

Taciana Matos de Souza

Reticulados Algébricos em Corpos
de Números Abelianos



1910001366





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

Reticulados Algébricos em Corpos de Números Abelianos

Taciana Matos de Souza

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



T. 1366/05

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

10101004

7512.91

5729A

04/03/2005

Doação

R\$ 26,00

Autor(a)

076/2005

80/05

Souza, Taciana Matos de.

Reticulados algébricos em corpos de números abelianos / Taciana Matos de Souza
– São José do Rio Preto : [s.n.], 2004
119 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



"Grandes realizações não são
feitas por impulso, mas por
uma soma de pequenas
realizações."

(Vincent Van Gogh)



Agradecimentos

Ao concluir este trabalho agradeço:

A Deus.

Aos meus pais, que vibram e rezam com minha glória e esperança, que são meu apoio e a quem devo minha vida.

Aos meus irmãos, pelo grande amor que sempre me deram e que foi muito importante nos momentos difíceis.

À minha família, avós, tios e primos pelo grande incentivo.

Ao meu noivo Rodrigo por seu amor, sua amizade e seu conhecimento.

A banca examinadora:

Ao Prof. Dr. Tapani Pires da Nobrega Neto, pela amizade e paciência.

Aos meus pais,

José Eduardo e Sonia

Aos meus irmãos,

Fabiano e Clarissa

E ao meu noivo

Rodrigo

À Marlene e ao Anderson, pela amizade, pelo apoio e pela não sempre presente tanto amor me trouxeram.

dedico.

Aos colegas da Pós-Graduação, pelo agradável convívio.

Agradecimentos

Ao concluir este trabalho agradeço:

À Deus.

Aos meus pais, que vibram e rezam com minhas glórias e esperança, que são meu apoio e a quem devo minha vida.

Aos meus irmãos, pelo grande amor que sempre me deram e que foi muito importante nos momentos difíceis.

À minha família, avós, tios e primos pelo grande incentivo.

Ao meu noivo Rodrigo por seu amor, sua amizade e seu conhecimento.

À banca examinadora.

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

Aos professores do Departamento de Matemática da FCT - UNESP (Campus de Presidente Prudente) pela amizade e pelo conhecimento transmitido. Em especial ao Prof. Dr. José Roberto Nogueira, pela paciência e amizade sempre presentes desde os tempos da graduação.

À Mariene e ao Anderson, pela amizade, pelo apoio e pelos risos sempre presentes e que tanto ânimo me trouxeram.

Aos colegas da Pós-Graduação, pelo agradável convívio.



Aos professores do Departamento de Matemática do IBILCE - UNESP pelo conhecimento transmitido. Em especial aos professores Aparecida Francisco da Silva e Waldemar Donizete Bastos pelos conselhos e pela acolhida.

À CAPES pelo apoio financeiro.

Resumo

Este trabalho é dedicado aos reticulados algébricos. Estudamos os reticulados de posto 2 e 3 obtidos via representação geométrica de $\mathbb{Z}$ -módulos de grau 2 e 3. Para os reticulados de posto 2, obtemos uma caracterização algébrica e geométrica. Para os reticulados de posto 3, obtemos uma caracterização algébrica e geométrica. A caracterização algébrica é dada em termos de determinantes e a caracterização geométrica é dada em termos de volumes.

Palavras-Chave: Reticulados, Reticulados Algébricos, Densidade de Gauss.

Resumo

Este trabalho é dedicado aos reticulados algébricos. Estudamos os reticulados de posto 2 e 3 obtidos via representação geométrica de $\mathbb{Z}$ -módulos do seu anel dos inteiros algébricos e os reticulados de posto 3 obtidos via representação geométrica de ideais. Visando calcular a densidade de centro de tais reticulados, é fundamental o estudo de seus discriminantes e minimização de uma forma quadrática e da norma de um ideal.

Palavras-Chave: Reticulados, Reticulados Algébricos, Densidade de Centro.

Sumário

Abstract

This work is dedicated to the algebraic lattices. We study the lattices of rank 2 and 3 generated from geometric representation of $\mathbb{Z}$ -modules of their algebraic integer ring and lattices of rank 3 generated from geometric representation of ideals. For calculating the center density of these lattices, it is fundamental to study of their discriminant and the minimization of a quadratic form and of the norm of ideal.

Keywords: Lattices, Algebraic Lattices, Center Density.

1.3	Ínteiros Algébricos	20
1.5	Normas e Traço	34
1.6	Decomposição em Irredutíveis	36
1.7	Fatoração de Ideais	40
1.8	Normas de um Ideal	50
2	Corpos Quadráticos e Ciclotômicos	54
2.1	Corpos Quadráticos	60
2.2	Corpos Ciclotômicos	60
2.2.1	O primeiro Corpo Ciclotômico	64
2.3	Corpos de Números Abelianos	72
2.4	Retângulos	80

Sumário

Introdução	12
1 Corpos de Números	16
1.1 Elementos Algébricos sobre um Corpo	17
1.2 Conjugados e Discriminantes	20
1.3 Inteiros Algébricos	26
1.4 Base Integral	29
1.5 Norma e Traço	34
1.6 Decomposição em Irredutíveis	36
1.7 Fatoração de Ideais	40
1.8 Norma de um Ideal	50
2 Corpos Quadráticos e Ciclotômicos	54
2.1 Corpos Quadráticos	55
2.2 Corpos Ciclotômicos	60
2.2.1 O p -ésimo Corpo Ciclotômico	64
2.3 Corpos de Números Abelianos	72
2.4 Reticulados	82

2.5	O Homomorfismo Canônico	85
3	Reticulados Algébricos e Aplicações	94
3.1	Reticulados Algébricos	95
3.1.1	K é Totalmente Real	95
3.1.2	K é Totalmente Imaginário	98
3.2	Reticulados de Posto 2	98
3.2.1	Caso K Totalmente Real	98
3.2.2	Caso K Totalmente Imaginário	101
3.3	Reticulados de Posto 3	104
3.4	Representação Geométrica de Ideais	109
	Bibliografia	118

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

$Tr_{L/K}$: 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

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

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

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

$Gal(L/K)$: grupo de Galois de L/K

Introdução

Entendemos por Empacotamento Esférico a disposição de esferas de mesmo raio no espaço euclidiano n -dimensional de tal modo que a intersecção de duas delas tenha no máximo um ponto.

Um problema associado ao Empacotamento Esférico é o de dispor essas esferas no espaço, de modo que elas ocupem a maior parte desse espaço, ou seja, que esta distribuição tenha alta densidade.

Devido à importância dessa questão, durante um Congresso em Paris, no ano de 1900, Hilbert citou-a como sendo o 18º Problema de uma seleta lista de desafios que viriam ocupar destaque no desenvolvimento da ciência moderna.

Dentre os empacotamentos esféricos aqueles cujo conjunto de centros das esferas constituía um subgrupo discreto do $\mathbb{R}^n$, despertaram particular interesse e passaram a se chamar empacotamentos reticulados.

Por volta de 1948, surgiu a idéia, pelo artigo de Claude Shannon, que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erro eficientes. A partir daí, passaram-se a associar o estudo dos códigos ao dos reticulados. Com isso, o interesse pelo 18º Problema de Hilbert aumentou consideravelmente, surgiram várias famílias de reticulados, cada uma destas visando dar uma melhor contribuição no que diz respeito à densidade de empacotamento.

Dentre tais modelos, destaca-se o descrito por Minkowski, chamado método algébrico baseado na teoria algébrica dos números, o qual utilizaremos neste trabalho.

Devido à complexidade e importância relevante dos resultados aqui abordados, este trabalho tem como objetivo obter reticulados algébricos de postos 2 e 3 e buscar resultados explícitos para a fórmula da densidade de centro de tais reticulados, usando a Teoria Algébrica dos Números.

Vale ressaltar que cada resultado aqui enunciado, será acompanhado de um número que representa a referência que o contém. Quando tal número não aparece é porque se trata de resultado de domínio público ou de nossa autoria.

O Capítulo 1 se destina aos leitores com menos conhecimentos em Teoria Algébrica dos Números, ao nível das referências ([13], [11]).

Introduzimos os conceitos de elemento algébrico, extensões algébricas, corpos de números, inteiro algébrico, base integral, anel dos inteiros algébricos, norma e traço de um elemento, fatoração de um ideal, norma de um ideal, entre outros.

A base integral tem sua importância no cálculo do discriminante e mostraremos este é sempre um número inteiro não nulo (Lema 1.4.1).

Com relação ao anel dos inteiros algébricos, mostraremos que este é um $\mathbb{Z}$ -módulo livre de posto n (Teorema 1.4.1) e ainda que é um anel de Dedekind (Teorema 1.7.1).

Quanto à fatoração de ideais, provaremos que o conjunto dos ideais fracionários do anel dos inteiros algébricos de um corpo K é um grupo abeliano multiplicativo (Teorema 1.7.2), e ainda, que todo ideal não nulo deste mesmo anel pode ser fatorado unicamente como um produto de ideais primos (Teorema 1.7.3).

Ainda neste capítulo, apresentamos o Lema de Kummer que será de grande importância para a decomposição de um ideal primo em uma extensão.



Por fim, definimos norma de um ideal e apresentamos alguns resultados que serão utilizados no decorrer deste trabalho.

No Capítulo 2 caracterizaremos base integral, o anel dos inteiros algébricos e o discriminante de corpos quadráticos e ciclotômicos. Também apresentaremos a decomposição de um ideal primo numa extensão galoisiana e em relação a este tipo de ideal serão definidos o grupo de decomposição e de inércia.

Definiremos ainda reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e apresentamos o Método de Minkowski (Homomorfismo Canônico), para obtenção de reticulados via representação geométrica de ideais. O Teorema 2.5.1 constitui um importante resultado deste capítulo, pois mostra que a representação geométrica de um ideal é um reticulado.

O terceiro Capítulo é dedicado aos reticulados algébricos e suas aplicações, nele empregamos toda a teoria desenvolvida nos capítulos anteriores.

O objetivo principal deste capítulo é o cálculo da densidade de centro de alguns reticulados. Nosso maior desafio no cálculo da densidade de centro está em minimizarmos uma forma quadrática, oriunda da função traço.

Iniciamos com os reticulados obtidos via representação geométrica de $\mathbb{Z}$ -módulos de anéis dos inteiros algébricos, neste calculamos a densidade de centro em dimensões 2 e 3, e em ambos os casos explicitamos uma família de reticulados cuja densidade de centro é recorde.

Em seguida estudamos os reticulados obtidos via representação geométrica de ideais, neste enfocamos a representação geométrica de ideais principais e a representação geométrica de ideais não principais, em ambos os casos calculamos a densidade de centro para alguns reticulados algébricos de posto 3.



É importante observar que a utilização dos softwares MAPLE 7, Microsoft Excel e GAP, foram indispensáveis aos cálculos aqui desenvolvidos.

Capítulo 1

Corpos de Números

O objetivo deste capítulo é introduzir conceitos básicos da Teoria Algébrica 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 às leituras que tenham conhecimentos elementares de Álgebra, que pode ser encontrado nas referências ([3], [8]).

Neste capítulo introduziremos conceitos importantes da Teoria Algébrica dos Números: seja corpo 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.

As três últimas seções serão dedicadas ao estudo da fatoração de ideais e normas de um ideal.

1.1 Elementos Algébricos sobre um Corpo

Capítulo 1

Corpos de Números

O objetivo deste capítulo é introduzir conceitos básicos da Teoria Algébrica 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 ([3], [5]).

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.

As três últimas seções serão dedicadas ao estudo da fatoração de ideais e norma de um ideal.

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 $\alpha = \sqrt{3} + \sqrt{-5}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio

$$X^4 + 4X^2 + 64 \in \mathbb{Q}[X].$$

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, 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 $K \subseteq A$. Se K é um corpo de números então $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ para finitos números algébricos $\alpha_1, \dots, \alpha_n$ (por exemplo uma base para K como espaço vetorial sobre $\mathbb{Q}$).

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:

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

e tomemos $\alpha_1 = \alpha$ e $\beta_1 = \beta$. Como os α'_i s e β'_j s são distintos, 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 racionais, logo $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$. Devemos mostrar que α e β estão em $\mathbb{Q}(\theta)$, para isto é suficiente mostrarmos 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 ζ . Se $r(\zeta) = q(\zeta)$, então ζ é um dos $\beta_1, \dots, \beta_m$ e também $\theta - c\zeta$ é um dos $\alpha_1, \dots, \alpha_n$.

Mas pela escolha de c , $\zeta = \beta$. 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 $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$, temos que $f(X) = X^2 - 3$ é o polinômio irredutível de $\sqrt{3}$ sobre $\mathbb{Q}$ e $g(X) = X^3 - 5$ é o polinômio irredutível de $\sqrt[3]{5}$ sobre $\mathbb{Q}$. As raízes de f são $\alpha_1 = \sqrt{3}$ e $\alpha_2 = -\sqrt{3}$ e as de g são $\beta_1 = \sqrt[3]{5}$, $\beta_2 = \sqrt[3]{5}\omega$ e $\beta_3 = \sqrt[3]{5}\omega^2$, 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 $K = \mathbb{Q}(\sqrt{3} + \sqrt[3]{5})$.

Proposição 1.1.1 ([7], 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 $\varphi : K(\alpha) \longrightarrow K(\beta)$, tal que $\varphi(\alpha) = \beta$.

1.2 Conjugados e Discriminantes

Em geral, dado $K = \mathbb{Q}(\theta)$ um corpo de números, 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

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

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 o polinômio (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 $\mathbb{Q}$, $\sqrt{7}$ e $-\sqrt{7}$ são os conjugados de $\sqrt{7}$, mas por outro lado $1 + \sqrt{3}$ e $\sqrt{3}$ não são $\mathbb{Q}$ -conjugados de $\sqrt{3}$. 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 7, 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 $K = \mathbb{Q}(\sqrt{11})$ um corpo de números e $\{1, \sqrt{11}\}$ uma base de K .

Então:

$$\Delta[1, \sqrt{11}] = \left(\det \begin{pmatrix} 1 & \sqrt{11} \\ 1 & -\sqrt{11} \end{pmatrix} \right)^2 = (-2\sqrt{11})^2 = 44.$$

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,

$$\Delta[\beta_1, \dots, \beta_n] = \left(\det \begin{pmatrix} \sigma_1(\beta_1) & \dots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \dots & \sigma_n(\beta_n) \end{pmatrix} \right)^2$$

$$\begin{aligned}
&= \left(\det \begin{pmatrix} \sum_{i=1}^n c_{i1}\sigma_1(\alpha_i) & \dots & \sum_{i=1}^n c_{in}\sigma_1(\alpha_i) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n c_{i1}\sigma_n(\alpha_i) & \dots & \sum_{i=1}^n c_{in}\sigma_n(\alpha_i) \end{pmatrix} \right)^2 \\
&= \left(\det \begin{pmatrix} \sum_{i=1}^n c_{i1}\sigma_1(\alpha_i) & \dots & \sum_{i=1}^n c_{i1}\sigma_n(\alpha_i) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n c_{in}\sigma_1(\alpha_i) & \dots & \sum_{i=1}^n c_{in}\sigma_n(\alpha_i) \end{pmatrix} \right)^2 \\
&= (\det(c_{ik}))^2 \cdot (\det(\sigma_i(\alpha_j)))^2 \\
&= (\det(c_{ik}))^2 \cdot \Delta[\alpha_1, \dots, \alpha_n].
\end{aligned}$$

■

Exemplo 1.2.2 Vimos no Exemplo 1.2.1 que o discriminante da base $\{1, \sqrt{11}\}$, do corpo de números $K = \mathbb{Q}(\sqrt{11})$ é 44. Agora, considerando uma outra base de K , por exemplo, $\{8 - \sqrt{11}, 5 + 3\sqrt{11}\}$, segue do Lema 1.2.1 que:

$$\Delta[8 - \sqrt{11}, 5 + 3\sqrt{11}] = \left(\det \begin{pmatrix} 8 & -1 \\ 5 & 3 \end{pmatrix} \right)^2 \cdot \Delta[1, \sqrt{11}] = 29^2 \cdot 44.$$

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

$$D = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j).$$

Assim,

$$\Delta = \left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2$$

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:

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

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:

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

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 . Dizemos que um elemento $\theta \in R$ é 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 $x = \sqrt{2} + \sqrt{3}$ e $\theta = \sqrt{-5}$ são inteiros algébricos sobre $\mathbb{Z}$.

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 $\theta \in R$, 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 temos 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, $\sqrt{2}$ e $\sqrt{3}$ são claramente inteiros algébricos. Então, pelo Teorema 1.3.1, os números, tais como, $\sqrt{2} + \sqrt{3}$, $9\sqrt{2} - 86\sqrt{3}$ e $(\sqrt{2})^3(1 + \sqrt{3})^2$, também são inteiros algébricos. E pelo Teorema 1.3.2 os zeros do polinômio

$$X^{23} - (14 + \sqrt[5]{3})X^9 + (\sqrt[3]{2})X^5 - 19\sqrt{3},$$

são inteiros algébricos.

Para todo corpo de números K escrevemos

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

e $\mathcal{O}_K$ é denominado 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, $\mathbb{Q}(\sqrt{13})$ é um corpo de números e $\sqrt{13}$ um inteiro algébrico. Mas,*

$$\frac{1 + \sqrt{13}}{2}$$

é um zero de $X^2 - X - 3 = 0$, e assim um inteiro algébrico contido em $\mathbb{Q}(\sqrt{13})$, então pertence a $\mathcal{O}_K$ e não pertence a $\mathbb{Z}[\sqrt{13}]$.

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 e 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 $\mathcal{O}_K$ pode ser 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 existe base integral, 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 's 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 $\omega_1, \dots, \omega_n$ elementos de K , com $n = [K : \mathbb{Q}]$, tais 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, o teorema a seguir nos ajuda a determinar algumas bases integrais.

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 's. Portanto $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral.

■

Exemplo 1.4.1 Em $\mathbb{Q}(\sqrt{17})$ a $\mathbb{Q}$ -base $\{1, \sqrt{17}\}$ não é base integral. De fato, um elemento de $\mathbb{Q}(\sqrt{17})$ é da forma $p + q\sqrt{17}$ para p, q racionais e tem polinômio minimal:

$$(X - p - q\sqrt{17})(X - p + q\sqrt{17}) = X^2 - 2pX + (p^2 - 17q^2)$$

Então, pelo Lema 1.3.3 $p + q\sqrt{17}$ é um inteiro algébrico se, e somente se, os coeficientes do polinômio minimal, ou seja, $2p$ e $(p^2 - 17q^2)$, são inteiros. Logo, $p = (1/2)P$, onde P é um inteiro e para P par, temos que p^2 é um inteiro, então $17q^2$ também é 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, $\mathcal{O}_K = \mathbb{Z} \left[\frac{1 + \sqrt{17}}{2} \right]$ e uma base integral é $\left\{ 1, \frac{1 + \sqrt{17}}{2} \right\}$.

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

os dois monomorfismos de $\mathbb{Q}(\sqrt{17})$ em $\mathbb{C}$ são dados por:

$$\sigma_1(p + q\sqrt{17}) = p + q\sqrt{17} \quad e \quad \sigma_2(p + q\sqrt{17}) = p - q\sqrt{17}.$$

Assim,

$$\Delta \left[1, \frac{1 + \sqrt{17}}{2} \right] = \left(\det \begin{pmatrix} \sigma_1(1) & \sigma_1 \left(\frac{1 + \sqrt{17}}{2} \right) \\ \sigma_2(1) & \sigma_2 \left(\frac{1 + \sqrt{17}}{2} \right) \end{pmatrix} \right)^2 = (-\sqrt{17})^2 = 17$$

e sendo este livre de quadrados, temos que $\left\{ 1, \frac{1 + \sqrt{17}}{2} \right\}$ 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 $K = \mathbb{Q}(\sqrt{7})$ que tem base integral $\{1, \sqrt{7}\}$ e discriminante 28, 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:

$$\begin{aligned} \Delta[\alpha_1, \dots, \alpha_n] &= (\det C)^2 \Delta[\beta_1, \dots, \beta_n] \\ &= (\pm 1)^2 \Delta[\beta_1, \dots, \beta_n] \\ &= \Delta[\beta_1, \dots, \beta_n], \end{aligned}$$

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:

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

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 algébrico 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 $Tr(\alpha)$, respectivamente.

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

$$(1) \quad Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta),$$

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

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

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

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

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. 55) *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,

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

■

Exemplo 1.5.1 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$ e $f(X) = X^3 - 2 = \text{irr}(\theta, \mathbb{Q})$. Então,

$$\Delta[1, \theta, \theta^2] = (-1)^3 N_{K/\mathbb{Q}}(3\theta^2) = -(3\theta^2)^3 = -27.4.$$

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, será utilizada a Lei do Cancelamento e então é necessário tomarmos o anel como sendo um domínio de integridade.

Sendo $r = m.n$, onde nem m ou n são unidades, então m e n são chamados fatores próprios e r 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.

Para um domínio D , temos os seguintes resultados:

- (a) x é uma unidade se, e somente se, $x \mid 1$,
- (b) x, y são associados se, e somente se, $x \mid y$ e $y \mid x$,
- (c) x é irredutível se, e somente se, todo divisor de x é um associado de x ou uma unidade,
- (d) $x \mid y$ se, e somente se, $\langle x \rangle \supseteq \langle y \rangle$.

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

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

Proposição 1.6.2 ([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 , e segue que:

- (i) $r=s$.
- (ii) 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 nos mostra que o mesmo não ocorre para a fatoração de ideais principais no anel dos inteiros algébricos $\mathcal{O}_K$.

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 $a^2 \equiv \pm 2 \pmod{5}$, 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

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

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, nos 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

$$\mathfrak{a}_1 = \mathfrak{a} + \mathfrak{b} \quad \text{e} \quad \mathfrak{a}_2 = \mathfrak{a} + \mathfrak{c}.$$

Então, $\mathfrak{a}_1 \mathfrak{a}_2 = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a}$, $\mathfrak{a}_1 \supsetneq \mathfrak{a}$ e $\mathfrak{a}_2 \supsetneq \mathfrak{a}$.

Pela maximalidade de $\mathfrak{a}$ existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \dots, \mathfrak{p}_r$, tais que,

$$\mathfrak{p}_1 \dots \mathfrak{p}_s \subseteq \mathfrak{a}_1 \quad \text{e} \quad \mathfrak{p}_{s+1} \dots \mathfrak{p}_r \subseteq \mathfrak{a}_2.$$

Assim,

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a},$$

o que contraria a escolha de $\mathfrak{a}$.

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

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

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

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

De fato:

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

Então,

$$n_1\mathfrak{a} + n_2\mathfrak{a} = (n_1 + n_2)\mathfrak{a}.$$

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

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

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

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

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

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

$$(x\mathfrak{a})y = x(\mathfrak{a}y) = x\mathfrak{a} \subseteq \mathcal{O}_K.$$

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 $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ 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 $\mathfrak{a}^{-1}$,

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1},$$

ou,

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1}.$$

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

concluimos 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 $\mathfrak{p}_i$'s 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 ([6], 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 ([6], 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 $\mathcal{O}_K \cap \mathfrak{q}$. Sabemos que $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ (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) ([6], 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:*

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

Lema 1.7.1 (Lema de Kummer) ([1], pag. 186) *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:

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

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:

$$N(\langle 25 \rangle) = 25^2.$$

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

Teorema 1.8.2 ([13], 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 ([13], 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 $K = \mathbb{Q}(\sqrt{-13})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$, o seu anel dos inteiros algébricos, $\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-13} \rangle$ 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, $\mathcal{O}_K = \mathbb{Z}[\sqrt{i}]$, $\mathfrak{a} = \langle 7 \rangle$. Aqui, 7 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, $\langle 7 \rangle$ é um ideal primo em $\mathbb{Z}[i]$, mas

$$N(\langle 7 \rangle) = |N(7)| = 7^2.$$

2.1 Corpos Quadráticos

Chamamos corpo quadrático a qualquer corpo de números de grau 2, o qual tem as seguintes propriedades:

Capítulo 2

Corpos Quadráticos e Ciclotômicos

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) caracterizamos os polinômios ciclotômicos, apresentando uma base integral e o cálculo do discriminante.

Em seguida, apresentamos alguns resultados que serão relevantes para o desenvolvimento das aplicações acima citadas. 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 2.1.2 ([13], pag. 67) *Sejam d um número inteiro livre de quadrados, $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}_K$ o anel dos inteiros algébricos de K . Então $\mathbb{O}_K = \mathbb{Z}[\alpha]$, onde*

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

2.1 Corpos Quadráticos

Chamamos corpo quadrático a qualquer corpo de números de grau 2, o qual 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:

$$X^2 - d, \text{ se } d \equiv 2 \text{ ou } 3 \pmod{4};$$

$$X^2 - X + \frac{1-d}{4}, \text{ se } d \equiv 1 \pmod{4}.$$

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 é um número inteiro, 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 $2r$ e $r^2 - ds^2$ são inteiros, consequentemente $4r^2 - 4ds^2 \in 4\mathbb{Z}$, donde segue que, $(2r)^2 - d(2s)^2 \in 4\mathbb{Z} \subset \mathbb{Z}$. Visto que $2r$ é inteiro, segue que $d(2s)^2$ também o é. Mostremos que $2s$ é um número inteiro.

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 $d(2s)^2$ é inteiro, 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, $2s$ é inteiro.

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

$$\gamma = \frac{u}{2} + \frac{v}{2}\sqrt{d}, \quad (2.2)$$

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:

$$\gamma = \frac{v+2t}{2} + \frac{v}{2}\sqrt{d} = t + v \left(\frac{1+\sqrt{d}}{2} \right) \in \mathbb{Z}[\alpha],$$

e portanto, $\mathcal{O}_K = \mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right]$.

■

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

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

Assim temos o seguinte cálculo para o discriminante:

Teorema 2.1.3 ([19], pag. 68)

- (i) Se $d \equiv 2$ ou $3 \pmod{4}$ então $\mathbb{Q}(\sqrt{d})$ tem discriminante 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:

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix} = (-2\sqrt{d})^2 = 4d$$

e

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

■

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,

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

Assim,

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

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

$$N(a + b\sqrt{d}) = a^2 - db^2;$$

$$Tr(a + b\sqrt{d}) = 2a.$$

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 $d < 0$.

Nos exemplos seguintes, mostraremos a fatoração em irredutíveis, 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:

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

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, $2 = x.y$, onde $x, y \in \mathcal{O}_K$, e não são unidades, então $4 = N(2) = N(x).N(y)$. 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 $N(2) = 4$, $N(1 + \sqrt{-5}) = 6$, do item (b) da Proposição 1.6.2 segue que 2 não é associado de $1 + \sqrt{-5}$ ou $1 - \sqrt{-5}$, e portanto a fatoração é única.

Exemplo 2.1.3 Sejam $K = \mathbb{Q}(\sqrt{11})$, $X^2 - 11$ o polinômio irredutível de $\sqrt{11}$ sobre $\mathbb{Q}$ e $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$ seu anel dos inteiros algébricos. Consideremos o ideal $5\mathbb{Z} \subset \mathbb{Z}$, temos que o polinômio $X^2 - 11$ fatora-se como:

$$X^2 - 11 \equiv (X + 1) \cdot (X + 4) \pmod{5\mathbb{Z}[X]}.$$

Assim, pelo Lema de Kummer, temos:

- (a) $\mathfrak{p}_1 = \langle 5, \theta + 1 \rangle$ e $\mathfrak{p}_2 = \langle 5, \theta + 4 \rangle$ são os ideais de $\mathcal{O}_K$ acima de $5\mathbb{Z}$,
- (b) $5\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$,
- (c) $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_1} : \frac{\mathbb{Z}}{5\mathbb{Z}} \right] = \left[\frac{\mathcal{O}_K}{\mathfrak{p}_2} : \frac{\mathbb{Z}}{5\mathbb{Z}} \right] = 1 = f_1 = f_2$.

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

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 $\Phi_n(X)$ é um polinômio mônico em $\mathbb{Z}[X]$, de grau $\phi(n)$, onde ϕ é a função de Euler.

Lema 2.2.1 ([7], 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 , $r > 1$, 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,

$$\Phi_{p^r}(X) = X^{p^{r-1} \cdot (p-1)} + X^{p^{r-1} \cdot (p-2)} + \dots + X^{p^{r-1}} + 1.$$

Obtemos o polinômio Φ_{15} da igualdade:

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

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

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

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



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

Lema 2.2.3 ([7], pag. 114) *Seja n um inteiro positivo. Então n -ésimo polinômio ciclotômico Φ_n tem coeficientes inteiros.*

Demonstração:

Faremos a demonstração por indução sobre n . Para $n = 1$, temos que o polinômio ciclotômico $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Suponhamos, então, 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 $f(X) \in \mathbb{Z}[X]$.

Notemos que:

$$X^n - 1 \in \mathbb{Z}[X] \subset \mathbb{Q}[X] \quad \text{e} \quad f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X].$$

Assim, pelo Lema 2.2.2, segue que, $\Phi_n(X) \in \mathbb{Q}[X]$. Logo, pelo Lema de Gauss 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 $\Phi_d(X)$ também o é. Portanto $\Phi_n(X) \in \mathbb{Z}[X]$.

Lema 2.2.4 ([7], pag. 116) *Seja n um inteiro positivo. Então o n -ésimo polinômio ciclotômico $\Phi_n(X)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração:

Seja $f(X) = irr(\xi_n, \mathbb{Q})$. 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 $p \mid k \implies k = p \cdot r$, assim,

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

onde $\bar{a}$ denota a classe de a em $\frac{\mathcal{O}_K}{\mathfrak{p}}$. Logo,

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

Pelo Pequeno Teorema de Fermat ([5], pag. 44), temos que $a^p \equiv a \pmod{p}$, assim,

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

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

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

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

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

Vimos no Lema 2.2.1 que

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

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

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

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 função ϕ de Euler é caracterizada por:

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

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:

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



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,

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

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:

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

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

$$\begin{aligned} \text{Tr}\left(\sum_{i=0}^{p-2} a_i \xi_p^i\right) &= \sum_{i=0}^{p-2} \text{Tr}(a_i \xi_p^i) = \text{Tr}(a_0) + \sum_{i=1}^{p-2} \text{Tr}(a_i \xi_p^i), \\ &= (p-1)a_0 - \sum_{i=0}^{p-2} a_i, = pa_0 - \sum_{i=0}^{p-2} a_i. \end{aligned}$$

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: Por (2.9) temos : $p = (1 - \xi_p)(1 - \xi_p^2) \dots (1 - \xi_p^{p-1})$. 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 ([4], 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], pags. 72, 74) (a) O anel dos inteiros algébricos de $K = \mathbb{Q}(\xi_p)$ é $\mathbb{Z}[\xi_p]$.

(b) O discriminante de $\mathbb{Q}(\xi_p)$, onde p é 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 ([15], 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 : 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,

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

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

$$\vdots$$

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

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 $\det M_i = \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$, pelo Lema 1.3.4. Vimos que,

$$\text{irr}(\xi_{p^a}, \mathbb{Q}) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \dots + X^{p^{a-1}} + 1, \quad (2.10)$$

logo, $m = \phi(p^a) = p^{a-1}(p-1)$. Sejam $\mathfrak{p} = (1 - \xi_{p^a})\mathcal{O}_L$, $x \in \mathfrak{p}$, x não nulo, 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:

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

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,

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

Logo, $s \cdot m + v_{\mathfrak{p}}(\alpha) = i_0 < m$. Sendo $v_{\mathfrak{p}}(\alpha) \geq 0$, 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,

$$m = [\mathbb{Q}(\xi_n) : K], \quad \mathbb{Q}(\xi_n) = K[\xi_{q^b}] \text{ e } K = \mathbb{Q}(\xi_{p^a g}),$$

$n = p^a \cdot q^b \cdot g$; $p \nmid g$, $q \nmid g$. 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, $\xi_n = \xi_{q^b}^i \cdot \xi_{p^a}^j$, pois, $n = p^a \cdot q^b \cdot g$, com $(p^a g, q^b) = 1$, logo, pela Identidade de Bezout, existem i, j inteiros, tais que:

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

Assim, $\xi_n = \xi_{p^a g q^b}^{i(p^a g) + jq^b} = \xi_{q^b}^i \cdot \xi_{p^a}^j$. 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 os $a'_i s \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$. 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, $a_i \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$. Logo, o anel dos inteiros algébricos de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$.

■

Teorema 2.2.3 ([15], 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 $\mathbb{Q}(\xi_{36})$ é $2^{12} \cdot 3^{18}$, a menos de sinal.*

2.3 Corpos de Números Abelianos

Dizemos que um corpo de números K é abeliano, se K é uma extensão galoisiana dos racionais e seu grupo de galois é abeliano.

Nos restringiremos ao estudo dos corpos de números abelianos, pois são nesses corpos que obtemos um maior número de ferramentas que serão de grande utilidade nos cálculos desenvolvidos no capítulo seguinte.

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.

Teorema 2.3.1 ([15], pag. 319) *Se $K/\mathbb{Q}$ é uma extensão finita abeliana, então $K \subseteq \mathbb{Q}(\xi_n)$.*

O cálculo do discriminante é definido, originalmente, sobre uma base integral, cuja obtenção é, geralmente, um problema complexo. Porém, existem resultados que fazem este cálculo sem o uso da base integral. Enunciaremos a seguir um deles, o qual é consequência do Teorema do Condutor-Discriminante.

Teorema 2.3.2 ([8], 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,

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

O resultado a seguir será muito importante para os exemplos do próximo capítulo.

Teorema 2.3.3 ([14], 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 $\mathbb{Z}\sigma_g(\theta) + \dots + \mathbb{Z}\sigma_{g^s}(\theta)$ é o anel dos inteiros algébricos de K . Além disso,*

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

Demonstração:

Mostremos inicialmente 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,

$$\begin{aligned} \sigma_{g^i}(\theta) &= \sigma_{g^i}(\xi_p^{g^s} + \dots + \xi_p^{g^{rs}}) = \sigma_{g^i}(\xi_p^{g^s}) + \dots + \sigma_{g^i}(\xi_p^{g^{rs}}) \\ &= (\xi_p^{g^s})^{g^i} + \dots + (\xi_p^{g^{rs}})^{g^i} = \xi_p^{g^{s+i}} + \dots + \xi_p^{g^{rs+i}}, \end{aligned}$$

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,

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

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:

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

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

Trataremos nesta subseção, o problema geral de determinar como um ideal primo de um anel dos inteiros algébricos se fatora numa extensão de corpos galoisiana.

Teorema 2.3.4 (Teorema da Evidência) ([6], pag. 70) *Dados L/K uma extensão galoisiana com grupo de Galois G e $\mathfrak{q}, \mathfrak{q}'$ dois ideais primos de 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:

$$\begin{cases} X \equiv 0 \pmod{\mathfrak{q}'} \\ X \equiv 1 \pmod{\sigma(\mathfrak{q})}, \end{cases}$$

para todo $\sigma \in G$. Seja $\alpha \in \mathcal{O}_L$, a tal solução, desse modo,

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

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 ([6], pag. 71) *Sejam L/K uma extensão galoisiana e $\mathfrak{q}, \mathfrak{q}'$ 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, suponhamos que $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Assim,

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

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

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

Defina,

$$\begin{aligned} \tilde{\sigma} : \frac{\mathcal{O}_L}{\mathfrak{q}_1} &\rightarrow \frac{\mathcal{O}_L}{\mathfrak{q}_2} \\ x + \mathfrak{q}_1 &\mapsto \tilde{\sigma}(x + \mathfrak{q}_1) = \sigma(x) + \mathfrak{q}_2. \end{aligned}$$

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

$$\left[\frac{\mathcal{O}_L}{\mathfrak{q}_1} : \frac{\mathcal{O}_K}{\mathfrak{p}} \right] = \left[\frac{\mathcal{O}_L}{\mathfrak{q}_2} : \frac{\mathcal{O}_K}{\mathfrak{p}} \right],$$

donde segue que $f_1 = f_2$.

■

O corolário acima nos mostra que no caso de uma extensão galoisiana, um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ fatora-se em $(\mathfrak{q}_1 \dots \mathfrak{q}_g)^e$ em $\mathcal{O}_L$, onde os $\mathfrak{q}_i$'s são os ideais primos distintos acima de $\mathfrak{p}$, todos tendo o mesmo grau residual f sobre $\mathfrak{p}$. E mais, pelo Teorema da Igualdade Fundamental, $n = [L : K] = g.e.f$.

Exemplo 2.3.1 Seja $K = \mathbb{Q}(\xi_{65})$, segue do Teorema 2.2.2, que o anel dos inteiros algébricos de K é $\mathbb{Z}[\xi_{65}]$. O polinômio minimal de ξ_{65} sobre $\mathbb{Q}$ é dado por:

$$\Phi_{65}(X) = X^{48} - X^{47} + X^{43} - X^{42} + X^{38} - X^{37} + \dots + X^5 - X + 1.$$

A decomposição do ideal $13\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ satisfaz:

$$\Phi_{65}(X) \equiv (X^4 + X^3 + X^2 + X + 1)^{12} \pmod{13\mathbb{Z}},$$

onde,

$$p(X) = X^4 + X^3 + X^2 + X + 1.$$

Assim, pelo Lema de Kummer temos:

- (a) $\mathfrak{p} = \langle 13, p(\xi_{65}) \rangle = 13\mathcal{O}_K + p(\xi_{65})\mathcal{O}_K$; é o ideal primo de $\mathcal{O}_K$ acima de $13\mathbb{Z}$,
- (b) $13\mathcal{O}_K = \mathfrak{p}^{12}$,
- (c) $\left[\frac{\mathcal{O}_K}{\mathfrak{p}} : \frac{\mathbb{Z}}{13\mathbb{Z}} \right] = 4$. Assim, temos $g = 1$, $e = 12$, $f = 4$ e $48 = g.e.f = 1.12.4$.

Sejam K_1 e K_2 corpos linearmente disjuntos (isto é, $K_1 \cap K_2 = \mathbb{Q}$). Dado um número primo p por ([6]) 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_i , e_i e f_i 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:

$$g = g_1g_2, e = e_1e_2 \text{ e } f = f_1f_2.$$

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

Para cada ideal primo $\mathfrak{q}$ acima de $\mathfrak{p}$, definimos dois grupos de G :

O grupo de decomposição

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

e o grupo inercial

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

Ambos são subgrupos de G e $E \subset G$, pois para $X \in \mathfrak{q}$, temos que, $X \equiv 0 \pmod{\mathfrak{q}}$, assim $\sigma(X) \equiv X \pmod{\mathfrak{q}}$, então, $\sigma(X) \equiv 0 \pmod{\mathfrak{q}}$, e 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 $\mathfrak{p}$, temos que:

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

Logo, se D é normal a G , para algum $\mathfrak{q}$, então,

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

Em particular, quando G é um grupo abeliano, $D(\mathfrak{p}_i)$ depende apenas de $\mathfrak{p}$, assim denotaremos apenas por $D(\mathfrak{p})$. 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 $\mathcal{O}_L \longrightarrow \frac{\mathcal{O}_L}{\mathfrak{q}}$ 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, se 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 $\psi : D \longrightarrow \tilde{G}$. 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 $\psi : D \longrightarrow \tilde{G}$ é sobrejetiva, assim $\frac{D}{E} \longrightarrow \tilde{G}$ é de fato um isomorfismo de grupos. Sabemos que $\tilde{G}$ 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 denominado corpo de decomposição e L_E corpo inercial.

Exemplo 2.3.2 Sejam $L = \mathbb{Q}(\xi_{15})$. Assim pelo Teorema 2.2.2 $\mathcal{O}_L = \mathbb{Z}(\xi_{15})$ e o polinômio minimal de ξ_{15} sobre $\mathbb{Q}$ é:

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

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,

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

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

e do Lema de Kummer, segue que:

(a) $\mathfrak{p}_i = \langle 7, p_i(\xi_{15}) \rangle = 7\mathcal{O}_L + p_i(\xi_{15})\mathcal{O}_L$; $i = 1, 2$, 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) $\left[\frac{\mathcal{O}_L}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{7\mathbb{Z}} \right] = 4$; $i = 1, 2$.

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:

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

e verificamos que, $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são conjugados, por exemplo, $\sigma_2(\mathfrak{p}_1) = \mathfrak{p}_2$ e $\sigma_2(\mathfrak{p}_2) = \mathfrak{p}_1$. Logo $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são ideais primos conjugados que tem 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:

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

Como,

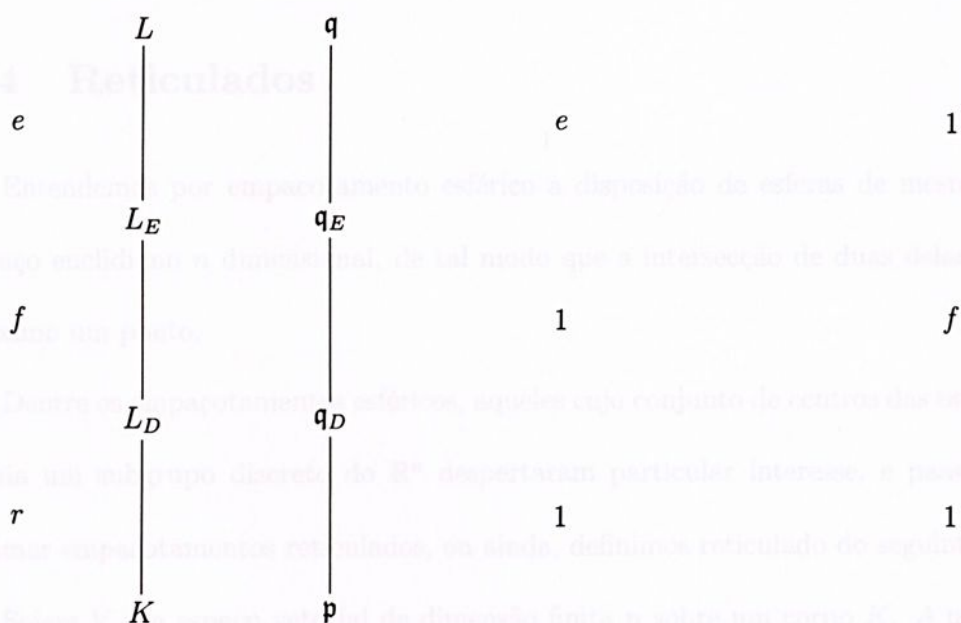
$$\# E(7\mathbb{Z}) = 4 \text{ e } E(7\mathbb{Z}) \subset D(7\mathbb{Z}),$$

temos,

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

Teorema 2.3.5 ([6], pag. 100) *Sejam $L, K, \mathcal{O}_K, \mathcal{O}_L, \mathfrak{p}, \mathfrak{q}, G, D, E, e, f$ e g como anteriormente. Então temos o seguinte diagrama:*

grau índice de ramificação grau de inércia



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 de $\mathcal{O}_{K'}$ abaixo de $\mathfrak{q}$.

Teorema 2.3.6 ([6], 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, $e(\mathfrak{q} | \mathfrak{p}') = [L : K']$).

Exemplo 2.3.3 Como vimos no exemplo 2.3.2, $e = 1$, $f = 4$ e $g = 2$. Logo, pelo Teorema 2.3.6, segue que:

$$L_D = \mathbb{Q}(\xi_3) \subset \mathbb{Q}(\xi_{15}) \text{ e } f(\mathfrak{q}_D | \mathfrak{p}) = e(\mathfrak{q}_D | \mathfrak{p}) = 1.$$

2.4 Reticulados

Entendemos por empacotamento esférico a disposição de esferas de mesmo raio no espaço euclidiano n dimensional, de tal modo que a intersecção de duas delas tenha no máximo um ponto.

Dentre os empacotamentos esféricos, aqueles cujo conjunto de centros das esferas constitua um subgrupo discreto do $\mathbb{R}^n$ despertaram particular interesse, e passaram a se chamar empacotamentos reticulados, ou ainda, definimos reticulado do seguinte modo:

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 independentes de V . Damos o nome de A -reticulado (ou simplesmente reticulado), com base $(v_1, \dots, v_r)$, ao conjunto de elementos da forma:

$$x = a_1 v_1 + \dots + a_r v_r, \text{ com } a_i \in A.$$

Doravante, em qualquer citação de reticulado, vamos supor que $K = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $r = n$.

Exemplo 2.4.1 Seja $\Lambda = \mathbb{Z}^2$. Temos que Λ é um reticulado, gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$.

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 o contrário, a partir de agora todos os empacotamentos considerados serão reticulados, e quando o conjunto de centros for A , dizemos que o empacotamento é associado a A . 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

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

é denominado 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 de uma Região Fundamental, e denotaremos por $v(\Lambda)$.

Este trabalho tem como objetivo tratar de empacotamentos associados ao reticulado Λ cujas esferas tenham raio máximo. Logo, o maior raio possível para distribuir esferas

centradas em cada ponto do reticulado Λ e obter um empacotamento é denominado raio de empacotamento (ρ), e é dado por:

$$\rho = \frac{\Lambda_{\min}}{2},$$

onde $\Lambda_{\min} = \min\{|v|; v \in \Lambda, v \neq 0\}$. É importante observarmos que ρ é o maior raio com 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 esferas de raio ρ , associado a um reticulado, estamos citando a densidade de um reticulado Λ , a qual denotaremos por $\Delta(\Lambda)$ e esta é dada 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. Assim, a densidade de um empacotamento reticulado Λ é dada por:

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

A fração que se destaca é outro parâmetro importante em empacotamentos reticulados, denominada densidade de centro, cuja expressão é dada por:

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

Exemplo 2.4.2 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 2.4.3 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 valor mínimo 1, quando algum dos $x_i = 1$, para $i = 1, \dots, n$ e os demais são todos nulos. Assim, $\rho = \frac{1}{2}$. Como $v(\Lambda) = |\det M|$, e M neste caso é a matriz identidade, então $v(\Lambda) = 1$ e portanto, $\delta(\Lambda) = \frac{1}{2^n}$.

2.5 O Homomorfismo Canônico

O propósito desta seção é apresentar o método de imersão de um corpo de números K no espaço euclidiano, de tal modo que ideais em $\mathcal{O}_K$ correspondam a reticulados neste espaço.

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 $\mathbb{C}$. Dizemos que um monomorfismo σ_i é real, se $\sigma_i(K) \subseteq \mathbb{R}$, caso contrário, dizemos que σ_i é imaginário. Um corpo K é denominado totalmente real, quando todos seus monomorfismos são reais, e K é denominado totalmente imaginário quando todos seus monomorfismos são imaginários.

Agora definiremos o homomorfismo canônico para o caso geral. Sejam 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 $K = \mathbb{Q}(\alpha)$, 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 em $\mathbb{R}^4$ de acordo com,

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

Exemplo 2.5.2 Sejam $K = \mathbb{Q}(\sqrt{7})$ com $\mathbb{Q}$ -base $\{1, \sqrt{7}\}$ e os monomorfismos de K em $\mathbb{C}$, σ_1 e σ_2 , que são, respectivamente, a inclusão e a conjugação complexa, isto é,

$$\sigma_2(a + b\sqrt{7}) = a - b\sqrt{7}; \quad a, b \in \mathbb{Q}.$$

Então, para $x = a + b\sqrt{7} \in K$, $a, b \in \mathbb{Q}$, temos:

$$\sigma(x) = (\sigma_1(x), \sigma_2(x)) = (a + b\sqrt{7}, a - b\sqrt{7}).$$

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. O Teorema a seguir representa um dos principais resultados desse capítulo.

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,

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

e pelo Teorema 1.2.3, $\Delta[x_1, \dots, x_n] \neq 0$. Assim $\det D \neq 0$, 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 seguinte 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 $\bar{\sigma}_i = \sigma_{r_2+i}$, 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 , e 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 $\mathfrak{a}$ também é um $\mathbb{Z}$ -módulo livre de posto n . 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 $K = \mathbb{Q}(\sqrt{19})$ e $\mathcal{O}_K = \mathbb{Z}[\sqrt{19}]$ o anel dos inteiros algébricos de K , com base $\{1, \sqrt{19}\}$. Sendo $r_2 = 0$, temos:

$$v(\sigma_K(\mathcal{O}_K)) = \left| \det \begin{pmatrix} 1 & \sqrt{19} \\ 1 & -\sqrt{19} \end{pmatrix} \right| = |-2\sqrt{19}| = 2\sqrt{19}.$$

Exemplo 2.5.4 Sejam $K = \mathbb{Q}(\sqrt{-7})$ e $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ o anel dos inteiros algébricos de K , com base $\{1, \frac{1+\sqrt{-7}}{2}\}$. Sendo $r_2 = 1$, temos:

$$v(\sigma_K(\mathcal{O}_K)) = 2^{-1} \left| \det \begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix} \right| = \frac{1}{2} |-\sqrt{-7}| = \frac{1}{2} |\sqrt{7}i| = \frac{\sqrt{7}}{2}.$$

Exemplo 2.5.5 Mais geralmente, sejam $K = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e

$$\sigma_K: \mathcal{O}_K \rightarrow \mathbb{R}^2$$

$$x \mapsto \sigma_K(x)$$

o homomorfismo canônico, então $M \subset \mathcal{O}_K$ é um $\mathbb{Z}$ -módulo de posto 2.

Suponhamos que $M = \mathcal{O}_K = \mathbb{Z}e_1 + \mathbb{Z}e_2$, então,

$$\sigma_K(M) = \mathbb{Z}\sigma_K(e_1) + \mathbb{Z}\sigma_K(e_2) \subset \mathbb{R}^2.$$

Consideremos os casos:

(1) $d > 0$, $d \equiv 2$ ou $3 \pmod{4}$.

Pelo Teorema 2.1.2, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Logo

$$\begin{aligned}\sigma_K : \quad \mathcal{O}_K &\longrightarrow \mathbb{R}^2 \\ a + b\sqrt{d} &\longmapsto (a + b\sqrt{d}, a - b\sqrt{d})\end{aligned}$$

Neste caso, $M = \mathbb{Z}e_1 + \mathbb{Z}e_2 = \mathbb{Z}.1 + \mathbb{Z}\sqrt{d}$

$$\sigma_K(a + b\sqrt{d}) = \sigma_K(1) = \sigma_K(1 + 0\sqrt{d}) = (1, 1)$$

$$\sigma_K(a + b\sqrt{d}) = \sigma_K(\sqrt{d}) = \sigma_K(0 + 1\sqrt{d}) = (\sqrt{d}, -\sqrt{d}).$$

Portanto, $\sigma_K(M) = \mathbb{Z}(1, 1) + \mathbb{Z}(\sqrt{d}, -\sqrt{d})$. Sejam $v_1 = (1, 1)$ e $v_2 = (\sqrt{d}, -\sqrt{d})$. Logo,

$$v(\sigma_K(M)) = \left| \det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix} \right| = |-2\sqrt{d}| = 2\sqrt{d}.$$

Temos que $v = (a + b\sqrt{d}, a - b\sqrt{d})$. Assim a forma quadrática $|v|^2 = 2(a^2 + db^2)$, assume valor mínimo 2 quando $a = 1$ e $b = 0$. Logo $|v| = \sqrt{2}$, donde segue que $\rho = \frac{\sqrt{2}}{2}$.

Portanto

$$\delta(\sigma_K(M)) = \frac{\rho^2}{v(\sigma_K(M))} = \frac{\left(\frac{\sqrt{2}}{2}\right)^2}{2\sqrt{d}} = \frac{1}{4\sqrt{d}}.$$

(2) $d < 0$, $d \equiv 1 \pmod{4}$.

Pelo Teorema 2.1.2, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$. Logo,

$$\begin{aligned}\sigma_K : \quad \mathcal{O}_K &\longrightarrow \mathbb{R}^2 \\ a + b\left(\frac{1+\sqrt{-d}}{2}\right) &\longmapsto \left(\frac{2a+b}{2}, \frac{b\sqrt{-d}}{2}\right)\end{aligned}$$

Neste caso, $M = \mathbb{Z}e_1 + \mathbb{Z}e_2 = \mathbb{Z}.1 + \mathbb{Z}\left(\frac{1+\sqrt{-d}}{2}\right)$, e

$$\sigma_K\left(a + b\left(\frac{1+\sqrt{-d}}{2}\right)\right) = \sigma_K(1) = (1, 0)$$

$$\sigma_K\left(a + b\left(\frac{1+\sqrt{-d}}{2}\right)\right) = \sigma_K\left(\frac{1+\sqrt{-d}}{2}\right) = \left(\frac{1}{2}, \frac{\sqrt{-d}}{2}\right).$$

Portanto, $\sigma_K(M) = \mathbb{Z}(1, 0) + \mathbb{Z}\left(\frac{1}{2}, \frac{\sqrt{-d}}{2}\right)$. Sejam $v_1 = (1, 0)$ e $v_2 = \left(\frac{1}{2}, \frac{\sqrt{-d}}{2}\right)$. Logo,

$$v(\sigma_K(M)) = \left| \det \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{-d}}{2} \end{pmatrix} \right| = \frac{\sqrt{-d}}{2}.$$

Temos que, $v = \left(\frac{2a+b}{2}, \frac{b\sqrt{-d}}{2}\right)$. Assim a forma quadrática $|v|^2 = (a + \frac{b}{2})^2 - \frac{db^2}{4}$, assume valor mínimo 1 quando $a = 1$ e $b = 0$. Logo $|v| = 1$, donde segue que $\rho = \frac{1}{2}$.

Portanto,

$$\delta(\sigma_K(M)) = \frac{\rho^2}{v(\sigma_K(M))} = \frac{\left(\frac{1}{2}\right)^2}{\frac{\sqrt{-d}}{2}} = \frac{1}{2\sqrt{-d}}.$$

Analogamente, para os casos:

(3) $d < 0$, $d \equiv 2$ ou $3 \pmod{4}$.

$$\delta(\sigma_K(M)) = \frac{1}{4\sqrt{-d}}.$$

(4) $d > 0$, $d \equiv 1 \pmod{4}$.

$$\delta(\sigma_K(M)) = \frac{1}{4\sqrt{d}}.$$

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,

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |D_K|^{1/2} \cdot N(\mathfrak{a}).$$

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, que:

$$v(\sigma_K(\mathfrak{a})) = |\det D|,$$

sendo

$$|\det D| = 2^{-r_2} \cdot |\det(\sigma_i(x_j))|. \quad (2.12)$$

Por outro lado, do Teorema 1.8.1, temos:

$$N(\mathfrak{a}) = \left| \frac{\Delta[x_1, \dots, x_n]}{D_K} \right|^{1/2},$$

assim,

$$|\Delta[x_1, \dots, x_n]|^{1/2} = |D_K|^{1/2} \cdot N(\mathfrak{a}), \quad (2.13)$$

e

$$\Delta[x_1, \dots, x_n] = (\det(\sigma_i(x_j)))^2. \quad (2.14)$$

Substituindo (2.14) em (2.13), vem:

$$|\det(\sigma_i(x_j))|^2^{1/2} = |D_K|^{1/2} \cdot N(\mathfrak{a}),$$

donde segue que,

$$|\det(\sigma_i(x_j))| = |D_K|^{1/2} \cdot N(\mathfrak{a}), \quad (2.15)$$

E por fim, substituindo (2.15) em (2.12), temos,

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |D_K|^{1/2} \cdot N(\mathfrak{a}).$$

■

Observação 2.5.1 De Teorema anterior, a expressão para a densidade de centro do reticulado $\sigma_K(\mathfrak{a})$ é dada por:

$$\delta(\sigma_K(\mathfrak{a})) = \frac{2^{r_2} \rho^n}{|D_K|^{1/2} \cdot N(\mathfrak{a})}.$$

Exemplo 2.5.6 Para $K = \mathbb{Q}(\sqrt{10})$, pelos Teoremas 2.1.2 e 2.1.3, temos respectivamente,

$\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ e $D_K = 40$. Dado $\alpha = a + b\sqrt{10} \in \mathcal{O}_K$, 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 2.5.7 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,

$$\alpha\bar{\alpha} = \left(a - \frac{25b}{2} \right)^2 + 2 \left(a - \frac{25b}{2} \right) \left(\frac{-b}{2} - 2a \right) \sqrt{13} + 13 \left(\frac{-b}{2} - 2a \right)^2.$$

Assim,

$$|\sigma_K(\alpha)|^2 = \text{Tr}_{K/\mathbb{Q}}(\alpha\bar{\alpha}) = 2 \left[\left(a - \frac{25b}{2} \right)^2 + 13 \left(\frac{-b}{2} - 2a \right)^2 \right],$$

atribuindo valores inteiros, não todos 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 Reticulados Algébricos

Capítulo 3

Reticulados Algébricos e Aplicações

O objetivo deste capítulo é o cálculo a densidade de centro de alguns reticulados algébricos. Visto que se trata de um capítulo de aplicações, alguns resultados serão demonstrados.

Iniciaremos com o estudo dos reticulados algébricos obtidos via representação geométrica de $\mathbb{Z}$ -módulos dos anéis dos inteiros algébricos e devido à complexidade em minimizarmos a forma quadrática, obtida a partir da função traço, faremos exemplos e em dimensões 2 e 3, e em ambos os casos explicitaremos uma "família" de reticulados cuja densidade de centro é recorde.

Em seguida, estudaremos os reticulados algébricos obtidos via representação geométrica de ideais, neste enfocamos a representação geométrica de ideais principais e não principais. Convém ressaltar que o Lema de Kummer é extremamente importante para determinar tais ideais, pois fornece meios de encontrarmos ideais não principais.

3.1 Reticulados Algébricos

Sejam $K/\mathbb{Q}$ uma extensão galoisiana de grau n , $G = \text{Gal}(K, \mathbb{Q})$, G abeliano, $K = \mathbb{Q}(\alpha)$ e $f(X) = \text{irr}(\alpha, \mathbb{Q}) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$. Consideraremos os casos K totalmente real e K totalmente imaginário.

3.1.1 K é Totalmente Real

Sejam $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$, $v_i = (\sigma_i(\alpha_1), \sigma_i(\alpha_2), \dots, \sigma_i(\alpha_n))$; $i = 1, \dots, n$ e

$$\Lambda_f = \left\{ \sum_{i=1}^n a_i v_i; a_i \in \mathbb{Z} \right\}.$$

Notemos que Λ_f nem sempre é um reticulado de posto n .

Exemplo 3.1.1 *Sejam $K = \mathbb{Q}(\sqrt{2})$ e $f(X) = \text{irr}(\sqrt{2}, \mathbb{Q})$. Logo, as raízes de $f(X)$ são $\alpha_1 = \sqrt{2}$ e $\alpha_2 = -\sqrt{2}$ e $G = \{\sigma_1, \sigma_2\}$, onde σ_1 é a inclusão e σ_2 é a conjugação. Notemos que v_1 e v_2 são linearmente dependentes. Portanto Λ_f não é um reticulado de posto 2.*

Exemplo 3.1.2 *Seja $K = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2})$. Nesse caso, $f(X) = \text{irr}(1 + \sqrt{2}, \mathbb{Q})$ e, então, as raízes de $f(X)$ são $\alpha_1 = 1 + \sqrt{2}$ e $\alpha_2 = 1 - \sqrt{2}$ e $G = \{\sigma_1, \sigma_2\}$, onde σ_1 é a inclusão e σ_2 é a conjugação. Logo, $\det(M) = (1 + \sqrt{2})^2 - (1 - \sqrt{2})^2 = 4\sqrt{2} \neq 0$. Portanto, Λ_f é um reticulado de posto 2.*

Em nosso trabalho, estaremos interessados nos casos em que Λ_f é um reticulado.

Lema 3.1.1 *Sejam $K = \mathbb{Q}(\alpha_1)$ uma extensão abeliana, $f(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0$, com $a_i \in \mathbb{Z}$, $\alpha_i; i = 1, \dots, n$ as raízes de f , Λ_f um reticulado de posto n , como definido anteriormente, e $v \in \Lambda_f$, tal que $v = X_1 v_1 + \dots + X_n v_n$; $X_i \in \mathbb{Q}$.*

Então,

$$|v|^2 = Q(X_1, \dots, X_n) = (a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^n X_i^2 + 2 \sum_{1 \leq i < j \leq n} \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) X_i X_j, \quad (3.0)$$

Demonstração:

Temos que,

$$|v|^2 = v.v = \left(\sum_{i=1}^n X_i v_i \right) \left(\sum_{j=1}^n X_j v_j \right) = \sum_{i=1}^n v_i v_i X_i^2 + 2 \sum_{1 \leq i < j \leq n} v_i v_j X_i X_j. \quad (3.1)$$

Sabemos que $v_i = (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n))$. Assim,

$$\begin{aligned} v_i v_i &= (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)) \cdot (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)) \\ &= \sigma_i(\alpha_1)^2 + \dots + \sigma_i(\alpha_n)^2 = \alpha_1^2 + \dots + \alpha_n^2, \end{aligned} \quad (3.2)$$

Portanto,

$$\begin{aligned} v_i v_i &= \alpha_1^2 + \dots + \alpha_n^2 \\ &= (\alpha_1 + \dots + \alpha_n)^2 - 2 \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j \\ &= a_{n-1}^2 - 2a_{n-2}; \end{aligned}$$

Desse modo, a primeira parcela para a forma quadrática $|v|^2$ pode ser reescrita da seguinte maneira:

$$(a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^n X_i^2.$$

Para a segunda parcela, temos:

$$v_i = (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)); i = 1, \dots, n.$$

Assim,

$$\begin{aligned} v_i v_j &= (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)) \cdot (\sigma_j(\alpha_1), \dots, \sigma_j(\alpha_n)) \\ &= \sigma_i(\alpha_1) \sigma_j(\alpha_1) + \dots + \sigma_i(\alpha_n) \sigma_j(\alpha_n). \end{aligned}$$

Logo,

$$\sigma_i^{-1}(v_i v_j) = \alpha_1 \sigma_k(\alpha_1) + \dots + \alpha_n \sigma_k(\alpha_n), \quad (3.3)$$

onde $\sigma_k = \sigma_i^{-1} \sigma_j$.

Como $\sum_{i=1}^n \alpha_i \sigma_k(\alpha_i) = \text{Tr}_{K/\mathbb{Q}}(\alpha_1 \sigma_k(\alpha_1))$, temos que:

$$v_i v_j = \text{Tr}_{K/\mathbb{Q}}(\alpha_1 \sigma_k(\alpha_1)) \in \mathbb{Z}. \quad (3.4)$$

Observando que:

$$\begin{cases} \sigma_1(\alpha_1) = \alpha_1 \\ \sigma_2(\alpha_1) = \alpha_2 \\ \vdots \\ \sigma_i(\alpha_1) = \alpha_i, \end{cases}$$

obtemos,

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) &= \sum_{l=1}^n \sigma_l(\alpha_i \alpha_j) = \sum_{l=1}^n \sigma_l(\sigma_i(\alpha_1) \sigma_j(\alpha_1)) \\ &= \sum_{l=1}^n \sigma_l(\sigma_i(\alpha_1)) \sigma_l(\sigma_j(\alpha_1)) = \sum_{l=1}^n \sigma_i(\sigma_l(\alpha_1)) \sigma_j(\sigma_l(\alpha_1)) \\ &= \sum_{l=1}^n \sigma_i(\alpha_l) \sigma_j(\alpha_l) = \sum_{l=1}^n \sigma_i^{-1} \sigma_i(\alpha_l) \sigma_i^{-1} \sigma_j(\alpha_l) \\ &= \sum_{l=1}^n \alpha_l \sigma_k(\alpha_l) = \text{Tr}_{K/\mathbb{Q}}(\alpha_1 \sigma_k(\alpha_1)). \end{aligned}$$

Então, $\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) = \text{Tr}_{K/\mathbb{Q}}(\alpha_1 \sigma_k(\alpha_1))$.

Portanto,

$$Q(X_1, \dots, X_n) = (a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^n X_i^2 + 2 \sum_{1 \leq i < j \leq n} \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) X_i X_j.$$

■

3.1.2 K é Totalmente Imaginário

Neste caso, $n = 2r_2$, donde segue que $r_2 = n/2$. Logo,

$$f(X) = (X - \alpha_1) \dots (X - \alpha_{r_2})(X - \bar{\alpha}_1) \dots (X - \bar{\alpha}_{r_2}).$$

Sejam $G = \{\sigma_1, \dots, \sigma_{r_2}, \bar{\sigma}_1, \dots, \bar{\sigma}_{r_2}\}$ e

$$\begin{aligned} v_i &= \sigma_i(u) = (\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_{r_2})) \\ &= (\operatorname{Re}\sigma_i(\alpha_1), \operatorname{Im}\sigma_i(\alpha_1), \dots, \operatorname{Re}\sigma_i(\alpha_{r_2}), \operatorname{Im}\sigma_i(\alpha_{r_2})) \in \mathbb{R}^n, i = 1, \dots, n. \end{aligned}$$

Definiremos a seguir a matriz geradora e a forma quadrática, que diferentemente do caso real não há como simplificá-las.

Assim,

$$M = \begin{pmatrix} \operatorname{Re}\sigma_1(\alpha_1) & \operatorname{Im}\sigma_1(\alpha_1) & \dots & \operatorname{Re}\sigma_1(\alpha_{r_2}) & \operatorname{Im}\sigma_1(\alpha_{r_2}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \operatorname{Re}\sigma_n(\alpha_1) & \operatorname{Im}\sigma_n(\alpha_1) & \dots & \operatorname{Re}\sigma_n(\alpha_{r_2}) & \operatorname{Im}\sigma_n(\alpha_{r_2}) \end{pmatrix}$$

e

$$Q(X_1, \dots, X_n) = \sum_{i=1}^n v_i v_i X_i^2 + 2 \sum_{1 \leq i < j \leq n} v_i v_j X_i X_j.$$

A forma quadrática é positiva definida, cujo menor valor com entradas inteiras, não todas nulas, nos fornece o dobro do quadrado do raio de empacotamento.

3.2 Reticulados de Posto 2

3.2.1 Caso K Totalmente Real

Sejam $f(X) = X^2 + aX + b$; $a, b \in \mathbb{Z}$ e α_1, α_2 as raízes de f . Para que α_1, α_2 sejam reais e distintas é necessário e suficiente que $\Delta = a^2 - 4b$ seja positivo.

Sejam,

$$v_1 = (\alpha_1, \alpha_2) \quad e \quad v_2 = (\alpha_2, \alpha_1),$$

dois vetores de $\mathbb{R}^2$ e Λ_f o reticulado gerado pelos vetores v_1, v_2 . A densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det M|},$$

sendo M a matriz de ordem 2, dada por:

$$M = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix}.$$

Lema 3.2.1 *O determinante da matriz M , definida acima vale $a\sqrt{\Delta}$, onde $\Delta = a^2 - 4b$.*

Demonstração:

Sejam

$$\alpha_1 = \frac{-a + \sqrt{\Delta}}{2} \quad e \quad \alpha_2 = \frac{-a - \sqrt{\Delta}}{2}.$$

Logo,

$$\begin{aligned} \det M &= \alpha_1^2 - \alpha_2^2 = \left(\frac{-a + \sqrt{\Delta}}{2} \right)^2 - \left(\frac{-a - \sqrt{\Delta}}{2} \right)^2 \\ &= \frac{4a\sqrt{\Delta}}{4} = a\sqrt{\Delta}. \end{aligned}$$

■

Lema 3.2.2 *Sejam $f(X) = X^2 + aX + b$; $a, b \in \mathbb{Z}$ e $v = X_1v_1 + X_2v_2$ um vetor de Λ_f , então:*

$$|v|^2 = a^2(X_1^2 + X_2^2) - 2b(X_1 - X_2)^2.$$

Demonstração:

Pelo Lema 3.1.1, temos que:

$$|v|^2 = (a_{n-1}^2 - 2a_{n-2}) \sum_{i=1}^n X_i^2 + 2 \sum_{1 \leq i < j \leq n} \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) X_i X_j.$$

Logo, para $n = 2$, temos:

$$\begin{aligned}|v|^2 &= (a^2 - 2b)(X_1^2 + X_2^2) + 2\text{Tr}(\alpha_1\alpha_2)X_1X_2 \\ &= (a^2 - 2b)(X_1^2 + X_2^2) + 2(2b)X_1X_2 \\ &= a^2(X_1^2 + X_2^2) - 2b(X_1 - X_2)^2.\end{aligned}$$



Exemplo 3.2.1 Com a notação anterior, sejam $f(X) = X^2 + 3X + 1$, α_1 e α_2 as raízes de f e $v = X_1v_1 + X_2v_2 \in \Lambda_f$. Pelo Lema 3.2.2 $|v|^2 = 9(X_1^2 + X_2^2) - 2(X_1 - X_2)^2$, assume valor mínimo 7 quando $X_1 = 1$ e $X_2 = 0$, donde segue que $\rho = \frac{\Lambda_{\min}}{2} = \frac{\sqrt{7}}{2}$ e pelo Lema 3.2.1 $v(\Lambda_f) = |a| \sqrt{a^2 - 4b} = 3\sqrt{5}$. Então,

$$\delta(\Lambda_f) = \frac{\rho^2}{v(\Lambda_f)} = \frac{(\frac{\sqrt{7}}{2})^2}{3\sqrt{5}} = \frac{7}{12\sqrt{5}} \cong 0,143.$$

Exemplo 3.2.2 Com a notação anterior, sejam $f(X) = X^2 + 6X + 6$, α_1 e α_2 as raízes de f e $v = X_1v_1 + X_2v_2 \in \Lambda_f$. Pelo Lema 3.2.2 $|v|^2 = 36(X_1^2 + X_2^2) - 12(X_1 - X_2)^2$, assume valor mínimo 24 quando $X_1 = 1$ e $X_2 = 0$, donde segue que $\rho = \frac{\Lambda_{\min}}{2} = \frac{\sqrt{24}}{2}$ e pelo Lema 3.2.1 $v(\Lambda_f) = |a| \sqrt{a^2 - 4b} = 6\sqrt{12}$. Então,

$$\delta(\Lambda_f) = \frac{\rho^2}{v(\Lambda_f)} = \frac{(\frac{\sqrt{24}}{2})^2}{12\sqrt{3}} = \frac{24}{48\sqrt{3}} = \frac{1}{2\sqrt{3}} \cong 0,2887.$$

Observação 3.2.1 O reticulado obtido no exemplo 3.2.2 tem densidade de centro recorde, para essa dimensão.

Teorema 3.2.1 Sejam $f(X) = X^2 + aX + b$, $a, b \in \mathbb{Z}$ e Λ_f um reticulado como definido anteriormente. Se $f(X)$ satisfaz:

$$\frac{a^2}{6} = b, \quad (3.5)$$

então o reticulado Λ_f possui densidade de centro recorde.



Demonstração:

Com efeito, temos que sua forma quadrática,

$$\begin{aligned} |v|^2 &= a^2(X_1^2 + X_2^2) - 2b(X_1 - X_2)^2 \\ &= 6b(X_1^2 + X_2^2) - 2b(X_1 - X_2)^2, \end{aligned}$$

assume valor mínimo $4b$ quando $X_1 = 1$, $X_2 = 0$. Logo, $\rho = \frac{\sqrt{4b}}{2}$ e $|\det M| = |a|\sqrt{2b}$,

donde segue que a densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{(\sqrt{4b}/2)^2}{|a|\sqrt{2b}} = \frac{4b}{4|a|\sqrt{2b}} = \frac{b}{2b\sqrt{3}} = \frac{1}{2\sqrt{3}} \cong 0,2887.$$

■

3.2.2 Caso K Totalmente Imaginário

Sejam $f(X) = X^2 + aX + b$; $a, b \in \mathbb{Z}$ e $\alpha, \bar{\alpha}$ as raízes de f . Para que $\alpha, \bar{\alpha}$ sejam imaginários é necessário e suficiente que $\Delta = a^2 - 4b$ seja negativo.

Sejam,

$$v_1 = (\operatorname{Re}\alpha, \operatorname{Im}\alpha) = \left(\frac{-a}{2}, \frac{\sqrt{-\Delta}}{2}\right)$$

$$v_2 = (\operatorname{Im}\bar{\alpha}, \operatorname{Re}\bar{\alpha}) = \left(\frac{-a}{2}, \frac{-\sqrt{-\Delta}}{2}\right) = (\operatorname{Re}\alpha, -\operatorname{Im}\alpha),$$

dois vetores de $\mathbb{R}^2$ e Λ_f o reticulado gerado pelos vetores v_1, v_2 . A densidade de centro de

Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{\rho^2}{|\det M|},$$

sendo M dada por:

$$M = \begin{pmatrix} \operatorname{Re}\alpha & \operatorname{Im}\alpha \\ \operatorname{Re}\alpha & -\operatorname{Im}\alpha \end{pmatrix}.$$

Lema 3.2.3 O determinante da matriz M , definida acima vale $\frac{a\sqrt{-\Delta}}{2}$, onde $\Delta = a^2 - 4b$.



Demonstração:

Sejam

$$\alpha = \frac{-a + \sqrt{-\Delta}}{2} \quad e \quad \bar{\alpha} = \frac{-a - \sqrt{-\Delta}}{2}.$$

Logo,

$$\det M = -2\operatorname{Re}\alpha\operatorname{Im}\alpha = -2\left(\frac{-a}{2}\right)\left(\frac{\sqrt{-\Delta}}{2}\right) = \frac{a\sqrt{-\Delta}}{2}.$$

■

Lema 3.2.4 *Seja $v = X_1v_1 + X_2v_2$ um vetor de Λ_f , então:*

$$|v|^2 = \frac{a^2}{4}(X_1 + X_2)^2 + \frac{(4b - a^2)}{4}(X_1 - X_2)^2.$$

Demonstração:

Temos que:

$$\begin{aligned} v &= X_1(\operatorname{Re}\alpha, \operatorname{Im}\alpha) + X_2(\operatorname{Re}\alpha, -\operatorname{Im}\alpha) \\ &= (\operatorname{Re}\alpha(X_1 + X_2), \operatorname{Im}\alpha(X_1 - X_2)). \end{aligned}$$

Logo,

$$\begin{aligned} |v|^2 = v \cdot v &= (\operatorname{Re}\alpha)^2(X_1 + X_2)^2 + (\operatorname{Im}\alpha)^2(X_1 - X_2)^2 \\ &= \left(\frac{-a}{2}\right)^2(X_1 + X_2)^2 + \left(\frac{\sqrt{-\Delta}}{2}\right)^2(X_1 - X_2)^2 \\ &= \frac{a^2}{4}(X_1 + X_2)^2 + \frac{(4b - a^2)}{4}(X_1 - X_2)^2. \end{aligned}$$

■

Exemplo 3.2.3 *Sejam $f(X) = X^2 + X + 3$ e $v \in \Lambda_f$, como definidos anteriormente.*

Pelo Lema 3.2.4, temos que:

$$|v|^2 = \frac{(X_1 + X_2)^2 + 11(X_1 - X_2)^2}{4},$$

assume valor mínimo 1 quando $X_1 = 1$ e $X_2 = 1$, donde segue que $\rho = \frac{\Lambda_{\min}}{2} = \frac{1}{2}$ e pelo

Lema 3.2.3 $v(\Lambda_f) = \frac{|a\sqrt{-\Delta}|}{2} = \frac{\sqrt{11}}{2}$. Então,

$$\delta(\Lambda_f) = \frac{\rho^2}{v(\Lambda_f)} = \frac{(\frac{1}{2})^2}{\left(\frac{\sqrt{11}}{2}\right)} = \frac{1}{2\sqrt{11}} \cong 0,15.$$

Exemplo 3.2.4 Sejam $f(X) = X^2 + X + 1$ e $v \in \Lambda_f$, como definidos anteriormente.

Pelo Lema 3.2.4, temos que:

$$|v|^2 = \frac{(X_1 + X_2)^2 - 2(X_1 - X_2)^2}{4},$$

assume valor mínimo 1 quando $X_1 = 1$ e $X_2 = 0$, donde segue que $\rho = \frac{\Lambda_{\min}}{2} = \frac{1}{2}$ e pelo

Lema 3.2.3 $v(\Lambda_f) = \frac{|a\sqrt{-\Delta}|}{2} = \frac{\sqrt{3}}{2}$. Então,

$$\delta(\Lambda_f) = \frac{\rho^2}{v(\Lambda_f)} = \frac{(\frac{1}{2})^2}{\frac{\sqrt{3}}{2}} = \frac{1}{2\sqrt{3}} \cong 0,2887.$$

Observação 3.2.2 Como vimos no caso real, o reticulado obtido no exemplo 3.2.4 tem a densidade de centro recorde.

Veremos na observação a seguir, que a partir de algumas condições é possível obtermos uma "família de recordes".

Teorema 3.2.2 Sejam $f(X) = X^2 + aX + b$, $a, b \in \mathbb{Z}$ e Λ_f o reticulado definido anteriormente. Supondo

$$a^2 = b,$$

então o reticulado Λ_f possui densidade de centro recorde.

Demonstração:

Com efeito, temos que sua forma quadrática,

$$|v|^2 = \frac{a^2(X_1 + X_2)^2 + (4b - a^2)(X_1 - X_2)^2}{4} = \frac{b(X_1 + X_2)^2 + 3b(X_1 - X_2)^2}{4},$$

assume valor mínimo b quando $X_1 = 1$, $X_2 = 0$. Logo $\rho = \frac{\sqrt{b}}{2}$ e $|\det M| = \frac{|a\sqrt{3b}|}{2}$, donde segue que a densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{(\sqrt{b}/2)^2}{\frac{|a\sqrt{3b}|}{2}} = \frac{2b}{4|a\sqrt{3b}|} = \frac{b}{2\sqrt{b}\sqrt{3b}} = \frac{b}{2b\sqrt{3}} = \frac{1}{2\sqrt{3}} \cong 0,2887.$$

■

Observação 3.2.3 A recíproca do Teorema 3.2.2 não é verdadeira, basta tomarmos o polinômio $f(X) = X^2 + 3X + 3$.

3.3 Reticulados de Posto 3

Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e $\alpha_1, \alpha_2, \alpha_3$ as raízes de f . Para que $\alpha_1, \alpha_2, \alpha_3$ sejam reais é necessário e suficiente que a derivada de f se anule em dois pontos distintos, digamos x_1 e x_2 , e que $f(x_1)$ e $f(x_2)$ tenham sinais distintos, isto é, $f(x_2) < 0 < f(x_1)$, admitindo, sem perda de generalidade, que $x_1 < x_2$.

Podemos resumir esse comentário formalmente no seguinte resultado:

Lema 3.3.1 ([8]) *Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e $\alpha_1, \alpha_2, \alpha_3$ as raízes de f . Para que $\alpha_1, \alpha_2, \alpha_3$ sejam reais é necessário e suficiente que*

$$a^2 - 3b > 0 \text{ e que } (\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|.$$

Demonstração:

Como $f(X) = X^3 + aX^2 + bX + c$, temos que a sua derivada é dada por:

$f'(X) = 3X^2 + 2aX + b$, cujas raízes são:

$$x_1 = \frac{-a - \sqrt{a^2 - 3b}}{3} \quad \text{e} \quad x_2 = \frac{-a + \sqrt{a^2 - 3b}}{3}.$$

Logo, segue que $a^2 - 3b$ deve ser um número positivo. Agora,

$$\begin{aligned} f(x_1) &= x_1^3 + ax_1^2 + bx_1 + c \\ &= \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^3 + a \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^2 + b \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right) + c \\ &= \frac{1}{27} (2a^3 + 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c) \end{aligned}$$

e, portanto, $f(x_1) > 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > \frac{-2a^3 + 9ab - 27c}{2}.$$

Analogamente,

$$f(x_2) = \frac{1}{27} (2a^3 - 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c)$$

e, portanto, $f(x_2) < 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > -\frac{-2a^3 + 9ab - 27c}{2}.$$

Visto que a recíproca é imediata, concluímos a demonstração. ■

Lema 3.3.2 ([2]) O determinante do cubo M , definida acima, vale $-a(a^2 - 3b)$.

Demonstração:

Das relações de Girard, sendo $\alpha_1, \alpha_2, \alpha_3$ as raízes de $f(X) = X^3 + aX^2 + bX + c$, podemos deduzir que:

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -a \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b \\ \alpha_1\alpha_2\alpha_3 = -c. \end{cases}$$

Supondo

$$(\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|.$$

Sejam,

$$\begin{cases} v_1 = (\alpha_1, \alpha_2, \alpha_3) \\ v_2 = (\alpha_3, \alpha_1, \alpha_2) \\ v_3 = (\alpha_2, \alpha_3, \alpha_1), \end{cases}$$

três vetores do $\mathbb{R}^3$ e Λ_f o reticulado gerado pelos vetores v_1, v_2, v_3 . A densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{\rho^3}{|\det M|},$$

sendo M a matriz de ordem 3 cujas entradas são as coordenadas dos vetores v_1, v_2 e v_3 , ou seja,

$$M = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_3 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_3 & \alpha_1 \end{pmatrix}$$

e ρ é o raio de empacotamento de Λ_f , isto é,

$$\rho = \frac{1}{2} \min\{|v|; v \in \Lambda, v \neq 0\}.$$

Lema 3.3.2 ([8]) *O determinante da matriz M , definida acima vale $-a(a^2 - 3b)$.*

Demonstração:

Podemos ver que $\det M = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3\alpha_1\alpha_2\alpha_3$. Por outro lado, sendo

$$\alpha_1 + \alpha_2 + \alpha_3 = -a,$$

segue que,

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = a^2,$$

isto é,

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = a^2 - 2b. \quad (3.6)$$

Multiplicando o lado esquerdo da equação (3.6) por $\alpha_1 + \alpha_2 + \alpha_3$ e o lado direito por $-a$ obtemos a equação:

$$\begin{aligned} & \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_1\alpha_2^2 + \alpha_1\alpha_3^2 + \alpha_2\alpha_1^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_3\alpha_2^2 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_1\alpha_2(\alpha_1 + \alpha_2) + \alpha_1\alpha_3(\alpha_1 + \alpha_3) + \alpha_2\alpha_3(\alpha_2 + \alpha_3) \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 - \alpha_1\alpha_2(\alpha_3 + a) - \alpha_1\alpha_3(\alpha_2 + a) - \alpha_2\alpha_3(\alpha_1 + a) \\ &= -a(a^2 - 2b). \end{aligned}$$

Mas, $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3\alpha_1\alpha_2\alpha_3 - a(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -a^3 + 2ab$, e conseqüentemente,

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 - 3\alpha_1\alpha_2\alpha_3 = -a^3 + 3ab.$$

Portanto, $\det M = -a^3 + 3ab$. ■

Lema 3.3.3 ([8]) *Seja $v = Xv_1 + Yv_2 + Zv_3$ um vetor de Λ_f , então*

$$|v|^2 = (a^2 - 2b)(X^2 + Y^2 + Z^2) + 2b(XY + XZ + YZ).$$

Demonstração:

Seja $v = (\alpha_1X + \alpha_2Y + \alpha_3Z, \alpha_3X + \alpha_1Y + \alpha_2Z, \alpha_2X + \alpha_3Y + \alpha_1Z)$, então:

$$\begin{aligned} |v|^2 &= (\alpha_1^2 + \alpha_2^2 + \alpha_3^2)(X^2 + Y^2 + Z^2) + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)(XY + XZ + YZ) \\ &= (a^2 - 2b)(X^2 + Y^2 + Z^2) + 2b(XY + XZ + YZ). \end{aligned}$$

Exemplo 3.3.1 *Seja $f(X) = (X - 1)(X - 3)(X - 5) = X^3 - 9X^2 + 23X - 15$. É claro que $f(X)$ satisfaz as condições do Lema 3.3.1, e sua forma quadrática*

$$|v|^2 = 35(X^2 + Y^2 + Z^2) + 46(XY + XZ + YZ),$$

assume valor mínimo 24 quando $X = 1$, $Y = -1$ e $Z = 0$. Logo $\rho = \frac{\sqrt{24}}{2}$ e $|\det M| = 108$, donde segue que a densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{(\sqrt{24}/2)^3}{108} = \frac{\sqrt{6}}{18} \cong 0,136.$$

Exemplo 3.3.2 Seja $f(X) = X^3 + 4X^2 + 4X + 1$. Não é difícil ver que $f(X)$ satisfaz as condições do Lema 3.3.1, e sua forma quadrática

$$|v|^2 = 8(X^2 + Y^2 + Z^2 + XY + XZ + YZ),$$

assume valor mínimo 8 quando $X = 1$, $Y = Z = 0$. Então $\rho = \frac{\sqrt{8}}{2}$ e $|\det M| = 16$, donde segue que a densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{(\sqrt{8}/2)^3}{16} = \frac{\sqrt{2}}{8} = \frac{1}{4\sqrt{2}} \cong 0,1768.$$

Observação 3.3.1 O reticulado obtido no exemplo 3.3.2 tem densidade de centro recorde, para essa dimensão.

Teorema 3.3.1 Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e Λ_f o reticulado definido anteriormente. Se $f(X)$ satisfaz:

$$\left(\frac{a}{2}\right)^2 = b \quad \text{e} \quad c(27c + 4a^3 - 18ab) < 0, \quad (3.7)$$

então o reticulado Λ_f possui densidade de centro recorde.

Demonstração:

Com efeito, temos que sua forma quadrática

$$|v|^2 = 2b(X^2 + Y^2 + Z^2 + XY + XZ + YZ),$$



assume valor mínimo $2b$ quando $X = 1$, $Y = Z = 0$. Então $\rho = \frac{\sqrt{2b}}{2}$ e $|\det M| = |ab|$,

donde segue que a densidade de centro de Λ_f é dada por:

$$\delta(\Lambda_f) = \frac{(\sqrt{2b}/2)^3}{|a|b} = \frac{\sqrt{2b\sqrt{2b}}}{8|a|b} = \frac{\sqrt{2}\sqrt{b}}{8\sqrt{b}} = \frac{\sqrt{2}}{8} = \frac{1}{4\sqrt{2}} \cong 0,1768.$$

■

Podemos resumir o Teorema acima dizendo que: Se $f(X)$ satisfaz (3.7), obtemos uma família de reticulados cuja densidade de centro é recorde. Convém ressaltar ainda, que para cada polinômio $f(X)$ obtemos reticulados distintos.

3.4 Representação Geométrica de Ideais

Sejam $K/\mathbb{Q}$ uma extensão abeliana de grau n , $\mathcal{O}_K$ o anel dos inteiros algébricos de K , I um ideal não nulo de $\mathcal{O}_K$ e $\sigma_K : K \rightarrow \mathbb{R}^n$ o homomorfismo canônico. Já vimos que, $\sigma_K(I)$ é um reticulado de posto n , cuja densidade de centro é dada por:

$$\delta(\sigma_K(I)) = \frac{2^{r_2} \rho^n}{|D_K|^{1/2} N(I)},$$

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

Nesse reticulado a distância entre seus pontos é medida pela função traço, como veremos a seguir:

Proposição 3.4.1 ([12], pag. 225) *Sejam K um corpo de números e $x \in K$. Então,*

$$|\sigma_K(x)|^2 = c_K \cdot \text{Tr}_{K/\mathbb{Q}}(x\bar{x}),$$

onde,

$$c_K = \begin{cases} 1, & \text{se } K \text{ é totalmente real;} \\ 1/2, & \text{se } K \text{ é totalmente imaginário.} \end{cases}$$

Demonstração:

No caso em que K é totalmente real, para $x \in K$, $\sigma_K(x) = (\sigma_1(x), \dots, \sigma_n(x))$. Assim,

$$\begin{aligned} |\sigma_K(x)|^2 &= \sigma_1(x)^2 + \dots + \sigma_n(x)^2 = \sigma_1(x^2) + \dots + \sigma_n(x^2) \\ &= \sigma_1(x\bar{x}) + \dots + \sigma_n(x\bar{x}) = \text{Tr}_{K/\mathbb{Q}}(x\bar{x}). \end{aligned}$$

No caso em que K é totalmente imaginário, para $x \in K$,

$$\sigma_K(x) = (\text{Re}\sigma_1(x), \text{Im}\sigma_1(x), \dots, \text{Re}\sigma_{n/2}(x), \text{Im}\sigma_{n/2}(x)).$$

Então,

$$\begin{aligned} |\sigma_K(x)|^2 &= (\text{Re}\sigma_1(x))^2 + (\text{Im}\sigma_1(x))^2 + \dots + (\text{Re}\sigma_{n/2}(x))^2 + (\text{Im}\sigma_{n/2}(x))^2 \\ &= \sigma_1(x)\sigma_1(\bar{x}) + \dots + \sigma_{n/2}(x)\sigma_{n/2}(\bar{x}) \\ &= \sigma_1(x\bar{x}) + \dots + \sigma_{n/2}(x\bar{x}). \end{aligned}$$

Por outro lado,

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{n/2}(x\bar{x}) + \bar{\sigma}_1(x\bar{x}) + \dots + \bar{\sigma}_{n/2}(x\bar{x}).$$

Visto que $\bar{\sigma}_1(x\bar{x}) = \sigma_1(x\bar{x})$, então

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = 2(\sigma_1(x\bar{x}) + \dots + \sigma_{n/2}(x\bar{x})).$$

Logo,

$$\frac{1}{2}\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{n/2}(x\bar{x}).$$

Portanto,

$$|\sigma_K(x)|^2 = \frac{1}{2}\text{Tr}_{K/\mathbb{Q}}(x\bar{x}).$$

■

Fazendo uso da Proposição 3.4.1, podemos reescrever o raio de empacotamento da seguinte maneira:

$$\rho = \frac{c^{1/2}}{2} \min\{\sqrt{\text{Tr}_{K/\mathbb{Q}}(x\bar{x})}; x \in I, x \neq 0\}.$$

Seendo $t = \min\{\sqrt{\text{Tr}_{K/\mathbb{Q}}(x\bar{x})}; x \in I, x \neq 0\}$ a densidade de centro do reticulado $\sigma_K(I)$, é dada por:

$$\delta(\sigma_K(I)) = \frac{2^{r_2} c^{n/2} t^{n/2}}{2^n |D_K|^{1/2} N(I)}. \quad (3.8)$$

Observemos que:

$$2^{r_2} c^{n/2} = 1.$$

Logo, a equação (3.8) vale:

$$\delta(\sigma_K(I)) = \frac{t^{n/2}}{2^n |D_K|^{1/2} N(I)}. \quad (3.9)$$

Teorema 3.4.1 (das Médias) *Sejam $x_1, \dots, x_n$ números reais positivos. Então,*

$$\frac{x_1 + \dots + x_n}{n} \geq (x_1 \dots x_n)^{1/n}.$$

Observação 3.4.1 *As expressões $\frac{x_1 + \dots + x_n}{n}$ e $(x_1 \dots x_n)^{1/n}$ são chamadas, respectivamente, de Média Aritmética e Média Geométrica.*

Observação 3.4.2 *Notemos que:*

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(x\bar{x}) &= \sigma_1(x\bar{x}) + \dots + \sigma_n(x\bar{x}) \\ &= \sigma_1(x)\overline{\sigma_1(x)} + \dots + \sigma_n(x)\overline{\sigma_n(x)}, \end{aligned}$$

e

$$N(x\bar{x}) = \sigma_1(x)\overline{\sigma_1(x)} \dots \sigma_n(x)\overline{\sigma_n(x)} = N(x)^2.$$

Assim, como $\sigma_i(x\bar{x})$ é um número real positivo, pelo Teorema 3.4.1, temos:

$$\frac{\sigma_1(x)\overline{\sigma_1(x)} + \dots + \sigma_n(x)\overline{\sigma_n(x)}}{n} \geq \left(\prod_{i=1}^n \sigma_i(x)\overline{\sigma_i(x)} \right)^{1/n} > 0.$$

Pela observação 3.4.2, obtemos que:

$$\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) \geq n \cdot N(x)^{2/n},$$

isto é,

$$t \geq n \cdot N(x)^{2/n}, \quad (3.10)$$

onde $t = \min\{Tr_{K/\mathbb{Q}}(x\bar{x}); x \in I, x \neq 0\}$.

Logo, substituindo a equação (3.10) em (3.9), temos a seguinte majoração para a densidade de centro:

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2} \cdot (N(x)^{2/n})^{n/2}}{2^n \cdot |D_K|^{1/2} \cdot N(I)} = \frac{n^{n/2}}{2^n \cdot |D_K|^{1/2}} \cdot \frac{N(x)}{N(I)},$$

onde $N(x) = \min\{N(y); y \in I, y \neq 0\}$.

Dedicaremos o final desta seção à apresentação de exemplos, e estes serão divididos em dois casos: quando o ideal I é principal e quando o ideal I é não principal.

Caso 1: Quando I é um ideal principal, a norma $|N(x)|$ é mínima quando x é um dos geradores de I , e nesse caso,

$$|N(x)| = N(I).$$

Logo, para tais ideais I ,

$$\frac{|N(x)|}{N(I)} = 1.$$

E neste caso, podemos escrever a densidade de centro dos reticulados $\sigma_K(I)$ da seguinte maneira:

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n \cdot |D_K|^{1/2}}.$$

Faremos exemplos para corpos de grau 3. Visto que, se K está contido em um corpo ciclotômico, então K é um corpo abeliano, estudaremos as cúbicas contidas em corpos ciclotômicos. A seguir enunciaremos dois resultados e, a partir deles será possível saber quais corpos ciclotômicos contêm cúbicas e quantas cúbicas existem em cada um deles.

Lema 3.4.1 ([14], pag. 83) *Dados n um número inteiro e $L = \mathbb{Q}(\xi_n)$, então L contém uma cúbica se, e somente se, 3 divide $\phi(n)$.*

Teorema 3.4.2 ([9], pag. 55) *Sejam $n = p_1^{a_1} \dots p_n^{a_n}$, sua fatoração em primos e*

$$r = \#\{p_i : 3 \mid \phi(p_i^{a_i}), i = 1, \dots, s\}.$$

Então, existem $\frac{3^r - 1}{2}$ cúbicas em $\mathbb{Q}(\xi_n)$.

A fim de simplificarmos os exemplos, calcularemos a expressão da norma para o caso geral.

Sejam $L = \mathbb{Q}(\xi_p)$, $K = \mathbb{Q}(\theta)$, $K \subset L$, onde $\theta = \text{Tr}_{L/K}(\xi_p)$ e $[K : \mathbb{Q}] = 3$, $\mathcal{O}_K$ o anel dos inteiros algébricos de K e $\alpha = a + b\theta + c\theta^2 \in \mathcal{O}_K$. Visto que:

$$\text{irr}(\theta, \mathbb{Q}) = X^3 - \text{Tr}_{K/\mathbb{Q}}(\theta)X^2 + \sum \sigma_i(\theta)\sigma_j(\theta)X - N_{K/\mathbb{Q}}(\theta) \quad e,$$

$$\text{irr}(\theta^2, \mathbb{Q}) = X^3 - \text{Tr}_{K/\mathbb{Q}}(\theta^2)X^2 + \sum \sigma_i(\theta^2)\sigma_j(\theta^2)X - N_{K/\mathbb{Q}}(\theta^2)$$

obtemos,

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) = & a^3 + N_{K/\mathbb{Q}}(\theta)b^3 + N_{K/\mathbb{Q}}(\theta^2)c^3 + \text{Tr}_{K/\mathbb{Q}}(\theta)a^2b + \text{Tr}_{K/\mathbb{Q}}(\theta^2)a^2c + \\ & \left(\sum \sigma_i(\theta)\sigma_j(\theta)\right)ab^2 + \left(\sum \sigma_i(\theta^2)\sigma_j(\theta^2)\right)ac^2 + N_{K/\mathbb{Q}}(\theta)\text{Tr}_{K/\mathbb{Q}}(\theta)b^2c + \\ & N_{K/\mathbb{Q}}(\theta)\left(\sum \sigma_i(\theta)\sigma_j(\theta)\right)bc^2 + \left(\sum \sigma_i(\theta)\sigma_j(\theta)\right)\text{Tr}_{K/\mathbb{Q}}(\theta) - 3N_{K/\mathbb{Q}}(\theta)abc. \end{aligned}$$

Exemplo 3.4.1 *Para $L = \mathbb{Q}(\xi_7)$, sendo $G = \text{Gal}(L, \mathbb{Q})$, $\theta = \text{Tr}_{L/K}(\xi_7) = \xi_7 + \xi_7^6 = \xi_7 + \xi_7^{-1}$, $\text{irr}(\theta, \mathbb{Q}) = X^3 + X^2 - 2X - 1$, $\text{irr}(\theta^2, \mathbb{Q}) = X^3 - 5X^2 + 6X - 1$ e $\alpha \in \mathcal{O}_K$, tal que $\alpha = a + b\theta + c\theta^2$; $a, b, c \in \mathbb{Z}$. Então,*

$$N_{K/\mathbb{Q}}(\alpha) = a^3 + b^3 + c^3 - a^2b + 5a^2c - 2ab^2 - b^2c + 6ac^2 - 2bc^2 - abc.$$

Calculamos a norma para $a, b, c \in \mathbb{Z}$ no intervalo de $[-5, 5]$ e não houve nenhuma ocorrência para $N_{K/\mathbb{Q}}(\alpha) = \pm 2$, mas obtivemos 28 ocorrências para $N_{K/\mathbb{Q}}(\alpha) = \pm 8 = \pm 2^3$,

e neste caso $I = \langle \alpha \rangle$ também será um ideal principal acima de $p = 2$. Uma das ocorrências foi obtida quando $a = -2, b = -4$ e $c = 0$. Assim, fazendo $\alpha = -2 - 4\theta \in \mathcal{O}_K$, temos que,

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n \cdot |D_K|^{1/2}} = \frac{3\sqrt{3}}{8 \cdot |D_K|^{1/2}}.$$

E através do Teorema 2.3.3, temos que $|D_K| = 7^2$ e, portanto,

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{56} \cong 0,09279.$$

Exemplo 3.4.2 Para $L = \mathbb{Q}(\xi_{13})$, sendo $G = \text{Gal}(L, \mathbb{Q})$, $\theta = \text{Tr}_{L/K}(\xi_{13}) = \xi_{13} + \xi_{13}^5 + \xi_{13}^{-1} + \xi_{13}^{-5}$, $\text{irr}(\theta, \mathbb{Q}) = X^3 + X^2 - 4X + 1$, $\text{irr}(\theta^2, \mathbb{Q}) = X^3 - 9X^2 + 14X - 1$ e $\alpha \in \mathcal{O}_K$, tal que $\alpha = a + b\theta + c\theta^2$; $a, b, c \in \mathbb{Z}$. Então,

$$N_{K/\mathbb{Q}}(\alpha) = a^3 - b^3 + c^3 - a^2b + 9a^2c - 4ab^2 + b^2c + 14ac^2 + 4bc^2 + 7abc.$$

Calculamos a norma para $a, b, c \in \mathbb{Z}$ no intervalo de $[-5, 5]$ e não houve nenhuma ocorrência para $N_{K/\mathbb{Q}}(\alpha) = \pm 2$, mas obtivemos 13 ocorrências para $N_{K/\mathbb{Q}}(\alpha) = \pm 8 = \pm 2^3$, que também são ideais principais acima de $p = 2$. Uma das ocorrências foi obtida quando $a = -2, b = 2$ e $c = 0$.

Então, seja $I = \langle \alpha \rangle$, onde $\alpha = -2 + 2\theta \in \mathcal{O}_K$. Logo,

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n \cdot |D_K|^{1/2}} = \frac{3\sqrt{3}}{8 \cdot |D_K|^{1/2}}.$$

Do Teorema 2.3.3, temos que $D_K = \pm p^{[K:\mathbb{Q}]-1} = 13^2$, portanto,

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{8 \cdot 13} = \frac{3\sqrt{3}}{104} \cong 0,04996.$$

Exemplo 3.4.3 Para $L = \mathbb{Q}(\xi_{31})$, sendo $G = \text{Gal}(L, \mathbb{Q})$, $\theta = \text{Tr}_{L/K}(\xi_{31}) = \xi_{31} + \xi_{31}^2 + \xi_{31}^4 + \xi_{31}^8 + \xi_{31}^{15} + \xi_{31}^{-1} + \xi_{31}^{-2} + \xi_{31}^{-4} + \xi_{31}^{-8} + \xi_{31}^{-15}$, $\text{irr}(\theta, \mathbb{Q}) = X^3 + X^2 - 10X -$

8, $\text{irr}(\theta^2, \mathbb{Q}) = X^3 - 21X^2 + 116X - 64$ e $\alpha \in \mathcal{O}_K$, tal que $\alpha = a + b\theta + c\theta^2$; $a, b, c \in \mathbb{Z}$.

Então,

$$N_{K/\mathbb{Q}}(\alpha) = a^3 + 8b^3 + 64c^3 - a^2b + 21a^2c - 10ab^2 - 8b^2c + 116ac^2 - 80bc^2 - 14abc.$$

Para $a = -5, b = -4$ e $c = 3$, temos que $|N_{K/\mathbb{Q}}(\alpha)| = 2$. Então, seja $I = \langle \alpha \rangle$, onde $\alpha = -5 - 4\theta + 3\theta^2 \in \mathcal{O}_K$. Logo,

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n \cdot |D_K|^{1/2}} = \frac{3\sqrt{3}}{8 \cdot |D_K|^{1/2}}.$$

Do Teorema 2.3.3, temos que $D_K = \pm p^{[K:\mathbb{Q}]-1} = 31^2$, portanto,

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{8 \cdot 31} = \frac{3\sqrt{3}}{248} \cong 0,02095.$$

Caso 2: Sejam I um ideal não principal e $x \in I$. Logo, $\langle x \rangle \subset I$, e o índice de $\langle x \rangle$ em I é um número inteiro sempre maior que 1. Assim, se denotarmos por h_I o menor índice de $\langle x \rangle$ em I , segue que:

$$N(\langle x \rangle) = N(I) \cdot h_I.$$

Nesse caso, temos que a densidade de centro dos reticulados $\sigma_K(I)$, pode ser dada pela seguinte expressão:

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n |D_K|^{1/2}} \cdot h_I.$$

Exemplo 3.4.4 Seja $L = \mathbb{Q}(\xi_{31})$. Pelo exemplo 3.4.3, sabemos que $f(X) = \text{irr}(\theta, \mathbb{Q}) = X^3 + X^2 - 10X - 8$ e considerando o ideal $29\mathbb{Z} \subset \mathbb{Z}$, temos a seguinte fatoração para $f(X)$:

$$f(X) \equiv (X + 5)(X + 7)(X + 18) \pmod{29\mathbb{Z}[X]}.$$

E pelo Lema de Kummer, temos:

(a) $\mathfrak{p}_1 = \langle 29, \theta + 5 \rangle$, $\mathfrak{p}_2 = \langle 29, \theta + 7 \rangle$ e $\mathfrak{p}_3 = \langle 29, \theta + 18 \rangle$ são os ideais primos de $\mathcal{O}_K$ acima de $29\mathbb{Z}$,

(b) $29\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$,

(c) $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{29\mathbb{Z}} \right] = 1 = f_i$

Logo $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = 29$. Mas, sendo $\alpha = a + b\theta + c\theta^2 \in \mathcal{O}_K$, do exemplo 3.4.3, sabemos que:

$$N_{K/\mathbb{Q}}(\alpha) = a^3 + 8b^3 + 64c^3 - a^2b + 21a^2c - 10ab^2 - 8b^2c + 116ac^2 - 80bc^2 - 14abc.$$

Tomando o ideal primo $\mathfrak{p}_2 = \langle 29, \theta + 7 \rangle$, temos que:

$$(\theta + 7)(x + y\theta + z\theta^2) = (5x + 8z) + (x + 5y + 10z)\theta + (y + 4z)\theta^2,$$

onde $\theta^3 = -\theta^2 + 10\theta + 8$. Assim, fazendo $a = 5x + 8z + 29u$, $b = x + 5y + 10z + 29v$ e $c = y + 4z + 29w$ e calculando as combinações para $x, y, z, u, v, w \in [-2, 2]$, temos que $|N(\alpha)|$ assume valor mínimo 232, quando $a = -22$, $b = -28$ e $c = 0$, logo $h_I = 8$. Como não encontramos nenhum elemento com norma ± 1 , não podemos afirmar, mas existem possibilidades plausíveis do ideal $I = \langle 29, -22 - 28\theta \rangle$ não ser principal. Neste caso, temos:

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n |D_K|^{1/2}} \cdot h_I.$$

E pelo exemplo 3.4.3, segue que:

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{248} \cdot 8 \cong 0,02095 \cdot 8 = 0,1676.$$

Exemplo 3.4.5 Seja $L = \mathbb{Q}(\xi_{37})$. Temos que $f(X) = \text{irr}(\theta, \mathbb{Q}) = X^3 + X^2 - 12X + 11$,

onde $\theta = \text{Tr}_{L/K}(\xi_{37}) = \xi_{37} + \xi_{37}^6 + \xi_{37}^8 + \xi_{37}^{10} + \xi_{37}^{11} + \xi_{37}^{23} + \xi_{37}^{-1} + \xi_{37}^{-6} + \xi_{37}^{-8} + \xi_{37}^{-10} + \xi_{37}^{-11} + \xi_{37}^{-23}$, e considerando o ideal $31\mathbb{Z} \subset \mathbb{Z}$, temos a seguinte fatoração para

$f(X)$:

$$f(X) \equiv (X+2)(X+8)(X+22) \pmod{31\mathbb{Z}[X]}.$$

E pelo Lema de Kummer, temos:

(a) $\mathfrak{p}_1 = \langle 31, \theta + 2 \rangle$, $\mathfrak{p}_2 = \langle 31, \theta + 8 \rangle$ e $\mathfrak{p}_3 = \langle 31, \theta + 22 \rangle$ são os ideais primos de $\mathcal{O}_K$ acima de $31\mathbb{Z}$,

(b) $31\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$,

(c) $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{31\mathbb{Z}} \right] = 1 = f_i$.

Logo $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = 31$. Mas, sendo $\alpha = a + b\theta + c\theta^2 \in \mathcal{O}_K$, temos que:

$$N_{K/\mathbb{Q}}(\alpha) = a^3 - 11b^3 + 121c^3 - a^2b + 25a^2c - 12ab^2 + 11b^2c + 122ac^2 + 132bc^2 + 45abc.$$

Tomando o ideal primo $\mathfrak{p}_3 = \langle 31, \theta + 22 \rangle$, temos que:

$$(\theta + 22)(x + y\theta + z\theta^2) = (22x - 11z) + (x + 22y + 12z)\theta + (y + 21z)\theta^2,$$

onde $\theta^3 = -\theta^2 + 12\theta - 11$. Assim, fazendo $a = 22x - 11z + 29u$, $b = x + 22y + 12z + 29v$

e $c = y + 21z + 29w$ e calculando as combinações para $x, y, z, u, v, w \in [-2, 2]$, temos que

$|N(\alpha)|$ assume valor mínimo 248, quando $a = -40$, $b = 14$ e $c = 2$, logo $h_I = 8$. Como

não encontramos nenhum elemento com norma ± 1 , não podemos afirmar, mas existem

possibilidades plausíveis do ideal $I = \langle 31, -40 + 14\theta + 2\theta^2 \rangle$ não ser principal. Neste

caso, temos:

$$\delta(\sigma_K(I)) \geq \frac{n^{n/2}}{2^n |D_K|^{1/2}} \cdot h_I.$$

Logo,

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{8 \cdot |D_K|^{1/2}} \cdot 8 = \frac{3\sqrt{3}}{|D_K|^{1/2}}.$$

Do Teorema 2.3.3, temos que $D_K = \pm p^{[K:\mathbb{Q}]-1} = 37^2$, portanto,

$$\delta(\sigma_K(I)) \geq \frac{3\sqrt{3}}{37} \cong 0,1404.$$

Referências Bibliográficas

- [1] Boutros, J.; *Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel*. IEEE Trans. Inform. Theory, V.44, n.4, 1998.
- [2] Endler, O.; *Teoria dos Números Algébricos*. Projeto Euclides, 1986.
- [3] Garcia, A.; Lequain, Y.; *Elementos de álgebra*. Projeto Euclides, 2002.
- [4] Gonçalves, A.; *Introdução à Álgebra*. Projeto Euclides, 1979.
- [5] Herstein, I.N.; *Topics in Algebra*. John Wiley and Sons, 1975.
- [6] Marcus, D.A.; *Number Fields*. Springer-Verlag, 1977.
- [7] Monteiro, L.H.J.; *Elementos de Álgebra*. Impa, 1969.
- [8] Nóbrega, T.P.; *Cúbicas Reais, Algumas Aplicações*. Anais do VI Encontro de Álgebra USP-UNICAMP, 1997.
- [9] Rodrigues, T.M.; *Cúbicas Galoisianas*. Dissertação de Mestrado, IBILCE-UNESP, 2003.
- [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] Vicente, J.P.G.; *Reticulados de Posto 3 em Corpos de Números*. Dissertação de Mestrado, IBILCE-UNESP, 2000.
- [15] Washington, L.; *Introduction to Cyclotomic Fields*. Springer-Verlag, 1982.



