$.

Definimos o polinômio:

$$r(X) = p(\theta - cX) \in \mathbb{Q}(\theta)[X],$$

então β é raiz dos polinômios r e q sobre $\mathbb{Q}(\theta)$. Esses polinômios tem somente uma raiz comum ξ . Se $r(\xi) = q(\xi)$, então ξ é um dos $\beta_1, \dots, \beta_m$ e também $\theta - c\xi$ é um dos $\alpha_1, \dots, \alpha_n$.

Mas pela escolha de c , $\xi = \beta$. Seja $h(X)$ o polinômio minimal de β sobre $\mathbb{Q}(\theta)$. Então $h(X) \mid q(X)$ e $h(X) \mid r(X)$. Visto que $q(X)$ e $r(X)$ tem exatamente uma raiz comum em $\mathbb{C}$ e todo polinômio irredutível em $\mathbb{C}$ não tem raízes repetidas, temos que $\partial h = 1$. Daí,

$$h(X) = X + \mu,$$

para $\mu \in \mathbb{Q}(\theta)$. Agora $0 = h(\beta) = \beta + \mu$, o que implica que $\beta = -\mu \in \mathbb{Q}(\theta)$ e portanto $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$, donde concluímos a demonstração.

■

Exemplo 1.1.2 Se $K = \mathbb{Q}(i, \sqrt[3]{2})$, temos que $f(X) = X^2 + 1$ é o polinômio irredutível de i sobre $\mathbb{Q}$ e $g(X) = X^3 - 2$ é o polinômio irredutível de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. As raízes de f são $\alpha_1 = i$ e $\alpha_2 = -i$ e as de g são $\beta_1 = \sqrt[3]{2}$, $\beta_2 = \sqrt[3]{2}\omega$ e $\beta_3 = \sqrt[3]{2}\omega^2$, onde $\omega = e^{\frac{2\pi i}{3}}$.

Devemos encontrar $c \in \mathbb{Q}$ de modo que,

$$c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}, \quad j \neq 1 \quad (1.1)$$

A equação (1.1) vale para todo $c \in \mathbb{Q}^*$, em particular para $c = 1$, temos $K = \mathbb{Q}(i + \sqrt[3]{2})$.

Proposição 1.1.1 ([8], pag. 38) Sejam K um corpo, $f(X) \in K[X]$ um polinômio irredutível e α, β raízes de $f(X)$ em alguma extensão de K . Então existe um único K -isomorfismo $\varphi: K(\alpha) \rightarrow K(\beta)$ tal que $\varphi(\alpha) = \beta$.

1.2 Conjugados e Discriminantes

Seja $K = \mathbb{Q}(\theta)$ um corpo de números. Em geral, existem muitos monomorfismos distintos de K em $\mathbb{C}$. O conjunto de tais monomorfismos forma a parte fundamental da teoria utilizada neste trabalho.

Teorema 1.2.1 ([13], pag. 41) Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n . Então existem exatamente n monomorfismos distintos

$$\sigma_i: K \rightarrow \mathbb{C}.$$

Os elementos $\sigma_i(\theta) = \theta_i$ são as raízes em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.

Demonstração:

Sejam $\theta_1, \dots, \theta_n$ as raízes (distintas) do polinômio minimal $f(X)$. Logo,

$$f(X) = (X - \theta_1) \dots (X - \theta_n).$$

Pela Proposição 1.1.1, existe um único isomorfismo:

$$\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_i), \quad i = 1, \dots, n,$$

tal que $\sigma_i(\theta) = \theta_i$. Por outro lado, se existe um monomorfismo $\sigma : K \longrightarrow \mathbb{C}$, precisamos mostrar que $\sigma(\theta)$ é raiz de $f(X)$. Visto que:

$$0 = \sigma \left(\sum_{i=0}^n a_i \theta^i \right) = f(\sigma(\theta))$$

então, $\sigma(\theta)$ é raiz de $f(X)$. Logo, $\sigma = \sigma_i$ para algum i e portanto os monomorfismos descritos são os únicos possíveis.

■

Sejam $K = \mathbb{Q}(\theta)$, um corpo de números de grau n e $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$. Para cada $\alpha \in K$, definimos o polinômio característico de α sobre $\mathbb{Q}$ como sendo:

$$f_\alpha(X) = \prod_{i=1}^n (X - \sigma_i(\alpha)). \quad (1.2)$$

Teorema 1.2.2 ([13], pag. 42) *Os coeficientes do polinômio característico são números racionais, de modo que $f_\alpha(X) \in \mathbb{Q}[X]$.*

Demonstração:

Podemos escrever (1.2) da seguinte maneira:

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

Por outro lado,

$$\text{irr}(\alpha, \mathbb{Q}) = \prod_{i=1}^m (X - \alpha_i),$$

sendo os α_i 's as raízes de $\text{irr}(\alpha, \mathbb{Q})$, $i = 1, \dots, m$.

Sejam $\varphi_1, \dots, \varphi_m$ os monomorfismos de $\mathbb{Q}(\alpha)$ em $\mathbb{C}$ definidos de modo que:

$$\alpha_i = \varphi_i(\alpha), \quad i = 1, \dots, m.$$

Visto que cada φ_i tem $[K : \mathbb{Q}(\alpha)]$ extensões de K em $\mathbb{C}$, concluímos que:

$$f_\alpha(X) = \text{irr}(\alpha, \mathbb{Q})^{[K:\mathbb{Q}(\alpha)]}.$$

Consequentemente, os coeficientes de $f_\alpha(X)$ e, em particular, $\sum_{i=1}^n \sigma_i(\alpha)$, $\prod_{i=1}^n \sigma_i(\alpha)$ são números racionais.

■

Desta demonstração temos duas consequências importantes: o polinômio característico f_α é uma potência do polinômio minimal p e os K -conjugados de α são as raízes de p em $\mathbb{C}$, cada uma repetida n/m vezes, onde $m = \partial p$.

Os elementos $\sigma_i(\alpha)$, para $i = 1, \dots, n$, são chamados K -conjugados de α . Por exemplo, sobre $\mathbb{Q}$, $\sqrt{2}$ e $-\sqrt{2}$ são os conjugados de $\sqrt{2}$, mas por outro lado $1 + \sqrt{7}$ e $\sqrt{7}$ não são $\mathbb{Q}$ -conjugados de $\sqrt{7}$. Embora os θ_i sejam distintos (e são K -conjugados de θ), nem sempre é verdade que os K -conjugados de α são distintos. Note que os K -conjugados de α não são necessariamente elementos de K , isto é, os θ_i não são necessariamente elementos de K . Por exemplo, seja θ a raiz real cúbica de 5. Então $\mathbb{Q}(\theta)$ é um subcorpo de $\mathbb{R}$. Os K -conjugados de θ são θ , $\omega\theta$, $\omega^2\theta$ onde $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. As duas últimas não são reais, assim não estão em $\mathbb{Q}(\theta)$.

Considerando $K = \mathbb{Q}(\theta)$ um corpo de números de grau n , $\{\alpha_1, \dots, \alpha_n\}$ uma n -upla de K e $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$, definimos o **discriminante** desta n -upla por:

$$\Delta[\alpha_1, \dots, \alpha_n] = (\det(\sigma_i(\alpha_j)))^2. \quad (1.3)$$



Exemplo 1.2.1 *Sejam $K = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\{1, \sqrt{7}\} \subset K$. Então:*

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

Lema 1.2.1 *Sejam K um corpo de números de grau n , $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ subconjuntos de K tais que $\beta_k = \sum_{i=1}^n c_{ik} \alpha_i$, com $c_{ik} \in \mathbb{Q}$, $k = 1, \dots, n$. Então:*

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

Demonstração:

Por definição,

$$\begin{aligned} \Delta[\beta_1, \dots, \beta_n] &= \left(\det \begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \dots & \sigma_n(\beta_n) \end{pmatrix} \right)^2 \\ &= (\det(c_{ik}))^2 (\det(\sigma_i(\alpha_j)))^2 = (\det(c_{ik}))^2 \Delta[\alpha_1, \dots, \alpha_n]. \end{aligned}$$

■

Exemplo 1.2.2 *Vimos no exemplo 1.2.1 que o discriminante da base $\{1, \sqrt{7}\}$, do corpo de números $K = \mathbb{Q}(\sqrt{7})$ é 28. Agora, considerando uma outra base de K , por exemplo, $\{2 - \sqrt{7}, 5 + 2\sqrt{7}\}$, segue do Lema 1.2.1 que*

$$\Delta[2 - \sqrt{7}, 5 + 2\sqrt{7}] = \left(\det \begin{pmatrix} 2 & -1 \\ 5 & 2 \end{pmatrix} \right)^2 \cdot \Delta[1, \sqrt{7}] = 9^2 \cdot 28$$

Teorema 1.2.3 ([13], pag. 44) *O discriminante de toda base para $K = \mathbb{Q}(\theta)$ é racional e não nulo, e se todos os K -conjugados de θ são reais, então o discriminante de toda base é positivo.*

Demonstração:

Seja $\{1, \theta, \dots, \theta^{n-1}\}$ uma base de K e suponhamos que os conjugados de θ sejam $\theta_1, \dots, \theta_n$. Pela definição de discriminante,

$$\Delta = \Delta[1, \theta, \dots, \theta^{n-1}] = \left(\det \begin{pmatrix} \sigma_1(\theta_1) & \dots & \sigma_1(\theta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\theta_1) & \dots & \sigma_n(\theta_n) \end{pmatrix} \right)^2 = (\det(\sigma_i(\theta_j)))^2.$$

Um determinante da forma $D = \det(\sigma_i(\theta_j))$ é chamado determinante de Vandermonde e tem valor

$$D = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j). \quad \text{Assim,} \quad \Delta = \left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2$$

e $\Delta \neq 0$, pois $\theta_i \neq \theta_j$, se $i \neq j$. Sendo $f(X) = \text{irr}(\theta, \mathbb{Q})$, então $f(X) = \prod_{i=1}^n (X - \theta_i)$ e sua derivada $f'(X) = \sum_{i=1}^n \frac{f(X)}{(X - \theta_i)}$. Calculando a derivada em cada θ_i , temos:

$$\begin{aligned} \prod_{i=1}^n f'(\theta_i) &= (\theta_1 - \theta_2)(\theta_1 - \theta_3) \dots (\theta_1 - \theta_n)(\theta_2 - \theta_1)(\theta_2 - \theta_3) \dots (\theta_2 - \theta_n) \dots \\ &\quad (\theta_n - \theta_1) \dots (\theta_n - \theta_{n-1}) \\ &= \pm \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2. \end{aligned}$$

Logo, $\pm \prod_{i=1}^n f'(\theta_i) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2$. Mas, $f'(\theta_i) = \sigma_i(f'(\theta))$ e $f'(\theta) \in \mathbb{Q}(\theta)$. Logo, o polinômio característico de $f'(\theta)$ sobre $\mathbb{Q}$ é:

$$\begin{aligned} f_{f'(\theta)}(X) &= \prod_{i=1}^n (X - \sigma_i(f'(\theta))) \\ &= X^n - \left(\sum_{i=1}^n \sigma_i(f'(\theta)) \right) X^{n-1} + \dots + (-1)^n \prod_{i=1}^n \sigma_i(f'(\theta)). \end{aligned}$$

Como cada coeficiente de $f_{f'(\theta)}(X)$ é racional, segue que Δ é um número racional. ■

Com a notação acima, Δ é zero se, e somente se, algum θ_i é igual a outro θ_j . Portanto, para que Δ não se anule passamos a discriminar os θ_i , o que motiva a nomenclatura de Δ .

1.3 Inteiros Algébricos

Sejam R um anel e A um subanel de R . Um elemento $\theta \in R$ é dito inteiro algébrico sobre A , se este é raiz de um polinômio mônico com coeficientes em A .

Em outras palavras,

$$\theta^n + a_{n-1}\theta^{n-1} + \dots + a_1\theta + a_0 = 0,$$

onde $a_i \in A$, para todo i .

Exemplo 1.3.1 Os elementos $x = \sqrt{5} + \sqrt{7}$ e $\theta = \sqrt{-11}$ são inteiros algébricos sobre $\mathbb{Z}$, pois $x^4 - 24x^2 + 4 = 0$ e $\theta^2 + 11 = 0$. Mas $\gamma = 37/13$ não é, pois ele não satisfaz equações do tipo $\gamma - 37 = 0$, cujos coeficientes são inteiros.

Segundo a definição, α é algébrico sobre um corpo K , se satisfaz uma equação do tipo:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0,$$

com $a_i \in K$, $a_n \neq 0$. Multiplicando esta equação por a_n^{-1} , temos:

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

Portanto, sobre um corpo, o conceito de elemento algébrico coincide com o de inteiro algébrico.

Sendo $[L : K]$ finito, então L é uma extensão algébrica de K . E como vimos, ser algébrico tem o mesmo significado de ser inteiro algébrico sobre um corpo, assim podemos



usar os resultados obtidos para elementos algébricos em inteiros algébricos. Logo, para $K \subset R$ e $x \in R$, x é algébrico sobre K se, e somente se, $[K[x] : K]$ é finito.

Chamamos de B o conjunto dos inteiros algébricos, ou seja, B é o conjunto dos $\theta \in R$, tais que θ é um inteiro algébrico sobre A . Um dos objetivos desta seção é mostrarmos que B é subanel de A .

Lema 1.3.1 ([13], pag. 46) *Um número complexo θ é um inteiro algébrico se, e somente se, o grupo aditivo gerado por todas potências $1, \theta, \theta^2, \dots$ é finitamente gerado.*

Teorema 1.3.1 ([13], pag. 47) *Os inteiros algébricos formam um subanel do corpo dos números algébricos.*

A partir de uma extensão simples desta técnica provamos o seguinte:

Teorema 1.3.2 ([13], pag. 47) *Seja θ um número complexo satisfazendo um polinômio mônico cujos coeficientes são inteiros algébricos. Então θ é um inteiro algébrico.*

A partir dos Teoremas 1.3.1 e 1.3.2 podemos construir novos inteiros algébricos desconhecidos, por exemplo, $\sqrt{7}$ e $\sqrt{13}$ são claramente inteiros algébricos. Então, pelo Teorema 1.3.1, os números, tais como, $\sqrt{7} + \sqrt{13}$, $9\sqrt{7} - 86\sqrt{13}$ e $(\sqrt{7})^3(1 + \sqrt{13})^2$, também são inteiros algébricos. E pelo Teorema 1.3.2 os zeros do polinômio

$$X^{23} - (14 + \sqrt[5]{7})X^9 + (\sqrt[3]{11})X^5 - 19\sqrt{5},$$

são inteiros algébricos.

Para todo corpo de números K escrevemos

$$\mathcal{O}_K = K \cap B$$

e $\mathcal{O}_K$ é dito o anel dos inteiros algébricos de K .

Lema 1.3.2 ([13], pag. 49) *Sejam K um corpo de números e α um elemento não nulo de K . Então, para algum c inteiro não nulo temos que $c\alpha \in \mathcal{O}_K$.*

Demonstração:

Seja $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = \text{irr}(\alpha, \mathbb{Q})$. Então, existe $c \in \mathbb{Z}^*$ tal que,

$$cf(X) = cX^n + ca_{n-1}X^{n-1} + \dots + ca_0 \in \mathbb{Z}[X].$$

Multiplicando $cf(X)$ por c^{n-1} , obtemos o polinômio:

$$g(X) = c^n f(X) = (cX)^n + ca_{n-1}(cX)^{n-1} + \dots + c^n a_0 \in \mathbb{Z}[X],$$

que tem α como raiz. Entretanto, substituindo cX por Y , obtemos o polinômio mônico:

$$h(Y) = Y^n + ca_{n-1}Y^{n-1} + \dots + c^n a_0,$$

cujos coeficientes são inteiros e tem $c\alpha$ como raiz. Portanto $c\alpha \in \mathcal{O}_K$.

■

Corolário 1.3.1 ([13], pag. 49) *Seja K um corpo de números. Então, $K = \mathbb{Q}(\theta)$, para algum θ inteiro algébrico.*

Observação 1.3.1 Para $\theta \in \mathbb{C}$, escrevemos $\mathbb{Z}[\theta]$ como sendo o conjunto dos elementos $p(\theta)$, para polinômios $p \in \mathbb{Z}[X]$. Se $K = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, então, certamente $\mathcal{O}_K$ contém $\mathbb{Z}[\theta]$, se $\mathcal{O}_K$ é um anel contendo θ . De qualquer modo, $\mathcal{O}_K$ não é necessariamente igual a $\mathbb{Z}[\theta]$. Por exemplo, $\mathbb{Q}(\sqrt{17})$ é um corpo de números e $\sqrt{17}$ um inteiro algébrico. Mas,

$$\frac{1 + \sqrt{17}}{2}$$

é um zero de $X^2 - X - 4 = 0$, e assim um inteiro algébrico contido em $\mathbb{Q}(\sqrt{17})$, então pertence a $\mathcal{O}_K$ e não pertence a $\mathbb{Z}[\sqrt{17}]$.

O critério abaixo é útil, em termos de polinômio minimal, para testar se um número é um inteiro algébrico.

Lema 1.3.3 ([13], pag. 49) *Um número algébrico α é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Demonstração:

Seja $p(X) = \text{irr}(\alpha, \mathbb{Q})$. Caso $p(X) \in \mathbb{Z}[X]$, então α é um inteiro algébrico. Reciprocamente, se α é um inteiro algébrico, então existe $q(X) \in \mathbb{Z}[X]$, mônico, tal que $q(\alpha) = 0$. Sendo $p(X) = \text{irr}(\alpha, \mathbb{Q})$ e $q(\alpha) = 0$, então $p(X)$ divide $q(X)$, ou seja, $q(X) = p(X)h(X)$ e pelo Lema de Gauss, existe $\lambda \in \mathbb{Q}^*$ de modo que $\lambda p(X)$ e $\lambda^{-1}h(X) \in \mathbb{Z}[X]$. Como $\lambda p(X) \in \mathbb{Z}[X]$, temos que $\lambda \in \mathbb{Z}$, pois $p(X)$ é mônico. Analogamente $\lambda^{-1}h(X) \in \mathbb{Z}[X]$, implicando que $\lambda^{-1} \in \mathbb{Z}$, logo $\lambda = \pm 1$ e, sem perda de generalidade, podemos supor $\lambda = 1$. Portanto $p(X) \in \mathbb{Z}[X]$.

■

Lema 1.3.4 ([13], pag. 50) *Um inteiro algébrico é um número racional se, e somente se, é um inteiro. Equivalentemente, $B \cap \mathbb{Q} = \mathbb{Z}$.*

Demonstração:

Temos que todo inteiro n é raiz do polinômio $X - n \in \mathbb{Z}[X]$, então n é um inteiro algébrico e portanto $\mathbb{Z} \subseteq B \cap \mathbb{Q}$. Reciprocamente, se $\alpha \in B \cap \mathbb{Q}$, então $\alpha \in B$ e $\alpha \in \mathbb{Q}$. Desde que $\alpha \in \mathbb{Q}$, seu polinômio irredutível sobre $\mathbb{Q}$ é $X - \alpha$, e pelo Lema 1.3.3 os coeficientes de $X - \alpha$ são inteiros logo $\alpha \in \mathbb{Z}$ e $B \cap \mathbb{Q} \subseteq \mathbb{Z}$. Portanto $B \cap \mathbb{Q} = \mathbb{Z}$.

■

1.4 Base Integral

Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n , θ um inteiro algébrico. Mostraremos a seguir que o anel $\mathcal{O}_K$ dos inteiros algébricos de K , é um $\mathbb{Z}$ -módulo livre de posto n , ou seja, admite uma base a qual denominamos base integral. Assim, $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral se, e somente se, todo α_i é um inteiro algébrico e cada elemento de $\mathcal{O}_K$ é expresso de modo único como,

$$a_1\alpha_1 + \dots + a_n\alpha_n$$

com $a_i \in \mathbb{Z}$. Vale observarmos que $\{1, \theta, \dots, \theta^{n-1}\}$ é uma $\mathbb{Q}$ -base de K , constituída de inteiros algébricos, mas nem sempre é uma base integral de $\mathcal{O}_K$. Por exemplo, $\{1, 2\sqrt{2}\}$ é uma $\mathbb{Q}$ -base de $\mathbb{Q}(\sqrt{2})$, mas não é uma base integral.

Assim, o problema é mostrarmos que base integral existe, o que equivale a provarmos que $(\mathcal{O}_K, +)$ é um grupo abeliano livre de posto n . Para provarmos isso, primeiro estabelecemos o seguinte resultado:

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

Demonstração:

Pelo Teorema 1.2.3, $\Delta = \Delta[\alpha_1, \dots, \alpha_n]$ é racional e não nulo. Visto que os α_i são inteiros algébricos, seus conjugados também são inteiros algébricos, logo Δ é um inteiro algébrico. Pelo Lema 1.3.4, Δ é um inteiro.

■

Logo podemos afirmar que:

Teorema 1.4.1 ([13], pag. 51) *Todo corpo de números K possui uma base integral, ou seja, existem $\omega_1, \dots, \omega_n \in K$ com $n = [K : \mathbb{Q}]$ tal que $\mathcal{O}_K = \sum_{i=1}^n \mathbb{Z}\omega_i$.*

Demonstração:

Seja $\{\omega_1, \dots, \omega_n\}$ uma base de K , com $\omega_i \in \mathcal{O}_K$, tal que $|\Delta[\omega_1, \dots, \omega_n]|$ seja mínimo.

Suponhamos que $\{\omega_1, \dots, \omega_n\}$ não seja base integral. Então existe $\omega \in \mathcal{O}_K$ tal que:

$$\omega = a_1\omega_1 + \dots + a_n\omega_n,$$

com $a_i \in \mathbb{Q}$, mas nem todos inteiros. Suponhamos, sem perda de generalidade, que $a_1 \notin \mathbb{Z}$. Então $a_1 = a + r$, onde $a \in \mathbb{Z}$ e $0 < r < 1$. Seja

$$\gamma_1 = \omega - a\omega_1 = r\omega_1 + a_2\omega_2 + \dots + a_n\omega_n$$

e $\gamma_i = \omega_i$; $i = 2, \dots, n$. Então $\{\gamma_1, \dots, \gamma_n\}$ é uma base constituída de inteiros algébricos e seu discriminante:

$$\Delta[\gamma_1, \dots, \gamma_n] = \left(\det \begin{pmatrix} r & a_2 & \dots & a_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \right)^2 \cdot \Delta[\omega_1, \dots, \omega_n] = r^2 \cdot \Delta[\omega_1, \dots, \omega_n]$$

Como $0 < r < 1$, segue que $|\Delta[\gamma_1, \dots, \gamma_n]| < |\Delta[\omega_1, \dots, \omega_n]|$, contradizendo a minimalidade de $|\Delta[\omega_1, \dots, \omega_n]|$. Logo $\{\omega_1, \dots, \omega_n\}$ é uma base integral de $\mathcal{O}_K$ e, portanto, $\mathcal{O}_K$ é abeliano livre de posto n .

■

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

Teorema 1.4.2 ([13], pag. 53) *Sejam K um corpo de números e $\alpha_1, \dots, \alpha_n$ elementos de $\mathcal{O}_K$. Se $\Delta[\alpha_1, \dots, \alpha_n]$ é um inteiro livre de quadrados então $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral.*

Demonstração:

Seja $\{\beta_1, \dots, \beta_n\}$ uma base integral. Então existem c'_{ij} s inteiros tais que $\alpha_i = \sum_{j=1}^n c'_{ij} \beta_j$; $i = 1, \dots, n$, e pelo Lema 1.2.1, temos:

$$\Delta = \Delta[\alpha_1, \dots, \alpha_n] = (\det(c'_{ij}))^2 \cdot \Delta[\beta_1, \dots, \beta_n]$$

Sendo Δ um inteiro livre de quadrados, então $\det(c'_{ij}) = \pm 1$ e a matriz (c'_{ij}) é inversível.

Seja $(d_{ij}) = (c'_{ij})^{-1}$; com $d_{ij} \in \mathbb{Z}$. Assim, $\beta_j = \sum_{i=1}^n d_{ij} \alpha_i$, ou seja, cada $\beta_j \in \mathcal{O}_K$ se escreve como combinação linear, a coeficientes inteiros, dos α_i . Portanto $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral.

■

Exemplo 1.4.1 *Em $\mathbb{Q}(\sqrt{13})$ a $\mathbb{Q}$ - base $\{1, \sqrt{13}\}$ não é base integral. De fato, um elemento de $\mathbb{Q}(\sqrt{13})$ é da forma $p + q\sqrt{13}$ para p, q racionais e tem polinômio minimal*

$$(X - p - q\sqrt{13})(X - p + q\sqrt{13}) = X^2 - 2pX + (p^2 - 13q^2)$$

Então $p + q\sqrt{13}$ é um inteiro algébrico se, e somente se, os coeficientes do polinômio minimal, ou seja, $2p$ e $(p^2 - 13q^2)$ são inteiros, pelo Lema 1.3.3. Logo, $p = (1/2)P$, onde P é um inteiro e para P par, temos que p^2 é um inteiro, então $13q^2$ também será um inteiro, o que implica q inteiro.

Para P ímpar, um cálculo direto (que será visto mais detalhadamente no próximo capítulo) mostra que $q = (1/2)Q$, onde Q também é um inteiro ímpar.

A partir disto segue que, $\mathcal{O}_K = \mathbb{Z} \left[\frac{1 + \sqrt{13}}{2} \right]$ e uma base integral é $\left\{ 1, \frac{1 + \sqrt{13}}{2} \right\}$.

Pelo Teorema 1.4.2 podemos provar isto usando discriminante da seguinte maneira:

os dois monomorfismos de $\mathbb{Q}(\sqrt{13})$ em $\mathbb{C}$ são dados por:

$$\sigma_1(p + q\sqrt{13}) = p + q\sqrt{13}, \quad \sigma_2(p + q\sqrt{13}) = p - q\sqrt{13}.$$

Assim,

$$\Delta \left[1, \frac{1 + \sqrt{13}}{2} \right] = \left(\det \begin{pmatrix} \sigma_1(1) & \sigma_1 \left(\frac{1 + \sqrt{13}}{2} \right) \\ \sigma_2(1) & \sigma_2 \left(\frac{1 + \sqrt{13}}{2} \right) \end{pmatrix} \right)^2 = (-\sqrt{13})^2 = 13$$

e sendo este livre de quadrados, temos que $\left\{ 1, \frac{1 + \sqrt{13}}{2} \right\}$ é uma base integral.

Observação 1.4.1 É importante notarmos que existem bases integrais cujo discriminante não é livre de quadrados. Portanto a recíproca do Teorema 1.4.2 é falsa. Por exemplo, consideremos o corpo $K = \mathbb{Q}(\sqrt{11})$ que tem base integral $\{1, \sqrt{11}\}$ e discriminante 44, o qual não é livre de quadrados.

Lema 1.4.2 Seja K um corpo de números de grau n e $\mathcal{O}_K$ o seu anel dos inteiros algébricos. Se $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ são duas bases integrais de $\mathcal{O}_K$ então

$$\Delta[\alpha_1, \dots, \alpha_n] = \Delta[\beta_1, \dots, \beta_n].$$

Demonstração:

Como existe uma matriz C inversível, com entradas inteiras, tal que $\alpha_i = \sum_{j=1}^n c_{ij} \beta_j$,

então, pelo Lema 1.2.1 temos:

$$\Delta[\alpha_1, \dots, \alpha_n] = (\det C)^2 \Delta[\beta_1, \dots, \beta_n] = \Delta[\beta_1, \dots, \beta_n],$$

pois a matriz mudança de base é unimodular.

■

Pelo Lema 1.4.2, podemos observar que o discriminante de uma base integral independe da escolha da base. Este valor comum, o qual denotamos por D_K , é chamado discriminante de K e é sempre um número inteiro não nulo. Corpos de números isomorfos tem o mesmo discriminante.

1.5 Norma e Traço

A partir da norma e do traço, é possível transformarmos alguns problemas de inteiros algébricos em problemas de números inteiros.

Sejam $K \subseteq L$ corpos de números, com $n = [L : K]$ e $\sigma_1, \dots, \sigma_n$ os monomorfismos de L em $\mathbb{C}$. Dado um elemento $\alpha \in L$, definimos a norma e o traço de α relativamente à extensão L/K como sendo, respectivamente:

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

Observação 1.5.1 Como vimos, o polinômio característico é uma potência do polinômio minimal, e então pelo Lema 1.3.3 e o Lema de Gauss ([13], pag. 19), segue que um elemento α de K é um inteiro se, e somente se, seu polinômio característico tem coeficientes inteiros. Portanto, se α é um inteiro algébrico a norma e o traço deste elemento são inteiros.

No contexto em que estiver explícito, a norma e o traço de α serão abreviados por $N(\alpha)$ e $\text{Tr}(\alpha)$, respectivamente.

Sejam $K \subset L$ corpos de números, $[L : K] = n$, $\alpha, \beta \in L$ e $c \in K$. Então valem as seguintes propriedades:

$$(1) \text{Tr}_{L/K}(\alpha + \beta) = \text{Tr}_{L/K}(\alpha) + \text{Tr}_{L/K}(\beta),$$



$$(2) \operatorname{Tr}_{L/K}(c\alpha) = c\operatorname{Tr}_{L/K}(\alpha),$$

$$(3) \operatorname{Tr}_{L/K}(c) = nc,$$

$$(4) N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta),$$

$$(5) N_{L/K}(c) = c^n.$$

No caso $K \subseteq L \subseteq M$, dado $\alpha \in M$, valem:

$$(6) N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)),$$

$$(7) \operatorname{Tr}_{M/K}(\alpha) = \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(\alpha)).$$

Em particular, se $\alpha \in L$, então:

$$(8) \operatorname{Tr}_{M/K}(\alpha) = [M : L]\operatorname{Tr}_{L/K}(\alpha),$$

$$(9) N_{M/K}(\alpha) = N_{L/K}(\alpha)^{[M:L]}.$$

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

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

onde p' é a derivada formal de p .

Demonstração:

Pelo Teorema 1.2.3, temos

$$\Delta[1, \theta, \dots, \theta^{n-1}] = \left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2 = (-1)^s \prod_{i=1}^n p'(\theta_i),$$

com $s = \frac{1}{2}n(n-1)$. Mas,

$$\prod_{i=1}^n p'(\theta_i) = \prod_{i=1}^n p'(\sigma_i(\theta)) = \prod_{i=1}^n \sigma_i(p'(\theta)) = N_{K/\mathbb{Q}}(p'(\theta)).$$

Portanto,

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

Exemplo 1.5.1 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[4]{5}$ e $f(X) = X^4 - 5 = \text{irr}(\theta, \mathbb{Q})$. Então,

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

1.6 Decomposição em Irredutíveis

O objetivo desta seção é introduzir alguns conceitos e propriedades que serão importantes no decorrer deste capítulo.

Para isso, definimos um domínio como sendo Noetheriano quando todo ideal é finitamente gerado. Devemos esta nomenclatura a Emmy Noether (1882 - 1935), que foi quem introduziu o conceito.

A seguir duas propriedades úteis:

A condição de Cadeia ascendente: Dada uma cadeia ascendente de ideais:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots,$$

então existe algum N tal que $I_n = I_N$, para todo $n \geq N$, ou seja, toda cadeia ascendente é estacionária.

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.

Proposição 1.6.1 ([13], pag. 86) Se D é um domínio, as seguintes condições são equivalentes:

(a) D é Noetheriano,



(b) D satisfaz a condição de cadeia ascendente,

(c) D satisfaz a condição maximal.

Teorema 1.6.1 ([13], pag. 87) *O anel dos inteiros algébricos $\mathcal{O}_K$ de um corpo de números K é noetheriano.*

Introduziremos a seguir as definições e algumas propriedades de unidades, elementos associados e irredutíveis, para isso, utilizaremos a Lei do Cancelamento e então é necessário tomarmos o anel como sendo um domínio de integridade.

Sendo $k = m.n$, onde nem m ou n são unidades, então m e n são chamados fatores próprios e k é dito redutível. Assim, ao fatorar um elemento não unitário x , em um domínio D , é natural buscarmos fatores próprios

$$x = p_1 \dots p_m,$$

onde cada p_i é irredutível. Geralmente isto não é possível, mas mostraremos no decorrer desta seção que no anel dos inteiros algébricos $\mathcal{O}$ de qualquer corpo de números, sempre é possível.

Seja u uma unidade de um anel R . Então qualquer elemento $x \in R$ pode ser trivialmente fatorado como:

$$x = uy,$$

onde $y = u^{-1}x$. Dizemos que o elemento y é associado de x se $x = uy$, onde u é uma unidade.

Proposição 1.6.2 ([13], pag. 84) *Para um domínio D ,*

(a) x é uma unidade se, e somente se, $x \mid 1$,



- (b) Quaisquer duas unidades são associadas e qualquer associado de uma unidade é uma unidade,
- (c) x, y são associados se, e somente se, $x \mid y$ e $y \mid x$,
- (d) x é irredutível se, e somente se, todo divisor de x é um associado de x ou uma unidade,
- (e) Um associado de um irredutível é irredutível.

Em termos de ideais, temos:

Proposição 1.6.3 ([13], pag. 84) *Sejam D um domínio, e x, y elementos não nulos de D , então:*

- (a) $x \mid y$ se, e somente se, $\langle x \rangle \supseteq \langle y \rangle$,
- (b) x e y são associados se, e somente se, $\langle x \rangle = \langle y \rangle$,
- (c) x é uma unidade se, e somente se, $\langle x \rangle = D$,
- (d) x é irredutível se, e somente se, $\langle x \rangle$ é maximal dentre os ideais principais próprios de D .

Corolário 1.6.1 ([13], pag. 88) *Fatoração em irredutíveis é possível em $\mathcal{O}_K$.*

A norma é uma ferramenta útil para se detectar unidades e irredutíveis em $\mathcal{O}_K$:

Proposição 1.6.4 ([13], pag. 88) *Sejam $\mathcal{O}_K$ o anel dos inteiros algébricos de um corpo K e $x, y \in \mathcal{O}_K$, então:*

- (a) x é unidade se, e somente se, $N(x) = \pm 1$,
- (b) Se x e y são associados, então $N(x) = \pm N(y)$,
- (c) Se $N(x)$ é um primo racional, então x é irredutível em $\mathcal{O}_K$.

Dizemos que a fatoração em um domínio D é única quando :

$$p_1 \dots p_r = q_1 \dots q_s,$$

onde todo p_i e q_j são irredutíveis em D , $r=s$ e existe uma permutação π de $\{1, \dots, r\}$, tal que p_i e $q_{\pi(i)}$ são associados, para todo i , com $i = 1, \dots, r$.

Dizemos que um anel de integridade A é fatorial se, a fatoração em A é única e todo elemento não nulo e não inversível a pode ser expresso como o produto de elementos irredutíveis, isto é, se $p_1, \dots, p_s$ são elementos irredutíveis de A , então $a = p_1 \dots p_s$.

Sejam p um elemento irredutível de um anel fatorial A e $a \in A^*$, então existe um único número natural s tal que p^s divide a e p^{s+1} não divide a ; denotaremos s por $v_p(a)$ e denominaremos multiplicidade de p em a . Obtemos assim uma aplicação $v_p : A^* \rightarrow \mathbb{N}$, a qual denominamos valorização p -ádica de A , que satisfaz as seguintes condições:

(i) Quaisquer que sejam $a, b \in A^*$, temos:

$$v_p(ab) = v_p(a) + v_p(b).$$

(ii) Quaisquer que sejam $a, b \in A^*$, se $a + b \neq 0$, então:

$$v_p(a + b) \geq \min\{v_p(a), v_p(b)\}.$$

Essa definição será necessária para demonstrarmos um resultado importante no próximo capítulo. Embora a unicidade da fatoração falhe para elementos de $\mathcal{O}_K$, o exemplo a seguir mostra que o mesmo não ocorre para a fatoração de ideais principais no anel dos inteiros $\mathcal{O}_K$.

Exemplo 1.6.1 Em inteiros algébricos de $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, temos a seguinte fatoração:

$$10 = (\sqrt{5})(\sqrt{5})(\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3}).$$

Se $K = \mathbb{Q}(\sqrt{15})$ esta fatoração permanece no anel dos inteiros algébricos $\mathcal{O}_K$. Em termos de ideais principais, temos:

$$\langle 10 \rangle = \langle \sqrt{5} \rangle \langle \sqrt{5} \rangle \langle \sqrt{5} \rangle \langle \sqrt{5} + \sqrt{3} \rangle \langle \sqrt{5} - \sqrt{3} \rangle.$$

Fazendo a intersecção dos ideais desta fatoração com $\mathcal{O}_K$ e mais uma vez obtemos ideais em $\mathcal{O}_K$, mas estes não são principais.

Por exemplo, tomando $I = \langle \sqrt{5} + \sqrt{3} \rangle \cap \mathcal{O}_K$. Então, $\sqrt{3}(\sqrt{5} + \sqrt{3}) = \sqrt{15} + 3 \in I$ e, $\sqrt{5}(\sqrt{5} + \sqrt{3}) = 5 + \sqrt{15} \in I$, e sua diferença é igual a

$$(5 + \sqrt{15}) - (3 + \sqrt{15}) = 2 \in I.$$

Suponhamos $I = \langle a + b\sqrt{15} \rangle$ principal, então 2 deveria ser um múltiplo de $a + b\sqrt{15}$, e tomando as normas destes elementos temos,

$$N(a + b\sqrt{15}) \mid N(2) \implies a^2 - 15b^2 \mid 4.$$

Novamente, tomando $I = \langle \alpha \rangle$ principal, temos que:

$$N(5 + \sqrt{15}) = 10 = 2 \cdot 5 \text{ e } N(3 + \sqrt{15}) = -6 = 2 \cdot (-3),$$

então $N(\alpha)$ divide 2. Visto que I é próprio, temos que $N(\alpha) \neq \pm 1$. Então, se $N(\alpha) = \pm 2$, existe $a, b \in \mathbb{Z}$ com $N(a + b\sqrt{15}) = \pm 2$, donde segue que $a^2 - 15b^2 = \pm 2$, mas tomando módulo 5, temos $a^2 \equiv \pm 2 \pmod{5}$, o que é uma contradição. Portanto I não é principal.

Logo, podemos concluir que: para fatorar o ideal principal $\langle x \rangle$ no anel dos inteiros $\mathcal{O}_K$, tomamos uma fatoração única de ideais

$$\langle x \rangle = I_1 \dots I_n,$$

mas, os ideais $I_1, \dots, I_n$ não são principais.

1.7 Fatoração de Ideais

O objetivo principal desta seção é mostrarmos que a fatoração de elementos de $\mathcal{O}_K$ em irredutíveis é única se, e somente se, todo ideal de $\mathcal{O}_K$ é principal. Deste modo unindo as duas teorias da fatoração, de elementos e de ideais.

A seguir, veremos algumas propriedades do anel dos inteiros algébricos de um corpo de números:

Teorema 1.7.1 ([13], pag. 115) *O anel dos inteiros algébricos $\mathcal{O}_K$ de um corpo de números K tem as seguintes propriedades:*

- (a) $\mathcal{O}_K$ é um domínio, com corpo de frações K ,
- (b) $\mathcal{O}_K$ é Noetheriano,
- (c) Se $\alpha \in K$ satisfaz um polinômio mônico com coeficientes em $\mathcal{O}_K$, então $\alpha \in \mathcal{O}_K$,
- (d) Todo ideal primo não nulo de $\mathcal{O}_K$ é maximal.

Demonstração:

(a) $\mathcal{O}_K$ é um anel comutativo com unidade, logo é um domínio. Denotemos por $Fr(\mathcal{O}_K)$ o corpo de frações de $\mathcal{O}_K$. É claro que $Fr(\mathcal{O}_K) \subset K$, pois $\mathcal{O}_K \subseteq K$. Por outro lado, dado $\alpha \in \mathcal{O}_K$, pelo Lema 1.3.2, $c\alpha \in \mathcal{O}_K$, com $c \in \mathbb{Z}^*$. Assim, $\frac{c\alpha}{c} \in Fr(\mathcal{O}_K)$, donde segue que $\alpha \in Fr(\mathcal{O}_K)$ e então $K \subseteq Fr(\mathcal{O}_K)$. Portanto $Fr(\mathcal{O}_K) = K$.

(b) Do Teorema 1.4.1, o grupo $(\mathcal{O}_K, +)$ é abeliano livre de posto n , logo, se $\mathfrak{a}$ é um ideal de $\mathcal{O}_K$, segue que $(\mathfrak{a}, +)$ é abeliano livre de posto menor ou igual a n . Temos que toda $\mathbb{Z}$ -base para $(\mathfrak{a}, +)$ gera $\mathfrak{a}$ como um ideal, então todo ideal de $\mathcal{O}_K$ é finitamente gerado e, portanto, $\mathcal{O}_K$ é Noetheriano.

(c) Segue do Teorema 1.3.2.



(d) Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $\alpha \neq 0$, $\alpha \in \mathfrak{p}$. Então,

$$N(\alpha) = \alpha_1 \dots \alpha_n = s,$$

sendo α_i os conjugados de α , com $\alpha_1 = \alpha$. Visto que $\alpha_1 \in \mathfrak{p}$, então $\langle s \rangle \subseteq \mathfrak{p}$ o que implica

$$\# \left(\frac{\mathcal{O}_K}{\langle s \rangle} \right) > \# \left(\frac{\mathcal{O}_K}{\mathfrak{p}} \right).$$

Logo, precisamos mostrar que o anel quociente $\mathcal{O}_K/\mathfrak{p}$ é finito, e para isso basta mostrarmos que o anel quociente $\frac{\mathcal{O}_K}{\langle s \rangle}$ é finito. Sejam $\{e_1, \dots, e_m\}$ uma base integral de $\mathcal{O}_K$ e

$$A = \{a_1 e_1 + \dots + a_m e_m : a_i \in \mathbb{Z}, 0 \leq a_i < s\}.$$

Assim, $\#A = s^m$. Dado $x \in \mathcal{O}_K$, $x = \sum_{i=1}^m b_i e_i$, $b_i \in \mathbb{Z}$.

Mas, pelo Algoritmo da Divisão $b_i = q_i s + r_i$. Logo,

$$x = \sum_{i=1}^m (sq_i + r_i) e_i = s \sum_{i=1}^m q_i e_i + \sum_{i=1}^m r_i e_i,$$

onde $0 \leq r_i < s$, e como $s \in \mathfrak{p}$ e $q_i e_i \in \mathcal{O}_K$, segue que $sq_i e_i \in \mathfrak{p}$ e a classe lateral

$$\bar{x} = \overline{\sum_{i=1}^m r_i e_i}.$$

Portanto, $\frac{\mathcal{O}_K}{\langle s \rangle}$ é finito. Entretanto, sendo $\mathfrak{p}$ um ideal primo, $\mathcal{O}_K/\mathfrak{p}$ é domínio e como

$\mathcal{O}_K/\mathfrak{p}$ é finito, segue que $\mathcal{O}_K/\mathfrak{p}$ é corpo. Portanto $\mathfrak{p}$ é maximal.

■

Um anel satisfazendo todas as condições do Teorema 1.7.1 é denominado Anel de Dedekind.

Observemos que um ideal deve ser descrito como um $\mathcal{O}_K$ -módulo de $\mathcal{O}_K$ e, assim, restringimos ao estudo de $\mathcal{O}_K$ -submódulos do corpo K . Os submódulos de interesse os

quais darão a estrutura de grupo desejada, serão aqueles caracterizados pela seguinte propriedade:

Seja $\mathcal{O}_K$ o anel dos inteiros algébricos de um corpo de números K . Dizemos que um $\mathcal{O}_K$ -submódulo $\mathfrak{a}$ de K é um ideal fracionário de $\mathcal{O}_K$, se existir um elemento c não nulo de $\mathcal{O}_K$, tal que $c\mathfrak{a}$ é um ideal de $\mathcal{O}_K$. Em outras palavras, o conjunto $\mathfrak{b} = c\mathfrak{a}$ é um ideal de $\mathcal{O}_K$ e $\mathfrak{a} = c^{-1}\mathfrak{b}$.

Exemplo 1.7.1 *Os ideais fracionários de $\mathbb{Z}$ são da forma $r\mathbb{Z}$, onde $r \in \mathbb{Q}$.*

O interesse em ideais fracionários é maior, pois $\mathcal{O}_K$ não é necessariamente um domínio de ideais principais. Em geral, um ideal é claramente um ideal fracionário e, reciprocamente um ideal fracionário $\mathfrak{a}$ é um ideal se, e somente se, $\mathfrak{a} \subseteq \mathcal{O}_K$.

Os dois teoremas abaixo enunciados representam os principais resultados desta seção e serão demonstrados juntos, em uma série de etapas.

Teorema 1.7.2 ([13], pag. 117) *Os ideais fracionários não nulos de $\mathcal{O}_K$ formam um grupo abeliano multiplicativo.*

Teorema 1.7.3 ([13], pag. 117) *Todo ideal não nulo de $\mathcal{O}_K$ pode ser escrito como um produto de ideais primos unicamente determinados a menos da ordem dos fatores.*

Demonstração:

(a) Seja $\mathfrak{a} \neq 0$ um ideal de $\mathcal{O}_K$. Então, existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ tais que:

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Por contradição, suponhamos que não. Então, sendo $\mathcal{O}_K$ Noetheriano devemos escolher $\mathfrak{a}$ maximal, sujeito a não existência de tais ideais primos $\mathfrak{p}$. Como tal ideal $\mathfrak{a}$ não é primo, então existem ideais $\mathfrak{b}, \mathfrak{c}$ de $\mathcal{O}_K$ com $\mathfrak{bc} \subseteq \mathfrak{a}$, $\mathfrak{b} \not\subseteq \mathfrak{a}$, $\mathfrak{c} \not\subseteq \mathfrak{a}$.

Sejam

$$a_1 = a + b \quad \text{e} \quad a_2 = a + c.$$

Então, $a_1 a_2 = (a + b)(a + c) \subseteq a$, $a_1 \not\supseteq a$ e $a_2 \not\supseteq a$.

Pela maximalidade de a existem ideais primos $p_1, \dots, p_s, p_{s+1}, \dots, p_r$, tais que,

$$p_1 \dots p_s \subseteq a_1 \quad \text{e} \quad p_{s+1} \dots p_r \subseteq a_2.$$

Assim,

$$p_1 \dots p_r \subseteq a_1 a_2 \subseteq a,$$

o que contraria a escolha de a .

(b) Definição do inverso de um ideal a de $\mathcal{O}_K$.

Para cada ideal a de $\mathcal{O}_K$, definimos

$$a^{-1} = \{x \in K \mid xa \subseteq \mathcal{O}_K\}.$$

Afirmção 1: a^{-1} é um $\mathcal{O}_K$ -submódulo.

De fato:

(i) Sejam $n_1, n_2 \in a^{-1}$, ou seja, $n_1 \in K$ tal que $n_1 a \subseteq \mathcal{O}_K$ e $n_2 \in K$ tal que, $n_2 a \subseteq \mathcal{O}_K$.

Então,

$$n_1 a + n_2 a = (n_1 + n_2) a.$$

Como o lado esquerdo da igualdade está em $\mathcal{O}_K$, segue que $(n_1 + n_2) a \subseteq \mathcal{O}_K$.

(ii) Para qualquer $\alpha \in \mathcal{O}_K$, $\alpha \in K$, pois $\mathcal{O}_K \subset K$ e dado $x \in a^{-1}$ segue que $x \in K$ e $xa \subseteq \mathcal{O}_K$, logo, $(\alpha x)a = \alpha(xa) \subseteq \mathcal{O}_K$, o que implica $\alpha x \in a^{-1}$.

Afirmção 2: a^{-1} é um ideal fracionário.

De fato, se $a \neq 0$ então para algum $c \in a$, não nulo, temos $c a^{-1} \subseteq \mathcal{O}_K$.

Afirmção 3: $\mathcal{O}_K \subseteq a^{-1}$.



De fato, dado $x \in \mathcal{O}_K$ temos que $xa \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$, logo, $x \in \mathfrak{a}^{-1}$. Portanto, $\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$.

Pela afirmação 3, $\mathfrak{a} = \mathfrak{a}\mathcal{O}_K \subseteq \mathfrak{a}\mathfrak{a}^{-1}$ e da definição de $\mathfrak{a}^{-1}$, $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$.

De fato, dado $x \in \mathfrak{a}^{-1}$, $xa \subseteq \mathcal{O}_K$ e $y \in \mathfrak{a}$, então:

$$(xa)y = x(ay) = xa \subseteq \mathcal{O}_K.$$

Portanto, $\mathfrak{a}\mathfrak{a}^{-1}$ é um ideal de $\mathcal{O}_K$. Observemos que dados $\mathfrak{p}$, $\mathfrak{a}$ ideais de $\mathcal{O}_K$, $\mathfrak{a} \subseteq \mathfrak{p}$ implica que $\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

(c) Se $\mathfrak{a}$ é um ideal próprio, então $\mathcal{O}_K \subsetneq \mathfrak{a}^{-1}$.

Sendo $\mathfrak{a} \subseteq \mathfrak{p}$, para algum ideal maximal $\mathfrak{p}$, então $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ e assim é suficiente provarmos que $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

Seja $a \in \mathfrak{p}$, $a \neq 0$.

Pelo item (a), consideremos o menor r tal que:

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \langle a \rangle,$$

para $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ primos. Visto que $\langle a \rangle \subseteq \mathfrak{p}$ e $\mathfrak{p}$ é ideal primo, então algum $\mathfrak{p}_i \subseteq \mathfrak{p}$.

Suponhamos sem perda de generalidade, que $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Daí $\mathfrak{p}_1 = \mathfrak{p}$ sendo que ideais primos em $\mathcal{O}_K$ são maximais, logo,

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq \langle a \rangle,$$

pela minimalidade de r . Portanto, existe $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ tal que b não pertença a $\langle a \rangle$.

Mas $b\mathfrak{p} \subseteq \langle a \rangle$ então $ba^{-1}\mathfrak{p} \subseteq \mathcal{O}_K$ e pela definição de ideal inverso segue que $ba^{-1} \in \mathfrak{p}^{-1}$.

Por outro lado $b \notin a\mathcal{O}_K$ e então $ba^{-1} \notin \mathcal{O}_K$, portanto, $\mathfrak{p}^{-1} \neq \mathcal{O}_K$ e, consequentemente $\mathfrak{a}^{-1} \neq \mathcal{O}_K$.

(d) Se $\mathfrak{a}$ é um ideal não nulo e $\mathfrak{a}S \subseteq \mathfrak{a}$ para qualquer subconjunto $S \subseteq K$, então $S \subseteq \mathcal{O}_K$.

Devemos mostrar que se $\mathfrak{a}\alpha \subseteq \mathfrak{a}$ para $\alpha \in S$, então $\alpha \in \mathcal{O}_K$. Já que $S \subseteq K$, $\alpha \in K$ e pelo item (c) do Teorema 1.7.1, temos que $\alpha \in \mathcal{O}_K$. Portanto, $S \subseteq \mathcal{O}_K$.

(e) Se $\mathfrak{p}$ é um ideal maximal, então $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Pelo item (b), $\mathfrak{p}\mathfrak{p}^{-1}$ é um ideal tal que,

$$\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K.$$

Visto que $\mathfrak{p}$ é maximal, $\mathfrak{p}\mathfrak{p}^{-1}$ é igual a $\mathfrak{p}$ ou a $\mathcal{O}_K$.

Se $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, então pelo item (d) temos que $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, o que contraria o item (c).

Logo, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Agora, podemos estender (d) para todo ideal $\mathfrak{a}$.

(f) Para todo ideal $\mathfrak{a} \neq 0$, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.

Seja $\mathfrak{a}$ maximal tal que $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathcal{O}_K$. Então, $\mathfrak{a} \subseteq \mathfrak{p}$, onde $\mathfrak{p}$ é maximal. Pelo item (b), temos $\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, logo,

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_K.$$

Em particular, $\mathfrak{a}\mathfrak{p}^{-1}$ é um ideal de $\mathcal{O}_K$. Deste modo, não vale a igualdade $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, pois implicaria, pelo item (d), $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, contradizendo mais uma vez o item (c).

Assim, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ e pela maximalidade de $\mathfrak{a}$, segue que:

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathcal{O}_K,$$

e pela definição de $\mathfrak{a}^{-1}$,

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}, \quad \text{ou,} \quad \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1}.$$

Assim,

$$\mathcal{O}_K \subseteq \mathfrak{a}\mathfrak{a}^{-1} \quad \text{e} \quad \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_K.$$

(g) Todo ideal fracionário $\mathfrak{a}$ tem um inverso $\mathfrak{a}^{-1}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.



Sabemos que o conjunto $\mathfrak{F}$, dos ideais fracionários, é um semi-grupo, isto é, vale a lei do fechamento e tem unidade. Então, dado um ideal fracionário $\mathfrak{a}$, precisamos encontrar outro ideal fracionário $\mathfrak{t}$ tal que $\mathfrak{a}\mathfrak{t} = \mathcal{O}_K$ e neste caso $\mathfrak{t}$ será o inverso. Mas existe um ideal $\mathfrak{b}$ e um elemento $c \neq 0$, $c \in \mathcal{O}_K$ tal que $\mathfrak{a} = c^{-1}\mathfrak{b}$ e considere $\mathfrak{t} = c\mathfrak{b}^{-1}$, então $\mathfrak{a}\mathfrak{t} = \mathcal{O}_K$ e, portanto, o conjunto dos ideais fracionários de $\mathcal{O}_K$ é um grupo abeliano multiplicativo.

(h) Todo ideal não nulo $\mathfrak{a}$ é um produto de ideais primos.

Suponhamos $\mathfrak{a}$ maximal e mais, que $\mathfrak{a}$ não se fatore em produto de ideais primos. Logo $\mathfrak{a}$ não é primo, mas $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p}$ maximal e pelo item (f) $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$.

Por outro lado, pela maximalidade de $\mathfrak{a}$ temos que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ ou $\mathfrak{a}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Logo,

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \dots \mathfrak{p}_r,$$

onde $\mathfrak{p}_i$, $i = 2, \dots, r$, são ideais primos e, portanto, $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r$.

(i) A fatoração em ideais primos é única.

Sejam $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ ideais primos não nulos, tais que:

$$\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s.$$

Suponhamos que, para todo $t < \min\{r, s\}$, seja verdadeira a seguinte afirmação:

Se $\mathfrak{a}_1, \dots, \mathfrak{a}_t, \mathfrak{b}_1, \dots, \mathfrak{b}_s$ são ideais primos não nulos de modo que

$$\mathfrak{a}_1 \dots \mathfrak{a}_t = \mathfrak{b}_1 \dots \mathfrak{b}_s \quad \text{então} \quad t = s \text{ e } \mathfrak{a}_i = \mathfrak{b}_i, \quad i = 1, \dots, s.$$

Se $\min\{r, s\} = 1$, consideremos por exemplo $r = 1$.

Então, $\mathfrak{a}_1 = \mathfrak{b}_1 \dots \mathfrak{b}_s$, e como $\mathfrak{a}_1$ é primo, temos $s = 1$. De $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{q}_1$, concluímos que $\mathfrak{q}_1$ divide $\mathfrak{p}_1 \dots \mathfrak{p}_r$ e sem perda de generalidade, podemos supor $\mathfrak{q}_1 = \mathfrak{p}_1$.

Obtemos assim,

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

O resultado segue da hipótese de indução.

Portanto, todo ideal de $\mathcal{O}_K$ pode ser fatorado de modo único como produto de ideais primos.

Teorema 1.7.4 *A Fatoração de elementos em $\mathcal{O}_K$ em produto de elementos irredutíveis é única se, e somente se, todo ideal de $\mathcal{O}_K$ é principal.*

Proposição 1.7.1 ([11], pag. 89) *Sejam $K \subset L$ corpos de números, com $[L : K] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^g \mathfrak{p}_i^{e_i}, \quad (1.4)$$

a decomposição de $\mathfrak{p}\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$. Então os ideais $\mathfrak{p}_i$, são necessariamente os ideais primos $\mathfrak{q}$ de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

A partir da equação (1.4) g é denominado número de decomposição de $\mathfrak{p}$ na extensão L/K . Notemos que, os ideais primos $\mathfrak{q}$ acima de um dado ideal primo $\mathfrak{p}$ são os únicos que ocorrem na decomposição prima de $\mathfrak{p}\mathcal{O}_L$. Os expoentes e_i 's com os quais ocorrem são chamados de índices de ramificação e denotaremos por $e(\mathfrak{q} | \mathfrak{p})$. Dizemos que um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ é ramificado em $\mathcal{O}_L$ (ou em L) se, $e(\mathfrak{q} | \mathfrak{p}) > 1$ para algum ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$.

Teorema 1.7.5 ([7], pag. 63) *Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$, $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$, então as seguintes condições são equivalentes:*

- (a) $\mathfrak{q} | \mathfrak{p}\mathcal{O}_L$,
- (b) $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}_L$,
- (c) $\mathfrak{q} \supset \mathfrak{p}$,

$$(d) \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p},$$

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

Teorema 1.7.6 ([7], pag. 63) *Todo ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ está acima de um único ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ e todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está abaixo de no mínimo um ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$.*

Há outro número importante associado com um par de ideais primos $\mathfrak{p}$ e $\mathfrak{q}$, com $\mathfrak{q}$ acima de $\mathfrak{p}$. Sabemos que os anéis quocientes $\mathcal{O}_K/\mathfrak{p}$ e $\mathcal{O}_L/\mathfrak{q}$ são corpos se $\mathfrak{p}$ e $\mathfrak{q}$ são ideais maximais.

Como $\mathcal{O}_K \subset \mathcal{O}_L$, temos que $\mathcal{O}_K$ em $\mathcal{O}_L$, induz um homomorfismo de anéis $\mathcal{O}_K \rightarrow \mathcal{O}_L/\mathfrak{q}$, e o núcleo é $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ (pelo Teorema 1.7.5, item (d)), então obtemos a imersão $\mathcal{O}_K/\mathfrak{p} \rightarrow \mathcal{O}_L/\mathfrak{q}$. Esses são chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$. Esses corpos são finitos e assim, $\mathcal{O}_L/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_K/\mathfrak{p}$ e seja f este grau. Então, f é chamado de **grau de inércia** ou **grau residual** de $\mathfrak{q}$ sobre $\mathfrak{p}$ e denotaremos 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 $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_U$, então

$$e(\mathfrak{u} | \mathfrak{p}) = e(\mathfrak{u} | \mathfrak{q})e(\mathfrak{q} | \mathfrak{p}),$$

$$f(\mathfrak{u} | \mathfrak{p}) = f(\mathfrak{u} | \mathfrak{q})f(\mathfrak{q} | \mathfrak{p}).$$

Teorema 1.7.7 (Igualdade Fundamental) ([7], pag. 65) *Sejam n o grau de L sobre K e $\mathfrak{q}_1, \dots, \mathfrak{q}_g$ os ideais primos de $\mathcal{O}_L$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Denotamos por $e_1, \dots, e_g$ e $f_1, \dots, f_g$ os correspondentes índices de ramificação e graus residuais. Então:*

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

Lema 1.7.1 (*Lema de Kummer*) ([1], pag. 39) *Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Dados um número primo p tal que p não divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ e $f(X)$ o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem $p_1(X), \dots, p_g(X) \in \mathbb{Z}[X]$, polinômios irredutíveis, $e_1, \dots, e_g \in \mathbb{N}^*$, tais que,*

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

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

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

(iii) $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}} \right] = \partial p_i(X) = f_i$.

Exemplos do Lema de Kummer e do Teorema 1.7.7, serão vistos no próximo capítulo.

1.8 Norma de um Ideal

Nesta seção, definiremos a norma de um ideal, como uma generalização da norma absoluta de um elemento de $\mathcal{O}_K$ e, em seguida, mostraremos que a função norma é multiplicativa.

Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Definimos a norma de $\mathfrak{a}$ como sendo a cardinalidade do quociente $\mathcal{O}_K/\mathfrak{a}$ e denotamos por $N(\mathfrak{a})$. Em outras palavras,

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

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

Teorema 1.8.1 ([13], pag. 126) *Sejam K um corpo de números de grau n e $\mathcal{O}_K$ o seu anel dos inteiros algébricos. Então,*

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

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

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

onde D_K é o discriminante de K .

Demonstração:

(a) Pelo Teorema 1.4.1, $\mathcal{O}_K$ é abeliano livre de posto n e visto que o anel quociente $\mathcal{O}_K/\mathfrak{a}$ é finito, então $\mathfrak{a}$ também é abeliano livre de posto n , e portanto, admite uma base $\{\alpha_1, \dots, \alpha_n\}$.

(b) Seja $\{\omega_1, \dots, \omega_n\}$ uma $\mathbb{Z}$ -base de $\mathcal{O}_K$ e suponhamos $\alpha_i = \sum_{j=1}^n c_{ij}\omega_j$; $j = 1, \dots, n$.

Visto que $\mathcal{O}_K$ e $\mathfrak{a}$ tem posto n , então

$$N(\mathfrak{a}) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{a}} \right) = | \det c_{ij} |.$$

Pelo Lema 1.2.1, temos:

$$\Delta[\alpha_1, \dots, \alpha_n] = (\det c_{ij})^2 \Delta[\omega_1, \dots, \omega_n] = (|N(\mathfrak{a})|)^2 D_K.$$

Portanto,

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \dots, \alpha_n]}{D_K} \right|^{1/2}.$$

■

Corolário 1.8.1 ([13], pag. 126) *Seja $\mathfrak{a} = \langle a \rangle$ um ideal principal, então $N(\mathfrak{a}) = |N(a)|$.*

Exemplo 1.8.1 *Seja $\mathcal{O}_K$ o anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, então*

$$N(\langle a + b\sqrt{d} \rangle) = |a^2 - b^2d|,$$

em particular, temos:

$$N(<15>) = 15^2.$$

A norma de ideais, como a norma de elementos, é multiplicativa:

Teorema 1.8.2 ([19], pag. 127) *Sejam K um corpo de números e $\mathfrak{a}$, $\mathfrak{b}$ ideais não nulos de $\mathcal{O}_K$. Então*

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

É conveniente introduzir ainda outro uso para a palavra "divide". Se $\mathfrak{a}$ é um ideal de $\mathcal{O}_K$ e b um elemento de $\mathcal{O}_K$ tal que $\mathfrak{a} \mid \langle b \rangle$, 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 1.8.3 ([19], pag. 129) *Seja $\mathfrak{a}$ um ideal de $\mathcal{O}_K$, $\mathfrak{a} \neq 0$.*

- (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 K .

Em particular, o item (c) do Teorema 1.8.3, pode ser escrito do seguinte modo: para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$, temos que, $N(\mathfrak{p}) = p^f$, onde f é o grau residual de $\mathfrak{p}$ e p o único número primo de $\mathfrak{p}$. De fato, como $\left[\frac{\mathcal{O}_K}{\mathfrak{p}} : \frac{\mathbb{Z}}{p\mathbb{Z}} \right] = f$, então resulta que $\mathcal{O}_K/\mathfrak{p}$ tem p^f elementos.

Exemplo 1.8.2 Sejam $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, o seu anel dos inteiros algébricos, $\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-5} \rangle$ ideal primo de $\mathcal{O}_K$. 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 1.8.3(item (b)).

Exemplo 1.8.3 Seja $\mathfrak{a}$ um ideal primo satisfazendo:

$$N(\mathfrak{a}) = p^m \quad ; \quad m > 1$$

Isto nos diz que um ideal primo não tem necessariamente uma norma que seja um primo, por exemplo, $\mathcal{O}_K = \mathbb{Z}[\sqrt{i}]$, $\mathfrak{a} = \langle 11 \rangle$. Aqui, 11 é irredutível em $\mathbb{Z}[i]$, logo é primo, pois $\mathbb{Z}[i]$ tem fatoração única. Se um elemento é primo, então o ideal que ele gera também é primo. Assim, $\langle 11 \rangle$ é um ideal primo em $\mathbb{Z}[i]$, mas

$$N(\langle 11 \rangle) = |N(11)| = 11^2.$$

2.1 Corpos Quadráticos

Chamamos corpo quadrático a qualquer corpo de número de grau 2, ou seja, com as seguintes características:

Capítulo 2

Corpos Quadráticos e Ciclotômicos

Seja K um corpo quadrático. Então $K = \mathbb{Q}(\theta)$, onde θ é um zero da equação

Neste capítulo temos por objetivo apresentar a Teoria Algébrica dos Números necessária à compreensão das aplicações a serem desenvolvidas no capítulo seguinte.

Inicialmente caracterizamos os corpos quadráticos, seu anel dos inteiros algébricos e o seu discriminante. Na seção (2.2) corpos ciclotômicos caracterizamos os polinômios ciclotômicos, apresentamos uma base integral e o cálculo do discriminante.

Em seguida, apresentamos alguns resultados que serão relevantes para o desenvolvimento das aplicações acima citada. Na seção seguinte, serão dadas as definições de empacotamento esférico, empacotamento reticulado, densidade de empacotamento e densidade de centro.

Finalizando, introduziremos o método algébrico para a obtenção de reticulados, bem como a fórmula para o cálculo da sua densidade de centro.

Teorema 2.1.3 ([13], pag. 67) Seja d um número inteiro não de quadrado. $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{O}_K$ o anel dos inteiros algébricos de K . Então $\mathbb{O}_K = \mathbb{Z}[\omega]$, onde

$$\omega = \begin{cases} \frac{\sqrt{d}}{2}, & \text{se } d \equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2}, & \text{se } d \equiv 0 \pmod{4} \end{cases} \quad (2.1)$$

2.1 Corpos Quadráticos

Chamamos corpo quadrático a qualquer corpo de números de grau 2, os quais tem as seguintes características:

Teorema 2.1.1 ([13], pag. 67) *Os corpos quadráticos são da forma $\mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrados.*

Demonstração:

Seja K um corpo quadrático. Então $K = \mathbb{Q}(\theta)$, onde θ é um zero da equação:

$$X^2 + aX + b = 0; \quad a, b \in \mathbb{Z},$$

ou seja, $\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$

Seja $a^2 - 4b = r^2d$, onde $r, d \in \mathbb{Z}$ e d é livre de quadrados. Assim

$$\theta = \frac{-a \pm r\sqrt{d}}{2}$$

E então,

$$\mathbb{Q}(\theta) = \mathbb{Q}\left(\frac{-a \pm r\sqrt{d}}{2}\right) = \mathbb{Q}\left(\frac{-a}{2} \pm \frac{r\sqrt{d}}{2}\right) = \mathbb{Q}(\sqrt{d})$$

Portanto,

$$\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$$

Teorema 2.1.2 ([13], pag. 67) *Sejam d um número inteiro livre de quadrados, $K = \mathbb{Q}(\sqrt{d})$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Então $\mathcal{O}_K = \mathbb{Z}[\alpha]$, onde*

$$\alpha = \begin{cases} \sqrt{d}, & \text{se } d \equiv 2 \text{ ou } 3 \pmod{4}; \\ \frac{1 + \sqrt{d}}{2}, & \text{se } d \equiv 1 \pmod{4}. \end{cases} \quad (2.1)$$

Demonstração:

Temos que α é raiz do polinômio irredutível: $X^2 - d$, se $d \equiv 2$ ou $3 \pmod{4}$; ou $X^2 - X + \frac{1-d}{4}$, se $d \equiv 1 \pmod{4}$. Notemos que ambos pertencem a $\mathbb{Z}[X]$, pois $d, \frac{1-d}{4} \in \mathbb{Z}$. Assim α é um inteiro algébrico, e portanto, $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$.

Reciprocamente, seja $\gamma = r + s\sqrt{d} \in \mathcal{O}_K$; $r, s \in \mathbb{Q}$. Assim, se $s = 0$, então $r \in \mathbb{Z}$, logo $\gamma \in \mathbb{Z} \subset \mathbb{Z}[\alpha]$. Se $s \neq 0$, então

$$\text{irr}(\gamma, \mathbb{Q}) = X^2 - 2rX + (r^2 - ds^2).$$

Logo $2r, r^2 - ds^2 \in \mathbb{Z}$, conseqüentemente $4r^2 - 4ds^2 \in 4\mathbb{Z}$, donde segue que, $(2r)^2 - d(2s)^2 \in 4\mathbb{Z} \subset \mathbb{Z}$. Visto que $2r \in \mathbb{Z}$, segue que $d(2s)^2 \in \mathbb{Z}$. Mostremos que $2s \in \mathbb{Z}$. De fato, suponhamos que $2s \notin \mathbb{Z}$, isto é, $2s = \frac{x}{y}$, com $(x, y) = 1$, $x, y \in \mathbb{Z}$. Sendo $y \neq 1$, existe um primo p tal que p^2 divide y^2 . Mas como $d(2s)^2 \in \mathbb{Z}$, temos que $d\frac{x^2}{y^2} \in \mathbb{Z}$, donde segue que p^2 divide d , o que é um absurdo, pois d é livre de quadrados, e portanto, $2s \in \mathbb{Z}$. Fazendo $r = \frac{u}{2}$ e $s = \frac{v}{2}$; $u, v \in \mathbb{Z}$, temos que $u^2 - dv^2 \in 4\mathbb{Z}$. Sendo $u^2 \equiv 0$ ou $1 \pmod{4}$, se $d \equiv 2$ ou $3 \pmod{4}$, então $u^2 - dv^2 \in 4\mathbb{Z}$ se, e somente se, $u \equiv v \equiv 0 \pmod{2}$, logo, $\gamma \in \mathbb{Z}[\sqrt{d}]$, e portanto, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Entretanto, se $d \equiv 1 \pmod{4}$, então $u^2 \equiv v^2 \equiv 1 \pmod{4}$ também é admissível, isto é, para que

$$\gamma = \frac{u}{2} + \frac{v}{2}\sqrt{d} \tag{2.2}$$

seja inteiro é suficiente que u e v tenham a mesma paridade. Logo, $u - v = 2t$ e daí, $u = v + 2t$, e de (2.2), segue que $\gamma = \frac{v+2t}{2} + \frac{v}{2}\sqrt{d} = t.1 + v(\frac{1+\sqrt{d}}{2}) \in \mathbb{Z}[\alpha]$, e portanto, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. ■

Os monomorfismos de K em $\mathbb{C}$ são dados por:

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}; \quad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Assim temos o seguinte cálculo para o discriminante:

Teorema 2.1.3 ([13], pag. 68)

- (i) Se $d \equiv 2$ ou $3 \pmod{4}$ então o discriminante de $\mathbb{Q}(\sqrt{d})$ é igual a $4d$.
 (ii) Se $d \equiv 1 \pmod{4}$ então $\mathbb{Q}(\sqrt{d})$ tem discriminante igual a d .

Demonstração:

Pelo Teorema 2.1.2 temos o seguinte cálculo para o discriminante:

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = (-2\sqrt{d})^2 = 4d \quad \text{e} \quad \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix} = (-\sqrt{d})^2 = d.$$

Exemplo 2.1.1 O primeiro corpo de números a ser estudado é o corpo de números Gaussiano $K = \mathbb{Q}(\sqrt{-1})$. Pelo Teorema 2.1.2, o anel dos inteiros algébricos de K é $\mathbb{Z}[\sqrt{-1}]$, também conhecido como anel dos inteiros algébricos Gaussianos, e do Teorema 2.1.3 temos que seu discriminante é -4 . Neste caso, os monomorfismos de K em $\mathbb{C}$ são dados pela inclusão e a conjugação complexa, isto é,

$$\sigma_1(a + b\sqrt{-1}) = a + b\sqrt{-1} \quad \text{e} \quad \sigma_2(a + b\sqrt{-1}) = a - b\sqrt{-1}.$$

Assim,

$$N(a + b\sqrt{-1}) = a^2 + b^2 \quad \text{e} \quad \text{Tr}(a + b\sqrt{-1}) = 2a.$$

Mais geralmente, se $K = \mathbb{Q}(\sqrt{d})$ e $N = N_{K/\mathbb{Q}}$ e $\text{Tr} = \text{Tr}(K/\mathbb{Q})$, temos:

$$N(a + b\sqrt{d}) = a^2 - db^2 \quad \text{e} \quad \text{Tr}(a + b\sqrt{d}) = 2a.$$



para $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

Um corpo quadrático $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, é dito real se $d > 0$ e imaginário se $d < 0$.

No exemplo a seguir mostramos a fatoração em irredutíveis, a aplicação do Lema de Kummer e do Teorema da Igualdade Fundamental em corpos quadráticos.

Exemplo 2.1.2 Em $K = \mathbb{Q}(\sqrt{-5})$ temos a seguinte fatoração:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

Como $-5 \equiv 3 \pmod{4}$, segue do Teorema 2.1.2 que $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, e assim os inteiros algébricos em $\mathcal{O}_K$ são da forma $a + b\sqrt{-5}$, para $a, b \in \mathbb{Z}$.

Afirmção: 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$, são irredutíveis em $\mathcal{O}_K$. Com efeito, como vimos, a norma é dada por:

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Logo as normas dos elementos citados acima são 4, 9, 6 e 6, respectivamente. Assim, se 2 fosse redutível em $\mathcal{O}_K$, isto é, $2 = x \cdot y$, onde $x, y \in \mathcal{O}_K$, e não são unidades, então $4 = N(2) = N(x) \cdot N(y)$. Logo $N(x) = \pm 2$ e $N(y) = \pm 2$. De modo análogo, os divisores não triviais de 3 devem, se existirem, ter norma ± 3 , e os divisores não triviais de $1 \pm \sqrt{-5}$ devem ter norma ± 2 ou ± 3 . Então temos as seguintes equações:

$$a^2 + 5b^2 = \pm 2 \quad \text{ou,} \quad a^2 + 5b^2 = \pm 3; \quad a, b \in \mathbb{Z}.$$

Se $|b| \geq 1$, então $|a^2 + 5b^2| \geq 5$, donde segue que a única possibilidade é $|b| = 0$. Assim $a^2 = \pm 2$ ou ± 3 , o que é impossível em $\mathbb{Z}$. Portanto 2, 3, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ são todos

irredutíveis em $\mathcal{O}_K$. Ainda, sendo $N(2) = 4$, $N(1 + \sqrt{-5}) = 6$, da Proposição 1.6.4 item (b) segue que 2 não é associado de $1 + \sqrt{-5}$ ou $1 - \sqrt{-5}$, e portanto a fatoração não é única.

Agora veremos uma aplicação do Lema de Kummer e do Teorema da Igualdade Fundamental.

Seja $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ o anel dos inteiros algébricos e $X^2 + 5$ o polinômio irredutível de $\sqrt{-5}$ sobre $\mathbb{Q}$. Consideremos o ideal $2\mathbb{Z} \subset \mathbb{Z}$. Fatoramos o polinômio $X^2 + 5$ como:

$$X^2 + 5 \equiv (X + 1)^2 \pmod{2\mathbb{Z}[X]}$$

e pelo Lema de Kummer temos:

(a) $\mathfrak{p} = \langle 2, \theta + 1 \rangle$ é o ideal de $\mathcal{O}_K$ acima de $2\mathbb{Z}$,

(b) $2\mathcal{O}_K = \mathfrak{p}^2$,

(c) $[\frac{\mathcal{O}_K}{\mathfrak{p}} : \frac{\mathbb{Z}}{2\mathbb{Z}}] = 1 = f_1$.

E pelo Teorema da Igualdade Fundamental, o grau residual é 1 e o índice de ramificação é 2.

Considerando agora o ideal $3\mathbb{Z} \subset \mathbb{Z}$, temos que o polinômio $X^2 + 5$ fatora-se como:

$$X^2 + 5 \equiv (X + 1) \cdot (X + 2) \pmod{3\mathbb{Z}[X]},$$

Assim, pelo Lema de Kummer, temos:

(a) $\mathfrak{p}_1 = \langle 3, \theta + 1 \rangle$ e $\mathfrak{p}_2 = \langle 3, \theta + 4 \rangle$ são os ideais de $\mathcal{O}_K$ acima de $3\mathbb{Z}$,

(b) $3\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$,

(c) $[\frac{\mathcal{O}_K}{\mathfrak{p}_1} : \frac{\mathbb{Z}}{3\mathbb{Z}}] = [\frac{\mathcal{O}_K}{\mathfrak{p}_2} : \frac{\mathbb{Z}}{3\mathbb{Z}}] = 1 = f_1 = f_2$.

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

2.2 Corpos Ciclotômicos

Chamamos n -ésimo corpo ciclotômico ao corpo $\mathbb{Q}(\xi_n)$, onde $\xi_n = e^{2\pi i/n}$ é uma raiz n -ésima primitiva da unidade e $\Phi_n(x) = \prod_{\substack{i=1 \\ (i,n)=1}}^n (x - \xi_n^i)$ é o n -ésimo polinômio ciclotômico. O polinômio ciclotômico Φ_n é um polinômio mônico em $\mathbb{Z}[X]$, de grau $\phi(n)$, onde ϕ é a função de Euler.

Lema 2.2.1 ([8], pag. 110) *Seja n um inteiro positivo, então*

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

Demonstração:

Sejam $1 = d_1 < d_2 < \dots < d_s = n$ todos os divisores de n . Logo,

$$X^n - 1 = \prod_{\substack{i=0 \\ (i,n)=d_1}}^{n-1} (X - \xi_n^i) \cdot \prod_{\substack{i=0 \\ (i,n)=d_2}}^{n-1} (X^n - \xi_n^i) \dots \prod_{\substack{i=0 \\ (i,n)=d_s}}^{n-1} (X^n - \xi_n^i),$$

e

$$\prod_{\substack{i=0 \\ (i,n)=d_1}}^{n-1} (X^n - \xi_n^i) = \Phi_{\frac{n}{d_1}}(X) = \Phi_n(X), \text{ pois } d_1 = 1.$$

Notemos que se $d = (j, n)$ então $\xi_n^j = \xi_{n/d}^{j/d}$, assim

$$\prod_{\substack{i=0 \\ (i,n)=d}}^{n-1} (X - \xi_n^i) = \prod_{\substack{j=0 \\ (j,t)=1}}^{t-1} (X^n - \xi_n^j) = \Phi_t(X)$$

com $t = n/d$ e $j = i/d$.

Repetindo esse mesmo argumento em todos os fatores temos

$$X^n - 1 = \Phi_{\frac{n}{d_1}}(X) \Phi_{\frac{n}{d_2}}(X) \dots \Phi_{\frac{n}{d_s}}(X)$$

como $\frac{n}{d_1}, \dots, \frac{n}{d_s}$ também são divisores de n , segue o resultado. ■

Exemplo 2.2.1 Seja, $X^p - 1 = \Phi_1 \cdot \Phi_p$, p primo. Assim,

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1.$$

Mais geralmente, para as potências de um número primo p , p^r temos

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

e portanto, $\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \dots + X^{p^{r-1}} + 1$. O polinômio Φ_{15} é obtido da igualdade:

$$X^{15} - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_5 \cdot \Phi_{15} = (X^5 - 1)(X^2 + X + 1)\Phi_{15}$$

ou seja, $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$.

Lema 2.2.2 Seja $p(X)$ um polinômio com coeficientes racionais, tal que $p(X) = f(X) \cdot g(X)$.

Se $f(X)$ tem coeficientes racionais então $g(X)$ também o tem.

Demonstração:

Faremos a demonstração por indução sobre $\partial g = k$. Sejam,

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0;$$

$$g(X) = b_n X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0;$$

polinômios tais que $f(X) \in \mathbb{Q}[X]$, com $a_m, b_n \neq 0$. Se $\partial(g) = 0$, é imediato que $g(X) \in \mathbb{Q}[X]$. Suponhamos que a afirmação é válida para $\partial g = 1, \dots, n-1$, e mostremos que vale para $\partial g = n$. Da hipótese, temos que $f(X) \cdot g(X) \in \mathbb{Q}[X]$, logo, $b_0 \in \mathbb{Q}$.

Visto que $a_m, a_m b_n \in \mathbb{Q}^*$, então $b_n \in \mathbb{Q}$ e

$$f(X)g(X) - f(X)b_n X^n = f(X)(b_{n-1} X^{n-1} + \dots + b_0) \in \mathbb{Q}[X].$$

Por hipótese de indução $b_n, \dots, b_0 \in \mathbb{Q}$ e portanto $g(X) \in \mathbb{Q}[X]$. ■



Lema 2.2.3 ([8], pag. 114) *Seja n um inteiro positivo. Então o n -ésimo polinômio ciclotômico Φ_n tem coeficientes inteiros.*

Demonstração:

Faremos a demonstração por indução sobre n . Para $n = 1$, temos que $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Suponhamos que a afirmação é válida para $2, \dots, n-1$, e mostremos que vale para n . Do Lema 2.2.1, segue que

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X) \cdot \prod_{\substack{d|n \\ d < n}} \Phi_d(X)$$

Seja $f(X) = \prod_{\substack{d|n \\ d < n}} \Phi_d(X)$. Assim $X^n - 1 = \Phi_n(X) \cdot f(X)$, e por hipótese de indução temos que $f(X) \in \mathbb{Z}[X]$. Note que $X^n - 1 \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ e $f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Assim, pelo Lema 2.2.2, segue que $\Phi_n(X) \in \mathbb{Q}[X]$. Logo, pelo Lema de Gauss ([6] pag. 146) existe $\alpha \in \mathbb{Q}$, tal que $\alpha\Phi_n(X), \alpha^{-1}f(X) \in \mathbb{Z}[X]$. Podemos supor $\alpha = 1$, pois $X^n - 1$ é mônico e cada $\Phi_d(X)$ é mônico, logo

$$\prod_{\substack{d|n \\ d < n}} \Phi_d(X)$$

também o é. Portanto $\Phi_n(X) \in \mathbb{Z}[X]$. ■

Lema 2.2.4 ([8], pag. 115) *Seja n um inteiro positivo. Então o n -ésimo polinômio ciclotômico $\Phi_n(X)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração:

Seja $f(X) = \text{irr}(\xi_n, \mathbb{Q})$. Suponhamos que $\Phi_n(X)$ seja redutível sobre $\mathbb{Q}$. Então existe $g(X) \in \mathbb{Q}[X]$, tal que

$$\Phi_n(X) = f(X) \cdot g(X)$$

e mostremos que $\Phi_n(X) = f(X)$. Sejam $K = \mathbb{Q}(\xi_n)$, $\mathcal{O}_K$ o anel dos inteiros algébricos de K , $\mathfrak{p}$ um ideal primo e k um inteiro tal que $(k, n) = 1$, $p \mid k$, onde p é um número primo e $p \in \mathfrak{p}$. Supondo que ξ_n^k não seja raiz de $f(X)$, então é raiz de $g(X)$. Seja $g(X) = c_0 + c_1X + \dots + c_tX^t$. Temos que em $\frac{\mathcal{O}_K}{\mathfrak{p}}$, vale,

$$g(\xi_n^k) = c_0 + c_1\xi_n^k + \dots + c_t\xi_n^{kt}.$$

Como $p \mid k \implies k = p.r$, assim,

$$\overline{g((\xi_n^r)^p)} = \overline{c_0 + c_1(\xi_n^r)^p + \dots + c_t(\xi_n^r)^{pt}} = \bar{0}, \quad \text{onde } \bar{a} \text{ denota a classe de } a \text{ em } \frac{\mathcal{O}_K}{\mathfrak{p}}.$$

Logo,

$$g((\xi_n^r)^p) \equiv c_0 + c_1(\xi_n^r)^p + \dots + c_t(\xi_n^r)^{pt} \pmod{p}$$

Pelo Pequeno Teorema de Fermat ([6], pag. 44) temos que $a^p \equiv a \pmod{p}$, assim,

$$g((\xi_n^r)^p) = c_0^p + (c_1\xi_n^r)^p + \dots + (c_t\xi_n^r)^{pt} + \alpha p$$

Assim, em $\frac{\mathcal{O}_K}{\mathfrak{p}}$, temos,

$$\overline{g((\xi_n^r)^p)} = \overline{c_0^p + (c_1\xi_n^r)^p + \dots + (c_t\xi_n^r)^{pt} + \alpha p} = \overline{c_0^p + (c_1\xi_n^r)^p + \dots + (c_t\xi_n^r)^{pt}}$$

E como $(X + Y)^p = X^p + Y^p$, segue

$$\overline{g((\xi_n^r)^p)} = \overline{(c_0 + c_1\xi_n^r + \dots + c_t\xi_n^{rt})^p} = \bar{0}$$

Vimos no Lema 2.2.1 que

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) = \Phi_n(X) \cdot \prod_{\substack{d \mid n \\ d < n}} \Phi_d(X) = f(X) \cdot g(X) \cdot \prod_{\substack{d \mid n \\ d < n}} \Phi_d(X).$$

Por outro lado, em $\frac{\mathcal{O}_K}{\mathfrak{p}}$,

$$\overline{X^n - 1} = \overline{f(X) \cdot g(X) \cdot \prod_{\substack{d|n \\ d < n}} \Phi_d(X)} \quad (2.3)$$

Logo $\overline{X^n - 1}$ tem raízes múltiplas, a menos que $g(X)$ seja constante.

Derivando o lado esquerdo da equação (2.3), temos $\overline{nX^{n-1}}$, como p não divide n , $\bar{0}$ é a única raiz para a derivada.

Sendo que $\bar{0}$ não é raiz de $\overline{X^n - 1}$, então $\overline{X^n - 1}$ não tem raízes múltiplas. Portanto, $g(X)$ é constante e, conseqüentemente, $f(X) = \Phi_n(X)$. ■

Assim o n -ésimo polinômio ciclotômico é o polinômio irredutível de ξ_n sobre $\mathbb{Q}$ de grau $\phi(n)$, onde ϕ é a função de Euler, a qual é caracterizada por

$$\phi\left(\prod_{i=1}^s p_i^{a_i}\right) = \prod_{i=1}^s (p_i - 1)p_i^{a_i-1}$$

2.2.1 O p -ésimo corpo ciclotômico.

Agora veremos o traço, a norma e o discriminante de $\mathbb{Q}(\xi_p)$, para qualquer p primo.

As potências $\xi_p, \xi_p^2, \dots, \xi_p^{p-1}$ também são raízes p -ésimas da unidade, distintas de 1, e também pelo mesmo argumento, têm $\Phi_p(X)$ como polinômio minimal.

Assim, temos que

$$\Phi_p(X) = X^{p-1} + \dots + X + 1 = (X - \xi_p)(X - \xi_p^2) \dots (X - \xi_p^{p-1}) \quad (2.4)$$

e então os conjugados de ξ_p são $\xi_p, \xi_p^2, \dots, \xi_p^{p-1}$. Isto significa que os monomorfismos de $\mathbb{Q}(\xi_p)$ em $\mathbb{C}$ são dados por

$$\sigma_i(\xi_p) = \xi_p^i, \quad 1 \leq i \leq p-1.$$

para um elemento geral

$$\alpha = a_0 + a_1 \xi_p + \dots + a_{p-2} \xi_p^{p-2}, a_i \in \mathbb{Q}.$$

temos

$$\sigma_i(\alpha) = a_0 + a_1 \xi_p^i + \dots + a_{p-2} \xi_p^{i(p-2)}.$$

Em particular,

$$N(\xi_p) = \xi_p \xi_p^2 \dots \xi_p^{p-1}.$$

Sendo ξ_p e ξ_p^i ($1 \leq i \leq p-1$) conjugados, então possuem a mesma norma,

$$N(\xi_p) = N(\xi_p^i) = (-1)^{p-1} = 1 \quad (2.5)$$

O traço de ξ_p pode ser calculado da seguinte maneira :

$$Tr(\xi_p^i) = Tr(\xi_p) = \xi_p + \xi_p^2 + \dots + \xi_p^{p-1}$$

e usando o fato que

$$\Phi_p(\xi_p) = 1 + \xi_p + \xi_p^2 + \dots + \xi_p^{p-1} = 0$$

temos

$$Tr(\xi_p^i) = -1, \quad Tr(1) = p-1; \quad 1 \leq i \leq p-1. \quad (2.6)$$

Assim,

$$Tr(1 - \xi_p^i) = Tr(1) - Tr(\xi_p^i) = p-1 - (-1) = p. \quad (2.7)$$

Sendo $\xi_p^p = 1$, podemos usar esta fórmula para estender a equação 2.6 para

$$Tr(\xi_p^s) = \begin{cases} -1, & \text{se } s \not\equiv 0 \pmod{p}; \\ p-1, & \text{se } s \equiv 0 \pmod{p}. \end{cases} \quad (2.8)$$

Para qualquer elemento de $\mathbb{Q}(\xi_p)$, o traço é calculado da seguinte maneira:

$$\text{Tr}\left(\sum_{i=0}^{p-2} a_i \xi_p^i\right) = pa_0 - \sum_{i=0}^{p-2} a_i.$$

A norma é mais complicada no caso geral, mas um caso muito útil é o seguinte:

$$N(1 - \xi_p) = \prod_{i=1}^{p-1} (1 - \xi_p^i)$$

a qual pode ser calculada colocando $X = 1$ na equação (2.4) para obter

$$N(1 - \xi_p) = \prod_{i=1}^{p-1} (1 - \xi_p^i) = p \quad (2.9)$$

então, $N(1 - \xi_p) = p$.

Observação 2.2.1 $(1 - \xi_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$. De fato: De (2.9) segue que : $p = (1 - \xi_p)(1 - \xi_p^2) \dots (1 - \xi_p^{p-1})$. Assim temos que $p \in (1 - \xi_p)\mathcal{O}_K$. Portanto $\langle p \rangle \subset (1 - \xi_p)\mathcal{O}_K \cap \mathbb{Z}$, (pois $\langle p \rangle$ é um ideal em $\mathbb{Z}$). Para mostrarmos a outra inclusão vamos supor que $p\mathbb{Z} \subsetneq (1 - \xi_p)\mathcal{O}_K \cap \mathbb{Z} \subseteq \mathbb{Z}$. Como $p\mathbb{Z}$ é maximal ([5], pag. 24), então $(1 - \xi_p)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$. Como $1 \in \mathbb{Z}$, então $1 = (1 - \xi_p)a$, $a \in \mathcal{O}_K$. Então $N(1) = N(1 - \xi_p).N(a)$, donde segue que $1 = p.N(a)$, com $N(a) \in \mathbb{Z}$, o que é um absurdo.

Observação 2.2.2 $\text{Tr}(y(1 - \xi_p)) \in p\mathbb{Z}$, para todo $y \in \mathcal{O}_K$. De fato: Cada conjugado $y_i(1 - \xi_p^i)$ de $y(1 - \xi_p)$ é um múltiplo em $\mathcal{O}_K$ de $(1 - \xi_p)$. Sendo o traço a soma dos conjugados, segue que $\text{Tr}(y(1 - \xi_p)) = y_1(1 - \xi_p) + y_2(1 - \xi_p^2) + \dots + y_{p-1}(1 - \xi_p^{p-1}) = \alpha(1 - \xi_p)$, com $\alpha \in \mathcal{O}_K$. Portanto $\text{Tr}(y(1 - \xi_p)) \in \mathcal{O}_K(1 - \xi_p)$. Pela observação 1.5.1 segue que $\text{Tr}(y(1 - \xi_p)) \in \mathbb{Z}$. Assim, $\text{Tr}(y(1 - \xi_p)) \in \mathbb{Z} \cap (1 - \xi_p)\mathcal{O}_K$. Ainda pela observação (2.2.1) temos que $\text{Tr}(y(1 - \xi_p)) \in p\mathbb{Z}$.

Teorema 2.2.1 ([13], pag. 74) (a) O anel dos inteiros algébricos de $K = \mathbb{Q}(\xi_p)$ é $\mathbb{Z}[\xi_p]$.

(b) O discriminante de $\mathbb{Q}(\xi_p)$, 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 $\mathbb{Q}(\xi_p)$, então é claro que $\mathbb{Z}[\xi_p] \subseteq \mathcal{O}_K$.

Seja $\alpha \in \mathcal{O}_K$. Então $\alpha \in \mathbb{Q}(\xi_p)$. Logo

$$\alpha = a_0 + a_1\xi_p + \dots + a_{p-2}\xi_p^{p-2},$$

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

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

Assim,

$$\text{Tr}(\alpha(1 - \xi_p)) = a_0\text{Tr}(1 - \xi_p) + a_1\text{Tr}(\xi_p - \xi_p^2) + \dots + a_{p-2}\text{Tr}(\xi_p^{p-2} - \xi_p^{p-1}),$$

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

$$a_0\text{Tr}(1 - \xi_p) = a_0p \in p\mathbb{Z},$$

donde segue que $a_0 \in \mathbb{Z}$. Analogamente mostramos que $a_i \in \mathbb{Z}$, para todo i . Portanto

$$\mathcal{O}_K = \mathbb{Z}[\xi_p].$$

(b) Vimos que uma base integral para $\mathbb{Q}(\xi_p)$ é $1, \xi_p, \dots, \xi_p^{p-2}$. Assim, pela Proposição

1.5.1 o discriminante é igual a

$$(-1)^{\frac{(p-1)(p-2)}{2}} N(\Phi'_p(\xi_p))$$

com $\Phi_p(X)$ como em 2.4. 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

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} \implies \Phi'_p(X) = \frac{(X - 1)pX^{p-1} - (X^p - 1)}{(X - 1)^2}.$$

Assim,

$$\Phi'_p(\xi_p) = \frac{(\xi_p - 1)p\xi_p^{p-1} - (\xi_p^p - 1)}{(\xi_p - 1)^2} = \frac{-(1 - \xi_p)p\xi_p^{p-1}}{(1 - \xi_p)^2} = \frac{-p\xi_p^{p-1}}{1 - \xi_p}.$$

Logo,

$$N(\Phi'_p(\xi_p)) = N\left(\frac{-p\xi_p^{p-1}}{1 - \xi_p}\right) = \frac{N(-p) \cdot N(\xi_p)^{p-1}}{N(1 - \xi_p)} = \frac{(-p)^{p-1}(1)^{p-1}}{p} = p^{p-2}.$$

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

Teorema 2.2.2 ([16], pag. 11) *Seja n um inteiro positivo. Então o anel dos inteiros algébricos de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$.*

Demonstração:

A demonstração será feita por indução sobre o número de divisores primos de n .

Consideremos dois casos.

Caso 1: Quando $n = p^a$, p um número primo. Sejam $L = \mathbb{Q}(\xi_{p^a})$, $m = \phi(p^a)$, $\alpha = a_0 + a_1(1 - \xi_{p^a}) + \dots + a_{m-1}(1 - \xi_{p^a})^{m-1} \in \mathcal{O}_L$, $a_i \in \mathbb{Q}$; $i = 0, \dots, m-1$ e $G = \text{Gal}(L|\mathbb{Q}) = \text{Aut}_{L|\mathbb{Q}} = \{\sigma_i, i = 1, \dots, p^a, (i, p) = 1\}$. Visto que $\sigma_i(\xi_{p^a}) = \xi_{p^a}^i$ e α é um inteiro algébrico, então

$$\alpha_i = \sigma_i(\alpha) = a_0 + a_1(1 - \xi_{p^a}^i) + \dots + a_{m-1}(1 - \xi_{p^a}^i)^{m-1}$$

é também um inteiro algébrico. Então sejam,

$$\alpha_{i_1} = \sigma_{i_1}(\alpha) = a_0 + a_1(1 - \xi_{p^a}^{i_1}) + \dots + a_{m-1}(1 - \xi_{p^a}^{i_1})^{m-1}$$

$$\alpha_{i_2} = \sigma_{i_2}(\alpha) = a_0 + a_1(1 - \xi_{p^a}^{i_2}) + \dots + a_{m-1}(1 - \xi_{p^a}^{i_2})^{m-1}$$

⋮

$$\alpha_{i_m} = \sigma_{i_m}(\alpha) = a_0 + a_1(1 - \xi_{p^a}^{i_m}) + \dots + a_{m-1}(1 - \xi_{p^a}^{i_m})^{m-1}$$

Colocando o sistema acima na forma matricial, temos:

$$\begin{pmatrix} \alpha_{i_1} \\ \alpha_{i_2} \\ \vdots \\ \alpha_{i_m} \end{pmatrix} = M \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix},$$

onde $M = ((1 - \xi_p^{a^i})^j)_{ij}$, $i = 1, \dots, p^a$ e $j = 1, \dots, m-1$; $(i, p) = 1$. Seja M_i a matriz obtida de M substituindo i -ésima coluna por

$$\begin{pmatrix} \alpha_{i_1} \\ \alpha_{i_2} \\ \vdots \\ \alpha_{i_m} \end{pmatrix}.$$

Pela Regra de Cramer $a_i = \frac{\det M_i}{\det M}$ e do fato de ξ_p^a e α_i 's serem inteiros algébricos, deduzimos que $\det M$ é um inteiro algébrico e $\det M_i$ também é inteiro algébrico. Por outro lado, sabemos que $\det M = \pm p^r$; para algum r . Assim $\pm p^r a_i = \det M_i \in \mathbb{Z}$, pois $\det M_i \in \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$, pelo Lema 1.3.4. Vimos que $\text{irr}(\xi_p^a, \mathbb{Q}) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \dots + X^{p^{a-1}} + 1$, logo $m = \phi(p^a) = p^{a-1}(p-1)$. Sejam $\mathfrak{p} = (1 - \xi_p^a)\mathcal{O}_L$, $0 \neq x \in \mathfrak{p}$ tal que $v_{\mathfrak{p}}(x) = \max\{t; x \in \mathfrak{p}^t\}$, logo $v_{\mathfrak{p}}(p) = p^{a-1}(p-1) = m$, pois

$$X^{p^{a-1}(p-1)} + \dots + X^{p^{a-1}} + 1 = \prod_{\substack{i=1 \\ (i,p)=1}}^{p^a-1} (X - \xi_p^{a^i})$$

assim para $X = 1$ temos

$$p = \prod_{\substack{i=1 \\ (i,p)=1}}^{p^a-1} (1 - \xi_p^{a^i}) = (1 - \xi_p^a)^n \cdot \epsilon$$

então

$$v_{\mathfrak{p}}(p) = v_{\mathfrak{p}}(1 - \xi_p^a)^n \cdot v_{\mathfrak{p}}(\epsilon) = m$$

Seja $s = \min\{t; p^t a_i \in \mathbb{Z}\}$. Então existe $i_0 \in \mathbb{N}$ tal que $p^s a_{i_0} \in \mathbb{Z} \setminus p\mathbb{Z}$. Assim,

$$p^s \alpha = p^s a_0 + p^s a_1(1 - \xi_{p^a}) + \dots + p^s a_{i_0}(1 - \xi_{p^a})^{i_0} + \dots + p^s a_{m-1}(1 - \xi_{p^a})^{m-1}.$$

Daí,

$$\begin{aligned} v_p(p^s \alpha) &= v_p(p^s a_0 + p^s a_1(1 - \xi_{p^a}) + \dots + p^s a_{i_0}(1 - \xi_{p^a})^{i_0} + \dots + p^s a_{m-1}(1 - \xi_{p^a})^{m-1}) \\ &= \min\{v_p(p^s a_0), \dots, v_p(p^s a_{i_0}(1 - \xi_{p^a})^{i_0}), \dots, v_p(p^s a_{m-1}(1 - \xi_{p^a})^{m-1})\} = i_0. \end{aligned}$$

Logo, $s \cdot m + v_p(\alpha) = i_0 < m$. Sendo $v_p(\alpha) \geq 0$, segue que $s = 0$. Portanto $a_i \in \mathbb{Z}$, para todo i e $\mathcal{O}_L = \mathbb{Z}[1 - \xi_{p^a}] = \mathbb{Z}[\xi_{p^a}]$.

Caso 2: Suponhamos que m tenha mais que um divisor primo, com $m = [\mathbb{Q}(\xi_n) : K]$, $\mathbb{Q}(\xi_n) = K[\xi_{q^b}]$ e $K = \mathbb{Q}(\xi_{p^a g})$, $n = p^a \cdot q^b \cdot g$; $p \nmid g$, $q \nmid g$. Por hipótese de indução temos que $\mathcal{O}_K = \mathbb{Z}[\xi_{p^a g}]$. Assim, dado $\alpha \in \mathcal{O}_{\mathbb{Q}(\xi_n)} \subset \mathbb{Q}(\xi_n)$,

$$\alpha = \sum_{i=0}^{\phi(n)-1} b_i \xi_n^i ; \quad b_i \in \mathbb{Q} \quad (2.10)$$

Sabemos que $\xi_n = \xi_{q^b}^i \cdot \xi_{\frac{n}{q^b}}^j$, pois $n = p^a \cdot q^b \cdot g$, com $(p^a g, q^b) = 1$, logo pela identidade de Bezout existem $i, j \in \mathbb{Z}$ tais que

$$i(p^a g) + jq^b = 1.$$

Assim, $\xi_n = \xi_{p^a g q^b}^{i(p^a g) + jq^b} = \xi_{q^b}^i \cdot \xi_{\frac{n}{q^b}}^j$. Daí, podemos reescrever a equação (2.10) da seguinte maneira:

$$\alpha = \sum_{i=0}^{\phi(q^b)-1} a_i \xi_{q^b}^i ; \quad a_i \in \mathbb{Q}(\xi_{\frac{n}{q^b}}).$$

De modo análogo ao caso 1, temos que $a_i = \frac{\det M_i}{\det M}$ onde $\det M_i$ e $\det M$ são inteiros algébricos. Sabemos que $\det M = \pm q^r$, logo $\pm q^r a_i = \det M_i \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$. Então para mostrarmos que os $b'_i s \in \mathbb{Z}$, é suficiente mostrarmos que $a'_i s \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$. Com efeito, como $\alpha \in \mathbb{Q}(\xi_n)$,

temos que existem $r, s \in \mathbb{N}$ tais que $p^r \alpha, q^s \alpha \in \mathbb{Z}[\xi_n]$ com $(p, q) = 1$. Assim, pela identidade de Bezout existem $u, v \in \mathbb{Z}$ tais que

$$up^r + vq^s = 1.$$

Daí

$$up^r \alpha + vq^s \alpha \in \mathbb{Z}[\xi_n].$$

Então

$$\alpha \cdot (up^r + vq^s) = \alpha \in \mathbb{Z}[\xi_n].$$

Portanto $a_i \in \mathbb{Z}[\xi_n]$. Logo o anel dos inteiros algébricos de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$. ■

Teorema 2.2.3 ([16], pag. 12) *O discriminante do corpo $K = \mathbb{Q}(\xi_n)$ é:*

$$D_K = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}.$$

Exemplo 2.2.2 *O discriminante de $\mathbb{Q}(\xi_{35})$ é $5^{18} \cdot 7^{20}$, a menos de sinal.*

2.3 Corpos de Números Abelianos

Um corpo de números K é denominado abeliano se, K é uma extensão galoisiana dos racionais e seu grupo de Galois é abeliano. Os nossos estudos são limitados aos Corpos de Números Abelianos pois, ele nos oferece um ambiente de trabalho com mais opções de ferramentas e os reticulados construídos nestes corpos coincidem com os reticulados mais densos conhecidos e até assumem novos recordes.

Da Teoria de Galois temos que se um corpo de números K está contido num corpo ciclotômico então K é um corpo abeliano. A recíproca dessa afirmação é o Teorema de Kronecker-Weber, enunciado abaixo, o qual é fundamental para a escolha de nossos ambientes de trabalho.

Teorema 2.3.1 ([16], pag. 319) *Se $K \mid \mathbb{Q}$ é uma extensão finita abeliana, então $K \subseteq \mathbb{Q}(\xi_n)$, para algum $n \in \mathbb{N}$.*

Vimos que o cálculo do discriminante utiliza a base integral, porém existem resultados que fazem este cálculo sem o uso da base integral. Enunciaremos a seguir um deles, o qual é consequência da fórmula do Condutor-Discriminante.

Os dois resultados seguintes (Teoremas 2.3.2 e 2.3.3) são fortemente utilizados nas aplicações desenvolvidas nas seções "Subcorpos de $\mathbb{Q}(\xi_{p^r})$ " e "Subcorpos de $\mathbb{Q}(\xi_{pq})$ " do próximo capítulo, respectivamente.

Teorema 2.3.2 ([9], pag. 64) *Sejam p um número primo ímpar, r um inteiro positivo e $K \subseteq \mathbb{Q}(\xi_{p^r})$, $[K : \mathbb{Q}] = up^j$, p não divide u . Então,*

$$D_K = \pm p^v$$

onde

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

Teorema 2.3.3 ([15], pag. 57) *Sejam $K \subset \mathbb{Q}(\xi_p)$, p primo, $r = [\mathbb{Q}(\xi_p) : K]$, $s = [K : \mathbb{Q}]$, $\theta = \text{Tr}_{\mathbb{Q}(\xi_p)|K}(\xi_p)$ e $g \in \mathbb{Z}$ tal que σ_g gera $G = \text{Gal}(\mathbb{Q}(\xi_p) : \mathbb{Q})$. Então $K = \mathbb{Q}(\theta)$ e $\mathbb{Z}\sigma_g(\theta) + \dots + \mathbb{Z}\sigma_{g^{r-1}}(\theta)$ é o anel dos inteiros algébricos de K . Além disso,*

$$D_K = \pm p^{[K:\mathbb{Q}]-1}.$$

Demonstração:

Mostremos que $K = \mathbb{Q}(\theta)$. De fato, como $\theta \in K$, segue que $\mathbb{Q}(\theta) \subset K$. Seja $G' = \text{Gal}(\mathbb{Q}(\xi_p) : K)$, por hipótese $G = \text{Gal}(\mathbb{Q}(\xi_p) : \mathbb{Q}) = \langle \sigma_g \rangle$ é cíclico então

$G' = \{\sigma_{g^s}, \sigma_{g^{2s}}, \dots, \sigma_{g^{rs}}\}$ e $\theta = \xi_p^{g^s} + \dots + \xi_p^{g^{rs}}$, daí temos que $\sigma_g(\theta), \dots, \sigma_{g^s}(\theta) \in \mathbb{Q}(\theta)$, pois $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão galoisiana. Sejam $a_1, \dots, a_s \in \mathbb{Q}$ tais que

$$a_1 \sigma_g(\theta) + \dots + a_s \sigma_{g^s}(\theta) = 0 \quad (2.11)$$

Sendo que

$$\sigma_{g^i}(\theta) = \sigma_{g^i}(\xi_p^{g^s}) + \dots + \sigma_{g^i}(\xi_p^{g^{rs}}) = \xi_p^{g^{s+i}} + \dots + \xi_p^{g^{rs+i}}$$

se $\xi_p^{g^{t_1s+i_1}} = \xi_p^{g^{t_2s+i_2}}$, com $1 \leq t_1, t_2 \leq r$ e $1 \leq i_1, i_2 \leq s$, teremos: $g^{t_1s+i_1} = g^{t_2s+i_2} \pmod{p}$, isto é, $g^{t_1s+i_1} - g^{t_2s+i_2} = pv$ supondo $t_1s+i_1 < t_2s+i_2$, temos:

$$g^{t_1s+i_1}(1 - g^{(t_2-t_1)s+(i_2-i_1)}) = pv.$$

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

$$g^{(t_2-t_1)s+(i_2-i_1)} \equiv 1 \pmod{p}, \text{ ou seja, } p-1 \mid g^{(t_2-t_1)s+(i_2-i_1)},$$

daí $(t_2 - t_1)s + (i_2 - i_1) = rsu$; como $1 - s \leq i_2 - i_1 \leq s - 1$, segue que $i_2 = i_1$ (isto é, $i_2 - i_1 = 0$). Analogamente, temos que $t_2 = t_1$. Assim temos

$$a_1(\xi_p^{g^{s+1}} + \dots + \xi_p^{g^{rs+1}}) + \dots + a_s(\xi_p^{g^{2s}} + \dots + \xi_p^{g^{rs+s}}) = 0$$

Como $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p-1$ e todos os $\xi_p^{g^{ts+i}}$ são distintos dois a dois, temos que ξ_p^i , $i = 1, \dots, p-1$ são todos distintos. Deste modo podemos reescrever a equação (2.11) da seguinte maneira

$$b_1 \xi_1 + \dots + b_{p-1} \xi_{p-1} = 0,$$

onde

$$\{b_i; i = 1, \dots, p-1\} = \{a_i; i = 1, \dots, s\}.$$

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

Como $\mathbb{Q}(\theta) \subset K$ e $[K : \mathbb{Q}] = s$ temos que $[\mathbb{Q}(\theta) : \mathbb{Q}] = s$ e $K = \mathbb{Q}(\theta)$. Agora mostremos que

$$\mathbb{Z}\sigma_g(\theta) + \dots + \mathbb{Z}\sigma_{g^s}(\theta) = \mathcal{O}_K.$$

É claro que $\mathbb{Z}\sigma_g(\theta) + \dots + \mathbb{Z}\sigma_{g^s}(\theta) \subset \mathcal{O}_K$, uma vez que $\sigma_{g^i}(\theta) \in \mathbb{Z}[\xi_p] \cap K$. Falta-nos provar a inclusão contrária. Assim, tomemos $\alpha \in \mathcal{O}_K$, então existem $a_1, \dots, a_s \in \mathbb{Q}$ tais que $\alpha = \sum_{i=1}^s a_i \sigma_{g^i}(\theta)$, uma vez que $\{\sigma_g(\theta), \dots, \sigma_{g^s}(\theta)\}$ é base de $K/\mathbb{Q}$. Então como $\alpha \in \mathbb{Z}[\xi_p]$, temos que

$$\alpha = \sum_{i=1}^s a_i \sigma_{g^i}(\theta) = \sum_{i=1}^s a_i \xi_p^{g^s+i}$$

pode ser expresso por

$$\alpha = \sum_{i=1}^{p-1} b_i \xi_p^i, \quad b_i \in \mathbb{Z}, \quad i = 1, \dots, p-1$$

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

O valor do discriminante decorre do Teorema 2.3.2. ■

Decomposição de ideais em uma extensão galoisiana

Veremos agora, como fatorar um ideal primo de um anel dos inteiros algébricos numa extensão de corpos galoisiana.

Teorema 2.3.4 (Da Evidência) ([7], pag. 70) *Dados L/K uma extensão galoisiana com grupo de Galois G e, $\mathfrak{q}$ e $\mathfrak{q}'$ dois ideais primos de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{q}' \cap \mathcal{O}_K$. Então existe $\sigma \in G$, tal que $\sigma(\mathfrak{q}) = \mathfrak{q}'$.*

Demonstração:

Suponhamos $\sigma(\mathfrak{q}) \neq \mathfrak{q}', \forall \sigma \in G$. Então pelo Teorema Chinês do Resto, existe uma

solução para o sistema de congruências

$$X \equiv 0 \pmod{q'}$$

$$X \equiv 1 \pmod{\sigma(q)}, \quad \forall \sigma \in G.$$

Seja $\alpha \in \mathcal{O}_L$ a tal solução, assim temos que

$$N_{L/K}(\alpha) \in \mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$$

onde um dos fatores de $N_{L/K}(\alpha)$ é $\alpha \in \mathfrak{q}'$. Por outro lado, temos que $\alpha \notin \sigma(\mathfrak{q}), \forall \sigma \in G$, então $\sigma^{-1}(\alpha) \notin \mathfrak{q}$. Podemos expressar $N_{L/K}(\alpha)$ como um produto de todos os $\sigma^{-1}(\alpha)$, e visto que nenhum destes são ideais primos de $\mathfrak{q}$, isto nos mostra que $N_{L/K}(\alpha) \notin \mathfrak{q}$. Absurdo, pois vimos que $N_{L/K}(\alpha) \in \mathfrak{p} \subset \mathfrak{q}$. Portanto $\sigma(\mathfrak{q}) = \mathfrak{q}'$. ■

Corolário 2.3.1 ([7], pag. 71) *Sejam L galoisiana sobre 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 $f(\mathfrak{q} | \mathfrak{p}) = f(\mathfrak{q}' | \mathfrak{p})$.*

Demonstração:

Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$, então pelo Lema de Kummer segue que $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \dots \mathfrak{q}_s^{e_s}$. Do Teorema da Evidência, temos que $\sigma(\mathfrak{q}) = \mathfrak{q}'$, deste modo, suponha-
mos que $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Assim,

$$\sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \dots \mathfrak{q}_s^{e_s}) = \sigma(\mathfrak{q}_1)^{e_1} \sigma(\mathfrak{q}_2)^{e_2} \dots \sigma(\mathfrak{q}_s)^{e_s} = \mathfrak{q}_2^{e_1} \sigma(\mathfrak{q}_2)^{e_2} \dots \sigma(\mathfrak{q}_s)^{e_s} = \mathfrak{p}\mathcal{O}_L.$$

Logo $\mathfrak{q}_2^{e_1} = \mathfrak{q}_2^{e_2} \Leftrightarrow e_1 = e_2$, portanto $e(\mathfrak{q} | \mathfrak{p}) = e(\mathfrak{q}' | \mathfrak{p})$.

Sejam

$$\left[\frac{\mathcal{O}_L}{\mathfrak{q}_1} : \frac{\mathcal{O}_K}{\mathfrak{p}} \right] = f_1 \quad e \quad \left[\frac{\mathcal{O}_L}{\mathfrak{q}_2} : \frac{\mathcal{O}_K}{\mathfrak{p}} \right] = f_2.$$

Defina

$$\tilde{\sigma} : \frac{\mathcal{O}_L}{\mathfrak{q}_1} \rightarrow \frac{\mathcal{O}_L}{\mathfrak{q}_2}$$

$$x + \mathfrak{q}_1 \mapsto \tilde{\sigma}(x + \mathfrak{q}_1) = \sigma(x) + \mathfrak{q}_2$$

Temos que $\tilde{\sigma}$ é um isomorfismo, logo

$$\left[\frac{\mathcal{O}_L}{q_1} : \frac{\mathcal{O}_K}{p} \right] = \left[\frac{\mathcal{O}_L}{q_2} : \frac{\mathcal{O}_K}{p} \right]$$

donde segue que $f_1 = f_2$. ■

O corolário acima mostra que no caso de uma extensão galoisiana, um ideal primo p de $\mathcal{O}_K$ fatora-se em $(q_1 \dots q_g)^e$ em $\mathcal{O}_L$, onde os q_i 's são os ideais primos distintos acima de p , todos tendo o mesmo grau residual f sobre p . E mais, pelo Teorema da Igualdade Fundamental, $n = [L : K] = g.e.f$.

Exemplo 2.3.1 Seja $K = \mathbb{Q}(\xi_{55})$, segue do Teorema 2.2.2, que o anel dos inteiros algébricos de K é $\mathbb{Z}[\xi_{55}]$. O polinômio minimal de ξ_{55} sobre $\mathbb{Q}$ é dado por

$$\Phi_{55}(X) = X^{40} - X^{39} + X^{35} - X^{34} + X^{30} - X^{28} + \dots + X^{15} - X^{12} + X^{10} - X^6 + X^5 - X + 1.$$

A decomposição do ideal $5\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ satisfaz

$$\Phi_{55}(X) \equiv (p_1(X))^4 \cdot (p_2(X))^4 \pmod{5\mathbb{Z}[X]}$$

onde

$$p_1(X) = X^5 + 4X^4 + 4X^3 + X^2 + 3X + 4 \quad e \quad p_2(X) = X^5 + 2X^4 + 4X^3 + X^2 + X + 4$$

Assim, pelo lema de Kummer temos:

(a) $p_i = \langle 5, p_i(\xi_{55}) \rangle$; $i = 1, 2$ são os ideais primos de $\mathcal{O}_K$ acima de $5\mathbb{Z}$,

(b) $5\mathcal{O}_K = p_1^4 \cdot p_2^4$,

(c) $\left[\frac{\mathcal{O}_K}{p_1} : \frac{\mathbb{Z}}{5\mathbb{Z}} \right] = \left[\frac{\mathcal{O}_K}{p_2} : \frac{\mathbb{Z}}{5\mathbb{Z}} \right] = 5$

Assim temos $g = 2, e = 4, f = 5$ e $40 = g.e.f = 2.4.5$.

Sejam K_1 e K_2 corpos linearmente disjuntos (isto é, $K_1 \cap K_2 = \mathbb{Q}$). Dado um número primo p por ([7], pag. 98) a decomposição do ideal $p\mathcal{O}_{K_1K_2}$ em K_1K_2 pode ser obtida através da decomposição em K_1 e em K_2 do seguinte modo: Sejam g_j, e_j e f_j os parâmetros relativos a decomposição de $p\mathcal{O}_{K_j}$ em K_j ; $j = 1, 2$. Em K_1K_2 estes parâmetros satisfazem a condição:

$$g = g_1g_2, e = e_1e_2 \quad e \quad f = f_1f_2.$$

Cada ideal primo de $\mathcal{O}_{K_1}$ acima de p se estende em $\mathcal{O}_{K_1K_2}$ de modo análogo à que p se estende em $\mathcal{O}_{K_2}$.

Seja L uma extensão galoisiana de K com grupo de Galois $G = \text{Gal}(L/K)$. Para cada ideal primo $\mathfrak{q}$ acima de $p \subseteq \mathcal{O}_K$ definimos dois subgrupos:

O grupo de decomposição

$$D = D(\mathfrak{q} \mid p) = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

e o grupo inercial

$$E = E(\mathfrak{q} \mid p) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}, \forall \alpha \in \mathcal{O}_L\}.$$

Ambos são subgrupos de G e $E \subset D$, pois para $x \in \mathfrak{q}$ temos $x \equiv 0 \pmod{\mathfrak{q}}$, assim $\sigma(x) \equiv x \pmod{\mathfrak{q}}$ então $\sigma(x) \equiv 0 \pmod{\mathfrak{q}}$, como $\mathfrak{q}$ é maximal, segue que $\sigma(\mathfrak{q}) = \mathfrak{q}$.

Dados $\mathfrak{q}$ e $\mathfrak{q}'$ dois ideais primos acima do ideal primo p , temos que

$$D(\mathfrak{q} \mid p) = \sigma D(\mathfrak{q}' \mid p) \sigma^{-1}.$$

Logo, se $D \triangleleft G$, para algum $\mathfrak{q}$ então

$$D(\mathfrak{q} \mid p) = D(p).$$

Em particular, quando G é um grupo abeliano, $D(\mathfrak{p}_i)$ depende somente de p , assim denotaremos apenas por $D(p)$. Como g denota o número de conjugados de $\mathfrak{q}$, então

$$\# G = g \cdot \# D(\mathfrak{p})$$

e, portanto

$$\# D(\mathfrak{p}) = \frac{n}{g} = e.f.$$

Os elementos de D induzem um automorfismo do corpo $\frac{\mathcal{O}_L}{\mathfrak{q}}$ de modo natural: Para todo $\sigma \in G$ restrito a um automorfismo de $\mathcal{O}_L$ e se $\sigma \in D$ então a aplicação induzida $\mathcal{O}_L \rightarrow \frac{\mathcal{O}_L}{\mathfrak{q}}$ tem núcleo $\mathfrak{q}$, logo cada $\sigma \in D$ induz um automorfismo $\tilde{\sigma}$ de $\frac{\mathcal{O}_L}{\mathfrak{q}}$, de tal modo que o diagrama a seguir comuta:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \pi \downarrow & & \downarrow \pi \\ \frac{\mathcal{O}_L}{\mathfrak{q}} & \xrightarrow{\tilde{\sigma}} & \frac{\mathcal{O}_L}{\mathfrak{q}} \end{array}$$

E mais, $\tilde{\sigma}$ fixa o subcorpo $\frac{\mathcal{O}_K}{\mathfrak{p}}$ ponto a ponto, pois σ fixa K . Logo fixa $\mathcal{O}_K$, ponto a ponto. Então $\tilde{\sigma}$ é um elemento do grupo de Galois $\tilde{G}$ de $\frac{\mathcal{O}_L}{\mathfrak{q}}$ sobre $\frac{\mathcal{O}_K}{\mathfrak{p}}$. Resumindo, temos um homomorfismo de grupos $\psi : D \rightarrow \tilde{G}$. Logo $\text{Ker} \psi = E$, assim E é um subgrupo normal de D e o grupo quociente $\frac{D}{E}$ é imerso em $\tilde{G}$. Temos que $\psi : D \rightarrow \tilde{G}$ é sobrejetiva, assim $\frac{D}{E} \rightarrow \tilde{G}$ é de fato um isomorfismo de grupos. Sabemos de $\tilde{G}$ é cíclico de ordem f , assim o mesmo é válido para $\frac{D}{E}$.

Sejam L_D e L_E corpos fixados por D e E respectivamente. L_D é dito corpo de decomposição e L_E corpo inercial.

Exemplo 2.3.2 $L = \mathbb{Q}(\xi_{15})$, $\mathcal{O}_L = \mathbb{Z}(\xi_{15})$ e

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^2 - X + 1.$$

o polinômio minimal de ξ_{15} sobre $\mathbb{Q}$. A decomposição do ideal $7\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$ satisfaz:

$$\Phi_{15}(X) \equiv (p_1(X)) \cdot (p_2(X)) \pmod{7\mathbb{Z}}$$

onde

$$p_1(X) = X^4 + 4X^3 + 2X^2 + X + 4, \quad p_2(X) = X^4 + 2X^3 + 4X^2 + X + 2$$

e do Lema de Kummer, segue que

(a) $\mathfrak{p}_i = \langle 7, p_i(\xi_{15}) \rangle$; $i = 1, 2$ são os ideais primos de $\mathcal{O}_L$ acima de $7\mathbb{Z}$,

(b) $7\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$

(c) $[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{7\mathbb{Z}}] = 4$; $i = 1, 2$.

Assim, temos $g = 2, e_1 = e_2 = 1, f_1 = f_2 = 4$. O grupo dos $\mathbb{Q}$ -automorfismos de K sobre $\mathbb{Q}$ é dado por

$$G = \{\sigma_i; (i, 15) = 1, i = 1, \dots, 15; \sigma_i(\xi_{15}) = \xi_{15}^i\}$$

e verificamos que $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são conjugados, por exemplo $\sigma_2(\mathfrak{p}_1) = \mathfrak{p}_2$ e $\sigma_7(\mathfrak{p}_2) = \mathfrak{p}_1$. Logo $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são ideais primos conjugados que têm o mesmo índice de ramificação ($e = 1$) e o mesmo grau residual ($f = 4$.)

O grupo de decomposição $D(7\mathbb{Z})$ é dado por

$$D(7\mathbb{Z}) = \{\sigma \in G / \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\},$$

Da mesma forma o grupo de inércia é

$$E(7\mathbb{Z}) = \{\sigma \in G / \sigma(x) = x \pmod{\mathfrak{p}_1}, x \in \mathcal{O}_K\} = \{\sigma \in D / \sigma(\xi_{15}) \equiv \xi_{15} \pmod{\mathfrak{p}_1}\}.$$

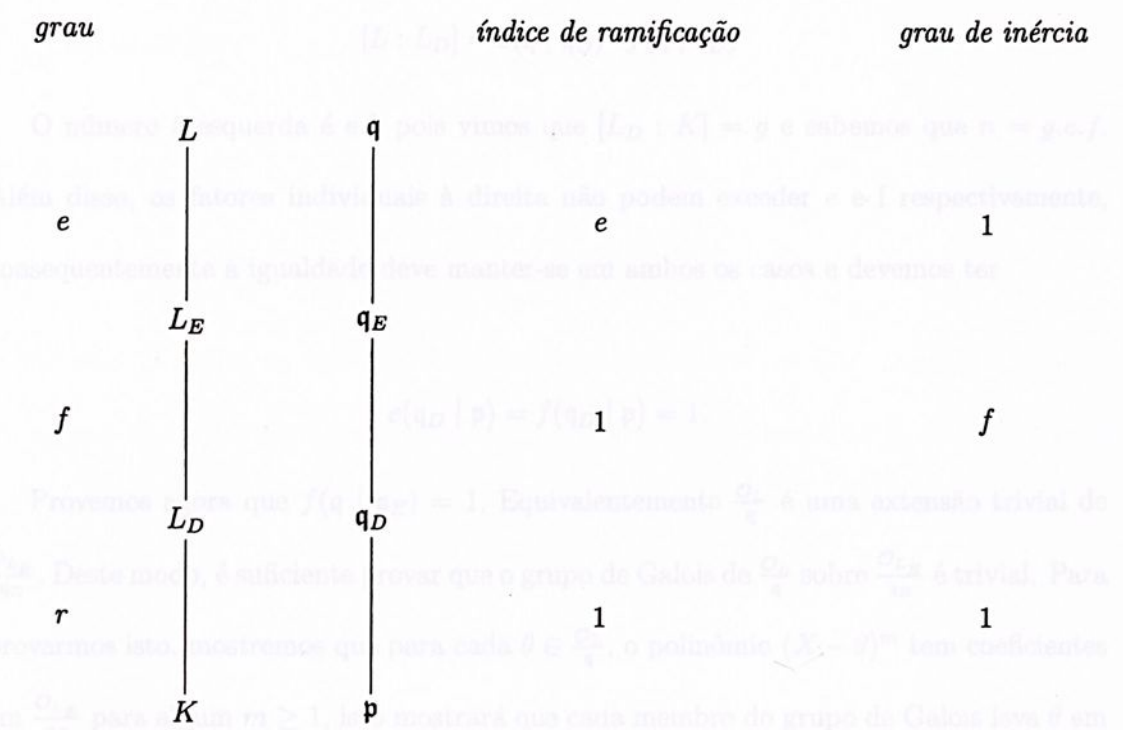
Como

$$\# E(7\mathbb{Z}) = 4 \quad \text{e} \quad E(7\mathbb{Z}) \subset D(7\mathbb{Z}),$$

temos

$E(7\mathbb{Z}) = D(7\mathbb{Z}).$

Teorema 2.3.5 ([7], pag. 100) *Sejam $L, K, \mathcal{O}_K, \mathcal{O}_L, \mathfrak{p}, \mathfrak{q}, G, D, E, e, f$ e g como acima. Então temos o seguinte diagrama:*



Demonstração:

Inicialmente mostremos que $[L_D : K] = g$. Do Teorema da Correspondência de Galois segue que $[L_D : K]$ é igual ao índice de D em G . Cada classe lateral à esquerda σD ($\sigma \in G$) leva $\mathfrak{q}$ em $\sigma \mathfrak{q}$ (isto é, cada elemento da classe lateral pertence à $\mathfrak{q}$), e é claro que $\sigma D = \tau D$ se $\sigma \mathfrak{q} = \tau \mathfrak{q}$. Estas estabelecem uma relação biunívoca entre as classes laterais à esquerda σD e os ideais primos $\sigma \mathfrak{q}$, pelo Teorema da Evidência , estes primos incluem todos os primos de $\mathcal{O}_L$ acima de $\mathfrak{p}$, portanto existem g deles.

Agora mostremos que $e(q_D | p)$ e $f(q_D | p)$ são ambos iguais a 1. Notemos que q é o único ideal primo de $\mathcal{O}_L$ acima de q_D , uma vez que todos os ideais primos serão necessariamente permutados transitivamente pelo Grupo de Galois de L sobre L_D (L é automaticamente uma extensão normal de L_D); este grupo de Galois é D , o qual não leva q a nenhum outro. Do Teorema da Igualdade Fundamental vem que:

$$[L : L_D] = e(q | q_D) \cdot f(q | q_D)$$

O número à esquerda é $e \cdot f$, pois vimos que $[L_D : K] = g$ e sabemos que $n = g \cdot e \cdot f$. Além disso, os fatores individuais à direita não podem exceder e e f respectivamente, consequentemente a igualdade deve manter-se em ambos os casos e devemos ter

$$e(q_D | p) = f(q_D | p) = 1.$$

Provemos agora que $f(q | q_E) = 1$. Equivalentemente $\frac{\mathcal{O}_L}{q}$ é uma extensão trivial de $\frac{\mathcal{O}_{L_E}}{q_E}$. Deste modo, é suficiente provar que o grupo de Galois de $\frac{\mathcal{O}_L}{q}$ sobre $\frac{\mathcal{O}_{L_E}}{q_E}$ é trivial. Para provarmos isto, mostremos que para cada $\theta \in \frac{\mathcal{O}_L}{q}$, o polinômio $(X - \theta)^m$ tem coeficientes em $\frac{\mathcal{O}_{L_E}}{q_E}$ para algum $m \geq 1$, isto mostrará que cada membro do grupo de Galois leva θ em uma raiz de $(X - \theta)^m$, a qual só pode ser θ . O que provará o que queremos.

Fixe $\alpha \in \mathcal{O}_L$ o correspondente a $\theta \in \frac{\mathcal{O}_L}{q}$, claramente o polinômio

$$g(X) = \prod_{\sigma \in E} (X - \sigma(\alpha))$$

tem coeficientes em $\mathcal{O}_{L_E}$, reduzindo os coeficientes ($\text{mod } q$), nós teremos que

$$\bar{g} \in \left(\frac{\mathcal{O}_L}{q} \right) [X]$$

realmente tem coeficientes em $\frac{\mathcal{O}_{L_E}}{\mathfrak{q}_E}$. Mas todo $\sigma(\alpha)$ é reduzido a $\theta \pmod{\mathfrak{q}}$, pois

$$\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$$

e $\sigma(\alpha) = \theta$; então

$$\bar{g}(X) = (X - \theta)^m,$$

onde $m = \#(E)$, daí segue o resultado.

Juntamente com

$$f(\mathfrak{q}_D | \mathfrak{p}) = 1,$$

isto mostra que

$$f(\mathfrak{q}_E | \mathfrak{q}_D) = f(\mathfrak{q} | \mathfrak{p}) = f.$$

Então pelo Teorema da Igualdade Fundamental nós temos que $[L_E : L_D] \geq f$. Mas já vimos que E é um subgrupo normal de D e que o grupo quociente $\frac{D}{E} \subset \tilde{G}$, o qual é um grupo de ordem f . Assim, $[L_E : L_D] = \#(\frac{D}{E}) \leq f$, portanto exatamente f . Logo $e(\mathfrak{q}_E | \mathfrak{q}_D) = 1$. Finalmente obtemos facilmente $[L : L_E] = e$ e $e(\mathfrak{q} | \mathfrak{q}_E) = e$, considerando o grau e o índice de ramificação já estabelecidos. ■

O teorema a seguir estabelece certas condições maximais e minimais para o corpo de decomposição, considerando agora K' o corpo fixado por um subgrupo $H \subset G$. E mais, seu anel dos inteiros algébricos é $\mathcal{O}_{K'} = B \cap K'$ e $\mathfrak{p}' = \mathfrak{q} \cap \mathcal{O}_{K'}$ é o único ideal primo abaixo de $\mathfrak{q}$.

Teorema 2.3.6 ([7], pag. 104) *Com as notações acima, temos:*

(a) L_D é o maior corpo intermediário de K' contendo K tal que $e(\mathfrak{p}' | \mathfrak{p}) = f(\mathfrak{p}' | \mathfrak{p}) = 1$;



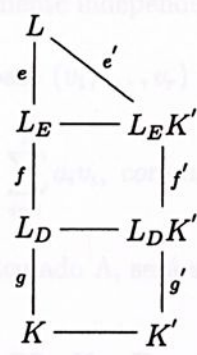
- (b) L_D é o menor subcorpo K' , tal que $\mathfrak{q}$ é o único ideal primo de $\mathcal{O}_L$ acima de $\mathfrak{p}$;
- (c) L_E é o maior subcorpo K' , tal que $e(\mathfrak{p}' | \mathfrak{p}) = 1$;
- (d) L_E é o menor subcorpo K' , tal que $\mathfrak{q}$ é totalmente ramificado sobre $\mathfrak{p}'$, (isto é, $e(\mathfrak{q} | \mathfrak{p}') = [L : K']$).

Demonstração:

Primeiro observe que nós já mostramos que L_D e L_E tem estas propriedades: por exemplo, nós vimos na demonstração do Teorema 2.3.5 que $\mathfrak{q}$ é o único ideal primo de $\mathcal{O}_L$ acima de $\mathfrak{q}_D$; esta também poderia ser obtida do fato de que

$$e(\mathfrak{q} | \mathfrak{q}_D) = f(\mathfrak{q} | \mathfrak{q}_D) = e.f = [L : L_D].$$

Suponha agora que $K' = L_H$ é um corpo intermediário para o qual $\mathfrak{q}$ é o único ideal primo acima de $\mathfrak{p}'$. Nós sabemos que todo $\sigma \in H$ leva $\mathfrak{q}$ em outro ideal primo acima de $\mathfrak{p}'$, deste modo nós devemos ter $H \subset D$. Isto implica $L_D \subset K'$, estabelecendo (b). Este resultado, também poderia ser obtido considerando o diagrama abaixo,



no qual o grau indicado foi obtido pela aplicação do Teorema 2.3.5 em ambas as situações ($\mathfrak{q}$ sobre $\mathfrak{p}$ e $\mathfrak{q}$ sobre $\mathfrak{p}'$). Aqui e', f' e g' são números associados à fatoração de $\mathfrak{p}'$ na extensão normal L .

Portanto g' é o número de ideais primos acima de p' . O diagrama mostra que se $g' = 1$, então $K' = L_D K'$, logo $L_D \subset K'$.

Agora assumamos que $e(p' | p) = f(p' | p) = 1$. Assim, $e = e'$ e $f = f'$ pela multiplicidade nas extensões. Considerando o diagrama nós vimos que L_D e $L_D K'$ ambos tem o mesmo índice em L . Visto que um contém o outro, eles podem ser iguais, implicando $K' \subset L_D$. Portanto nós obtemos (a).

(c) é análogo: se $e(p' | p) = 1$, então $e' = e$ logo $L_E = L_E K'$, portanto $K' \subset L_E$.

Finalmente, se q é totalmente ramificado sobre p' então $[L : K'] = e'$. Considerando o diagrama nós temos que $K' = L_E K'$, logo $L_E \subset K'$. ■

Exemplo 2.3.3 Como vimos no exemplo (2.3.2), $e = 1$, $f = 4$ e $g = 2$. Pelo Teorema 2.3.6 segue que $L_D = \mathbb{Q}(\xi_3) \subset \mathbb{Q}(\xi_{15})$ e $e(q_D | p) = f(q_D | p) = 1$.

2.4 Reticulados

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

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

Doravante quando citarmos um reticulado Λ , será suposto que

$$V = \mathbb{R}^n, K = \mathbb{R} \text{ e } A = \mathbb{Z}.$$

À disposição de esferas de mesmo raio no espaço euclidiano $\mathbb{R}^n$ de tal modo que a intersecção de duas delas tenha no máximo um ponto damos o nome de empacotamento esférico. A forma de dispor essas esferas de modo a cobrir a maior proporção do espaço

sempre foi um desafio e mereceu citação de Hilbert, que em 1.900 colocou-o na lista de problemas em aberto mais relevantes do século.

Um empacotamento reticulado é um empacotamento em que o conjunto de centros formam um reticulado Λ de $\mathbb{R}^n$ e, a menos que se diga ao contrário, a partir de agora todos os empacotamentos considerados serão reticulados, e quando o conjunto de centros for Λ , dizemos que o empacotamento é associado a Λ . Definimos a densidade de um dado empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas.

A seguir, introduziremos os elementos básicos que possibilitarão obter uma expressão para a densidade de empacotamento.

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

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

é dito a Região Fundamental de Λ associada a base β . Observamos que a Região Fundamental depende da escolha da base do reticulado.

Fazendo

$$v_i = (v_{i1}, \dots, v_{in}) \in \mathbb{R}^n, i = 1, \dots, n$$

o volume de R_β , $v(R_\beta)$ é o módulo do determinante da matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \dots & v_{nn} \end{pmatrix}$$

a qual é denominada matriz geradora para o reticulado Λ .

O volume da Região Fundamental, R_β , independe da base, pois a matriz mudança de base é invertível, com entradas inteiras, ou seja, tem determinante ± 1 . Deste modo, faz

sentido definir o volume de Λ como sendo o volume da Região Fundamental, e denotaremos por $v(\Lambda)$.

Temos interesse pelos empacotamento associado ao reticulado Λ tal que as esferas tenham raio máximo. Para determinação deste raio, observemos que fixado $a > 0$, a intersecção do conjunto compacto

$$\{x \in \mathbb{R}^n; |x| \leq a\}$$

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.

Notemos que $\rho = \frac{\Lambda_{\min}}{2}$ 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.

Ao mencionarmos densidade de empacotamento com esfera de raio ρ associado a um reticulado, estamos citando a densidade de um reticulado Λ , a qual denotaremos por $\Delta(\Lambda)$ e expressamos por

$$\Delta(\Lambda) = \frac{\text{volume de uma esfera de raio } \rho}{\text{volume do reticulado}}.$$

O volume de uma esfera n -dimensional de raio ρ é

$$v(B(\rho)) = v(B(1)) \cdot \rho^n$$

onde $v(B(1))$ é o volume de uma esfera de raio 1. Deste modo, a densidade de um empacotamento reticulado Λ é dada por

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



A densidade de centro é outro parâmetro importante, cuja expressão é:

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

Exemplo 2.4.1 Seja Λ um reticulado hexagonal gerado pelos vetores $(1, 0)$ e $(\frac{-1}{2}, \frac{\sqrt{3}}{2})$, assim $\rho = \frac{1}{2}$ e $\delta(\Lambda) = \frac{1}{\sqrt{12}} \cong 0,2887$

Exemplo 2.4.2 Seja $\Lambda = \mathbb{Z}^n$ um reticulado do $\mathbb{R}^n$ gerado pela base $\beta = \{e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)\}$. A forma quadrática $|v|^2 = x_1^2 + \dots + x_n^2$ assume o valor mínimo 1 quando um dos $x_i = 1$ para $i = 1, \dots, n$ e os demais nulos, logo $\rho = \frac{1}{2}$. Como $v(\Lambda) = |\det M| = 1$, então $\delta = \frac{1}{2^n}$.

2.5 O Homomorfismo Canônico

Definimos nesta seção o homomorfismo canônico de um corpo de números K , o qual é usado para descrever reticulados de posto n em $\mathbb{R}^n$, originados de um ideal ordinário não nulo do anel dos inteiros algébricos de K .

Sejam K um corpo de números de grau n e

$$\sigma_i : K \longrightarrow \mathbb{C}, \quad i = 1, \dots, n$$

os monomorfismos de K em $\mathbb{C}$. Se $\sigma_i(K) \subseteq \mathbb{R}$ dizemos que σ_i é real, caso contrário σ_i é imaginário. Um corpo K é dito totalmente real quando todos seus monomorfismos são reais, e K é dito totalmente imaginário quando todos seus monomorfismos são imaginários.

Agora definiremos o homomorfismo canônico para o caso geral: Dados K um corpo de números de grau n , r_1 a quantidade de monomorfismos reais e $2r_2$ a quantidade de monomorfismos imaginários. Podemos ordenar os monomorfismos $\sigma_1, \dots, \sigma_n$ do seguinte

modo

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$$

onde $\sigma_1, \dots, \sigma_{r_1}$ são os monomorfismos reais e os demais imaginários. Assim definimos o homomorfismo canônico

$$\sigma_K : K \longrightarrow \mathbb{R}^n$$

por

$$\sigma_K(\alpha) = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \operatorname{Re}\sigma_{r_1+1}(\alpha), \operatorname{Im}\sigma_{r_1+1}(\alpha), \dots, \operatorname{Re}\sigma_{r_1+r_2}(\alpha), \operatorname{Im}\sigma_{r_1+r_2}(\alpha)),$$

onde $\operatorname{Re}(z)$ e $\operatorname{Im}(z)$ representam as partes real e imaginária do número complexo z , respectivamente.

Exemplo 2.5.1 Sejam $K = \mathbb{Q}(\sqrt{-3})$ com $\mathbb{Q}$ -base $\{1, \frac{1+\sqrt{-3}}{2}\}$ e os monomorfismos de K em $\mathbb{C}$, σ_1 e σ_2 que são respectivamente a inclusão e a conjugação complexa, onde

$$\sigma_2\left(a + b\left(\frac{1+\sqrt{-3}}{2}\right)\right) = a + b\left(\frac{1-\sqrt{-3}}{2}\right); \quad a, b \in \mathbb{Q}.$$

Então para

$$x = a + b\left(\frac{1+\sqrt{-3}}{2}\right) \in K, \quad a, b \in \mathbb{Q}$$

temos

$$\sigma(x) = (\sigma_1(x), \sigma_2(x)) = \left(a + b\left(\frac{1+\sqrt{-3}}{2}\right), a + b\left(\frac{1-\sqrt{-3}}{2}\right)\right)$$

Exemplo 2.5.2 Sejam $K = \mathbb{Q}(\alpha)$ onde $\alpha \in \mathbb{R}$ satisfaz $\alpha^4 - 2 = 0$. Os conjugados de $\alpha = \sqrt[4]{2}$ são $\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3$ onde ω é a raiz primitiva da unidade. Um elemento de K , por exemplo $x = a + b\alpha + c\alpha^2 + d\alpha^3$, onde $a, b, c, d \in \mathbb{Q}$, é levado a $\mathbb{R}^4$ de acordo com

$$\begin{aligned} \sigma(x) &= (\sigma_1(x), \sigma_2(x), \operatorname{Re}\sigma_3(x), \operatorname{Im}\sigma_3(x)) \\ &= (a + b\alpha + c\alpha^2 + d\alpha^3, a - b\alpha + c\alpha^2 - d\alpha^3, a - c\alpha^2, b\alpha - d\alpha^3). \end{aligned}$$

Uma das principais aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$ e alguns parâmetros associados são obtidos via Teoria Algébrica dos Números.

Teorema 2.5.1 ([11], pag. 56) *Sejam K um corpo de números de grau n , $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$ e $M \subseteq K$ um $\mathbb{Z}$ -módulo livre de posto n com $\mathbb{Z}$ -base $(x_i)_{1 \leq i \leq n}$.*

Então,

(a) $\sigma_K(M)$ é um reticulado.

(b) $v(\sigma_K(M)) = 2^{-r_2} |\det(\sigma_i(x_j))|$.

Demonstração:

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

$$\sigma_K(x_i) = (\sigma_1(x_i), \dots, \sigma_n(x_i)), \quad i = 1, \dots, n$$

Seja

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

Assim,

$$\det D = \det(\sigma_i(x_j)).$$

Por outro lado, sabemos que

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

Logo

$$(\det D)^2 = (\det(\sigma_i(x_j)))^2 = \Delta[x_1, \dots, x_n] \neq 0,$$

implicando que $\sigma_K(x_1), \dots, \sigma_K(x_n)$ são vetores linearmente independentes sobre $\mathbb{R}$. Por construção $\sigma_K(x_1), \dots, \sigma_K(x_n)$ geram $\sigma_K(M)$ logo $\{\sigma_K(x_1), \dots, \sigma_K(x_n)\}$ é uma base de $\sigma_K(M)$ e, portanto, $\sigma_K(M)$ é um reticulado.

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

(b) Mostremos que $v(\sigma_K(M)) = 2^{-r_2} |\det(\sigma_i(x_j))|$, quando K é totalmente imaginário.

Nesse caso

$$\sigma_K(x_i) = (\operatorname{Re}\sigma_1(x_i), \operatorname{Im}\sigma_1(x_i), \dots, \operatorname{Re}\sigma_{r_2}(x_i), \operatorname{Im}\sigma_{r_2}(x_i)), \quad i = 1, \dots, n.$$

Seja

$$D = \begin{pmatrix} \operatorname{Re}\sigma_1(x_1) & \operatorname{Im}\sigma_1(x_1) & \dots & \operatorname{Re}\sigma_{r_2}(x_1) & \operatorname{Im}\sigma_{r_2}(x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \operatorname{Re}\sigma_1(x_n) & \operatorname{Im}\sigma_1(x_n) & \dots & \operatorname{Re}\sigma_{r_2}(x_n) & \operatorname{Im}\sigma_{r_2}(x_n) \end{pmatrix}$$

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

$$D_1 = \begin{pmatrix} \sigma_1(x_1) & \overline{\sigma_1(x_1)} & \dots & \sigma_{r_2}(x_1) & \overline{\sigma_{r_2}(x_1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(x_n) & \overline{\sigma_1(x_n)} & \dots & \sigma_{r_2}(x_n) & \overline{\sigma_{r_2}(x_n)} \end{pmatrix}$$

Como $\det D = (2i)^{-r_2} \det D_1$ e $\overline{\sigma_i} = \sigma_{r_2+i}$, então

$$v(\sigma_K(M)) = |\det D| = |(2i)^{-r_2}| \cdot |\det D_1| = 2^{-r_2} \cdot |\det(\sigma_i(x_j))|.$$

■

Vimos anteriormente, que $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n , se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_K$, então $\mathfrak{a}$ é um $\mathbb{Z}$ -módulo livre de posto menor ou igual a n . Como o índice de $\mathfrak{a}$ sobre $\mathcal{O}_K$ é finito, temos que $\mathfrak{a}$ é um $\mathbb{Z}$ -módulo livre de posto n , também. Assim, pelo Teorema 2.5.1 $\sigma_K(\mathcal{O}_K)$ e $\sigma_K(\mathfrak{a})$ são reticulados. E mais, definimos por realização geométrica do ideal $\mathfrak{a}$ ao reticulado $\sigma_K(\mathfrak{a})$.

Exemplo 2.5.3 Sejam $K = \mathbb{Q}(\sqrt{10})$ e $M = \mathbb{Z}[\sqrt{10}]$ o anel dos inteiros algébricos de K , com base $\{1, \sqrt{10}\}$. Sendo $r_2 = 0$, temos:

$$v(\sigma_K(M)) = \left| \det \begin{pmatrix} 1 & \sqrt{10} \\ 1 & -\sqrt{10} \end{pmatrix} \right| = |-2\sqrt{10}| = 2\sqrt{10}$$

Exemplo 2.5.4 Sejam $K = \mathbb{Q}(\sqrt{-17})$ e $M = \mathbb{Z}[\sqrt{-17}]$ o anel dos inteiros algébricos de K , com base $\{1, \sqrt{-17}\}$. Sendo $r_2 = 1$, temos:

$$v(\sigma_K(M)) = 2^{-1} \left| \det \begin{pmatrix} 1 & \sqrt{-17} \\ 1 & -\sqrt{-17} \end{pmatrix} \right| = \frac{1}{2} |-2\sqrt{-17}| = |\sqrt{-17}| = |\sqrt{17}i| = \sqrt{17}$$

Teorema 2.5.2 ([11], pag. 57) Sejam K um corpo de números de grau n , com discriminante D_K e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então,

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |D_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})$$

Demonstração:

Seja $\{x_1, \dots, x_n\}$ uma base do ideal $\mathfrak{a}$ e como $\mathcal{O}_K \subseteq K$, segue do Teorema 2.5.1, $v(\sigma_K(\mathfrak{a})) = |\det D|$, sendo $|\det D| = 2^{-r_2} \cdot |\det(\sigma_i(x_j))|$. Por outro lado, temos

$$|\Delta[x_1, \dots, x_n]|^{\frac{1}{2}} = |D_K|^{\frac{1}{2}} \cdot N(\mathfrak{a}) \quad \text{e} \quad \Delta[x_1, \dots, x_n] = (\det(\sigma_i(x_j)))^2$$

Logo

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |D_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})$$



A expressão para a densidade de centro do reticulado $\sigma_K(\mathfrak{a})$, é dada por

$$\delta(\sigma_K(\mathfrak{a})) = \frac{2^{r_2} \rho^n}{|D_K|^{\frac{1}{2}} N(\mathfrak{a})}.$$

Exemplo 2.5.5 Para $K = \mathbb{Q}(\sqrt{10})$, segue dos Teoremas 2.1.2 e 2.1.3, respectivamente, que $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ e $D_K = 40$. Dado $\alpha = a + b\sqrt{10}$, temos

$$|\sigma_K(\alpha)|^2 = \sigma_1 \overline{\sigma_1} + \sigma_2 \overline{\sigma_2} = 2(a^2 + 10b^2)$$

e esta fórmula assume valor mínimo 2, quando $a = 1$ e $b = 0$. Portanto,

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{4\sqrt{10}} \cong 0,07906$$

Exemplo 2.5.6 Sejam $K = \mathbb{Q}(\sqrt{13})$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$ e $\mathfrak{a}$ o ideal principal de $\mathcal{O}_K$, gerado por $\theta = 1 - 2\sqrt{13}$. Para $\alpha \in \theta\mathcal{O}_K$, existem $a, b \in \mathbb{Z}$ tais que

$$\alpha = (1 - 2\sqrt{13}) \left(a + b \left(\frac{1 + \sqrt{13}}{2} \right) \right) = \left(a - \frac{25b}{2} \right) + \left(\frac{-b}{2} - 2a \right) \sqrt{13}.$$

Logo

$$\alpha \overline{\alpha} = \left(a - \frac{25b}{2} \right)^2 + 2 \left(a - \frac{25b}{2} \right) \left(\frac{-b}{2} - 2a \right) \sqrt{13} + 13 \left(\frac{-b}{2} - 2a \right)^2.$$

Assim,

$$|\sigma_K(\alpha)|^2 = \text{Tr}_{K/\mathbb{Q}}(\alpha \overline{\alpha}) = 2 \left[\left(a - \frac{25b}{2} \right)^2 + 13 \left(\frac{-b}{2} - 2a \right)^2 \right]$$

atribuindo valores inteiros não nulos para a forma quadrática acima, concluímos que esta assume valor mínimo 106 quando $a = 1$ e $b = 0$.

Sendo $D_K = 13$ e $|N_{K/\mathbb{Q}}(\theta)| = |-51| = 51$ temos

$$\delta(\sigma_K(\mathfrak{a})) = \frac{106}{204\sqrt{13}} \cong 0,14411$$

3.1 A forma quadrática no corpo ciclotômico $\mathbb{Q}(\xi_n)$

Seja $K/\mathbb{Q}$ uma extensão finita abeliana, então pelo Teorema de Kronecker-Weber K está contido em um corpo ciclotômico $\mathbb{Q}(\xi_n)$, para algum n . Dessa modo, o estudo de

Capítulo 3

Nos reticulados $\pi_K(I)$ de $\mathbb{R}^n$, onde I é um ideal não nulo de $\mathcal{O}_K$, a distância entre seus pontos é medida pela função traço, como veremos na proposição a seguir:

Corpos Abelianos

Proposição 3.1.1 ([24], pag. 220) Seja K um corpo de números e $x \in K$. Então

$$|N_K(x)|^2 = n \cdot \text{Tr}_K(x^2)$$

Este capítulo tem o objetivo estudar a densidade de centro da realização geométrica de um ideal não nulo em corpos abelianos.

Sabemos que a expressão da densidade de centro para estes reticulados envolve alguns parâmetros importantes da Teoria Algébrica dos Números, tais como discriminante de um corpo, norma de um ideal e a minimização da forma quadrática obtida da função traço.

Como a minimização da forma quadrática apresenta um alto grau de dificuldade, optamos por famílias de ideais que apresentam determinada característica em relação à sua decomposição.

Faz parte de nossa opção buscar tais famílias de ideais em subcorpos de $\mathbb{Q}(\xi_{p^r})$ com p primo e, em subcorpo de $\mathbb{Q}(\xi_{pq})$ com p, q números primos ímpares distintos. Assim apresentamos uma fórmula específica para a densidade de centro dos ideais gerados por estas famílias.

Embora não faz parte de nosso objetivo obter família de reticulados com densidade recorde, é importante destacar que os reticulados de maior interesse são aqueles com maior densidade de centro.

3.1 A forma quadrática no corpo ciclotômico $\mathbb{Q}(\xi_n)$

Seja $K/\mathbb{Q}$ uma extensão finita abeliana, então pelo Teorema de Kronecker-Weber K está contido em um corpo ciclotômico $\mathbb{Q}(\xi_n)$, para algum n . Deste modo, o estudo de corpos de números abelianos é equivalente ao estudo de subcorpos dos corpos ciclotômicos.

Nos reticulados $\sigma_K(I)$ do $\mathbb{R}^n$, onde I é um ideal ordinário não nulo de $\mathcal{O}_K$, a distância entre seus pontos é medida pela função traço, como veremos na proposição a seguir:

Proposição 3.1.1 ([12], pag. 225) *Sejam K um corpo de números e $x \in K$. Então*

$$|\sigma_K(x)|^2 = c \cdot \text{Tr}_{K/\mathbb{Q}}(x\bar{x})$$

onde

$$c = \begin{cases} 1, & \text{se } r_2 = 0; \\ 1/2, & \text{se } r_1 = 0. \end{cases}$$

Demonstração:

No caso em que $r_2 = 0$, isto é, K é totalmente real, para $x \in K$ e $\sigma_K(x) = (\sigma_1(x), \dots, \sigma_n(x))$, segue que :

$$|\sigma_K(x)|^2 = \sigma_1^2(x) + \dots + \sigma_n^2(x) = \sigma_1(x^2) + \dots + \sigma_n(x^2) = \sigma_1(x\bar{x}) + \dots + \sigma_n(x\bar{x}) = \text{Tr}(x\bar{x})$$

Agora, suponhamos $r_1 = 0$, ou seja, K totalmente imaginário. Então para $x \in K$, $n = 2r_2$ e $\sigma_K(x) = (\text{Re}\sigma_1(x), \text{Im}\sigma_1(x), \dots, \text{Re}\sigma_{r_2}(x), \text{Im}\sigma_{r_2}(x))$, temos:

$$|\sigma_K(x)|^2 = \sigma_1(x)\overline{\sigma_1(x)} + \dots + \sigma_{\frac{n}{2}}(x)\overline{\sigma_{\frac{n}{2}}(x)} = \sigma_1(x)\overline{\sigma_1(x)} + \dots + \sigma_{\frac{n}{2}}(x)\overline{\sigma_{\frac{n}{2}}(x)} = \sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x})$$

Sendo

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x}) + \bar{\sigma}_1(x\bar{x}) + \dots + \bar{\sigma}_{\frac{n}{2}}(x\bar{x})$$

e

$$\bar{\sigma}_i(x\bar{x}) = \sigma_i(x\bar{x}), \quad \forall i = 1, \dots, \frac{n}{2},$$

segue que

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = 2(\sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x})).$$

Portanto

$$|\sigma_K(x)|^2 = \frac{1}{2} Tr(x\bar{x}).$$

■

A seguir apresentamos alguns resultados sobre o traço em extensões ciclotômicas, os quais serão relevantes na demonstração do Teorema 3.1.2

Lema 3.1.1 ([14], pag. 52) *Sejam i, n inteiros, $i < n$. Se $d = (i, n)$ então,*

$$Tr_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^i) = \frac{\phi(n)}{\phi(n/d)} Tr_{\mathbb{Q}(\xi_{n/d})/\mathbb{Q}}(\xi_{n/d}^{i/d})$$

Demonstração:

Consideremos a seguinte extensão $\mathbb{Q} \subset \mathbb{Q}(\xi_{n/d}^{i/d}) \subset \mathbb{Q}(\xi_n)$. Pela propriedade do traço temos

$$Tr_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^i) = [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_{n/d}^{i/d})] Tr_{\mathbb{Q}(\xi_{n/d})/\mathbb{Q}}(\xi_{n/d}^{i/d}). \quad (3.1)$$

Uma vez que $[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_{n/d}^{i/d})] = \phi(n)/\phi(n/d)$, substituindo na equação (3.1) completamos a demonstração. ■

Lema 3.1.2 ([14], pag. 52) *Sejam j e $p_i^{a_i}$ inteiros e primos entre si então,*

$$Tr_{\mathbb{Q}(\xi_{p_i^{a_i}})/\mathbb{Q}}(\xi_{p_i^{a_i}}^j) = \begin{cases} -1, & \text{se } a_i = 1 \\ 0, & \text{se } a_i > 1. \end{cases}$$

Teorema 3.1.1 ([14], pag. 52) *Sejam $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_s^{a_s}$, $i \in \mathbb{N}$ e $d = (i, n)$ então,*

$$\text{Tr}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^i) = \frac{\phi(n)}{\phi(n/d)} \mu\left(\frac{n}{d}\right), \text{ onde } \mu \text{ é a função de Möbius.}$$

Demonstração:

Faremos a prova em três etapas:

(a) Para $n = d$ segue pelo Lema 3.1.1 que $\text{Tr}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^i) = \frac{\phi(n)}{\phi(n/d)}$.

(b) Quando n é livre de quadrados, faremos a demonstração por indução, sobre s (a quantidade de números primos da decomposição de n .)

Para $s = 1$, vale o Lema 3.1.2 e assim o resultado é válido.

Suponhamos verdadeira a afirmação para $s = k$, isto é,

$$\text{Tr}_{\mathbb{Q}(\xi_{p_1 \dots p_k})/\mathbb{Q}}(\xi_{p_1 \dots p_k}^i) = (-1)^k.$$

Agora provemos a afirmação para $s = k + 1$.

Dado $n = p_1 \dots p_{k+1}$, sejam $a = p_1 \dots p_k$, $b = p_{k+1}$ e u, v inteiros tais que $au + bv = 1$,

temos:

$$\xi_n^i = \xi_n^{i(au+bv)} = \xi_{ab}^{ia u} \xi_{ab}^{ib v} = \xi_b^{iu} \xi_a^{iv}$$

onde $(iu, b) = (iv, a) = 1$. Então, para $K = \mathbb{Q}(\xi_n)$ e $M = \mathbb{Q}(\xi_a)$ temos pelas propriedades

do traço que

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(\xi_n^i) &= \text{Tr}_{M/\mathbb{Q}}(\text{Tr}_{K/M}(\xi_b^{iu} \xi_a^{iv})) = \text{Tr}_{M/\mathbb{Q}}(\xi_a^{iv} \text{Tr}_{K/M}(\xi_b^{iu})) \\ &= (-1)(-1)^k = (-1)^{k+1}. \end{aligned}$$

Então, $\text{Tr}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^i) = (-1)^s$.

(c) Suponhamos que n não é livre de quadrados e sejam $a = p_1^{a_1}$, $b = p_2^{a_2} \dots p_s^{a_s}$, tomemos

$a_1 > 1$ e l, r inteiros tais que $al + br = 1$, logo

$$\xi_n^i = \xi_{ab}^{i(al+br)} = \xi_{ab}^{ial} \xi_{ab}^{ibr} = \xi_b^{il} \xi_a^{ir},$$

onde $(il, b) = (ir, a) = 1$. Assim, para $K = \mathbb{Q}(\xi_n)$ e $M = \mathbb{Q}(\xi_a)$ temos:

$$\text{Tr}_{K/\mathbb{Q}}(\xi_n^i) = \text{Tr}_{M/\mathbb{Q}}(\text{Tr}_{K/M}(\xi_b^{il} \xi_a^{ir})) = \text{Tr}_{K/M}(\xi_b^{il}) \cdot 0 = 0.$$

■

Teorema 3.1.2 ([14], pag. 60) *Dados*

$$n = \prod_{i=1}^s p_i^{a_i}, \quad P = \prod_{i=1}^s p_i, \quad K = \mathbb{Q}(\xi_n), \quad \mathcal{O}_K = \mathbb{Z}[\xi_n] \quad \text{e} \quad x = \sum_{j=0}^{\phi(n)-1} b_j \xi_n^j,$$

temos que:

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \frac{2n}{P} \left[\frac{\phi(P)}{2} \sum_{j=0}^{\phi(n)-1} b_j^2 + \mu(P) \sum_{i=1}^{\phi(P)-1} A_{\frac{n}{P}i} \phi((i, P)) \mu((i, P)) \right].$$

Demonstração:

Pela Proposição 3.1.1, temos que

$$|\sigma_K(x)|^2 = \frac{1}{2} \text{Tr}_{K/\mathbb{Q}}(x\bar{x}). \quad (3.2)$$

Em (3.2), calcular $|\sigma_K(x)|$ é equivalente a encontrar o traço do elemento $x\bar{x}$. Então, seja

$x \in \mathcal{O}_K = \mathbb{Z}[\xi_n]$, tal que

$$x = b_0 + b_1 \xi_n + b_2 \xi_n^2 + \dots + b_{m-1} \xi_n^{m-1},$$

com $m = \phi(n)$. Assim,

$$\bar{x} = b_0 + b_1 \xi_n^{-1} + b_2 \xi_n^{-2} + \dots + b_{m-1} \xi_n^{-(m-1)},$$

e queremos demonstrar

$$x\bar{x} = (b_0^2 + b_1^2 + \dots + b_{m-1}^2) + [b_0b_1(\xi_n + \xi_n^{-1}) + \dots + b_0b_{m-1}(\xi_n^{m-1} + \xi_n^{-(m-1)}) \\ + b_1b_2(\xi_n + \xi_n^{-1}) + \dots + b_1b_{m-1}(\xi_n^{m-2} + \xi_n^{-(m-2)}) + \dots + b_{m-2}b_{m-1}(\xi_n + \xi_n^{-1})].$$

Fazendo $A_i = b_0b_i + b_1b_{i+1} + \dots + b_{m-1-i}b_{m-1}$, e $\alpha_i = \xi_n^i + \xi_n^{-i}$, $\forall i, i = 1, \dots, m-1$,

temos:

$$x\bar{x} = \sum_{i=0}^{m-1} b_i^2 + \sum_{i=1}^{m-1} A_i \alpha_i.$$

Deste modo, nós podemos obter o valor da função traço:

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = Tr_{K/\mathbb{Q}}\left(\sum_{i=0}^{m-1} b_i^2\right) + Tr_{K/\mathbb{Q}}\left(\sum_{i=1}^{m-1} A_i \alpha_i\right) = m \cdot \sum_{i=0}^{m-1} b_i^2 + \sum_{i=1}^{m-1} A_i Tr_{K/\mathbb{Q}}(\alpha_i).$$

Como

$$Tr_{K/\mathbb{Q}}(\alpha_i) = Tr_{K/\mathbb{Q}}(\xi_n^i + \xi_n^{-i}) = 2 \cdot Tr_{K/\mathbb{Q}}(\xi_n^i),$$

temos

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = m \cdot \sum_{i=0}^{m-1} b_i^2 + 2 \cdot \sum_{i=1}^{m-1} A_i Tr_{K/\mathbb{Q}}(\xi_n^i) \quad (3.3)$$

Pelo Teorema 3.1.1, podemos reescrever a equação (3.3) do seguinte modo:

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = m \cdot \sum_{i=0}^{m-1} b_i^2 + 2 \cdot \sum_{i=1}^{m-1} A_i \frac{\mu(\frac{n}{d})}{\phi(\frac{n}{d})} m \quad (3.4)$$

onde $d = (n, i)$. Temos que $\mu(\frac{n}{d}) = 0$ se $d \neq \frac{n}{P} t_j$, onde $t_j = (j, P)$ para $j = 1, \dots, \phi(P) - 1$.

Deste modo,

$$\sum_{i=1}^{m-1} A_i \frac{\mu(\frac{n}{d})}{\phi(\frac{n}{d})} m = \sum_{j=1}^{\phi(P)-1} A_{\frac{n}{P}j} \mu(P) \mu(t_j) \phi(t_j) \cdot \frac{n}{P}. \quad (3.5)$$

Substituindo (3.5) em (3.4), obtemos

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = \frac{2n}{P} \left[\frac{\phi(P)}{2} \sum_{j=0}^{\phi(n)-1} b_j^2 + \mu(P) \sum_{i=1}^{\phi(P)-1} A_{\frac{n}{P}i} \phi((i, P)) \mu((i, P)) \right]. \quad (3.6)$$

Como queríamos demonstrar. ■

A expressão obtida para $Tr_{K/\mathbb{Q}}(x\bar{x})$ em (3.6) é uma forma quadrática, cuja minimização constitui um de nossos objetivos.

3.2 Os Reticulados Algébricos

Vimos que os reticulados do tipo $\sigma_K(I)$ é a realização geométrica de um ideal ordinário não nulo I de $\mathcal{O}_K$. Nesta seção estudaremos a densidade de centro destes reticulados, onde I satisfaz a seguinte propriedade:

Propriedade 3.2.1

$$\sigma(I) = I, \forall \sigma \in G = \text{Gal}(K/\mathbb{Q}); \text{ ou seja, } \sigma(x) \in I, \forall x \in I.$$

Uma consequência da propriedade acima é o Lema a seguir.

Lema 3.2.1 *Seja*

$$0 \neq I \subseteq \mathcal{O}_K; \quad \sigma(I) = I, \forall \sigma \in G = \text{Gal}(K/\mathbb{Q}) \text{ e } x \in I \text{ então}$$

$$Tr_{K/\mathbb{Q}}(x) \equiv 0 \pmod{r}, \quad r\mathbb{Z} = I \cap \mathbb{Z}.$$

Demonstração:

Seja $I \subset \mathcal{O}_K$ um ideal ordinário não nulo satisfazendo a Propriedade 3.2.1 então

$\sigma(x) \in I, \forall x \in I$. Assim,

$$Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x) \in I, \quad \forall x \in I. \quad (3.7)$$

Logo $Tr_{K/\mathbb{Q}}(x) \equiv 0 \pmod{I}$. Portanto, $Tr_{K/\mathbb{Q}}(x) \equiv 0 \pmod{r}$ com $r\mathbb{Z} = I \cap \mathbb{Z}$.

Por outro lado, $Tr_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, deste modo

$$Tr_{K/\mathbb{Q}}(x) \in I \cap \mathbb{Z} = r\mathbb{Z}.$$

Notemos que se $I \neq 0$, então $I \cap \mathbb{Z} \neq 0$ e para $x \in I$ temos $N(x) \in I$.

Pelo corolário 2.3.1 temos que em uma extensão galoisiana L/K , podemos fatorar um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ em $(\mathfrak{q}_1 \dots \mathfrak{q}_g \bar{\mathfrak{q}}_1 \dots \bar{\mathfrak{q}}_g)^e$ no anel dos inteiros algébricos $\mathcal{O}_L$, onde os $\mathfrak{q}_i$'s e os $\bar{\mathfrak{q}}_i$'s são ideais primos distintos, todos tendo o mesmo grau residual f sobre $\mathfrak{p}$. Um ideal primo ordinário não nulo I de $\mathcal{O}_K$ tem a Propriedade 3.2.1 se, I decompõe-se em $\mathfrak{q}_1 \dots \mathfrak{q}_g$ no anel dos inteiros algébricos $\mathcal{O}_L$.

Exemplo 3.2.1 Sejam $K/\mathbb{Q}$ uma extensão galoisiana com $G = \text{Gal}(K/\mathbb{Q})$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Seja $\mathfrak{p}\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_s \bar{\mathfrak{p}}_1 \dots \bar{\mathfrak{p}}_s)^e$ a decomposição do ideal primo $\mathfrak{p}$ em $\mathcal{O}_K$, tomando $I = \mathfrak{p}_1 \dots \mathfrak{p}_s$ então $\bar{I} = \bar{\mathfrak{p}}_1 \dots \bar{\mathfrak{p}}_s$. O ideal $I\bar{I}$ tem a Propriedade 3.2.1, pois

$$\sigma(I\bar{I}) = \sigma(\mathfrak{p}_1 \dots \mathfrak{p}_s \bar{\mathfrak{p}}_1 \dots \bar{\mathfrak{p}}_s) = \sigma(\mathfrak{p}_1) \dots \sigma(\mathfrak{p}_s) \sigma(\bar{\mathfrak{p}}_1) \dots \sigma(\bar{\mathfrak{p}}_s).$$

Pelo Teorema 2.3.4, temos que $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$, $i, j = 1, \dots, s$. Logo

$$\sigma(I\bar{I}) = \mathfrak{p}_1 \dots \mathfrak{p}_s \bar{\mathfrak{p}}_1 \dots \bar{\mathfrak{p}}_s,$$

a menos da ordem. Assim, se $x \in I$ então $x\bar{x} \in I\bar{I}$. Consequentemente

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) \in I\bar{I} \cap \mathbb{Z} = \mathfrak{p}\mathbb{Z}.$$

Vimos que a expressão para a densidade de centro dos reticulados $\sigma_K(I)$ é dada por

$$\delta(\sigma_K(I)) = \frac{2^{r_2} \rho^n}{|D_K|^{\frac{1}{2}} N(I)}. \quad (3.7)$$

Sabemos que $\rho = \frac{1}{2} \min \{|\sigma_K(x)|; 0 \neq x \in I\}$ e da Proposição 3.1.1 segue que

$$|\sigma_K(x)|^2 = c \cdot \text{Tr}_{K/\mathbb{Q}}(x\bar{x})$$

Logo, tomando

$$t = \min\{Tr_{K/\mathbb{Q}}(x\bar{x}); 0 \neq x \in I, \} \quad (3.8)$$

temos

$$\rho^n = \frac{c^{\frac{n}{2}}}{2^n} t^{\frac{n}{2}}.$$

Substituindo a expressão encontrada para ρ^n em (3.7), obtemos

$$\delta(\sigma_K(I)) = \frac{2^{r_2} c^{\frac{n}{2}} t^{\frac{n}{2}}}{2^n |D_K|^{\frac{1}{2}} N(I)}.$$

Notemos que: $2^{r_2} c^{\frac{n}{2}} = 1$.

Deste modo,

$$\delta(\sigma_K(I)) = \frac{1}{|D_K|^{\frac{1}{2}}} \cdot \left(\frac{t}{4}\right)^{\frac{n}{2}} \quad (3.9)$$

Seja $K/\mathbb{Q}$ uma extensão galoisiana de grau n ; sabemos pelo Teorema da Igualdade Fundamental que $n = e.f.g$, onde e é o índice de ramificação, f é o grau residual de qualquer ideal primo $\mathfrak{p}_i \subset \mathcal{O}_K$ e g é dito número de decomposição do ideal primo $\mathfrak{p}$ em $K/\mathbb{Q}$.

Observamos que a partir do Teorema da Igualdade Fundamental existem vários tipos de decomposição de um ideal primo $\mathfrak{p}$. Indicaremos abaixo alguns casos:

- (a) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \dots, g$, é totalmente ramificado em L/K , se $g = f_i = 1$ e $e_i = n$.
- (b) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \dots, g$, é totalmente inerte em L/K , se $f_i = n$ e $g = e_i = 1$.
- (c) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \dots, g$, é totalmente decomposto em L/K , se $g = n$ e $e_i = f_i = 1$.

Exemplo 3.2.2 Sejam $K = \mathbb{Q}(\xi_9)$ e $\mathcal{O}_K = \mathbb{Z}[\xi_9]$. O polinômio minimal de ξ_9 sobre $\mathbb{Q}$ é dado por

$$\Phi_9(X) = X^6 + X^3 + 1$$

A decomposição do ideal $3\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ satisfaz

$$\Phi_9(X) \equiv (X - 1)^6 \pmod{3\mathbb{Z}}$$

Assim temos $g = f = 1$ e $e = 6$, ou seja, o ideal $3\mathcal{O}_K$ é totalmente ramificado. O ideal $2\mathcal{O}_K$ decompõem-se em ideais primos de $\mathcal{O}_K$ satisfazendo

$$\Phi_9(X) \equiv X^6 + X^3 + 1 \pmod{2\mathbb{Z}}.$$

Logo, temos $g = e = 1$ e $f = 6$, logo o ideal $2\mathcal{O}_K$ é totalmente inerte. Agora tomando a decomposição do ideal $19\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ temos:

$$\Phi_9(X) \equiv p_1(X) \dots p_6(X) \pmod{19\mathbb{Z}}$$

onde

$$p_1(X) = X + 2, \quad p_2(X) = X + 3, \quad p_3(X) = X + 10,$$

$$p_4(X) = X + 13, \quad p_5(X) = X + 14 \quad e \quad p_6(X) = X + 15.$$

Logo temos $g = 6$, e $e = f = 1$, portanto o ideal $19\mathcal{O}_K$ é totalmente decomposto.

Um dos parâmetros que envolve o cálculo da densidade de centro de um reticulado $\sigma_K(I)$ é o parâmetro t , o qual consiste na minimização da forma quadrática. Diante da dificuldade em obtermos t , optamos por restringir os nossos estudos aos subcorpos de $\mathbb{Q}(\xi_m)$ onde $m = p^r$ com p primo ou $m = pq$ onde p e q são primos distintos.



T. 1365/05



3.3 Subcorpos de $\mathbb{Q}(\xi_{p^r})$

Estamos interessados na compreensão do cálculo da densidade de centro (3.9). Se enfocarmos o quociente

$$\frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{N(I)},$$

para maximizá-lo teríamos que minimizar $N(I)$, e esta assume seu menor valor $N(I) = 1$ quando $I = \mathcal{O}_K$, porém nem sempre obtemos bons resultados, pois minimizando $N(I)$ podemos eventualmente perder em t , ou seja, o quociente diminui.

Uma outra opção seria tomar $N(I) \neq 1$, vislumbrando um ganho em t , aumentando assim o nosso quociente. Deste modo, quando estamos estudando os subcorpos de $\mathbb{Q}(\xi_{p^r})$ optamos por ideais que ramificam-se completamente. Na seção seguinte, estudaremos os subcorpos de $\mathbb{Q}(\xi_{pq})$, assim optaremos pelos ideais que decompõe-se completamente em uma direção e ramificam-se completamente na outra direção.

Para $L = \mathbb{Q}(\xi_{p^r})$, $m = \phi(p^r) = p^{r-1}(p-1)$, $n = u \cdot p^j$ onde $u|(p-1)$ e $j \leq r-1$, p um ideal primo, segue o diagrama.

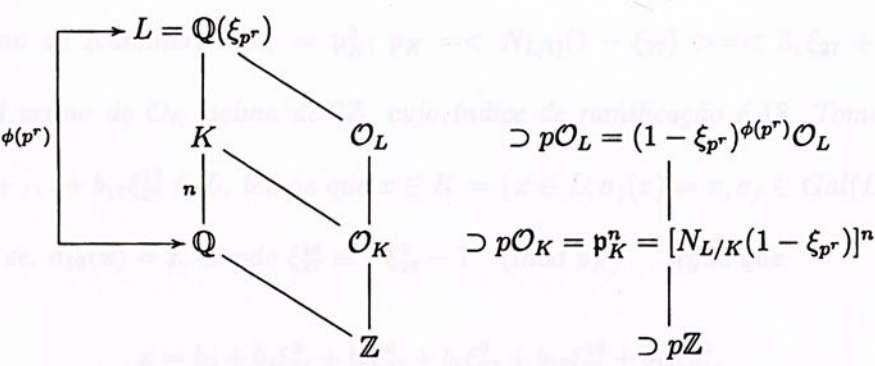


Figura 1: Diagrama dos Subcorpos de $\mathbb{Q}(\xi_{p^r})$

Sejam $K \subseteq L$, $I = \mathfrak{p}_K = \langle N_{L/K}(1 - \xi_{p^r}) \rangle$, e p o ideal que é totalmente ramificado em

$L/\mathbb{Q}$ e $\bar{\sigma}$ é a conjugação complexa, temos que

$$\bar{\sigma} \in D(p) = \{\sigma \in G/\sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Logo, para todo $x \in \mathfrak{p}_K$, temos que $x\bar{x} \in \mathfrak{p}_K^2$. Como $\mathfrak{p}_K^2$ satisfaz a Propriedade 3.2.1 então $\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) \in p\mathbb{Z}$. Assim, por (3.8) $t = p.h$; $h \in \mathbb{N}$.

Dos Teoremas 1.8.3 e 2.3.2 segue, respectivamente, que $N(\mathfrak{p}_K) = p$ e $|D_K| = p^v$, onde

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

Substituindo as expressões encontradas para t , $N(I)$ e D_K em (3.9) obtemos

$$\delta(\sigma_K(\mathfrak{p}_K)) = \frac{1}{p^{\frac{v}{2}}} \cdot \frac{p^{\frac{n}{2}} \left(\frac{h}{4}\right)^{\frac{n}{2}}}{p} = p^{\frac{n-v-2}{2}} \left(\frac{h}{4}\right)^{\frac{n}{2}}.$$

Exemplo 3.3.1 *Sejam K um subcorpo de $L = \mathbb{Q}(\xi_{27})$ tal que $[K : \mathbb{Q}] = 6$, $\mathcal{O}_K$ o anel dos inteiros de K e $\Phi_{27}(X) = X^{18} + X^9 + 1$. Consideremos o ideal $3\mathbb{Z}$, o polinômio $\Phi_{27}(X)$ fatora-se como*

$$X^{18} + X^9 + 1 \equiv (X+2)^{18} \pmod{3\mathbb{Z}[X]}$$

e pelo Lema de Kummer, $3\mathcal{O}_K = \mathfrak{p}_K^6$; $\mathfrak{p}_K = \langle N_{L/\mathbb{Q}}(1 - \xi_{27}) \rangle = \langle 3, \xi_{27} + 2 \rangle$ é o único ideal primo de $\mathcal{O}_K$ acima de $3\mathbb{Z}$, cujo índice de ramificação é 18. Tomando $x = b_0 + b_1\xi_{27} + \dots + b_{17}\xi_{27}^{17} \in L$, temos que $x \in K = \{x \in L; \sigma_j(x) = x, \sigma_j \in \text{Gal}(L/K)\}$ se, e somente se, $\sigma_{10}(x) = x$. Sendo $\xi_{27}^{18} \equiv -\xi_{27}^9 - 1 \pmod{\mathfrak{p}_K}$ segue que

$$x = b_0 + b_3\xi_{27}^3 + b_6\xi_{27}^6 + b_9\xi_{27}^9 + b_{12}\xi_{27}^{12} + b_{15}\xi_{27}^{15}.$$

Como $\mathfrak{p}_K$ está acima de $3\mathbb{Z}$ então $x \in \mathfrak{p}_K$ se, e somente se,

$$b_0 + b_3 + b_6 + b_9 + b_{12} + b_{15} \in 3\mathbb{Z} = \mathfrak{p}_K \cap \mathbb{Z}.$$

Atribuindo valores para $b_0, b_3, b_6, b_9, b_{12}$ e b_{15} temos que a forma quadrática

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \frac{1}{3} \text{Tr}_{L/\mathbb{Q}}(x\bar{x}) = 6(b_0^2 + b_3^2 + b_6^2 + b_9^2 + b_{12}^2 + b_{15}^2 - b_0b_9 - b_3b_{12} - b_6b_{15})$$

assume valor mínimo $t = 12$, quando $b_0 = b_3 = b_9 = 1$ ou $b_0 = b_3 = b_9 = -1$ e $b_6 = b_{12} = b_{15} = 0$, logo $h = 4$. De $n = 6$ e $p = 3$ temos $v = 9$, portanto

$$\delta(\sigma_K(\mathfrak{p}_K)) = \frac{1}{\sqrt{3^5}} \cong 0,06415.$$

Exemplo 3.3.2 Sejam K um subcorpo de $L = \mathbb{Q}(\xi_{25})$ tal que $[K : \mathbb{Q}] = 5$, $\mathcal{O}_K$ o anel dos inteiros de K e $\Phi_{25}(X) = X^{20} + X^{15} + X^{10} + X^5 + 1$. Consideremos o ideal $5\mathbb{Z}$, o polinômio $\Phi_{25}(X)$ fatora-se como

$$X^{20} + X^{15} + X^{10} + X^5 + 1 \equiv (X + 4)^{20} \pmod{5\mathbb{Z}[X]}$$

e pelo Lema de Kummer, $5\mathcal{O}_K = \mathfrak{p}_K^5$; $\mathfrak{p}_K = \langle N_{L/\mathbb{Q}}(1 - \xi_{25}) \rangle = \langle 5, \xi_{25} + 4 \rangle$ é o único ideal primo de $\mathcal{O}_K$ acima de $5\mathbb{Z}$ cujo índice de ramificação é 20. Tomando $x = b_0 + b_1\xi_{25} + \dots + b_{19}\xi_{25}^{19} \in L$, temos que $x \in K$ se, e somente se, $\sigma_7(x) = x$. Sendo $\xi_{25}^{20} \equiv -\xi_{25}^{15} - \xi_{25}^{10} - \xi_{25}^5 - 1 \pmod{\mathfrak{p}_K}$ segue que

$$\begin{aligned} x &= b_0 + b_1\xi_{25} + b_2\xi_{25}^2 - b_2\xi_{25}^3 - b_1\xi_{25}^4 + b_6\xi_{25}^6 + b_1\xi_{25}^7 + (b_6 - b_2)\xi_{25}^8 \\ &\quad + b_9\xi_{25}^9 + b_2\xi_{25}^{11} + (b_9 - b_2 + b_1)\xi_{25}^{13} + (b_2 - b_1)\xi_{25}^{14} \\ &\quad + (b_9 + b_1)\xi_{25}^{16} + b_6\xi_{25}^{17} + (b_1 - b_2)\xi_{25}^{18} + (b_6 - b_1)\xi_{25}^{19}. \end{aligned}$$

Como $\mathfrak{p}_K$ está acima de $5\mathbb{Z}$ então $x \in \mathfrak{p}_K$ se, e somente se,

$$b_0 + 3b_1 - b_2 + 4b_6 + 4b_9 \in 5\mathbb{Z} = \mathfrak{p}_K \cap \mathbb{Z}.$$

Atribuindo valores para b_0, b_1, b_2, b_6 e b_9 temos que a forma quadrática

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(x\bar{x}) &= \frac{1}{4} \text{Tr}_{L/\mathbb{Q}}(x\bar{x}) = 5[b_0^2 + (b_6 - b_2)^2 + (b_6 - 2b_1)^2 + (b_9 - b_1)^2 + (b_9 - b_2)^2 \\ &\quad + (b_2 - b_1)^2 + (b_9 - b_6)^2 + b_2^2 + b_6^2 + b_9^2 - 2b_2b_1 - 4b_9b_1] \end{aligned}$$

assume valor mínimo $t = 25$, quando $b_0 = b_6 = 1$ ou $b_0 = b_6 = -1$ e $b_1 = b_2 = b_9 = 0$, logo $h = 5$. De $n = 5$ e $p = 5$ temos $v = 8$, portanto

$$\delta(\sigma_K(\mathfrak{p}_K)) = \frac{1}{32} \cong 0,03125.$$

3.4 Subcorpos de $\mathbb{Q}(\xi_{pq})$

Nesta seção faremos uso de alguns resultados da Teoria de Galois, deste modo supomos que o leitor tenha um conhecimento prévio deste assunto, o qual pode ser encontrado nas referências ([5] e ([6]).

O resultado a seguir é muito importante para a construção dos nossos exemplos.

Teorema 3.4.1 ([7], pag. 263) *Sejam L uma extensão galoisiana de K e M uma extensão de K em $\mathbb{C}$. Então o corpo LM é galoisiana sobre M e $H = \text{Gal}(LM/M)$ é imerso no $G = \text{Gal}(L/K)$ pelos automorfismos de G restritos a L . Além disso, a imersão é um isomorfismo se $L \cap M = K$.*

Demonstração:

Seja $L = K[\alpha]$. Então $LM = M[\alpha]$ o qual é galoisiano sobre M , pois os conjugados de α sobre M estão entre os conjugados de α sobre K , os quais estão todos em L .

Existe um homomorfismo φ de H em G , obtido pelos automorfismos σ de G restritos a L , e o núcleo é facilmente visto por ser trivial. Se σ fixa M e L ponto-a-ponto, então ele fixa LM ponto-a-ponto.

Finalmente consideremos H' a imagem de H em G , H' fixa o corpo $L \cap M = K$, pois o corpo fixado por H é M e pelo Teorema da Correspondência de Galois $H' = \text{Gal}(L/M \cap L)$. Então $H' = \text{Gal}(L/K)$ se, e somente se, $L \cap M = K$. ■

A seguir, mostraremos alguns resultados que possibilitarão uma melhor caracterização dos nossos ideais.

Teorema 3.4.2 ([3], pag. 70) *Sejam $L = \mathbb{Q}(\xi_{pq})$, K um subcorpo de L , q e q' ideais primos de $\mathcal{O}_K$ e $\mathcal{O}_L$, respectivamente, ambos acima de $q\mathbb{Z}$, $D_K(q)$ e $D_L(q)$ os respectivos grupos de decomposição de q e q' e $\bar{\sigma}$ a conjugação complexa. Então,*

$$\bar{\sigma} \in D_L(q) \iff \bar{\sigma} \in D_K(q).$$

Demonstração:

Seja $\sigma_i \in D_K(q)$ definido por

$$\sigma_i(\xi_p) = \xi_p^i.$$

Para cada $\sigma_i \in D_K(q)$, existem $q-1$ extensões $\sigma_{i,j}$ de $D_L(q)$. Cada $\sigma_{i,j}$ é definido por seu valor em ξ_{pq} . Sejam u e v tais que $1 = pu + qv$. Deste modo, segue que

$$\sigma_{i,j}(\xi_{pq}) = \sigma_{i,j}(\xi_{pq}^{pu+qv}) = \xi_{pq}^{puj+qvi}.$$

Assim $\bar{\sigma} \in D_L(q)$ se, e somente se, existem i, j tais que

$$puj + qvi \equiv -1 \pmod{pq},$$

que equivale a

$$\begin{cases} puj + qvi \equiv -1 \pmod{p}; \\ \text{e} \\ puj + qvi \equiv -1 \pmod{q}. \end{cases}$$

A segunda condição vale sempre, já que j pode assumir qualquer valor não nulo módulo q . Quanto à primeira, esta equivale a $\bar{\sigma} \in D_K(p)$, o que conclui a prova. ■

Corolário 3.4.1 ([3], pag. 71) *Sejam $L = \mathbb{Q}(\xi_{pq})$, $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$ acima de $q\mathbb{Z}$, $D_L(q)$ o grupo de decomposição de $\mathfrak{q}$, $\bar{\sigma}$ a conjugação complexa e $o_m(n)$ a ordem de n módulo m , quando $(m, n) = 1$. Então*

$$\bar{\sigma} \in D_L(q) \iff o_p(q) \equiv 0 \pmod{2}.$$

Quando p e q satisfazem às condições $o_q(p) \equiv o_p(q) \equiv 1 \pmod{2}$, isto é, $\bar{\sigma} \notin D_L(q)$ então existem em $\mathbb{Z}[\xi_{pq}]$ as decomposições em ideais primos

$$p\mathcal{O}_L = (p_1p_2 \dots p_r\overline{p_1}\overline{p_2} \dots \overline{p_r})^{p-1} \quad \text{e} \quad q\mathcal{O}_L = (q_1q_2 \dots q_s\overline{q_1}\overline{q_2} \dots \overline{q_s})^{q-1}.$$

Temos particular interesse no ideal

$$I = p_1p_2 \dots p_rq_1q_2 \dots q_s$$

Sejam $L = \mathbb{Q}(\xi_{pq})$ com p, q primos ímpares distintos onde $o_q(p) \equiv o_p(q) \equiv 1 \pmod{2}$, $K_p \subset \mathbb{Q}(\xi_q)$, $K_q \subset \mathbb{Q}(\xi_p)$ tais que $[K_p : \mathbb{Q}] = 2s$, $[K_q : \mathbb{Q}] = 2r$ e $K = K_pK_q$ o menor corpo contendo K_p e K_q com $[K : \mathbb{Q}] = 4rs$.

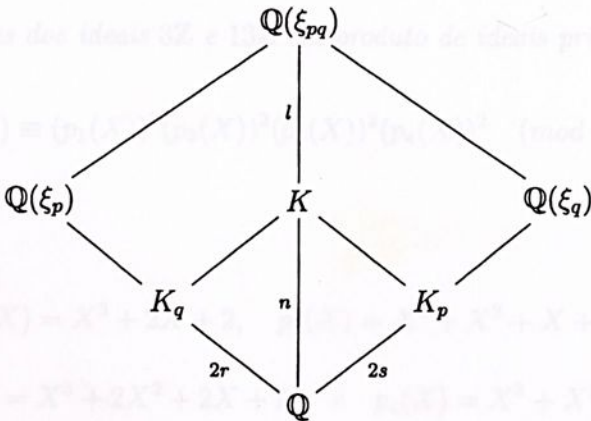


Figura 2: Diagrama dos subcorpos de $\mathbb{Q}(\xi_{pq})$

Sendo K_p e K_q corpos imaginários, temos que a conjugação complexa $\bar{\sigma}$ não está contida no grupo de decomposição $D_L(p)$. Assim, dados os ideais $p\mathcal{O}_{K_p} = (p_1p_2 \dots p_s\overline{p_1}\overline{p_2} \dots \overline{p_s})$

e $q\mathcal{O}_{K_q} = (q_1q_2 \dots q_r \overline{q_1q_2} \dots \overline{q_r})$ onde $p_i\mathcal{O}_K = P_i^{2r}$ e $q_j\mathcal{O}_K = Q_j^{2s}$; $i = 1, \dots, s$, $j = 1, \dots, r$.

Tomemos $I = P_1P_2 \dots P_sQ_1Q_2 \dots Q_r$. Como $I\bar{I}$ tem a Propriedade 3.2.1, temos que: se $x \in I$ então $Tr_{K/\mathbb{Q}}(x\bar{x}) \in I\bar{I} \cap \mathbb{Z} = pq\mathbb{Z}$, ou seja, $t = pqh$; $h \in \mathbb{N}$. Sabemos, pelo Teorema 3.1.2, que $Tr_{L/\mathbb{Q}}(x\bar{x})$ é par. Sendo $Tr_{K/\mathbb{Q}}(x\bar{x}) = \frac{1}{t}Tr_{L/\mathbb{Q}}(x\bar{x})$ então $Tr_{K/\mathbb{Q}}(x\bar{x})$ também é par.

Do Teorema 2.3.3, segue que $D_{K_p} = q^{2s-1}$ e $D_{K_q} = p^{2r-1}$, como K_p e K_q são linearmente disjuntos (isto é, $K_p \cap K_q = \mathbb{Q}$) temos $D_K = q^{(2s-1)2r}p^{(2r-1)2s}$. Sabemos que $N(I) = p^s q^r$. Para os valores de t , $N(I)$ e D_K acima obtidos, a expressão (3.9) será dada por:

$$\delta(\sigma_K(I)) = \left(\frac{h}{4}\right)^{\frac{[K:\mathbb{Q}]}{2}}$$

Exemplo 3.4.1 Sejam $L = \mathbb{Q}(\xi_{39})$, $K_{13} = \mathbb{Q}(\xi_3)$, $K_3 \subset \mathbb{Q}(\xi_{13})$ tais que $[K_3 : \mathbb{Q}] = 4$, $[K_{13} : \mathbb{Q}] = 2$ e $K = K_3K_{13}$. Dado

$$\Phi_{39}(X) = X^{24} - X^{23} + X^{21} - X^{20} + \dots + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1,$$

vejamos as fatorações dos ideais $3\mathbb{Z}$ e $13\mathbb{Z}$ em produto de ideais primos de $\mathcal{O}_L$.

$$\Phi_{39}(X) \equiv (p_1(X))^2(p_2(X))^2(p_3(X))^2(p_4(X))^2 \pmod{3\mathbb{Z}[X]}$$

onde

$$p_1(X) = X^3 + 2X + 2, \quad p_2(X) = X^3 + X^2 + X + 2,$$

$$p_3(X) = X^3 + 2X^2 + 2X + 2, \quad e \quad p_4(X) = X^3 + X^2 + 2,$$

e pelo Lema de Kummer temos $p_i = \langle 3, p_i(\xi_3) \rangle$, $\forall i = 1, \dots, 4$. Sabemos que $\sigma_{13}(3) = 3 \equiv 1 \pmod{2}$, logo $\bar{\sigma} = \sigma_{38} \notin D_L(3) = \{\sigma_1, \sigma_{14}, \sigma_{16}, \sigma_{22}, \sigma_{29}, \sigma_{35}\}$. Neste caso, temos que $p_4 = \bar{p}_1$, $p_3 = \bar{p}_2$ e $3\mathcal{O}_{K_3} = p_1p_2\bar{p}_1\bar{p}_2$ onde $p_i\mathcal{O}_K = P_i^2$.

Para o ideal $13\mathbb{Z}$, temos:

$$\Phi_{39}(X) \equiv (q_1(X))^{12}(q_2(X))^{12} \pmod{13\mathbb{Z}[X]}$$

onde $q_1(X) = X + 4$ e $q_2(X) = X + 10$. Pelo Lema de Kummer $q_i = \langle 13, q_i(\xi_{13}) \rangle$ $i = 1, 2$. Observemos que $\bar{\sigma} \notin D_L(13) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{10}, \sigma_{16}, \sigma_{19}, \sigma_{22}, \sigma_{28}, \sigma_{31}, \sigma_{34}, \sigma_{37}\}$ pois $\sigma_3(13) = 1 \equiv 1 \pmod{2}$, assim temos que $q_2 = \bar{q}_2$, e $13\mathcal{O}_{K_{13}} = q_1\bar{q}_1$ onde $q\mathcal{O}_K = Q^4$.

Consideremos o ideal $I = P_1P_2Q \subset \mathcal{O}_K$. Sendo $I\bar{I}$ um ideal que satisfaz a Propriedade 3.2.1, temos que para $x \in I$, $t = 39h$; $h \in \mathbb{N}$. Como a forma quadrática obtida para o $Tr_{K/\mathbb{Q}}$ em (3.6) é par, segue que $t \geq 2.39$. Tomando $t = 2.39$ segue que $h = 2$, assim

$$\delta(\sigma_K(I)) = \left(\frac{2}{4}\right)^4 = 0,0625.$$

Exemplo 3.4.2 Sejam $L = \mathbb{Q}(\xi_{55})$, $K_{11} = \mathbb{Q}(\xi_5)$, $K_5 \subset \mathbb{Q}(\xi_{11})$ tais que $[K_5 : \mathbb{Q}] = 2$, $[K_{11} : \mathbb{Q}] = 4$, e $K = K_5K_{11}$. Dado

$$\Phi_{55}(X) = X^{40} - X^{39} + X^{35} - X^{34} + X^{30} + \dots + X^{15} - X^{12} + X^{10} - X^6 + X^5 - X + 1,$$

vejamos as fatorações dos ideais $11\mathbb{Z}$ e $5\mathbb{Z}$ em produto de ideais primos de $\mathcal{O}_L$.

$$\Phi_{55}(X) \equiv (p_1(X))^{10}(p_2(X))^{10}(p_3(X))^{10}(p_4(X))^{10} \pmod{11\mathbb{Z}[X]}$$

onde

$$p_1(X) = X + 2, \quad p_2(X) = X + 6, \quad p_3(X) = X + 7, \quad e \quad p_4(X) = X + 8,$$

e pelo Lema de Kummer temos $p_i = \langle 11, p_i(\xi_5) \rangle$, $\forall i = 1, \dots, 4$. Sabemos que $\sigma_5(11) = 1 \equiv 1 \pmod{2}$, logo $\bar{\sigma} = \sigma_{54} \notin D_L(11) = \{\sigma_1, \sigma_6, \sigma_{16}, \sigma_{21}, \sigma_{26}, \sigma_{31}, \sigma_{41}, \sigma_{46}, \sigma_{41}\}$. Neste caso, temos que $p_2 = \bar{p}_1$, $p_4 = \bar{p}_3$ e $11\mathcal{O}_{K_{11}} = p_1p_3\bar{p}_1\bar{p}_3$ onde $p_i\mathcal{O}_K = P_i^2$.

Para o ideal $5\mathbb{Z}$, temos:

$$\Phi_{55}(X) \equiv (q_1(X))^4(q_2(X))^4 \pmod{5\mathbb{Z}[X]}$$

onde $q_1(X) = X^5 + 4X^4 + 4X^3 + X^2 + 3X + 4$ e $q_2(X) = X^5 + 2X^4 + 4X^3 + X^2 + X + 4$.

Pelo Lema de Kummer $q_i = \langle 5, q_i(\xi_{11}) \rangle$, $i = 1, 2$. Observemos que $\bar{\sigma} \notin D_L(5)$ pois $o_{11}(5) = 5 \equiv 1 \pmod{2}$, assim temos que $q_2 = \bar{q}_2$, e $5\mathcal{O}_{K_5} = q_1\bar{q}_1$ onde $q\mathcal{O}_K = Q^4$.

Consideremos o ideal $I = P_1P_3Q \subset \mathcal{O}_K$. Sendo $I\bar{I}$ um ideal que satisfaz a Propriedade 3.2.1, temos que para $x \in I$, $t = 55h$; $h \in \mathbb{N}$. Como a forma quadrática obtida para o $Tr_{K/\mathbb{Q}}$ em (3.6) é par, segue que $t \geq 2.55$. Tomando

$$\begin{aligned} x = & (a_5 - a_7)\xi_{55}^{39} + (a_3 - a_5)\xi_{55}^{36} + (a_5 - a_1 - a_7)\xi_{55}^{34} + a_6\xi_{55}^{33} + (a_7 - a_5)\xi_{55}^{32} + \\ & + (a_3 - a_5)\xi_{55}^{31} + (a_5 - a_7)\xi_{55}^{29} + (a_5 - a_7)\xi_{55}^{28} + a_7\xi_{55}^{27} + \dots + \\ & + (a_2 - a_5 - a_7)\xi_{55}^{11} + (a_7 - a_5)\xi_{55}^{10} - a_7\xi_{55}^9 + (a_5 - a_7)\xi_{55}^8 + (a_1 - \\ & - a_5 + a_7)\xi_{55}^5 - a_7\xi_{55}^4 - a_7\xi_{55}^3 + (a_3 - a_1)\xi_{55} + (a_0 - a_5 + a_7) \in K; a_i \in \mathbb{Q}, \end{aligned}$$

temos que

$$\begin{aligned} Tr_{K/\mathbb{Q}}(x\bar{x}) = & 2.[20a_6^2 + 831a_7^2 + 20a_0^2 - 85a_0a_5 + 77a_0a_7 + 941a_5^2 - 1343a_5a_7 + \\ & + 140a_3^2 - 51a_3a_1 + 260a_1^2 + 177a_7a_1 - 528a_5a_1 + 77a_7a_2 + \dots + \\ & + 20a_2a_3 + 10a_2a_4 + 10a_6a_4 + 10a_0a_2 + 10a_0a_4 + 10a_6a_2 + 10a_6a_0] \neq \\ & \neq y.55 \pmod{z}, \text{ isto é,} \\ & \exists x \in K / t = y.55; y = 2, 4, 6, 8 \text{ e } z = 6, 25, 25, 6. \end{aligned}$$

Portanto $Tr_{K/\mathbb{Q}}(x\bar{x}) \geq 10.55$, assim tomando $a_1 = a_2 = 1$ e $a_0 = a_3 = a_4 = a_5 = a_6 = a_7 = 0$, temos $t = 550$, ou seja, $h = 2$. Logo

$$\delta(\sigma_K(I)) = \left(\frac{2}{4}\right)^4 \cong 0,0625.$$

Para a dimensão 8 a densidade de centro obtida nos exemplos é a maior conhecida.



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] Endler, O.; *Teoria dos Números Algébricos*. Projeto Euclides, 1986.
- [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] Rotman, J.; *Galois Theory*. Springer-Verlag, 1990.
- [11] Samuel, P.; *Algebraic Theory of Numbers*. Hermann, 1970.



- [12] Sloane, N.J.A.; Conway, J.H.; *Sphere Packing, Lattices and Groups*. Springer-Verlag, 1999.
- [13] Stewart, I.; Tall, D.; *Algebraic Number Theory*. Chapman & Hall, 1987.
- [14] Rodrigues, T.M.; *Cúbicas Galoisianas*. Dissertação de Mestrado, IBILCE-UNESP, 2003.
- [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*. Springer-Verlag, 1982.



