unesp Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Biociências, Letras e Ciências Exatas

Cúbicas Galoisianas

Tatiana Miguel Rodrigues

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto

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

São José do Rio Preto - SP
Julho - 2003

"O mistério não é um muro
onde a inteligência esbarra, mas
um oceano onde ela mergulha."

Gustav Thibon

Aos meus pais,
Ruben e Suely
E aos meus irmãos,
Nayhana e Vladimir
dedico.

Agradecimentos

Ao concluir este trabalho, agradeço:

Em nome de Jesus Cristo sobre nós na Terra ao Varão Perfeito que tudo tem.

Aos meus pais que me ensinam, incentivam e possibilitam a sonhar e a crer que tudo é possível. Que a todo momento, através de um abraço forte e um sorriso sincero, me fazem ver a vida com outros olhos.

Aos meus irmãos que entenderam a minha ausência em momentos importantes, que compartilharam nos momentos de alegria e me ajudaram nas dificuldades.

Aos meus avós que plantaram a semente no meu coração de perseverança e solidariedade, humanidade e confiança, de amor e paz.

Ao Prof. Dr. Trajano Pires da Nóbrega Neto pela sua inteligência, paciência, amizade e pela valiosa orientação, pela disponibilidade no atendimento de minhas dúvidas, por toda dedicação.

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

À Prof. Dra. Maria Gorete que além dos ensinamentos matemáticos me fez perseverar e ver com olhos de alegria a minha caminhada. Ao Prof. Dr. Antônio Aparecido Andrade pelos ensinamentos e pelas sugestões para o meu crescimento.

Às Profas. Helia M. Kodama, Aparecida Francisco da Silva e Ermínia de Lourdes C. Fanti, pela sabedoria, pelos conselhos nos momentos de indecisão, e por todo apoio e incentivo desde o início desta etapa vencida.

Ao Prof. e amigo Hermes Pedroso, que me mostrou que ensinar é muito mais do que giz e lousa.

Aos demais professores do Departamento de Matemática, pela formação acadêmica.

Aos companheiros da pós-graduação pelo agradável convívio.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

À CAPES, pelo auxílio financeiro.

Resumo

O propósito deste trabalho é abordar as cúbicas galoisianas as quais, pelo Teorema de Kronecker-Weber, estão contidas em uma extensão ciclotômica $\mathbb{Q}(\zeta_n)$, para algum n.

Estudamos a representação geométrica do seu anel dos inteiros algébricos, que são reticulados de posto 3. Visando calcular a densidade de centro de tais reticulados, é necessário o estudo do discriminante dessas cúbicas e a minimização da função traço.

Palavras-chave: Cúbicas Galoisianas, Reticulados, Densidade de centro.

Abstract

The purpose of this work is to deal with the galoisian cubics which, by Kronecker-Weber Theorem, are contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$, for some n.

We study the geometric representation of their algebraic integer ring, which are lattices with rank 3. For calculating the center density of these lattices, it is necessary to study the discriminant of those cubics and the minimization of trace form.

Keywords: Galoisian cubic, Lattices, Center density.

Sumário

Índice de Símbolos

$\mathbb{N}$: o conjunto dos números naturais

$\mathbb{Z}$: o conjunto dos números inteiros

$\mathbb{Q}$: o conjunto dos números racionais

$\mathbb{R}$: o conjunto dos números reais

$\mathbb{C}$: o conjunto dos números complexos

$\overline{\mathbb{Q}}$: o conjunto de todos os números complexos, algébricos sobre $\mathbb{Q}$

∂f : grau do polinômio f

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

$(E : F)$: índice de F em E

$\prod$: produtório

$\sum$: somatório

$detA$: determinante de A

(a_{ij}) : matriz

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

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

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

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

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

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

$\#X$: cardinalidade do conjunto X

$A \times B$: 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

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

$R[\alpha_1, \ldots, \alpha_n]$: anel gerado por R e $\alpha_1, \ldots, \alpha_n$

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

$\forall$: para todo

$\exists$: existe

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

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

D_K : discriminante absoluto do corpo K

$Tr_{L/K}$: traço em relação a L/K

$N_{L/K}$: norma em relação a L/K

A : conjunto de todos números algébricos

B : conjunto dos inteiros algébricos

$irr(x, K)$: polinômio minimal de x sobre K

$Nuc(f)$: núcleo do homomorfismo f

$|a| = \sqrt{a\overline{a}} = \sqrt{a_1^2 + \ldots + a_n^2},\ a = (a_1, \ldots, a_n) \in \mathbb{R}^n$

$< x_1, \ldots, x_n >$: ideal gerado por $x_1, \ldots, x_n$

$\underline{X} = (X_1, \ldots, X_n) \in \mathbb{R}^n$

$Gal(L/K)$: Grupo de Galois de L/K.

Apresentação

Dá-se o nome de Empacotamento Esférico a distribuição de esferas de mesmo raio no espaço Euclidiano de modo que duas a duas toquem-se no máximo em um ponto.

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

Em Paris, no ano de 1900, devido a importância desta questão, Hilbert citou-a como sendo o 18^{o} dentre os 23 problemas relevantes para a matemática, naquele século.

Diz-se que um Empacotamento é Reticulado, quando os centros destas esferas formam um subgrupo discreto do $\mathbb{R}^n$, ou seja, um reticulado.

Trocando-se esferas por laranjas, ou balas de canhão, e observando o modo como os feirantes empilham as frutas, os centros destas formam um reticulado, chamado face-centered cubic (ou fcc).

Este empacotamento reticulado é considerado o mais denso em três dimensões, pois as esferas ocupam $0,7405$ do espaço e nenhum outro empacotamento deste tipo, até o momento, tem densidade maior.

Buscar um arranjo de esferas que tivesse alta densidade era um problema conhecido há muito tempo. No século 16, Walter Rayleigh propôs esta questão ao seu assistente Thomas Harriot. Naquela época Harriot estava interessado em ótica e correspondia-se sobre este assunto com o astrônomo alemão Kepler. Harriot forneceu a Kepler dados preciosos em ótica, tentando também persuadir Kepler com a idéia de que o mistério mais profundo da ótica deveria ser descoberto através dos átomos. Kepler era cético neste sentido, mas Harriot insistiu e ele cedeu. Em 1611, Kepler escreveu um artigo que influenciou a cristalografia durante dois séculos. Na discussão sobre o empacotamento esférico, ele construiu o empacotamento fcc e assegurou que esse deveria ser o arranjo mais denso de bolas. Esta afirmação tornou-se conhecida como a conjectura de Kepler.

Segundo [16], em 1831 Gauss provou a conjectura de Kepler, mostrando que se todos os centros das esferas de um empacotamento são alinhadas ao longo dos pontos de um reticulado,

então tal empacotamento não pode ser melhor do que o empacotamento fcc.

O problema do Empacotamento Esférico, o qual tem extensa conexão com a matemática e suas aplicações, aparece também na química, na física, cristalografia e no "design" de códigos para transmissão, armazenamento e recebimento de dados. Desde então, muitas e diferentes técnicas foram usadas para solucioná-lo. Algumas têm contribuído com soluções parciais, entretanto, a questão continua esperando por uma resposta mais abrangente. Na matemática, tal problema é estudado na teoria dos grupos finitos, formas quadráticas, combinatória e nos métodos numéricos para o cálculo de integrais.

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.

Muitas das técnicas desenvolvidas para se obter reticulados são baseadas em códigos corretores de erro e existe o chamado método algébrico, baseado na teoria algébrica dos números, o qual será utilizado neste trabalho.

A relação entre reticulados e a teoria algébrica dos números têm sido estudada por muitos matemáticos a partir de Minkowski. Neste trabalho será descrito como alguns reticulados são obtidos a partir de ideais em corpos de números algébricos.

Um parâmetro associado ao empacotamento reticulado é a densidade de centro, a qual envolve conceitos da Teoria Algébrica dos Números.

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

No Capítulo 1, serão introduzidos conceitos de elemento algébrico, extensões algébricas, corpos de números, elemento inteiro algébrico, base integral, anel dos inteiros algébricos, discriminante de uma base, norma e traço de um elemento, norma de um ideal, discriminante de um corpo, etc. Será também apresentado o Lema de Kummer, que será usado para decomposição de um ideal primo em uma extensão.

No Capítulo seguinte, serão apresentados uma base integral, o anel dos inteiros algébricos e o discriminante de corpos quadráticos e ciclotômicos. Também será feita a decomposição de um ideal primo numa extensão galoisiana e em relação a este tipo de ideal serão apresentados o grupo de decomposição e o grupo de inércia. Neste capítulo serão definidos de empacotamento esférico, empacotamento reticulado, raio de empacotamento e densidade de centro, bem como descrito o método algébrico e a fórmula para a densidade de centro.

No terceiro Capítulo, serão caracterizadas as cúbicas galoisianas, quanto à sua localização e quantidade. Para desenvolver a fórmula da densidade de centro dos reticulados algébricos,

em extensões cúbicas galoisianas, será estudado o raio de empacotamento, o discriminante do corpo de números envolvido e a norma de um ideal. O cálculo desta última está relacionado com a teoria de decomposição de ideais em uma extensão.

Nesse capítulo é usada uma técnica para calcular o discriminante de um corpo de números, sem o uso da base integral, envolvendo os caracteres de Dirichlet, os quais serão introduzidos aqui. É importante ressaltar o interesse histórico em encontrar um corpo de números com discriminante mínimo.

Encontrar a menor distância do reticulado é equivalente a minimizar uma forma quadrática oriunda da função traço. Esta é positiva definida em n variáveis com entradas inteiras e obedecendo as restrições que caracterizam o ideal.

Finalizando o capítulo, será feito o estudo das cúbicas contidas em $\mathbb{Q}(\zeta_{p^r})$, p primo, $r > 1$ e dados exemplos do cálculo da densidade de centro de alguns reticulados algébricos de posto 3, obtidos tanto pela representação geométrica do anel dos inteiros algébricos, quanto de ideais deste anel.

É importante observar que o uso dos softwares MAPLE 7 e GAP, foram indispensáveis aos cálculos aqui desenvolvidos.

Capítulo 1

Corpos de Números

O objetivo deste capítulo é introduzir conceitos que serão usados nos capítulos posteriores. As demonstrações serão apresentadas apenas quando necessárias à compreensão do trabalho. Supõe-se que o leitor tenha um conhecimento razoável de Álgebra, que pode ser encontrado nas referências ([5]) e ([7]).

Neste capítulo será dada uma introdução sobre conceitos importantes da Teoria Algébrica dos Números tais como elementos algébricos, inteiros e será observada uma relação entre eles. Também serão vistas definições relacionadas a um corpo de números, por exemplo: anel dos inteiros algébricos, discriminante de um corpo de números, base integral, norma e traço de um elemento.

Será visto que o conjunto dos inteiros algébricos de um corpo de números é um anel e um $\mathbb{Z}$-módulo livre e que todo ideal deste anel pode ser fatorado unicamente como produto de ideais primos. Também será mostrado como calcula-se a norma de um ideal para ser usada no terceiro capítulo.

1.1 Elementos Algébricos sobre um Corpo

Seja K é um subcorpo do corpo L, diz-se que L é uma extensão do corpo K e denota-se por L/K uma extensão de corpos. A dimensão de L visto como espaço vetorial sobre K é chamado o grau de L sobre K e denotado por $[L : K]$. Diz-se que L/K é uma extensão finita se $[L : K]$ é finito.

Dados $K \subset L$ corpos e α um elemento de L, o conjunto de todas as expressões polinomiais em α e coeficientes em K será denotado por $K[\alpha]$.

Sejam R um anel e K um subcorpo de R. Um elemento $\alpha \in R$ é chamado **algébrico** sobre K se α é uma raiz de algum polinômio não nulo com coeficientes em K. Caso contrário α é dito

transcedente sobre K.

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

$$X^4 - 2X^2 + 49 \in \mathbb{Q}[X].$$

Uma extensão L/K é dita algébrica se todo elemento de L é algébrico sobre K e uma extensão L/K é dita 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 $J = \{p \in K[X] | p(\alpha) = 0\}$. J contém um único polinômio mônico, $p_0 = x^n + a_1 x^{n-1} + \ldots + a_n$ de grau mínimo : p_0 é irredutível sobre K e se $\alpha \neq 0$, então $a_n \neq 0$. O polinômio p_0 definido acima é chamado polinômio minimal de α sobre K, e seu grau é chamado de grau de α sobre K.

Para α algébrico tem-se 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, $[K(\alpha) : K] = \partial p$, 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, e somente se, L é uma extensão algébrica de K e L é um corpo algebricamente fechado.

Denota-se por A o conjunto de todos números algébricos, o qual é corpo em virtude de:

Teorema 1.1.1 ([*17*], pag. 39) *O conjunto* A *dos números algébricos é um subcorpo de* $\mathbb{C}$.

Um corpo de números é definido 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 $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ para finitos números algébricos $\alpha_1, \ldots, \alpha_n$ (por exemplo uma base para K como espaço vetorial sobre $\mathbb{Q}$).

Teorema 1.1.2 ([*17*], pag. 40) *Seja* K *é um corpo de números e* $\theta \in K$, *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, supõe-se $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. A demonstração será feita por indução sobre n e é suficiente provar que se $K = K_1(\alpha,\ \beta)$ então $K = K_1(\theta)$ para algum θ, onde K_1 é um subcorpo de K. Sejam p e q os polinômios minimais de α e β sobre K, respectivamente, e suponha que sobre $\mathbb{C}$ estes fatorem-se como:

$$\begin{aligned} p(X) &= (X - \alpha_1) \ldots (X - \alpha_n) \\ q(X) &= (X - \beta_1) \ldots (X - \beta_m), \end{aligned}$$

onde toma-se $\alpha_1 = \alpha$ e $\beta_1 = \beta$.

Por ([17], pag. 18) os α_i são distintos, como também são os β_j. Assim, para cada i e cada $k \neq 1$, existe no mínimo um elemento $x \in K$, tal que

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

Se existem somente algumas destas equações, escolhe-se $c \neq 0$ em K_1, diferente de qualquer um destes $x^{'}$s, e então

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1,$$

para $1 \leq i \leq n,\ 2 \leq k \leq m$. Seja

$$\theta = \alpha + c\beta.$$

Afirmação: $K_1(\theta) = K_1(\alpha,\ \beta)$. De fato, tem-se que $K_1(\theta) \subseteq K_1(\alpha,\ \beta)$ e é suficiente provar que $\beta \in K_1(\theta)$ se $\alpha = \theta - c\beta$. Agora, $p(\theta - c\beta) = p(\alpha) = 0$. Define-se o polinômio

$$r(X) = p(\theta - cX) \in K_1(\theta)[X],$$

então β é raiz dos polinômios r e q sobre $K_1(\theta)$. Esses polinômios têm somente uma raiz comum, ξ. Se $q(\xi) = r(\xi)$ então ξ é um dos $\beta_1, \ldots, \beta_m$ e também $\theta - c\xi$ é um dos $\alpha_1, \ldots, \alpha_n$. A escolha de c implica em $\xi = \beta$. Seja $h(X)$ o polinômio minimal de β sobre $K_1(\theta)$. Então, $h(X) \mid q(X)$ e $h(X) \mid r(X)$. Se q e r têm apenas uma raiz em comum em $\mathbb{C}$ então $\partial h = 1$. Daí

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

para $\mu \in K_1(\theta)$. Agora, $0 = h(\beta) = \beta + \mu$, o que implica $\beta = -\mu \in K_1(\theta)$, concluindo assim a demonstração. ■

Exemplo 1.1.2 *Se* $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ *tem-se* $f(X) = X^2 - 3$, *o polinômio irredutível de* $\sqrt{3}$ *sobre* $\mathbb{Q}$ *e* $g(X) = X^3 - 5$, *o polinômio irredutível de* $\sqrt[3]{5}$ *sobre* $\mathbb{Q}$. *As raízes de* f *são* $\alpha_1 = \sqrt{3}$ *e* $\alpha_2 = -\sqrt{3}$. *As de* g *são* $\beta_1 = \sqrt[3]{5},\ \beta_2 = w\sqrt[3]{5}$ *e* $\beta_3 = w^2\sqrt[3]{5}$, *onde*

$$w = e^{2\pi i/3} = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = \frac{-1}{2} + i\frac{\sqrt{3}}{2}.$$

Deve-se encontrar $c \in \mathbb{Q}$ *de modo que*

$$c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j},\ j \neq 1. \tag{1.1}$$

A equação (1.1) vale para todo $c \in \mathbb{Q}^*$; *em particular para* $c = 1$ *tem-se* $K = \mathbb{Q}(\sqrt{3} + \sqrt[3]{5})$.

Proposição 1.1.1 ([*11*], pag. 38) *Sejam* K *um corpo,* $f(X) \in K[X]$ *um polinômio irredutível e* $\alpha,\ \beta$ *raízes de* $f(X)$ *em alguma extensão de* K. *Então existe um único* K*-isomorfismo* $\varphi : K(\alpha) \longrightarrow K(\beta)$ *tal que* $\varphi(\alpha) = \beta$.

Demonstração: Dado $x \in K(\alpha)$, seja $g \in K[X]$ tal que $x = g(\alpha)$. Considere a aplicação $\varphi : K(\alpha) \longrightarrow K(x)$ tal que $\varphi(a) = a,\ \forall a \in K,\ \varphi(\alpha^i) = \beta^i,\ i = 1, \ldots, n-1$ e estenda φ por linearidade a todo $K(\alpha)$, isto é, $\varphi(g(\alpha)) = g(\beta)$, para qualquer $g(X) \in K[X]$.
Afirmação 1: φ está bem definida. De fato, sejam $g(X),\ h(X) \in K[X]$ tal que $g(\alpha) = h(\alpha) = 0$. Então,

$$g(\alpha) - h(\alpha) = 0 \Longrightarrow (g-h)(\alpha) = 0 \Longrightarrow f \mid (g-h) \Longrightarrow (g-h)(\beta) = 0 \Longrightarrow g(\beta) = h(\beta).$$

Afirmação 2: φ é um K-isomorfismo. De fato, se $\varphi(g(\alpha)) = g(\beta) = 0$, então $f(X)$ divide $g(X)$, portanto, $g(\alpha) = 0$.
Afirmação 3: φ é única. De fato, seja

$$\begin{aligned} \sigma : K(\alpha) &\longrightarrow K(\beta) \\ \alpha &\longmapsto \beta. \end{aligned}$$

Assim, $\sigma(\alpha^j) = \beta^j$ e mais, $\sigma(a_j\alpha_j) = a_j\beta^j$, pois σ é um K-homomorfismo. Finalmente,

$$\sigma\left(\sum_{j=0}^{n-1} a_j\alpha^j\right) = \sum_{j=0}^{n-1} a_j\beta^j = \varphi\left(\sum_{j=0}^{n-1} a_j\alpha^j\right),$$

concluindo assim a demonstração. ∎

1.2 Conjugados e Discriminantes

Seja $K = \mathbb{Q}(\theta)$ um corpo de números. Em geral, existem muitos monomorfismos distintos $\sigma : K \longrightarrow \mathbb{C}$. Por exemplo, se $K = \mathbb{Q}(i)$ tem-se as seguintes possibilidades:

$$\begin{aligned} \sigma_1(x+iy) &= x+iy \\ \sigma_2(x+iy) &= x-iy \end{aligned}$$

para $x, y \in \mathbb{Q}$.

O conjunto de tais monomorfismos forma a parte fundamental da teoria utilizada neste trabalho.

Teorema 1.2.1 ([17], pag. 41) *Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n. Então existem exatamente n monomorfismos distintos.*

$$\sigma_i : K \longrightarrow \mathbb{C} \qquad (i = 1, \ldots, n).$$

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

Usando-se esta notação, para cada $\alpha \in K$ define-se o polinômio característico de α sobre K como sendo:

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

Teorema 1.2.2 ([17], pag. 42) *Os coeficientes do polinômio característico são números racionais tal que* $f_\alpha(X) \in \mathbb{Q}[X]$.

Demonstração: Pode-se escrever (1.2) da seguinte maneira

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

Por outro lado,

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

sendo α_i as raízes de $irr(\alpha, \mathbb{Q}), i = 1, \ldots, m$. Sejam $\tau_1, \ldots, \tau_m$ os monomorfismos de $\mathbb{Q}(\alpha)$ em $\mathbb{C}$ definidos de modo que

$$\alpha_i = \tau_i(\alpha),\ i = 1, \ldots, m.$$

Visto que cada τ_i tem $[K : \mathbb{Q}(\alpha)]$ extensões de K em $\mathbb{C}$, conclui-se que

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

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

Desta demonstração tem-se duas conseqüências 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 $i = 1, \ldots, n$, são chamados K-conjugados de α. Por exemplo, sobre $\mathbb{Q}$, $\sqrt{5}$ e $-\sqrt{5}$ são conjugados, mas por outro lado $1+\sqrt{7}$ e $\sqrt{7}$ não são $\mathbb{Q}$-conjugados. Embora os θ_i sejam distintos (e são K-conjugados de θ), não é sempre verdade que os K-conjugados de α são distintos. Note que os K-conjugados de α não são necessariamente elementos de K. Os θ_i não são necessariamente elementos de K. Por exemplo, seja θ a raiz real cúbica de 2. 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 contidos em $\mathbb{Q}(\theta)$.

Considerando $K = \mathbb{Q}(\theta)$ um corpo de números de grau n, $\{\alpha_1, \ldots, \alpha_n\}$ uma base de K (como espaço vetorial sobre $\mathbb{Q}$) e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$, define-se o **discriminante** desta base por

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det(\sigma_i(\alpha_j)))^2. \tag{1.3}$$

Exemplo 1.2.1 *Sejam $K = \mathbb{Q}[\sqrt{11}]$ um corpo de números e $\{1, \sqrt{11}\} \subset K$. Então,*

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

Observação 1.2.1 *Se for tomada outra base $\{\beta_1, \ldots, \beta_n\}$ então*

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i, \quad c_{ik} \in \mathbb{Q},$$

para $k = 1, \ldots, n$ e $det(c_{ik}) \neq 0$. A partir do produto da fórmula de determinantes e o fato de os σ_i serem monomorfismos tem-se que

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

Exemplo 1.2.2 *Foi visto 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-se outra base, $\{8 - \sqrt{11}, \ 5 + 3\sqrt{11}\}$ de K, pela observação anterior, segue 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 ([17], pag. 44) *O discriminante de toda base para $K = \mathbb{Q}(\theta)$ é racional e não nulo. Se todos os K-conjugados de θ são reais então o discriminante de toda base é positivo.*

Demonstração: Primeiro escolhe-se uma base com a qual possa ser calculado o discriminante, por exemplo $\{1, \theta, \ldots, \theta^{n-1}\}$. Se os conjugados de θ são $\theta_1, \ldots, \theta_n$ então,

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

Um determinante da forma $D = det(\theta_i^j)$ é chamado determinante de Vandermonde e tem valor:

$$D = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j). \tag{1.4}$$

Assim,

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = [\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)]^2$$

e $\Delta \neq 0$, pois $\theta_i \neq \theta_j$ se $i \neq j$. Sendo $f(X) = irr(\theta,\ \mathbb{Q})$ 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, tem-se:

$$\pm \prod_{i=1}^{n} f'(\theta_i) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Mas, $f'(\theta_i) = \sigma_i(f'(\theta_i))$ e $f'(\theta) \in \mathbb{Q}(\theta)$. Logo o polinômio característico de $f'(\theta)$ sobre $\mathbb{Q}$ é

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

Visto que cada coeficiente de $f_{f'(\theta)}(X)$ é racional, tem-se 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 passa-se a discriminar os θ_i, o que motiva a nomenclatura de Δ.

1.3 Inteiros Algébricos

Dados os anéis $A \subset R$, um elemento $\theta \in R$ é dito inteiro algébrico sobre A, se este é raiz de um polinômio mônico com coeficientes em A.

Em outras palavras,

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

onde $a_i \in A, \forall i$. Por exemplo, $\theta = \sqrt{-5}$ é um inteiro algébrico, pois $\theta^2 + 5 = 0$ e $\tau = \frac{1}{2}(1 + \sqrt{5})$ é um inteiro algébrico pois $\tau^2 - \tau - 1 = 0$. Mas $\phi = 32/17$ não é, pois ele satisfaz equações do tipo $17\phi - 32 = 0$, a qual não é mônico ou do tipo $\phi - 32/17 = 0$, cujos coeficientes não são inteiros.

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

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

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

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

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 foi visto, ser algébrico tem o mesmo significado de ser inteiro algébrico sobre um corpo, é possível usar os resultados obtidos para elementos inteiros algébricos em elementos algébricos. Logo, para $K \subset R$ e $x \in R$, x é algébrico sobre K se, e somente se, $[K[x] : K]$ é finito.

Um resultado importante da Teoria da Extensão de Corpos é o seguinte: Sejam $F \subset D \subset E$ corpos tais que $[E : D]$ e $[D : F]$ são finitos, então E/F é finito e

$$[E : F] = [E : D].[D : F].$$

Chama-se B o conjunto dos inteiros algébricos. Um dos objetivos desta seção é provar que B é subanel de A.

Lema 1.3.1 ([*17*], pag. 46) *Um número complexo θ é um inteiro algébrico se, e somente se, o grupo aditivo gerado por todas potências $1, \theta, \theta^2, \ldots$ é finitamente gerado.*

Teorema 1.3.1 ([*17*], pag. 47) *Os inteiros algébricos formam um subanel do corpo dos números algébricos.*

A partir de uma extensão simples desta técnica tem-se o seguinte:

Teorema 1.3.2 ([*17*], 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 pode-se construir novos inteiros algébricos desconhecidos, por exemplo, $\sqrt{5}$ e $\sqrt{7}$ são claramente inteiros algébricos. Então, pelo Teorema 1.3.1, os números, $\sqrt{5} + \sqrt{7}$, $9\sqrt{7} - 86\sqrt{7}$ e $(\sqrt{5})^3(1 + \sqrt{7})^2$, 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 escreve-se

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

e $\mathcal{O}_K$ é dito o anel dos inteiros algébricos de K. Nos casos onde não está claro qual o corpo de números envolvido, este será denotado mais explicitamente por $\mathcal{O}_K$.

Lema 1.3.2 ([17], pag. 49) *Dado $\alpha \in K$ então para algum $c \in \mathbb{Z}$ não-nulo tem-se que $c\alpha \in \mathcal{O}_K$.*

Corolário 1.3.1 ([17], pag. 49) *Seja K um corpo de números. Então $K = \mathbb{Q}(\theta)$ para algum θ inteiro algébrico.*

Observação 1.3.1 *Para $\theta \in \mathbb{C}$ escreve-se $\mathbb{Z}[\theta]$ 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 $\mathbb{Z}[\theta]$, já que $\mathcal{O}_K$ 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 $X^2 - X - 3$, logo é um inteiro algébrico. Como ele está 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 ([17], pag. 49) *Um número algébrico α é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Lema 1.3.4 ([17], pag. 50) *Um inteiro algébrico é um número racional se, e somente se, é um inteiro. Equivalentemente, $B \cap \mathbb{Q} = \mathbb{Z}$.*

1.4 Base Integral

Seja K um corpo de números de grau n. Uma base (ou $\mathbb{Q}$-base para enfatizar) de K é uma base para K como um espaço vetorial sobre $\mathbb{Q}$. Pelo Corolário 1.3.1 tem-se $K = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, e segue que seu polinômio minimal p de θ tem grau n e que $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base para K.

Será mostrado que o anel $\mathcal{O}_K$ dos inteiros algébricos de K é um grupo abeliano sob a adição. Uma $\mathbb{Z}$-base para $(\mathcal{O}_K, +)$ é chamada uma base integral para K (ou para $\mathcal{O}_K$). Então, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral se, e somente se, qualquer elemento α de $\mathcal{O}_K$ e todo elemento de $\mathcal{O}_K$ é unicamente expresso na forma

$$a_1\alpha_1 + \ldots + a_s\alpha_s,$$

para inteiros $a_1, \ldots, a_s$.

A partir do Lema 1.3.2 tem-se que toda base integral de K é uma $\mathbb{Q}$-base. Assim, em particular $s = n$.

Por exemplo, pode-se afirmar que $K = \mathbb{Q}[\theta](= \mathbb{Q}(\theta))$ para um θ inteiro algébrico (Corolário 1.3.1), tal que $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma $\mathbb{Q}$-base para K a qual consiste de inteiros algébricos, mas não segue que $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base integral. Como exemplo, seja $K = \mathbb{Q}(\sqrt{13})$; o elemento $\frac{1}{2} + \frac{1}{2}\sqrt{13}$ satisfaz à equação

$$X^2 - X - 3 = 0$$

e então é um inteiro algébrico em $\mathbb{Q}(\sqrt{13})$ mas, não é um elemento de $\mathbb{Z}[\sqrt{13}]$.

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

Lema 1.4.1 ([17], pag. 51) *Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de K consistindo de inteiros algébricos. Então o discriminante $\Delta[\alpha_1, \ldots, \alpha_n]$ é um inteiro não-nulo.*

Logo pode-se afirmar que:

Teorema 1.4.1 ([17], pag. 51) *Todo corpo de números K possui uma base integral e o grupo aditivo $\mathcal{O}_K$ é abeliano livre de posto n, igual ao grau de K.*

Por exemplo em $\mathbb{Q}(\sqrt{13})$ a $\mathbb{Q}$-base $\{1, \sqrt{13}\}$ não é base integral. De fato, um elemento de $\mathbb{Q}(\sqrt{13})$ é da forma $p + q\sqrt{13}$ para $p,\ q \in \mathbb{Q}$ e tem polinômio minimal

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

Então $p + q\sqrt{13}$ é um inteiro algébrico se, e somente se, os coeficientes do polinômio minimal, ou seja, $2p$ e $(p^2 - 13q^2)$, são inteiros, pelo Lema 1.3.3. Logo, $p = (1/2)P$ onde P é um inteiro e para P par, tem-se que $p^2 \in \mathbb{Z}$, então $13q^2 \in \mathbb{Z}$, o que implica q é um 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 número inteiro ímpar. A partir disto segue que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{13}\right]$ e uma base integral é $\left\{1,\ \frac{1}{2} + \frac{1}{2}\sqrt{13}\right\}$.

Pode-se provar isto usando discriminante da seguinte maneira: os dois monomorfismos de $\mathbb{Q}(\sqrt{13})$ em $\mathbb{C}$ são dados por:

$$\begin{aligned} \sigma_1(p + q\sqrt{13}) &= p + q\sqrt{13}, \\ \sigma_2(p + q\sqrt{13}) &= p - q\sqrt{13}. \end{aligned}$$

Assim, o discriminante $\Delta\left[1, \frac{1}{2}+\frac{1}{2}\sqrt{13}\right]$ vale:

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

Define-se um número inteiro como sendo **livre de quadrados** se ele não for divisível pelo quadrado de um primo. Por exemplo, 5 é livre de quadrados, assim como 6 e 7, mas não 8 e 9.

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

Teorema 1.4.2 ([17], pag. 53) *Sejam K um corpo de números e $\alpha_1, \ldots, \alpha_n$ elementos de $\mathcal{O}_K$. Se $\Delta[\alpha_1, \ldots, \alpha_n]$ é um inteiro livre de quadrados então $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral.*

Por exemplo, como foi a visto, a $\mathbb{Q}$-base $\left\{1, \frac{1}{2}+\frac{1}{2}\sqrt{13}\right\}$ para $\mathbb{Q}(\sqrt{13})$ consiste de inteiros algébricos e tem discriminante 13 e sendo este livre de quadrados, aquela é uma base integral.

É importante observar que existem bases integrais cujo discriminante não é livre de quadrados. Portanto, a recíproca do Teorema 1.4.2 é falsa. Por exemplo, considere o corpo $K = \mathbb{Q}(\sqrt{7})$ que tem base integral $\{1, \sqrt{7}\}$ e discriminante $4.7 = 28$, o qual não é livre de quadrados.

Para duas bases integrais $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ de um corpo de números K, tem-se

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2.\Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n],$$

pois como foi visto na demonstração anterior a matriz correspondente à mudança de base é unimodular. Portanto, o discriminante de uma base integral independe da escolha da base. Este valor comum, denotado por D_K, é chamado discriminante de K e é sempre um número inteiro não nulo. Corpos de números isomorfos têm o mesmo discriminante.

1.5 Norma e Traço

A partir da norma e do traço, conceitos importantes da Teoria Algébrica dos Números, é possível transformar um problema de inteiros algébricos em um de números inteiros.

Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$.

Como foi visto, o polinômio característico é uma potência do polinômio minimal, e então pelo Lema 1.3.3 e o Lema de Gauss ([17], pag. 19), segue que um elemento α de K é um inteiro

algébrico se, e somente se, seu polinômio característico tem coeficientes inteiros. Pelo Teorema 1.2.2 garante-se que os coeficientes do polinômio característico, ou seja,

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

são racionais.

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

$$\begin{aligned} N_{L/K}(\alpha) &= \prod_{i=1}^{n}\sigma_i(\alpha), \\ Tr_{L/K} &= \sum_{i=1}^{n}\sigma_i(\alpha). \end{aligned}$$

Portanto, se α é inteiro algébrico a norma e o traço deste elemento são inteiros. No contexto onde estiver explícito, a norma e o traço de α serão abreviados por $N(\alpha)$ e $Tr(\alpha)$, respectivamente.

Sejam a e b números racionais então

$$Tr(a\alpha + b\beta) = aTr(\alpha) + bTr(\beta).$$

Por exemplo, se $K = \mathbb{Q}(\sqrt{11})$ então os inteiros algébricos de K estão em $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$. As aplicações σ_i são dadas por:

$$\begin{aligned} \sigma_1(r + s\sqrt{11}) &= r + s\sqrt{11}, \\ \sigma_2(r + s\sqrt{11}) &= r - s\sqrt{11}. \end{aligned}$$

Assim,

$$\begin{aligned} N(r + s\sqrt{11}) = \sigma_1(r + s\sqrt{11}).\sigma_2(r + s\sqrt{11}) &= r^2 - 11s^2, \\ Tr(r + s\sqrt{11}) = \sigma_1(r + s\sqrt{11}) + \sigma_2(r + s\sqrt{11}) &= 2r. \end{aligned}$$

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

(1) $Tr_{L/K}(x + y) = Tr_{L/K}(x) + Tr_{L/K}(y)$,

(2) $Tr_{L/K}(cx) = cTr_{L/K}(x)$,

(3) $Tr_{L/K}(c) = nc$,

(4) $N_{L/K}(xy) = N_{L/K}(x).N_{L/K}(y)$,

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

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

(a) $N_{M/K}(x) = N_{L/K}(N_{M/L}(x))$,

(b) $Tr_{M/K}(x) = Tr_{L/K}(Tr_{M/L}(x))$.

Em particular, se $x \in L$, então:

(c) $Tr_{M/K}(x) = [M : L]Tr_{L/K}(x)$,

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

Proposição 1.5.1 ([17], pag. 55) *Seja $K = \mathbb{Q}(\theta)$ um corpo de números onde θ tem polinômio minimal p de grau n. A $\mathbb{Q}$-base $\{1, \theta, \ldots, \theta^{n-1}\}$ tem discriminante*

$$\Delta[1, \ldots, \theta^{n-1}] = (-1)^{n(n-1)/2} N(p'(\theta)),$$

onde p' é a derivada formal de p.

Exemplo 1.5.1 *Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[4]{5}$ e $f(X) = X^4 - 5 = irr(\theta, \mathbb{Q})$. Então,* $\Delta[1, \theta, \theta^2, \theta^3] = (-1)^6 . N_{K/\mathbb{Q}}(4\theta^3) = (4\theta^3)^4 = 256 \cdot 125$.

Esta seção será concluída observando-se uma simples identidade, relacionando o discriminante e o traço:

Proposição 1.5.2 ([17], pag. 56) *Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma $\mathbb{Q}$-base de K. Então*

$$\Delta[\alpha_1, \ldots, \alpha_n] = det(Tr(\alpha_i \alpha_j)).$$

1.6 Decomposição em Irredutíveis

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

Será provada a possibilidade de fatoração em $\mathcal{O}_K$ introduzindo um conceito mais geral: Define-se um domínio como sendo Noetheriano quando todo ideal é finitamente gerado. Esta nomenclatura deve-se a Emmy Noether (1882-1935), quem introduziu o conceito.

A seguir duas propriedades úteis:

A condição de Cadeia ascendente

Dada uma cadeia ascendente de ideais:

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

então se existe algum N para o qual $I_n = I_N$ para todo $n \geq N$.

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 ([17], 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 ([17], pag. 87) *O anel dos inteiros algébricos $\mathcal{O}_K$ de um corpo de números K é noetheriano.*

Agora, é necessário introduzir conceitos que serão úteis para os objetivos desta seção. Assim, serão listadas propriedades de unidades, elementos associados e irredutíveis. Para isto, será utilizada a Lei do Cancelamento; sendo assim, é necessário tomar o anel como sendo um domínio de integridade.

Ao fatorar um elemento não unitário x em um domínio D, é natural buscar-se fatores próprios $x = a.b$ ($k = m.n$ onde nem m ou n são unidades, então m e n são chamados fatores próprios e k é dito redutível). Se a ou b são redutíveis, pode-se expressá-los como produto de fatores próprios até que se obtenha a seguinte decomposição:

$$x = p_1 \ldots p_m$$

onde cada p_i é irredutível. Em geral isto não é possível, mas é no anel dos inteiros algébricos $\mathcal{O}$ de qualquer corpo de números, o que será mostrado no decorrer desta seção.

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

$$x = uy,$$

onde $y = u^{-1}x$. O elemento y é chamado associado de x se $x = uy$ onde u é uma unidade.

Proposição 1.6.2 ([17], pag. 84) *Para um domínio D,*
(a) *x é uma unidade se, e somente se, $x \mid 1$;*

(b) *quaisquer duas unidades são associadas e qualquer associado de uma unidade é uma unidade;*

(c) x, y *são associados se, e somente se,* $x \mid y$ *e* $y \mid x$*;*

(d) x *é irredutível se, e somente se, todo divisor de* x *é um associado de* x *ou uma unidade;*

(e) *um associado de um irredutível é irredutível.*

Algumas destas idéias podem ser expressas em termos de ideais:

Proposição 1.6.3 ([17], pag. 84) *Sejam* D *um domínio, e* x, y *elementos não nulos de* D*. Então:*

(a) $x \mid y$ *se, e somente se,* $< x > \supseteq < y >$;

(b) x *e* y *são associados se, e somente se,* $< x > = < y >$*;*

(c) x *é uma unidade se, e somente se,* $< x > = D$;

(d) x *é irredutível se, e somente se,* $< x >$ *é maximal dentre os ideais principais próprios de* D*.*

Corolário 1.6.1 ([17], pag. 88) *Fatoração em irredutíveis é possível em* $\mathcal{O}_K$*.*

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

Proposição 1.6.4 ([17], pag. 88) *Sejam* $\mathcal{O}_K$ *um 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* $\mathcal{O}_K$*.*

Diz-se 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 $i = 1, \dots, r$.

Os exemplos serão dados para corpos quadráticos no próximo capítulo. Será mostrado que, embora a unicidade da fatoração falhe para elementos em $\mathcal{O}_K$, a teoria da fatoração única vale para ideais. Primeiro, considera-se o seguinte exemplo:

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

em inteiros algébricos de $\mathbb{Q}(\sqrt{3},\sqrt{5})$. Se $K = \mathbb{Q}(\sqrt{15})$ e $L = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Então esta fatoração permanece no anel dos inteiros algébricos $\mathcal{O}_K$. Neste anel também tem-se a fatoração correspondente de ideais principais:

$$< 10 >=< \sqrt{5} >< \sqrt{5} >< \sqrt{5} >< \sqrt{5}+\sqrt{3} >< \sqrt{5}-\sqrt{3} > .$$

Fazendo a intersecção dos ideais desta fatoração com $\mathcal{O}_K$, e mais uma vez obtém-se ideais em $\mathcal{O}_K$, mas estes ideais não são principais. Por exemplo, seja $I =< \sqrt{5}+\sqrt{3} > \cap\, \mathcal{O}_K$. 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

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

Supõe-se I principal, por exemplo da forma $< a+b\sqrt{15} >= I$, então 2 deveria ser um múltiplo de $a+b\sqrt{15}$, e tomando-se a norma destes elementos tem-se,

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

Novamente tomando I principal, por exemplo $I =< k >$, tem-se $N(5+\sqrt{15}) = 2.5$ e $N(3+\sqrt{15}) = 2.(-3)$, então $N(k) \mid 2$. Sabe-se que $N(k) \neq \pm 1$, sendo I próprio. Se $N(k) = \pm 2$ então existe $a, b \in \mathbb{Z}$ com $N(a+b\sqrt{15}) = \pm 2 \Longrightarrow a^2 - 15b^2 = \pm 2$, mas tomando-se módulo 5, tem-se uma contradição. Então I não é principal.

A conclusão agora é clara: para fatorar o ideal principal $< x >$ no anel dos inteiros algébricos $\mathcal{O}_K$, então toma-se uma fatoração única de ideais

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

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

Fatoração de Ideais

Seja R um anel. Então um ideal $\mathfrak{a}$ de R é maximal se $\mathfrak{a}$ é um ideal próprio de R e não existem ideais de R estritamente entre $\mathfrak{a}$ e R, ou seja, um ideal $\mathfrak{a}$ de R, é dito ideal maximal se $\mathfrak{a} \neq R$ e não existe ideal J tal que $I \subsetneq J \subsetneq R$. Um ideal $\mathfrak{a} \neq R$ de R é primo, quando $\mathfrak{b}$ e $\mathfrak{c}$ são ideais de R com $\mathfrak{bc} \subseteq \mathfrak{a}$, então ou $\mathfrak{b} \subseteq \mathfrak{a}$ ou $\mathfrak{c} \subseteq \mathfrak{a}$.

Sejam $\mathfrak{a} = \langle a \rangle$, $\mathfrak{b} = \langle b \rangle$ e $\mathfrak{c} = \langle c \rangle$ ideais principais. Então $x \mid y$ é equivalente a seguinte inclusão $\langle y \rangle \subseteq \langle x \rangle$. Assim, a afirmação

$$\mathfrak{bc} \subseteq \mathfrak{a}$$

implica em $\mathfrak{b} \subseteq \mathfrak{a}$ ou $\mathfrak{c} \subseteq \mathfrak{a}$, e isto se traduz em

$$a \mid bc \quad \text{implica} \quad a \mid b \quad \text{ou} \quad a \mid c.$$

Dado um domínio de integridade R, o ideal nulo é primo. E aqui define-se $< p >$ como ideal primo se, e somente se, p é um número primo ou nulo.

A partir da definição que foi dada para um ideal primo pode-se fazer as seguintes caracterizações simples:

Lema 1.6.1 ([17], pag. 115) *Seja R um anel e $\mathfrak{a}$ um ideal de R. Então:*
(a) *$\mathfrak{a}$ é maximal se, e somente se, $R/\mathfrak{a}$ é um corpo.*
(b) *$\mathfrak{a}$ é primo se, e somente se, $R/\mathfrak{a}$ é um domínio.*

Corolário 1.6.2 ([17], pag. 115) *Todo ideal maximal é primo.*

Agora serão listados algumas propriedades do anel dos inteiros algébricos de um corpo de números, as quais serão importantes mais à frente:

Teorema 1.6.2 ([17], 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 de fato um domínio, pois é um anel comutativo, com unidade. Denota-se por $Fr(\mathcal{O}_K)$ o corpo de frações de $\mathcal{O}_K$. Claramente $Fr(\mathcal{O}_K) \subset K$, pois $\mathcal{O}_K \subseteq K$. Por outro lado, $K \subseteq Fr(\mathcal{O}_K)$ pois, dado $\alpha \in K$, pelo Lema 1.3.2, $c.\alpha \in \mathcal{O}_K$, com $c \in \mathbb{Z}^*$. Assim $\frac{c\alpha}{c} \in Fr(\mathcal{O}_K)$ e, portanto, $Fr(\mathcal{O}_K) = K$.

(b) Pelo Teorema 1.4.1 o grupo $(\mathcal{O}_K, +)$ é abeliano livre de posto n. Segue que se $\mathfrak{a}$ é um ideal de $\mathcal{O}_K$, então $(\mathfrak{a}, +)$ é abeliano livre de posto $\leq n$ (pois todo subgrupo abeliano livre de um grupo abeliano livre tem posto $\leq n$). Tem-se 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.
O item **(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 $s \in \mathfrak{p}$ e daí $\langle s \rangle \subseteq \mathfrak{p}$ e isto implica que

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

Então, é necessário mostrar que o anel quociente $\mathcal{O}_K/\mathfrak{p}$ é finito. Logo, é suficiente mostrar que o anel quociente $\dfrac{\mathcal{O}_K}{\langle s\rangle}$ é finito. Sejam $\{e_1,\ldots,e_m\}$ uma base integral de $\mathcal{O}_K$ e

$$A=\{a_1e_1+\ldots+a_me_m : a_i\in\mathbb{Z},\ 0\leq a_i<s\},$$

logo $\#A=m^s$. Seja $x\in\mathcal{O}_K,\ x=\sum_{i=1}^{m}b_ie_i, b_i\in\mathbb{Z}$. Tem-se,

$$x=s\sum_{i=1}^{m}q_ie_i+\sum_{i=1}^{m}r_ie_i$$

onde $0\leq r_i<b_i$, e como $s\in\mathfrak{p}$ e $q_ie_i\in\mathcal{O}_K$, segue que $sq_ie_i\in\mathfrak{p}$ e

$$\overline{x}=\overline{\sum_{i=1}^{m}r_ie_i}$$

Portanto, $\dfrac{\mathcal{O}_K}{\langle s\rangle}$ é finito. Porém, sendo $\mathfrak{p}$ um ideal primo, $\mathcal{O}_K/\mathfrak{p}$ é um domínio (pelo item (b) do Lema 1.6.1) e como $\mathcal{O}_K/\mathfrak{p}$ é finito segue que $\mathcal{O}_K/\mathfrak{p}$ é um corpo. Portanto, pelo item (a) do Lema 1.6.1, $\mathfrak{p}$ é maximal. ∎

Um anel que satisfaça as 4 propriedades do Teorema 1.6.2 é chamado **Anel de Dedekind**. A prova da fatoração única de ideais é válida em todos os anéis de Dedekind, embora em aplicações precisa-se somente requerer o caso especial, quando o anel é o anel $\mathcal{O}_K$ de inteiros algébricos de um corpo de números K.

Nota-se que um ideal deve ser descrito como um $\mathcal{O}_K$-módulo de $\mathcal{O}_K$, e assim restringe-se ao estudo de $\mathcal{O}_K$-submódulos do corpo K. Os submódulos de interesse os quais darão estrutura de grupo desejada serão aqueles caracterizados pela seguinte propriedade:

Um $\mathcal{O}_K$-módulo $\mathfrak{a}$ de K é chamado um ideal fracionário de $\mathcal{O}_K$ se existe um c não nulo de $\mathcal{O}_K$ tal que $c\mathfrak{a}\subseteq\mathcal{O}_K$. Em outras palavras, o conjunto $\mathfrak{b}=c.\mathfrak{a}$ é um ideal de $\mathcal{O}_K$ e $\mathfrak{a}=c^{-1}\mathfrak{b}$. Assim os ideais fracionários de $\mathcal{O}_K$ são subconjuntos K da forma $c^{-1}\mathfrak{b}$ onde $\mathfrak{b}$ é um ideal de $\mathcal{O}_K$ e c um elemento não nulo de $\mathcal{O}_K$.

Exemplo 1.6.1 *Os ideais fracionários de $\mathbb{Z}$ são da forma $r\mathbb{Z}$ onde $r\in\mathbb{Q}$.*

É claro que se todo ideal de $\mathcal{O}_K$ é principal, então os ideais fracionários são da forma $c^{-1}\langle d\rangle=c^{-1}d\mathcal{O}_K$, onde d é um gerador. Pelo Teorema 1.6.2 item (a), isto significa que os ideais fracionários em um domínio de ideais principais $\mathcal{O}_K$ são apenas $\alpha\mathcal{O}_K$ onde $\alpha\in K$. 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, $\mathfrak{a}\subseteq\mathcal{O}_K$.

Teorema 1.6.3 ([17], pag. 117) *Os ideais fracionários não nulos de $\mathcal{O}_K$ formam um grupo abeliano multiplicativo.*

É conveniente provar este resultado juntamente com o teorema principal desta seção.

Teorema 1.6.4 ([17], pag. 117) *Todo ideal não nulo de $\mathcal{O}_K$ pode ser escrito como um produto de ideais primos unicamente a menos da ordem dos fatores.*

Demonstração:

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

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Para uma contradição, supõe-se que não. Então sendo $\mathcal{O}_K$ Noetheriano deve-se 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 $\mathfrak{bc} \subseteq \mathfrak{a},\ \mathfrak{b} \nsubseteq \mathfrak{a},\ \mathfrak{c} \nsubseteq \mathfrak{a}$. Sejam

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

Então $\mathfrak{a}_1.\mathfrak{a}_2 = (\mathfrak{a} + \mathfrak{b}).(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a},\ \mathfrak{a}_1 \supsetneqq \mathfrak{a}$ e $\mathfrak{a}_2 \supsetneqq \mathfrak{a}$. Pela maximalidade de $\mathfrak{a}$ existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ tais que

$$\begin{aligned} \mathfrak{p}_1 \ldots \mathfrak{p}_s &\subseteq \mathfrak{a}_1, \\ \mathfrak{p}_{s+1} \ldots \mathfrak{p}_r &\subseteq \mathfrak{a}_2. \end{aligned}$$

Assim,

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

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

(ii) Definição do inverso de um ideal $\mathfrak{a}$ de $\mathcal{O}_K$. Para cada ideal $\mathfrak{a}$ de $\mathcal{O}_K$, define-se

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

Afirmação 1: $\mathfrak{a}^{-1}$ é um $\mathcal{O}_K$-submódulo. De fato,

(a) 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 $(n_1 + n_2)\mathfrak{a} \subseteq \mathcal{O}_K$.

(b) 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 $\alpha x \in \mathfrak{a}^{-1}$.

Afirmação 2: $\mathfrak{a}^{-1}$ é um ideal fracionário. De fato, se $\mathfrak{a} \neq 0$ então para algum $c \in \mathfrak{a},\ c \neq 0$ temos $c.\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$.

Afirmação 3: $\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$. De fato, dado $x \in \mathcal{O}_K$ tem-se 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 $\mathcal{O}_K$.

Observa-se que dados $\mathfrak{p},\ \mathfrak{a}$ ideais de $\mathcal{O}_K,\ \mathfrak{a} \subseteq \mathfrak{p}$ implica que $\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

(iii) Se $\mathfrak{a}$ é um ideal próprio, então $\mathfrak{a}^{-1} \supsetneqq \mathcal{O}_K$. Sendo $\mathfrak{a} \subseteq \mathfrak{p}$, para algum ideal maximal $\mathfrak{p}$, logo $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ e assim é suficiente provar $\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Seja $a \in \mathfrak{p},\ a \neq 0$. Usando **(i)** toma-se 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 $\mathfrak{p}_i \subseteq \mathfrak{p}$. Sem perda de generalidade, suponha $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Daí $\mathfrak{p}_1 = \mathfrak{p}$ sendo que ideais primos em $\mathcal{O}_K$ são maximais, logo

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \nsubseteq \langle a \rangle,$$

pela minimalidade de r. Assim, pode-se afirmar que existe $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ tal que $b \notin \langle a \rangle$. 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 $ba^{-1} \in \mathfrak{p}^{-1}$. Mas $b \notin a\mathcal{O}_K$ e então $ba^{-1} \notin \mathcal{O}_K$, portanto, $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

(iv) Se $\mathfrak{a}$ é um ideal não nulo e $\mathfrak{a}S \subseteq \mathfrak{a}$ para qualquer subconjunto $S \subseteq K$, então $S \subseteq \mathcal{O}_K$. Deve-se mostrar que se $\mathfrak{a}\theta \subseteq \mathfrak{a}$ para $\theta \in S$, então $\theta \in \mathcal{O}_K$. Já que $S \subseteq K,\ \theta \in K$ e pelo Teorema 1.6.2 item **(c)**, tem-se que $\theta \in \mathcal{O}_K$, portanto, $S \subseteq \mathcal{O}_K$.

O próximo passo é importante para provar o Teorema 1.6.3.

(v) Se $\mathfrak{p}$ é um ideal maximal, então $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. Pelo item **(ii)**, $\mathfrak{p}\mathfrak{p}^{-1}$ é um ideal, onde

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

Sendo $\mathfrak{p}$ maximal, $\mathfrak{p}\mathfrak{p}^{-1}$ é igual a $\mathfrak{p}$ ou a $\mathcal{O}_K$. Mas se $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, então pelo item **(iv)** tem-se que $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, o que contraria o item **(iii)**. Assim, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Agora pode-se extender **(iv)** para todo ideal $\mathfrak{a}$:

(vi) 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 **(ii)**, tem-se $\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, 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 $\mathcal{O}_K$. Assim sendo, não vale $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, pois pelo item **(iv)** implicaria, $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, contradizendo mais uma vez o item **(iii)**. Assim, $\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1}$ e pela maximalidade de $\mathfrak{a}$ implica que $\mathfrak{a}\mathfrak{p}^{-1}$ satisfaz

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

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

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

ou,

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

Portanto,

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

(vii) Todo ideal fracionário $\mathfrak{a}$ tem um inverso $\mathfrak{a}^{-1}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$. Sabe-se que $\mathfrak{F}$, o conjunto dos ideais fracionários, é um semi-grupo, isto é, vale a lei do fechamento e tem unidade. Então, dado um ideal fracionário $\mathfrak{a}$, somente é necessário 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.

(viii) Todo ideal não nulo $\mathfrak{a}$ é um produto de ideais primos. Supõe-se $\mathfrak{a}$ 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 **(vi)** $\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Por outro lado, pela maximalidade de $\mathfrak{a}$ tem-se 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, $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r$.

(ix) 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:

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

Supõe-se que para todo $t < min\{r, s\}$ seja verdadeira a seguinte afirmação: Sejam $\mathfrak{a}_1, \dots, \mathfrak{a}_t, \mathfrak{b}_1, \dots, \mathfrak{b}_s$ ideais primos não nulos de modo que

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

Sendo $min\{r, s\} = 1$, considera-se por exemplo $r = 1$. Então, $\mathfrak{a}_1 = \mathfrak{b}_1 \dots \mathfrak{b}_s$, e como $\mathfrak{a}_1$ é primo, tem-se $s = 1$. De $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{q}_1$, conclui-se que $\mathfrak{q}_1$ divide $\mathfrak{p}_1 \dots \mathfrak{p}_r$ e, sem perda de generalidade, pode-se supor $\mathfrak{q}_1 = \mathfrak{p}_1$. Obtendo-se 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 1.6.5 *Fatoração de elementos em $\mathcal{O}_K$ em irredutíveis é única se, e somente se, todo ideal de $\mathcal{O}_K$ é principal.*

Ideais fracionários também fatoram-se unicamente se forem permitidas potências negativas de ideais primos.

A seguir serão estudadas a decomposição de $\mathfrak{p}$ em L, isto é, a fatoração do ideal estendido $\mathfrak{p}\mathcal{O}_L$ em ideais $\mathfrak{p}_i'$ de $\mathcal{O}_L$.

Proposição 1.6.5 ([*15*], 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*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \tag{1.5}$$

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 relação 1.5 usa-se a seguinte terminologia: g é chamado o **número de decomposição** de $\mathfrak{p}$ na extensão L/K. Como foi notado, os ideais primos acima de um dado ideal primo $\mathfrak{p}$ são os únicos que ocorrem na decomposição prima de $\mathfrak{p}\mathcal{O}_L$. Os expoentes com os quais ocorrem são chamados de **índices de ramificação** e serão denotados por $e(\mathfrak{q} \mid \mathfrak{p})$. Diz-se que um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ é ramificado em $\mathcal{O}_L$ (ou em L) se, e somente se, $e(\mathfrak{q}|\mathfrak{p}) > 1$ para algum ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$.

Nas condições da Proposição anterior, diz-se que os ideais $\mathfrak{p}_{i's}$ estão acima de $\mathfrak{p}$ ou $\mathfrak{p}$ está abaixo dos $\mathfrak{p}_{i's}$. Esta propriedade é equivalente a validade de um dos itens do Teorema abaixo:

Teorema 1.6.6 ([*10*], 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) $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$,

(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 1.6.7 ([*10*], 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* $\mathcal{O}_L$.

Existe outro número importante associado com um par de ideais primos $\mathfrak{p}$ e $\mathfrak{q}$, $\mathfrak{q}$ está acima de $\mathfrak{p}$. Sabe-se 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.

Existe um modo no qual $\mathcal{O}_K/\mathfrak{p}$ pode ser visto como um subcorpo de $\mathcal{O}_L/\mathfrak{q}$: como $\mathcal{O}_K \subset \mathcal{O}_L$ tem-se que $\mathcal{O}_K$ em $\mathcal{O}_L$ induz um homomorfismo de anéis $\mathcal{O}_K \longrightarrow \mathcal{O}_L/\mathfrak{q}$, e o núcleo é $\mathcal{O}_K \cap \mathfrak{q}$. Sabe-se que $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ (pelo Teorema 1.6.6, item (d)), então obtém-se a imersão $\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{q}$. Estes são chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$. Estes corpos são finitos e assim $\mathcal{O}_L/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_K/\mathfrak{p}$. Seja f este grau. Então f é chamado de **grau inercial** ou **grau residual** de $\mathfrak{q}$ sobre $\mathfrak{p}$ e é denotado por $f(\mathfrak{q} \mid \mathfrak{p})$.

Nota-se que e e f são multiplicativos nas extensões de ideais, isto é, 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

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

Os resultados a seguir serão importantes para o desenvolvimento desta teoria, e conseqüêntemente deste trabalho.

Teorema 1.6.8 *(Igualdade Fundamental)* ([*10*], pag. 65) *Sejam* n *o grau de* L *sobre* K *e* $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *os ideais primos de* $\mathcal{O}_L$ *acima do ideal primo* $\mathfrak{p}$ *de* $\mathcal{O}_K$. *Denota-se por* $e_1, \ldots, e_n$ *e* $f_1, \ldots, f_n$ *os correspondentes índices de ramificação e graus residuais. Então:*

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

Esta igualdade rege a decomposição de cada ideal primo $\mathfrak{p}$ no anel $\mathcal{O}_L$ e também permite tipos de decomposição diferentes de $\mathfrak{p}$ as quais serão vistas no capítulo 3.

Teorema 1.6.9 ([*10*], pag. 72) *Seja* K *um corpo de números. Uma condição necessária e suficiente para que um ideal primo* $p\mathbb{Z}$ *de* $\mathbb{Z}$ *se ramifique em* $\mathcal{O}_K$ *é que* p *divida* D_K.

Em decorrência deste resultado, existe apenas um número finito de primos que se ramifique em $\mathcal{O}_K$.

Lema 1.6.2 *(Lema de Kummer)*([*1*], pag. 186) *Sejam* K *um corpo de números,* $\mathcal{O}_K$ *o seu anel de inteiros algébricos e* $\theta \in \mathcal{O}_K$ *tal que* $K = \mathbb{Q}(\theta)$. *Dados um número primo* p *tal que não divide*

$[\mathcal{O}_K : \mathbb{Z}[\theta]]$ *e* $f(X)$ *o polinômio irredutível de* θ *sobre* $\mathbb{Q}$, *então existem* $p_1(X), \ldots, p_g(X) \in \mathbb{Z}[X]$, *polinômios irredutíveis,* $e_1, \ldots, e_g \in \mathbb{N}^*$ *tais que*

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

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

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

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

Exemplos do Lema de Kummer e do Teorema 1.6.8 serão vistos no próximo capítulo.

Na seção seguinte serão consideradas a norma de um ideal e sua propriedade multiplicativa, uma vez já tendo tratado algumas conseqüências simples da fatoração única.

1.7 Norma de um Ideal

Define-se norma de um ideal como sendo uma generalização da norma absoluta $\mid N_{K/\mathbb{Q}} \mid$, a qual também é multiplicativa, como será visto nesta seção.

Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Define-se $N(\mathfrak{a})$, norma do ideal $\mathfrak{a}$, onde $\mathfrak{a}$ é um ideal não nulo, como sendo o número de elementos de $\mathcal{O}_K/\mathfrak{a}$, ou seja,

$$N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a}).$$

Assim, $N(\mathfrak{a})$ é um inteiro não negativo. A norma definida acima aplica-se somente a ideais, o que não ocorre com a definida anteriormente.

Existe uma conexão entre as duas normas a qual será mostrada a seguir:

Teorema 1.7.1 ([*17*], pag. 126)
(a) *Todo ideal* $\mathfrak{a} \in \mathcal{O}_K$, *com* $\mathfrak{a} \neq 0$, *tem-se uma* $\mathbb{Z}$*-base* $\{\alpha_1, \ldots, \alpha_n\}$, *onde* n *é o grau de* K.
(b) *Tem-se*

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

onde D_K *é o discriminante de* K.

Corolário 1.7.1 ([*17*], pag. 126) *Seja* $\mathfrak{a} = \langle a \rangle$ *um ideal principal não nulo. Então* $N(\mathfrak{a}) =\mid N(a) \mid$.

Exemplo 1.7.1 *Seja $\mathcal{O}_K$ o anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt{d})$, para d inteiro livre de quadrados. Então*

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

em particular, tem-se

$$N(\langle 18\rangle) = 18^2.$$

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

Teorema 1.7.2 ([17], pag. 127) *Sejam K um corpo de números e $\mathfrak{a}$, $\mathfrak{b}$ ideais não nulos de $\mathcal{O}_K$. Então*

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

Exemplo 1.7.2 *Sejam $K = \mathbb{Q}(\sqrt{-21})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-21}]$ seu anel dos inteiros algébricos e os ideais primos de $\mathcal{O}_K$, $\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-21}\rangle$ e $\mathfrak{p}_2 = \langle 11, 1 - \sqrt{-21}\rangle$. Todo elemento em $\mathbb{Z}[\sqrt{-21}]$ está ou em $\mathfrak{p}_1$ ou é da forma $1 + x$, para $x \in \mathfrak{p}_1$, tem-se assim,*

$$|\mathbb{Z}[\sqrt{-21}]/\mathfrak{p}_1| = 2 = N(\mathfrak{p}_1).$$

Analogamente,

$$|\mathbb{Z}[\sqrt{-21}]/\mathfrak{p}_2| = 11 = N(\mathfrak{p}_2).$$

Logo, pelo Teorema 1.7.2, segue que

$$N(\mathfrak{p}_1^2\mathfrak{p}_2^3) = 2^2 11^3.$$

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 escreve-se também $\mathfrak{a} \mid b$ e diz-se que $\mathfrak{a}$ divide b. É claro que $\mathfrak{a} \mid b$ se, e somente se, $b \in \mathfrak{a}$.

Por exemplo, se $\mathfrak{p}$ é um ideal primo e $\mathfrak{p} \mid \langle a\rangle\langle b\rangle$, então deve-se ter $\mathfrak{p} \mid \langle a\rangle$ ou $\mathfrak{p} \mid \langle b\rangle$. Logo, para $\mathfrak{p}$ primo, $\mathfrak{p} \mid ab$ implica $\mathfrak{p} \mid a$ ou $\mathfrak{p} \mid b$.

Teorema 1.7.3 ([17], 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.

Mais particularmente, o item (c) do Teorema 1.7.3 pode ser escrito da seguinte maneira: para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$ tem-se que $N(\mathfrak{p}) = p^f$, onde f é o grau residual de $\mathfrak{p}$ e p o único número primo em $\mathfrak{p}$. De fato, como $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = f$ então resulta que $\mathcal{O}_K/\mathfrak{p}$ tem p^f elementos.

Exemplo 1.7.3 *Sejam* $K = \mathbb{Q}(\sqrt{-17})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$, *seu anel dos inteiros algébricos,* $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-17}\rangle$, *ideal primo de* $\mathcal{O}_K$. *Então* $N(\mathfrak{p}_1) = 2$ *e pode-se imediatamente deduzir que* $\mathfrak{p}_1$ *é primo. Nota-se que* $N(\mathfrak{p}_1) = 2 \in \mathfrak{p}_1$, *como assegura o Teorema 1.7.3 item* **(b)**.

Exemplo 1.7.4 *Seja* $\mathfrak{a}$ *um ideal primo satisfazendo:*

$$N(\mathfrak{a}) = p^m, \quad \textit{onde } m{>}1.$$

Isto significa que um ideal primo não tem necessariamente uma norma que seja um primo, por exemplo, $\mathcal{O}_K = \mathbb{Z}[i]$, $\mathfrak{a} = \langle 3\rangle$. *Aqui, 3 é irredutível em* $\mathbb{Z}[i]$, *logo é primo, pois* $\mathbb{Z}[i]$ *tem fatoração única. Como um elemento que é primo então o ideal que ele gera também é primo. Assim,* $\langle 3\rangle$ *é primo em* $\mathbb{Z}[i]$, *mas*

$$N(\langle 3\rangle) = \mid N(3) \mid = 3^2.$$

Capítulo 2

Corpos Quadráticos e Ciclotômicos

Este capítulo tem por objetivo apresentar o método algébrico para obtenção de reticulados e a fórmula da sua densidade de centro.

Para tanto serão caracterizados o anel dos inteiros algébricos e o discriminante de um corpo quadrático e de um corpo ciclotômico. Para este último também é apresentado o cálculo para encontrar seu polinômio ciclotômico.

Na seção de Corpos Abelianos, o Teorema de Kronecker-Weber será relevante para o estudo das cúbicas. Além de enunciá-lo, será visto também a decomposição de um ideal em uma extensão galoisiana. Logo em seguida serão dadas as definições de empacotamento esférico, empacotamento reticulado, raio de empacotamento e densidade de empacotamento.

A seção será finalizada introduzindo o método algébrico. Este método descreve um reticulado via representação geométrica de ideais. Além disso, será visto que a densidade de centro de tais reticulados depende do discriminante do Corpo de Números, da norma do ideal considerado e do menor valor assumido por uma forma quadrática.

2.1 Corpos Quadráticos

Um corpo quadrático é um corpo de números K de grau 2. Então $K = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, e θ é um zero da seguinte equação:

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

Logo

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

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

Assim,

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

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

Teorema 2.1.1 ([17], pag. 67) *Os corpos quadráticos são da forma* $\mathbb{Q}(\sqrt{d})$, *onde* d *é um inteiro livre de quadrados.*

Agora será determinado o anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados, o qual depende de propriedades algébricas da congruência de d módulo 4, que serão vistas na demonstração do teorema a seguir.

Teorema 2.1.2 ([17], 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*

$$\alpha = \begin{cases} \sqrt{d}, & se \;\; d \equiv 2 \;\; ou \;\; 3 \;\; (mod \;\; 4); \\ \dfrac{1+\sqrt{d}}{2}, & se \;\; d \equiv 1 \;\; (mod \;\; 4). \end{cases} \tag{2.1}$$

Demonstração: Tem-se que α é raiz do polinômio irredutível $X^2 - d$ ou $X^2 - X + \frac{d-1}{4}$ ambos pertencentes a $\mathbb{Z}[X]$, conforme $d \equiv 2$ ou $3 \equiv (mod\ 4)$, ou a $d \equiv 1\ (mod\ 4)$, ou seja, α é um inteiro algébrico e, portanto, $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$. Reciprocamente, seja $\gamma = r + s\sqrt{d} \in \mathcal{O}_K,\ r,\ s \in \mathbb{Q}$. Supõe-se que $s = 0$, então $r \in \mathbb{Z}$, logo $\gamma \in \mathbb{Z} \subset \mathbb{Z}[\alpha]$. Pode-se supor agora que $s \neq 0$, então

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

Logo, $2r,\ r^2 - ds^2 \in \mathbb{Z}$, conseqüentemente $(2r^2) - d(2s)^2 \in \mathbb{Z}$. Visto que $2r \in \mathbb{Z}$, então $d(2s)^2 \in \mathbb{Z}$ e agora será mostrado que $2s \in \mathbb{Z}$. Supõe-se que $2s \notin \mathbb{Z}$, isto é, $2s = \dfrac{x}{y}$, com $(x, y) = 1$. Sendo $y \neq 1$, existe um primo p tal que p^2 divide y^2. Mas, para que $d(2s)^2$ seja inteiro é necessário que p^2 divida d, o que contrario o fato de d ser livre de quadrados, portanto, $2s \in \mathbb{Z}$. Fazendo $r = \dfrac{u}{2},\ s = \dfrac{v}{2},\ u,\ v \in \mathbb{Z}$, tem-se que $u^2 - dv^2 \in 4\mathbb{Z}$. Sendo $u^2 \equiv 0$ ou $1(mod\ 4)$ se $d \equiv 2$ ou $3(mod\ 4)$ a única possibilidade para que $u^2 - dv^2 \in 4\mathbb{Z}$ é $u \equiv v \equiv 0\ (mod\ 2)$ e, portanto, $\gamma \in \mathbb{Z}[\sqrt{d}]$. Assim, $\mathbb{Z}[\alpha] = \mathcal{O}_K$ se $d \equiv 2$ ou $3\ (mod\ 4)$. Entretanto, se $d \equiv 1\ (mod\ 4)$, então $u^2 \equiv v^2 \equiv 1\ (mod\ 4)$ também é admissível, isto é, para que $\gamma = \dfrac{u}{2} + \dfrac{v}{2}\sqrt{d}$ seja inteiro algébrico é suficiente que u e v tenham a mesma paridade. Logo $u - v = 2t$, portanto, $u = 2t + v$ e $\gamma = t.1 + v.\left(\dfrac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\alpha]$ e conseqüentemente, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ quando $d \equiv 1\ (mod\ 4)$. ∎

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

$$\begin{aligned} \sigma_1(r + s\sqrt{d}) &= r + s\sqrt{d}; \\ \sigma_2(r + s\sqrt{d}) &= r - s\sqrt{d}. \end{aligned}$$

Assim tem-se o seguinte cálculo para o discriminante:

Teorema 2.1.3 ([*17*], pag. 68)
(i) *Se* $d \equiv 2$ *ou* 3 $(mod\ 4)$ *então* $\mathbb{Q}(\sqrt{d})$ *tem discriminante* $4d$.
(ii) *Se* $d \equiv 1$ $(mod\ 4)$ *então* $\mathbb{Q}(\sqrt{d})$ *tem discriminante* d.

Demonstração: Usando o Teorema 2.1.2 tem-se o seguinte cálculo para o discriminante:

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

e

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

■

Um exemplo especial, é o primeiro corpo de números a ser estudado: o corpo de números Gaussiano $K = \mathbb{Q}(\sqrt{-1})$. Conforme o Teorema 2.1.2, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, também conhecido como anel dos inteiros algébricos Gaussianos e seu discriminante, pelo Teorema 2.1.3, é 4. Neste caso, os monomorfismos σ_i de K em $\mathbb{C}$ são σ_1 a inclusão e σ_2 a conjugação, isto é,

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

Logo,

$$\begin{aligned} N(r+s\sqrt{-1}) &= r^2+s^2; \\ Tr(r+s\sqrt{-1}) &= 2r. \end{aligned}$$

Mais geralmente, tem-se que a norma e o traço do elemento $r+s\sqrt{d}$ de $\mathbb{Q}(\sqrt{d})$ (ou K) são, respectivamente,

$$r^2-ds^2 \quad \text{e} \quad 2r.$$

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

Abaixo serão mostrados exemplos de fatoração em irredutíveis, aplicação do Lema de Kummer e igualdade fundamental em corpos quadráticos.

Exemplo 2.1.1 *Em* $\mathbb{Q}(\sqrt{-5})$ *tem-se a seguinte fatoração:*

$$6 = 2.3 = (1+\sqrt{-5}).(1-\sqrt{-5}).$$

Afirmação: $2,\ 3,\ 1+\sqrt{-5}$ *e* $1-\sqrt{-5}$ *são irredutíveis em* $\mathcal{O}_K$*, o anel dos inteiros algébricos de* $\mathbb{Q}(\sqrt{-5})$*. De fato, como foi visto, a norma é dada por:*

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

Então as normas dos elementos acima citados são $4,\ 9,\ 6$ *e* 6*, respectivamente. Se* $2 = x\cdot y$*, onde* $x,\ y \in \mathcal{O}_K,$ *e não são unidades, então* $4 = N(2) = N(x)\cdot N(y)$*. Logo* $N(x) = \pm 2,\ N(y) = \pm 2$*. Analogamente, os divisores não triviais de 3 devem, se existirem, ter norma* ± 3*, enquanto os divisores não triviais de* $1\pm\sqrt{-5}$ *devem ter norma* ± 2 *ou* ± 3*. Como* $-5 \not\equiv 1\ (mod\ 4)$*, os inteiros algébricos em* $\mathcal{O}_K$ *são da forma* $a+b\sqrt{-5}$ *para* $a,\ b \in \mathbb{Z}$*. Então tem-se as seguintes equações:*

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

Agora, $|b| \geq 1$ *implica* $|a^2+5b^2| \geq 5$*; e então a única possibilidade é* $|b| = 0$*. No entanto tem-se* $a^2 = \pm 2$ *ou* ± 3 *o que é impossível em* $\mathbb{Z}$*. Então os supostos divisores não existem e os quatro fatores são todos irredutíveis. Sendo* $N(2) = 4,\ N(1+\sqrt{-5}) = 6$*, pela Proposição 1.6.4 item* **(b)***, 2 não é associado de* $1+\sqrt{-5}$ *ou* $1-\sqrt{-5}$*, então a fatoração não é única.*

Exemplo 2.1.2 *Sejam* $K = \mathbb{Q}(\sqrt{7}),\ \mathbb{Z}[\sqrt{7}]$ *o anel dos inteiros algébricos de* K *e* X^2-7 *o polinômio irredutível de* $\sqrt{7}$ *sobre* $\mathbb{Q}$*. Considera-se o ideal* $2\mathbb{Z} \subset \mathbb{Z}$*. O polinômio* X^2-7 *fatora-se como:*

$$X^2-7 \equiv (X+1)^2\ (mod\ 2\mathbb{Z}[X])$$

e pelo Lema de Kummer 1.6.4 e pela Igualdade Fundamental 1.6.8, $2\mathcal{O}_K = \mathfrak{p}^2,\ \mathfrak{p} = \langle 2, \theta+1\rangle$ *sendo o único ideal primo de* $\mathcal{O}_K$ *acima de* $2\mathbb{Z}$ *e novamente pela Igualdade Fundamental o grau residual é 1 e a norma é 2. Agora, considerando o ideal* $5\mathbb{Z} \subset \mathbb{Z}$ *tem-se que o polinômio* X^2-7 *fatora-se como:*

$$X^2-7 \equiv (X+3)(X+2)\ (mod\ 5\mathbb{Z}[X])$$

e novamente pelo Lema de Kummer e pela Igualdade Fundamental, $3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$*, sendo*

$$\mathfrak{p}_1 = \langle 3, \theta+3\rangle \quad e \quad \mathfrak{p}_2 = \langle 3, \theta+2\rangle$$

os ideais de $\mathcal{O}_K$ *acima de* $5\mathbb{Z}$ *e, da Igualdade Fundamental tem-se que os graus residuais são iguais a 1 e,* $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 3$*.*

2.2 Corpos Ciclotômicos

O corpo $\mathbb{Q}(\zeta_n)$ é chamado n-ésimo corpo ciclotômico, onde $\zeta_n = e^{2\pi i/n}$ é uma raiz n-ésima primitiva da unidade e $\Phi_n(X) = \prod_{\substack{i=1\\(i,n)=1}}^{n} (X-\zeta_n^i)$ é o n-ésimo polinômio ciclotômico. O polinômio

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

Lema 2.2.1 ([*11*], pag. 110) *Se n é um inteiro positivo então*

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

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

$$X^n - 1 = \prod_{\substack{i=0 \\ (i,n)=d_1}}^{n-1} (X - \zeta_n^i). \prod_{\substack{i=0 \\ (i,n)=d_2}}^{n-1} (X - \zeta_n^i) \ldots \prod_{\substack{i=0 \\ (i,n)=d_s}}^{n-1} (X - \zeta_n^i),$$

e

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

Note que se $d = (j, n)$ então $\zeta_n^j = \zeta_{n/d}^{j/d}$, assim

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

com $t = \frac{n}{d}$ e $j = \frac{i}{d}$. Repetindo o mesmo argumento em todos os fatores tem-se

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

como $\frac{n}{d_1}, \ldots, \frac{n}{d_s}$ também são todos os divisores de n, segue o resultado. ∎

Exemplo 2.2.1 *Tem-se que, $X^p - 1 = \Phi_1 \cdot \Phi_p$, p primo. Assim*

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

Mais geralmente, para as potências de um número primo p, $p^r, r > 1$ tem-se

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

e, portanto, $\Phi_{p^r}(X) = X^{p^{r-1}.(p-1)} + X^{p^{r-1}.(p-2)} + \ldots + X^{p^{r-1}} + 1$. O polinômio Φ_{10} obtém-se da igualdade:

$$X^{10} - 1 = \Phi_1 \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_{10} = (X^5 - 1)(X + 1)\Phi_{10},$$

ou seja, $\Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1$.

Lema 2.2.2 ([*11*], pag. 114) *Seja n um inteiro positivo. Então o n-ésimo polinômio ciclotômico Φ_n tem coeficientes inteiros.*

Demonstração: A demonstração é feita por indução sobre n. No caso em que $n = 1$ tem-se que $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Supõe-se que esta afirmação é verdadeira para $2,\ 3, \ldots,\ n-1$ e será provado que vale para n. Sendo

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

e tomando $\prod_{\substack{d|n \\ d<n}} \Phi_d = f(X)$ tem-se $X^n - 1 = \Phi_n(X).f(X)$, e por hipótese de indução, $f(X) \in \mathbb{Z}[X]$. Sejam

$$\begin{aligned} \Phi_n(X) &= X^m + a_{m-1}X^{m-1} + \ldots + a_0; \\ f(X) &= X^r + b_{r-1}X^{r-1} + \ldots + b_0; \end{aligned}$$

$b_j \in \mathbb{Z},\ j = 1, \ldots, r-1$.

Afirmação: $a_i \in \mathbb{Z},\ i = 1, \ldots, m-1$. De fato, supõe-se que $a_{m-1},\ a_{m-2}, \ldots, a_v \in \mathbb{Z}$ e $a_{v-1} \notin \mathbb{Z}$. Então,

$$X^n - 1 = X^{m+r} + (b_{r-1} + a_{m-1})X^{m+r-1} + \ldots + a_0 b_0$$

e, pela igualdade de polinômios, conclui-se que os coeficientes de $\Phi_n(X)f(X)$ são inteiros, logo $a_{v-1} \in \mathbb{Z}$, absurdo, pois por hipótese $a_{v-1} \notin \mathbb{Z}$. Portanto, $\Phi_n(X) \in \mathbb{Z}[X]$. ∎

Lema 2.2.3 ([*11*], pag. 116) *Seja n inteiro positivo. Então o n-ésimo polinômio ciclotômico* $\Phi_n(X)$ *é irredutível sobre* $\mathbb{Q}$.

Demonstração: Seja $f(X) = irr(\zeta_n, \mathbb{Q})$. Então existe $g(X) \in \mathbb{Q}[X]$ mônico, tal que,

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

Afirmação: $\Phi_n(X) = f(X)$. De fato, sejam $K = \mathbb{Q}(\zeta_n),\ \mathcal{O}_K$ o anel dos inteiros algébricos de K, $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $p \in \mathfrak{p}$ um número primo, $(p, n) = 1$. Supondo que ζ_n^p não é raiz de $f(X)$, então é raiz de $g(X)$. Seja $g(X) = c_0 + c_1X + \ldots + c_tX^t$. Tem-se que em $\mathcal{O}_K/\mathfrak{p}$ vale

$$\overline{g(\zeta_n^p)} = \overline{c_0 + c_1\zeta_n^p + \ldots + c_t(\zeta_n^t)^p} = \overline{0},$$

onde $\overline{a}$ denota a classe de a em $\mathcal{O}_K/\mathfrak{p}$.

Considera-se o seguinte homomorfismo:

$$\begin{array}{rccc} \psi : & \dfrac{\mathcal{O}_K}{\mathfrak{p}} & \longrightarrow & \dfrac{\mathcal{O}_K}{\mathfrak{p}} \\ & X & \longmapsto & X^p \end{array}$$

e visto que $p \in \mathfrak{p}$, tem-se que ψ é injetiva e pela demonstração do Teorema 1.6.2, $\mathcal{O}_K/\mathfrak{p}$ é finito; segue que a aplicação é sobrejetiva. Assim

$$\overline{g(\zeta_n^p)} = \overline{c_0 + (c_1\zeta_n)^p + \ldots + (c_t\zeta_n^t)^p} = \overline{(c_0 + c_1\zeta_n + \ldots + c_t\zeta_n^t)^p} = \overline{0}$$

e, portanto,

$$\overline{g(X)} = \overline{(c_0 + c_1X + \ldots + c_tX^t)^p}.$$

Como foi visto,

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

e por outro lado, em $\mathcal{O}_K/\mathfrak{p}$,

$$\overline{X^n - 1} = \overline{f(X)g(X)}.\overline{\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}. \tag{2.2}$$

Logo $\overline{X^n - 1}$ tem raízes múltiplas, a menos que $g(X)$ seja constante. Derivando o lado esquerdo da equação (2.2), tem-se $\overline{nX^{n-1}}$; como p não divide n, $\overline{0}$ é a única raiz para a derivada. Sendo que $\overline{0}$ 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 ζ_n sobre $\mathbb{Q}$ de grau $\phi(n)$, onde ϕ é a função de Euler.
Uma propriedade importante é que dado $n = p_1^{a_1} \ldots p_s^{a_s}$, sua fatoração em primos, então $\phi(n) = (p_1 - 1)\ldots(p_s - 1)p_1^{a_1-1}\ldots p_s^{a_s-1}$.

Corpos Ciclotômicos do tipo $\mathbb{Q}(\zeta_p)$

Nesta seção serão vistos o traço, a norma e o discriminante de $\mathbb{Q}(\zeta_p)$, para qualquer número primo ímpar p ($p \neq 2$, pois caso contrário $\mathbb{Q}(\zeta_2) = \mathbb{Q}$).

As potências $\zeta_p,\ \zeta_p^2, \ldots,\ \zeta_p^{p-1}$ também são raízes p-ésimas da unidade, não iguais a 1, e também pelo mesmo argumento, têm $\Phi_p(X)$ como polinômio minimal. Assim, tem-se que

$$X^{p-1} + \ldots + X + 1 = \Phi_p(X) = (X - \zeta_p)(X - \zeta_p^2)\ldots(X - \zeta_p{}^{p-1}) \tag{2.3}$$

e então os conjugados de ζ_p são $\zeta_p,\ \zeta_p^2, \ldots,\ \zeta_p^{p-1}$. Isto significa que os monomorfismos de K em $\mathbb{C}$ são dados por

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

Para um elemento geral

$$\alpha = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}, a_i \in \mathbb{Q},$$

tem-se

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

A partir disto calcula-se norma e traço obtendo-se assim:

$$N(\alpha) = \prod_{i=1}^{p-1}\sigma_i(\alpha) \quad \text{e} \quad Tr(\alpha) = \sum_{i=1}^{p-1}\sigma_i(\alpha).$$

Em particular,

$$N(\zeta_p) = \zeta_p\zeta_p^2\ldots\zeta_p^{p-1}.$$

O traço de ζ_p pode ser calculado da seguinte maneira:

$$Tr(\zeta_p^i) = Tr(\zeta_p) = \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1}$$

e usando o fato que

$$f(\zeta_p) = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = 0$$

tem-se

$$Tr(\zeta_p^i) = -1,\ 1 \leq i \leq p-1. \tag{2.4}$$

Sendo $\zeta_p^p = 1$, pode-se usar esta fórmula para extender a equação (2.4) para

$$Tr(\zeta_p^s) = \begin{cases} -1, & \text{se} \quad s \not\equiv 0\ (mod\ p); \\ p-1, & \text{se} \quad s \equiv 0\ (mod\ p). \end{cases} \tag{2.5}$$

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

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

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

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

a qual pode ser calculada colocando $X = 1$ na equação (2.3) para obter

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

então, $N(1-\zeta_p) = p$.

Estes cálculos serão usados para encontrar o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_p)$.

Teorema 2.2.1 ([17], pags. 72, 74)
(a) *O anel dos inteiros algébricos de* $K = \mathbb{Q}(\zeta_p)$ *é* $\mathbb{Z}(\zeta_p)$*;*
(b) *O discriminante de* $\mathbb{Q}(\zeta_p)$*, onde* $\zeta_p = e^{2\pi i/p}$ *e* p *um primo ímpar é*

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

Demonstração: O item **(a)** decorre dos resultados obtidos anteriormente, então somente o item **(b)** será demonstrado.

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

$$(-1)^{(p-1)(p-2)/2}.N(f'(\zeta_p))$$

com $f(X)$ como acima. Sendo p um primo ímpar, o primeiro fator se reduz a $(-1)^{(p-1)/2}$. Para desenvolver o segundo toma-se

$$f(X) = \frac{X^p - 1}{X - 1},$$

então

$$f'(X) = \frac{(X-1)p\ X^{p-1} - (X^p - 1)}{(X-1)^2}$$

assim

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

Logo

$$\begin{aligned} N(f'(\zeta_p)) &= \frac{N(-p).N(\zeta_p)^{p-1}}{N(1-\zeta_p)} \\ &= \frac{(-p)^{p-1}.1^{p-1}}{p} = p^{p-2}. \end{aligned}$$

■

O Teorema abaixo identifica o anel dos inteiros algébricos do corpo $\mathbb{Q}(\zeta_n)$, para qualquer valor de n.

Teorema 2.2.2 ([19], pag. 11) *Seja n um inteiro positivo. Então o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$.*

Teorema 2.2.3 ([19], pag. 12) *O discriminante do corpo $K = \mathbb{Q}(\zeta_n)$ é:*

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

Demonstração: Pelo Lema 2.2.1,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{2.6}$$

Derivando ambos os lados da equação acima tem-se

$$nX^{n-1} = \Phi'_{d_1}(X)\left(\frac{X^n-1}{\Phi_{d_1}(X)}\right) + \ldots + \Phi'_{d_s}(X)\left(\frac{X^n-1}{\Phi_{d_s}(X)}\right)$$

em que $d_1, \ldots, d_s$ são divisores de n. Substituindo X por ζ_n, calculando a norma e usando a Proposição 1.5.1, segue que

$$n^{\phi(n)} = \pm D_K . N_{K/\mathbb{Q}}\left(\prod_{\substack{d|n \\ d<n}} \Phi_d(\zeta_n)\right).$$

Logo,

$$D_K = \pm \frac{n^{\phi(n)}}{N_{K/\mathbb{Q}}\left(\prod_{\substack{d|n \\ d<n}} \Phi_d(\zeta_n)\right)}.$$

Assim, falta provar que

$$N_{K/\mathbb{Q}}\left(\prod_{\substack{d|n \\ d<n}} \Phi_d(\zeta_n)\right) = \prod_{p|n} p^{\frac{\phi(n)}{p-1}}.$$

Fazendo

$$\frac{X^n-1}{\Phi_n(X)} = \frac{\prod_{i=0}^{n-1}(X-\zeta_n^i)}{\Phi_n(X)}$$

obtém-se,

$$\prod_{\substack{d|n \\ d<n}} \Phi_d(X) = \prod_{\substack{i=1 \\ (i,n)>1}}^{n} (X-\zeta_n^i)$$

e daí,

$$\prod_{\substack{d|n \\ d<n}} \Phi_d(\zeta_n) = \prod_{\substack{i=1 \\ (i,n)>1}}^{n} (\zeta_n - \zeta_n^i) = \prod_{\substack{i=1 \\ (i,n)>1}}^{n} (1-\zeta_n^{i-1}).$$

Logo,

$$\begin{aligned} N_{K/\mathbb{Q}}\left(\prod_{\substack{d|n\\ d<n}}\Phi_d(\zeta_n)\right) &= \prod_{\substack{i=1\\(i,n)>1}}^{n}\left(N_{K/\mathbb{Q}}(1-\zeta_n^{i-1})\right) \\ &= \prod_{\substack{i=2\\(i,n)>1}}^{n-1} N_{K/\mathbb{Q}}(1-\zeta_n^{i-1}) \\ &= \prod_{j=1}^{s}\left[\prod_{\substack{i=2\\(i,n)>1,\frac{n}{(i-1,n)}=p_j^{b_j}}}^{n-1} N_{K/\mathbb{Q}}(1-\zeta_n^{i-1})\right]. \end{aligned}$$

Quando $n=p^r$ já foi visto que $N_{K/\mathbb{Q}}(1-\zeta_{p^r}^i)=p$, e além disso, tem-se:

$$\begin{aligned} N_{K/\mathbb{Q}}(1-\zeta_{p^r}^i) &= N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(N_{K/\mathbb{Q}(\zeta_{p^r})}(1-\zeta_{p^r}^i)) \\ &= N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}^i)^{[K:\mathbb{Q}(\zeta_{p^r})]} = p^{[K:\mathbb{Q}(\zeta_{p^r})]}. \end{aligned}$$

Caso $n=n_1n_2,\ (n_1,n_2)=1$ tem-se $N_{K/\mathbb{Q}}(1-\zeta_n^i)=1$. De fato, seja

$$X^{n-1}+X^{n-2}+\ldots+X+1=\prod_{i=1}^{n-1}(X-\zeta_n^i).$$

Substituindo X por 1 tem-se

$$\begin{aligned} n &= \prod_{i=1}^{n-1}(1-\zeta_n^i) \\ &= \prod_{i=1}^{n_2-1}(1-\zeta_n^{in_1}).\prod_{i=1}^{n_1-1}(1-\zeta_n^{in_2}).\prod_{\substack{k=1\\n_1\nmid k,n_2\nmid k}}^{n-1}(1-\zeta_n^k) \\ &= \prod_{i=1}^{n_2-1}(1-\zeta_{n_2}^{i}).\prod_{i=1}^{n_1-1}(1-\zeta_{n_1}^{i}).\prod_{\substack{k=1\\n_1\nmid k,n_2\nmid k}}^{n-1}(1-\zeta_n^k) \end{aligned}$$

logo, $1=\prod_{\substack{k=1\\n_1\nmid k,n_2\nmid k}}^{n-1}(1-\zeta_n^k)$ e, portanto, $1=N_{K/\mathbb{Q}}\left(\prod_{\substack{k=1\\n_1\nmid k,n_2\nmid k}}^{n-1}(1-\zeta_n^k)\right)$. Diante de tais considerações, segue que:

$$N_{K/\mathbb{Q}}(1-\zeta_n^i)=\begin{cases} p^{[K:\mathbb{Q}(\zeta_{p^r})]}, & \text{se } \dfrac{n}{(i,n)}=p^r \\ 1, & \text{caso contrário.} \end{cases} \tag{2.7}$$

Impõe-se que $\dfrac{n}{(i-1,n)}=p_j^{b_j}, (i,n)>1$. Sendo $n=p_1^{a_1}\ldots p_s^{a_s}$ e $i-1=p_1^{a_1-1}\ldots p_s^{a_s-1}.v$, para $v=1,\ldots,p_s^{a_s}-1$, então

$$i-1=\frac{n}{p_j^{b_j}}.v,\ v=1,\ldots,p_j^{b_j}-1$$

e

$$(i-1,n)=\frac{n}{p_j^{b_j}},\ b_j\leq a_j.$$

Visto que $v=1,\ldots,p_j^{b_j}-1,\ p_j$ não divide v, então existe um único $v\in\{1,\ldots,p-1\}$ tal que

$$i=\frac{n}{p_j^{b_j}}v+1\equiv 0\ (mod\ p_j).$$

Logo, $(i-1,n)>p_j$ implicando $b_j=a_j$ e, portanto,

$$\prod_{j=1}^{s}\left[\prod_{\substack{i=2\\(i,n)>1,\frac{n}{(i-1,n)}=p_j^{b_j}}}^{n-1}N_{K/\mathbb{Q}}(1-\zeta_n^{i-1})\right]=\prod_{j=1}^{s}\left[\prod_{\substack{i=\frac{n}{p_j^{a_j}}v+1\\v=1,\ldots,p_j^{a_j}-1,\ i\equiv 0(mod\ p_j)}}^{p_{j-1}^{a_j-1}}N_{K/\mathbb{Q}}\left(1-\zeta_n^{\frac{n}{p_j^{a_j}}v+up_j}\right)\right]$$

$$=\prod_{j=1}^{s}\left[\prod_{\substack{u=0\\v:\text{conveniente}}}^{p_{j-1}^{a_j-1}}N_{K/\mathbb{Q}}(1-\zeta_{p_j^{a_j}}^{v+up_j})\right]$$

$$=\prod_{j=1}^{s}\left[\prod_{u=0}^{p_{j-1}^{a_j-1}}N_{\mathbb{Q}(\zeta_{p_j^{a_j}})/\mathbb{Q}}(N_{K/\mathbb{Q}(\zeta_{p_j^{a_j}})}(1-\zeta_{p_j^{a_j}}^{v+up_j}))\right]$$

$$=\prod_{j=1}^{s}\left[\prod_{u=0}^{p_{j-1}^{a_j-1}}N_{\mathbb{Q}(\zeta_{p_j^{a_j}})/\mathbb{Q}}(1-\zeta_{p_j^{a_j}}^{v+up_j})^{\phi(n)/\phi(p_j^{a_j})}\right]$$

$$=\prod_{j=1}^{s}\left[p_j^{\phi(n)/\phi(p_j^{a_j})}\right]^{p_j^{a_j-1}}=\prod_{j=1}^{s}\left[p_j^{\phi(n)/(p_j-1)}\right].$$

Portanto, $D_K=\pm\dfrac{n^{\phi(n)}}{\prod\limits_{p|n}p^{\phi(n)/(p-1)}}$. ∎

Exemplo 2.2.2 *O discriminante de* $\mathbb{Q}(\zeta_{24})$ *é* $2^{16}\cdot 3^4$, *a menos de sinal.*

Exemplo de fatoração de ideais no anel dos inteiros algébricos de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$.

Exemplo 2.2.3 *Neste exemplo será visto que a fatoração não é única no anel dos inteiros algébricos do corpo ciclotômico* $\mathbb{Q}(\zeta_{23})$. *Seja* $K = \mathbb{Q}(\zeta)$, *onde* $\zeta = e^{2\pi i/23}$. *Pelo Teorema 2.2.2 o anel dos inteiros algébricos de* K *é* $\mathbb{Z}[\zeta]$. *O grupo das unidades de* $\mathbb{Z}_{23}$ *é gerado por -2,*

$$1,\ -2,\ 4,\ -8,\ -7,\ 14,\ -5,\ \ldots \tag{2.8}$$

Por motivos que serão melhor entendidos à frente, introduz-se os seguintes elementos:

$$\begin{aligned}\theta_0 &= \zeta + \zeta^4 + \zeta^{-7} + \zeta^{-5} + \ldots = \sum_i \zeta^{(-2)^{2i+1}} \\ \theta_1 &= \zeta^{-2} + \zeta^{-8} + \zeta^{14} + \ldots = \sum_i \zeta^{(-2)^{2i}}\end{aligned}$$

As potências que ocorrem são elementos alternados na seqüência (2.8). Tem-se:

$$\begin{aligned}\theta_0 + \theta_1 &= \sum_i \zeta^{(-2)^{2i+1}} + \sum_i \zeta^{(-2)^{2i}} = \sum_i (\zeta^{(-2)^{2i+1}} + \zeta^{(-2)^{2i}}) = -1, \\ \theta_0\theta_1 &= 6.\end{aligned}$$

A norma de um elemento qualquer $f(\zeta)$, *onde* f *é um polinômio sobre* $\mathbb{Z}$ *de grau* ≤ 22, *pode ser calculada por*

$$\begin{aligned}N(f(\zeta)) &= \prod_{j=1}^{22} N(f(\zeta^j)) && (2.9)\\ &= \prod_{j\ par} N(f(\zeta^j)) \cdot \prod_{j\ \acute{i}mpar} N(f(\zeta^j)) && (2.10)\\ &= G(\zeta^2)G(\zeta^{-2}), && (2.11)\end{aligned}$$

onde

$$G(\zeta) = f(\zeta)f(\zeta^4)f(\zeta^{-7})f(\zeta^{-5})f(\zeta^3)f(\zeta^{-11})f(\zeta^2)f(\zeta^8)f(\zeta^9)f(\zeta^{-10})f(\zeta^6).$$

Por definição, $G(\zeta)$ *é invariante sob a aplicação linear* α *a qual leva* ζ^j *em* ζ^{4j}. *Um elemento fixado por* α *deve ser da forma* $a + b\theta_0$ *para* $a,\ b \in \mathbb{Z}$. *O elemento abaixo,*

$$\mu = 1 - \zeta + \zeta^{21} = 1 - \zeta + \zeta^{-2}$$

foi encontrado por Kummer através de um detalhe de experimentação. Usando (2.9) e por meio de muitas contas tem-se

$$N(\mu) = (-31 + 28\theta_0) \cdot (-31 + 28\theta_1) = 6533 = 47 \cdot 139.$$

Pelo Teorema 1.7.3 o ideal principal $\mathfrak{m} =< \mu >$ *não pode ser primo, assim este deve ser produto não trivial de ideais primos, por exemplo* $\mathfrak{m} = \mathfrak{pq}$. *Tomando a norma desta igualdade tem-se (sem perda de generalidade),* $N(\mathfrak{p}) = 47$ *e* $N(\mathfrak{q}) = 139$. *Se* K *é um corpo de fatoração única*

então pelo Teorema 1.6.5 todo ideal, em particular $\mathfrak{p}$*, é principal. Logo* $\mathfrak{p} =< \nu >$ *para algum* $\nu \in \mathbb{Z}[\zeta]$*. Pelo Corolário 1.7.1 tem-se que* $N(\nu) = \pm 47$*. Isto é impossível, pois observou-se que* $G(\zeta)$ *pode ser sempre expresso na forma* $a + b\theta_0$*, para* $a,\ b \in \mathbb{Z}$ *e então* $G(\zeta^{-2})$ *deve ser igual a* $a + b\theta_1$*. Assim, tomando* $f(\zeta) = \nu$*, tem-se*

$$\pm 47 = (a + b\theta_0).(a + b\theta_1) = a^2 - ab + 6b^2.$$

Multiplicando por 4 e reagrupando tem-se,

$$(2a - b)^2 + 23b^2 = \pm 188.$$

O sinal deve ser sempre positivo. Uma análise de tentativa e erro mostra que 188 não pode ser escrito na forma $P^2 + 23Q^2$*. Isto contradiz a afirmação que fatoração prima de elementos não pode ser única em* $\mathcal{O}_K$*.*

2.3 Corpos de Números Abelianos

Uma extensão L sobre K é normal se L é uma extensão algébrica sobre K e todo polinômio irredutível e unitário sobre K que admite uma raiz em L decompõe-se num produto de fatores lineares em $L[X]$.

Uma extensão L/K é dita uma extensão Galoisiana quando L é normal e separável sobre K. Como $K = \mathbb{Q}$, por L ser um corpo de números, segue que L/K é uma extensão separável, portanto, se L/K for normal é galoisiana.

Um corpo de números é dito abeliano se K é uma extensão galoisiana dos racionais e seu grupo de Galois é abeliano.

Segue da teoria de Galois que se um corpo de números K está contido em um corpo ciclotômico então K é um corpo abeliano. A recíproca desta afirmação é o teorema de Kronecker-Weber, que será enunciado abaixo.

Teorema 2.3.1 ([*19*], pag. 319) *Se* $K/\mathbb{Q}$ *é uma extensão finita abeliana, então* $K \subseteq \mathbb{Q}(\zeta_n)$ *para algum* n*.*

Como foi visto no capítulo anterior, o cálculo do discriminante utiliza a base integral. Existem resultados que fazem este cálculo sem o uso da base integral. Um deles, que será enunciado abaixo, é conseqüência do Teorema do Condutor-Discriminante ver ([19], pag. 27).

Teorema 2.3.2 ([*12*], pag. 64) *Sejam* p *um número primo ímpar,* r *um inteiro positivo e* $K \subset \mathbb{Q}(\zeta_{p^r})$*,* $[K : \mathbb{Q}] = up^j$*,* p *não divide* u*. Então,* $D_K = \pm p^v$*, sendo*

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

O resultado abaixo será importante para os exemplos do próximo capítulo.

Teorema 2.3.3 ([*18*], pag. 57) *Sejam* $K \subset \mathbb{Q}(\zeta_p)$, p *primo,* $r = [\mathbb{Q}(\zeta_p) : K]$, $s = [K : \mathbb{Q}]$, $\theta = Tr_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$ *e* $g \in \mathbb{Z}$ *tal que* σ_g *gera* $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. *Então,* $K = \mathbb{Q}(\theta)$ *e*

$$\mathbb{Z}\sigma_g(\theta) + \ldots + \mathbb{Z}\sigma_{g^s}(\theta)$$

é o anel dos inteiros algébricos de K. *Além disso,*

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

Demonstração: Primeiramente será mostrado que $K = \mathbb{Q}(\theta)$. Como $\theta \in K$, segue que $\mathbb{Q}(\theta) \subset K$. Seja $G = Gal(\mathbb{Q}(\zeta_p)/K) = \{\sigma_{g^s},\ \sigma_{g^{2s}}, \ldots,\ \sigma_{g^{rs}}\}$ e $\theta = \zeta_p^{g^s} + \ldots + \zeta_p^{g^{rs}}$ então tem-se que $\sigma_g(\theta), \ldots,\ \sigma_{g^s}(\theta) \in \mathbb{Q}(\theta)$, pois $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão galoisiana. Sejam $a_1, \ldots, a_s \in \mathbb{Q}$ tais que

$$a_1\sigma_g(\theta) + \ldots + a_s\sigma_{g^s}(\theta) = 0. \tag{2.12}$$

Visto que $\sigma_{g^i}(\theta) = \zeta_p^{g^{s+i}} + \ldots + \zeta_p^{g^{rs+i}}$, se $\zeta_p^{g^{t_1 s+i_1}} = \zeta_p^{g^{t_2 s+i_2}}$, com $1 \leq t_1,\ t_2 \leq r$ e $1 \leq i_1,\ i_2 \leq s$ então $t_1 = t_2$ e $i_1 = i_2$. Com isso a equação (2.12), pode ser reescrita da seguinte maneira:

$$b_1\zeta_p + b_2\zeta_p^2 + \ldots + b_{p-1}\zeta_p^{p-1} = 0,$$

onde $\{b_i;\ i = 1, \ldots, p-1\} = \{a_i;\ i = 1, \ldots, s\}$. Por outro lado, $\{\zeta_p^i;\ i = 1, \ldots, p-1\}$ é um conjunto linearmente independente sobre $\mathbb{Q}$, logo $b_i = 0,\ i = 1, \ldots, p-1$ e, portanto, $a_i = 0,\ i = 1, \ldots, s$, ou seja, $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq s$. Como $\mathbb{Q}(\theta) \subset K$ e $[K : \mathbb{Q}] = s$ tem-se que $K = \mathbb{Q}(\theta)$. Sendo $\sigma_{g^i}(\theta) \in \mathbb{Z}[\zeta_p] \cap K$ então,

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

Agora, será provada a recíproca. Considera-se $\alpha \in \mathcal{O}_K$, então existem $a_1, \ldots, a_s \in \mathbb{Q}$ tais que $\alpha = \sum_{i=1}^{s} a_i\sigma_{g^i}(\theta)$, já que $\{\sigma_g(\theta), \ldots, \sigma_{g^s}(\theta)\}$ é base de $K/\mathbb{Q}$. Então, como $\alpha \in \mathbb{Z}[\zeta_p]$ e repetindo o argumento que foi usado na demonstração que $K = \mathbb{Q}(\theta)$, conclui-se que $a_i \in \mathbb{Z},\ i = 1, \ldots, s$, isto é,

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

O valor do discriminante decorre do Teorema 2.3.2 ∎

Decomposição de ideais em um extensão galoisiana

Nesta subseção será tratado o problema geral de determinar como um ideal primo de um anel dos inteiros algébricos fatora-se numa extensão de corpos, sendo esta uma extensão Galoisiana.

Sejam L uma extensão normal de K e $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$. O grupo de Galois $G = Gal(L/K)$, consistindo de todos os automorfismos de L os quais fixam K ponto a ponto, tem ordem n e permuta os ideais primos acima de $\mathfrak{p}$: se $\mathfrak{q}$ é um dos tais ideais primos e $\sigma \in G$, então $\sigma(\mathfrak{q})$ é um ideal primo de $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, e está acima de $\sigma(\mathfrak{p}) = \mathfrak{p}$. Além disso, G permuta-os transitivamente:

Teorema 2.3.4 ([*10*], pag. 70) *Com a notação acima, sejam $\mathfrak{q}$ e $\mathfrak{q}'$ dois ideais primos de $\mathcal{O}_L$ que estão acima do mesmo ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Então, $\sigma(\mathfrak{q}) = \mathfrak{q}'$, para algum $\sigma \in G$.*

A partir disto obtém-se:

Corolário 2.3.1 ([*10*], pag. 71) *Se L é normal sobre K e $\mathfrak{q}$, $\mathfrak{q}'$ são ideais primos acima de $\mathfrak{p}$, então $e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}'|\mathfrak{p})$ e $f(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p})$.*

O corolário acima mostra que no caso de uma extensão normal, um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ fatora-se em $(\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$ em $\mathcal{O}_L$ onde os $\mathfrak{q}_i$ são ideais primos distintos, todos tendo o mesmo grau residual f sobre $\mathfrak{p}$. E mais, por ([10], pag. 65) $n = [L : K] = gef$.

Exemplo 2.3.1 *Seja $K = \mathbb{Q}(\zeta_{91})$, pelo Teorema 2.2.2 tem-se que o anel dos inteiros algébricos de K é $\mathbb{Z}[\zeta_{91}]$. O polinômio minimal de ζ_{91} sobre $\mathbb{Q}$ é :*

$$\begin{aligned} g(X) &= X^{72} - X^{71} - X^{64} + X^{59} - X^{57} + X^{52} - X^{50} + X^{46} - X^{43} + X^{39} - X^{36} + X^{33} \\ &- X^{29} + X^{26} - X^{22} + X^{20} - X^{15} + X^{13} - X^8 + X^7 - X + 1. \end{aligned}$$

Primeiramente, $7\mathcal{O}_K$ será fatorado usando o Lema de Kummer (Teorema 1.6.2). Com a notação acima, a redução de $g(x)$ módulo 7 é

$$g_7(X) = (X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^6.$$

Logo $e_i = 6$ e sendo o grau residual igual ao grau do polinômio $g(X)$ conclui-se que $f_i = 12$, para $i = 1$. Portanto,

$$7\mathcal{O}_K = \mathfrak{p}_1^6$$

onde

$$\mathfrak{p}_1 = 7\mathcal{O}_K + g(\zeta_{91})\mathcal{O}_K.$$

Para a fatoração de $13\mathcal{O}_K$*, tem-se que o polinômio* g *reduzido módulo* 13 *é*

$$g_{13}(X) = p_1(X)^{12} \cdot p_2(X)^{12} \cdot p_3(X)^{12}$$

onde

$$\begin{aligned} p_1(X) &= X^2 + 5X + 1; \\ p_2(X) &= X^2 + 3X + 1; \\ p_3(X) &= X^2 + 6X + 1. \end{aligned}$$

Assim, $e_i = 12$ *e sendo o grau residual igual ao grau de* $p_i(X)$*, conclui-se que* $f_i = 2,\ i = 1,\ 2,\ 3$ *e* $72 = g \cdot e \cdot f = 3 \cdot 12 \cdot 2$*. Portanto,*

$$13\mathcal{O}_K = \mathfrak{p}_1^{12} \cdot \mathfrak{p}_2^{12} \cdot \mathfrak{p}_3^{12}$$

onde,

$$\mathfrak{p}_i = 13\mathcal{O}_K + p_i(\zeta_{91})\mathcal{O}_K, i = 1,\ 2,\ 3.$$

Sejam K_1 e K_2 corpos de números linearmente disjuntos (isto é, $[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$). Dado um número primo p, por ([10]) 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 da seguinte maneira: sejam $e_i,\ f_i$ e g_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: $g = g_1g_2,\ e = e_1e_2$ e $f = f_1f_2$. Cada ideal primo de $\mathcal{O}_{K_1}$ acima de p se estende em $\mathcal{O}_{K_1K_2}$ de maneira análoga à que p se estende em $\mathcal{O}_{K_2}$.

Para cada ideal primo $\mathfrak{q}$ acima de $\mathfrak{p}$, define-se dois subgrupos 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**

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

Ambos são subgrupos de G e $E \subset D$, pois $\sigma(\mathfrak{q}) = \mathfrak{q}$ pode ser expresso como $\sigma(\alpha) \equiv 0\ (mod\ \mathfrak{q})$ se, e somente se, $\alpha \equiv 0\ (mod\ \mathfrak{q})$.

Quando G é um grupo abeliano, $D(\mathfrak{p}_i)$ depende apenas de $\mathfrak{p}$, assim este será denotado por apenas $D(\mathfrak{p})$. Como g denota o número de conjugados de $\mathfrak{q}$, então

$$card(G)card(D(\mathfrak{p}))^{-1} = g \quad \text{e, portanto,} \quad card(D(\mathfrak{p})) = \frac{n}{g} = ef.$$

Os membros de D induzem um automorfismo do corpo $\mathcal{O}_L/\mathfrak{q}$ de modo natural: todo $\sigma \in G$ restrito a um automorfismo de $\mathcal{O}_L$ e se $\sigma \in D$ então a aplicação induzida $\mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{q}$ tem núcleo $\mathfrak{q}$, logo cada $\sigma \in D$ induz um automorfismo $\overline{\sigma}$ de $\mathcal{O}_L$, de tal modo que o diagrama abaixo comuta:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/\mathfrak{q} & \xrightarrow{\overline{\sigma}} & \mathcal{O}_L/\mathfrak{q} \end{array}$$

E mais, $\overline{\sigma}$ fixa o subcorpo $\mathcal{O}_K/\mathfrak{p}$ ponto a ponto se σ fixa K. Logo fixa $\mathcal{O}_K$, ponto a ponto. Então $\overline{\sigma}$ é um membro do grupo de Galois $\overline{G}$ de $\mathcal{O}_L/\mathfrak{q}$ sobre $\mathcal{O}_K/\mathfrak{p}$.

Tudo isto pode ser resumido dizendo que tem-se a aplicação $\psi : D \longrightarrow \overline{G}$ e ψ é um homomorfismo de grupos (pois composição de automorfismos em D corresponde a composição em $\overline{G}$). Logo $Nuc(\psi) = E$; assim E é um subgrupo normal de D e o grupo quociente D/E é imerso em $\overline{G}$. Tem-se que $\psi : D \longrightarrow \overline{G}$ é sobrejetora, assim $D/E \longrightarrow \overline{G}$ é de fato um isomorfismo de grupos. Sabe-se que $\overline{G}$ é cíclico de ordem f, assim o mesmo é válido para D/E.

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

Exemplo 2.3.2 *Sejam $K = \mathbb{Q}(\zeta_{15})$, $\mathcal{O}_K = \mathbb{Z}[\zeta_{15}]$ e $f(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ o polinômio minimal de ζ_{15} sobre $\mathbb{Q}$. A decomposição do ideal $7\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ satisfaz:*

$$f(X) \equiv (X^4 + 4X^3 + 2X^2 + X + 4) \cdot (X^4 + 2X^3 + 4X^2 + X + 2)(mod\ 7\mathbb{Z}[X]).$$

Tem-se que $g = 2$, $p_1(X) = X^4 + 4X^3 + 2X^2 + X + 4$, $p_2 = X^4 + 2X^3 + 4X^2 + X + 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 4$ e $\mathfrak{p}_1 = 7\mathcal{O}_K + p_1(\zeta_{15})\mathcal{O}_K$ e $\mathfrak{p}_2 = 7\mathcal{O}_K + p_2(\zeta_{15})\mathcal{O}_K$. Portanto, $7\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2)$, onde $\mathfrak{p}_1$, $\mathfrak{p}_2$ são ideais primos de $\mathcal{O}_K$. O grupo dos $\mathbb{Q}$-automorfismos de K sobre $\mathbb{Q}$ é dado por

$$G = \{\sigma_i; (i, 15) = 1,\ i = 1, \ldots, 15 : \sigma_i(\zeta_{15}) = \zeta_{15}^i\} = \{\sigma_1,\ \sigma_2,\ \sigma_4,\ \sigma_7,\ \sigma_8,\ \sigma_{11},\ \sigma_{13},\ \sigma_{14}\}.$$

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

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

$$D(7\mathbb{Z}) = \{\sigma \in G; \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\sigma_1,\ \sigma_7,\ \sigma_{11},\ \sigma_{13}\}.$$

Da mesma forma o grupo de inércia $E(7\mathbb{Z})$ é:

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

Como $card(E(7\mathbb{Z})) = 4$ e sendo $E(7\mathbb{Z})$ um subgrupo de $D(7\mathbb{Z})$ tem-se que $E(7\mathbb{Z}) = D(7\mathbb{Z})$.

Teorema 2.3.5 ([*10*], pag. 100) *Sejam L, K, $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathfrak{p}$, $\mathfrak{q}$, G, D, E, g, e, e f como acima. Então tem-se o seguinte diagrama:*

grau			*índice de ramificação*	*grau de inércia*
	L	$\mathfrak{q}$		
e			e	1
	L_E	$\mathfrak{q}_E$		
f			1	f
	L_D	$\mathfrak{q}_D$		
g			1	1
	K	$\mathfrak{p}$		

O próximo teorema 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 $S_H = B \cap K^{'}$ e $\mathfrak{p}^{'} = \mathfrak{q} \cap S_H$ é o único ideal primo de S_H abaixo de $\mathfrak{q}$.

Teorema 2.3.6 ([*10*], pag. 104) *Com as notações acima tem-se:*
(i) *$L_{D(\mathfrak{p})}$ é o maior corpo intermediário de L contendo K tal que $e(\mathfrak{p}^{'}|\mathfrak{p}) = f(\mathfrak{p}^{'}|\mathfrak{p}) = 1$;*
(ii) *$L_{D(\mathfrak{p})}$ é o menor subcorpo $K^{'}$, tal que $\mathfrak{q}$ é o único ideal primo de $\mathcal{O}_L$ acima de $\mathfrak{p}^{'}$.*

Exemplo 2.3.3 *Como foi visto no Exemplo 2.3.2 tem-se que $e = 1$, $f = 4$, e $g = 2$. Pelo Teorema 2.3.6 segue que $L_D = \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_{15})$ e $e(\mathfrak{q}_D|\mathfrak{p}) = f(\mathfrak{q}_D|\mathfrak{p}) = 1$.*

2.4 Reticulados

Entende-se por empacotamento esférico a disposição de esferas de mesmo raio no espaço euclidiano $\mathbb{R}^n$ de tal modo que a intersecção de duas delas tenha no máximo um ponto. A forma de dispor essas esferas de modo a cobrir a maior parte do espaço sempre foi um desafio

e mereceu citação de Hilbert, que em 1900 colocou-o na lista de problemas em aberto mais relevantes do século.

Dentre os empacotamentos esféricos aqueles cujo conjunto de centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$ serão denominados empacotamentos reticulados, ou define-se reticulados da seguinte maneira: sejam V um espaço vetorial de dimensão finita n sobre um corpo K, A um subanel de K e $v_1, \ldots, v_r,\ r \leq n$, vetores linearmente independentes de V. Dá-se o nome de A-reticulado com base $(v_1, \ldots, v_r)$ ao conjunto de elementos da forma

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

A partir de agora, toda vez que for citado reticulado, supõe-se que $V = \mathbb{R}^n,\ K = \mathbb{R},\ A = \mathbb{Z}$ e $r = n$.

Daqui por diante todos os empacotamentos considerados serão reticulados e quando o conjunto de centros for A, diz-se que o empacotamento é associado a A. Define-se a densidade de um dado empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas.

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\gamma = \{v_1, \ldots, v_n\}$. O conjunto

$$R_\gamma = \{x \in \mathbb{R}^n : x = \lambda_1 v_1 + \ldots + \lambda_n v_n, 0 \leq \lambda_i < 1, \lambda \in \mathbb{R}\}$$

é dito a **Região Fundamental** de Λ associada a base γ. Nota-se que a Região Fundamental depende da escolha da base do reticulado.

A densidade de empacotamento é definida como sendo a proporção do espaço coberto pela união das esferas. A seguir serão introduzidos conceitos para este cálculo.

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

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

a qual é denominada matriz geradora para o reticulado Λ.

O volume da Região Fundamental, R_γ, independe da base, pois a matriz mudança de base é invertível, com entradas inteiras, ou seja, tem determinante ± 1. Assim define-se volume do reticulado Λ como sendo o volume de uma Região Fundamental, e este será denotado 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 $\rho = \Lambda_{min}/2$, onde $\Lambda_{min} = min\{\mid v \mid; v \in \Lambda, v \neq 0\}$. É importante

notar que $\rho = \Lambda_{min}/2$ é o maior raio com o qual é possível distribuir esferas centradas nos pontos de Λ e obter-se um empacotamento. Desta forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Ao mencionar densidade de empacotamento com esferas de raio ρ associado a um reticulado, está citando-se densidade de um reticulado Λ, a qual será denotada por $\Delta(\Lambda)$ e esta é dada por:

$$\Delta(\Lambda) \quad = \quad \frac{\text{Vol.de uma esfera de raio } \rho}{\text{Vol. do reticulado}} \tag{2.13}$$

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

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

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

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

A fração que se destaca é outro parâmetro importante em empacotamento reticulado, chamado de densidade de centro, a qual é dada por

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

Em dimensão um, uma esfera uni-dimensional é um segmento de reta e a partir daí os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja densidade de empacotamento $\Delta = 1$.

A resposta também é conhecida em duas dimensões: é o reticulado hexagonal gerado pelos vetores $(1,0)$ e $\left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$, obtendo-se assim o raio $\rho = \frac{1}{2}$ e densidade de empacotamento $\Delta = \pi/\sqrt{12} \cong 0,9069$.

Em três dimensões, a resposta é desconhecida. Mas se forem considerados somente empacotamentos reticulados então Gauss obteve a resposta em 1831, o reticulado denominado face-centered-cubic, denotado por fcc (pilha de laranjas ou bala de canhões), é o empacotamento reticulado mais denso, segundo [16]. O fcc consiste de todos os pontos (x, y, z), onde $x,\ y,\ z$ são inteiros com soma par.

Para dimensão 4, por exemplo, o empacotamento esférico mais denso conhecido é o reticulado denominado checkerboard D_4, no qual os centros das esferas são todos os pontos (u_1, u_2, u_3, u_4) onde os u_i são inteiros, tais que $\sum_{i=1}^{4} u_i = 2k,\ k \in \mathbb{Z}$. Então, por exemplo $(0,0,0,0)$ é admitido e $(1,1,0,0)$ também, mas $(1,0,0,0)$ não. Quaisquer dois centros distintos, devem diferir de 1 e em no mínimo duas coordenadas, ou de no mínimo 2 em uma

coordenada; logo a distância mínima entre os centros é $\sqrt{2}$. Então, o raio de empacotamento vale $\rho = \sqrt{2}/2$.

Em 1872, segundo [16], Korkine e Zolotareff provaram que esta é a maior densidade possível para um empacotamento reticulado em 4-dimensões.

Exemplo 2.4.1 *Seja $\Lambda = \mathbb{Z}^n$ um reticulado do $\mathbb{R}^n$ gerado pela base $\gamma = \{e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)\}$. A forma quadrática é $\mid v \mid^2 = x_1^2 + \ldots + x_n^2$ assume o valor mínimo 1 quando um dos $x_i = 1$ para $i = 1, \ldots, n$ e os demais valores são nulos, logo $\rho = \frac{1}{2}$. Visto que $v(\Lambda) = \mid detM \mid$, e sendo neste caso M a matriz identidade tem-se $v(\Lambda) = 1$ e, portanto, $\delta = \frac{1}{2^n}$.*

Um outro modelo destacado é o algébrico, descrito por Minkowski que consiste no seguinte: seja K um corpo de números de grau n e o seu anel dos inteiros algébricos $\mathcal{O}_K$, obtém-se um homomorfismo de K em $\mathbb{R}^n$, de modo que a imagem de um ideal ordinário não nulo de $\mathcal{O}_K$ por este homomorfismo é um reticulado de posto n em $\mathbb{R}^n$. Este é o modelo que será tratado a partir de agora, pois com este método é conhecido, em algumas dimensões, reticulados com densidade de centro máxima.

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.

Recorda-se que, dada uma extensão K de $\mathbb{Q}$ de grau n existem exatamente n monomorfismos de K em $\mathbb{C}$.

Um monomorfismo σ_i é dito real se $\sigma_i(K) \subseteq \mathbb{R}$; caso contrário é dito imaginário. Um corpo K é dito totalmente real quando todos monomorfismos são reais, e K é dito totalmente imaginário se todos são imaginários.

Sejam K um corpo de números de grau n, r_1 a quantidade de monomorfismos reais e $2r_2$ a quantidade de monomorfismos imaginários. A ordem dos monomorfismos é ordenada de tal modo que os monomorfismos de K em $\mathbb{C}$ são

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

onde $\sigma_1, \ldots, \sigma_{r_1}$ são monomorfismos reais e os demais são imaginários, e $\overline{\sigma_{r_1+i}} = \sigma_{r_1+r_2+i}$, para $i = 1, \ldots, r_2$. Assim, define-se o homomorfismo canônico

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

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x),\ Re\sigma_{r_1+1}(x),\ Im\sigma_{r_1+1}(x), \ldots,\ Re\sigma_{r_1+r_2}(x),\ Im\sigma_{r_1+r_2}(x))$$

onde $Re(z)$ e $Im(z)$ indicam, respectivamente, as partes real e imaginária do número complexo z.

Exemplo 2.5.1 *Seja* $K = \mathbb{Q}(\theta)$ *onde* $\theta \in \mathbb{R}$ *satisfaz*

$$\theta^3 - 5 = 0.$$

Os conjugados de $\theta = \sqrt[3]{5}$ *são* $\theta,\ \theta\omega,\ \theta\omega^2$ *onde* ω *é uma raiz cúbica primitiva da unidade. Um elemento de* K*, por exemplo*

$$x = q + r\theta + s\theta^2,$$

onde $q,\ r,\ s \in \mathbb{Q}$*, é levado a* $\mathbb{R}^3$ *de acordo com*

$$\begin{aligned} \sigma(x) &= (\sigma_1(x), Re\sigma_2(x), Im\sigma_2(x)) \\ &= (q + r\theta + s\theta^2, q - \frac{r\theta}{2} - \frac{s\theta^2}{2}, \frac{r\theta\sqrt{3}}{2} - \frac{s\theta^2\sqrt{3}}{2}). \end{aligned}$$

Exemplo 2.5.2 *Sejam* $K = \mathbb{Q}(\sqrt{11})$ *com* $\mathbb{Q}$*-base* $\{1, \sqrt{11}\}$ *e os monomorfismos de* K *em* $\mathbb{C}$*,* σ_1 *e* σ_2*, onde* σ_1 *é a aplicação inclusão e* σ_2 *a conjugação, isto é,* $\sigma_2(a + b\sqrt{11}) = a - b\sqrt{11}$*,* $a,\ b \in \mathbb{Q}$*. Então para* $x = a + b\sqrt{11} \in K$*,* $a, b \in \mathbb{Q}$ *tem-se*

$$\sigma(x) = (\sigma_1(x), \sigma_2(x)) = (a + b\sqrt{11}, a - b\sqrt{11})$$

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

Teorema 2.5.1 ([*15*], pag. 56) *Sejam* K *um corpo de números de grau* n*,* $\sigma_1, \ldots, \sigma_n$ *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*
(i) $\sigma(M)$ *é um reticulado*
(ii) $v(\sigma(M)) = 2^{-r_2}.\ |\ det(\sigma_i(x_j))\ |\ .$

Exemplo 2.5.3 *Sejam* $K = \mathbb{Q}(\sqrt{11})$ *e* $M = \mathbb{Z}[\sqrt{11}]$ *o anel dos inteiros algébricos de* K*, com base* $\{1, \sqrt{11}\}$*. Sendo* $r_2 = 0$ *tem-se,*

$$v(\sigma_k(M)) = \left| det \begin{pmatrix} 1 & \sqrt{11} \\ 1 & -\sqrt{11} \end{pmatrix} \right| = 2\sqrt{11}$$

Exemplo 2.5.4 *Sejam* $K = \mathbb{Q}(\sqrt{21})$ *e* $M = \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{21}\right]$ *o anel dos inteiros algébricos de* K*, com base* $\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{21}\right\}$*. Sendo* $r_2 = 1$ *então,*

$$v(\sigma_k(M)) = 2^{-1} \left| det \begin{pmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{21} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{21} \end{pmatrix} \right| = \frac{\sqrt{21}}{2}$$

Teorema 2.5.2 ([15], pag. 57) *Sejam K um corpo de números de grau n, cujo discriminante é D_K e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então,*

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

A expressão para densidade de centro dos reticulados $\sigma_K(\mathfrak{a})$, chamada de realização geométrica de um ideal $\mathfrak{a}$, é dada por

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

Exemplo 2.5.5 *Para $K = \mathbb{Q}(\sqrt{11})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$ e $D_K = 44$ pelos Teoremas 2.1.2 e 2.1.3. Dado $\alpha = a + b\sqrt{11} \in \mathcal{O}_K$, tem-se $\alpha\overline{\alpha} = a^2 + 2ab\sqrt{11} + 11b^2$. Logo,*

$$|\sigma_K(\alpha)|^2 = Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = 2(a^2 + 11b^2)$$

e esta forma quadrática assume valor mínimo 2 quando $a = 1$ e $b = 0$. Portanto,

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{4\sqrt{11}} \cong 0,07538.$$

Exemplo 2.5.6 *Sejam $K = \mathbb{Q}(\sqrt{13})$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$ e $\mathfrak{a}$ o ideal principal de $\mathcal{O}_K$, gerado por $\gamma = 1 - 2\sqrt{13}$. Dado $\alpha \in \gamma\mathcal{O}_K$ existem $a,\ b \in \mathbb{Z}$ tais que*

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

Logo,

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

Assim,

$$Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = 2\left[\left(a - \frac{25b}{2}\right)^2 + 13\left(\frac{-b}{2} - 2a\right)^2\right].$$

Atribuindo valores inteiros não todos nulos para a forma quadrática acima, conclui-se que esta assume valor mínimo 106 quando $a = 1$ e $b = 0$.

Sendo $D_K = 13$ e $|N_{K/\mathbb{Q}}(\gamma)| = 25$ tem-se

$$\delta(\sigma_K(\mathfrak{a})) = \frac{106}{100\sqrt{13}} \cong 0,2940.$$

Capítulo 3

Cúbicas e Reticulados Algébricos

O objetivo deste capítulo é enfocar as extensão cúbicas contidas em $\mathbb{Q}(\zeta_n)$, caracterizá-las em relação a localização, quantidade e dar exemplo de reticulados obtidos pelo método algébrico nas extensões cúbicas.

Como foi visto no capítulo anterior, a fórmula da densidade de centro para reticulados algébricos envolve conceitos importantes da teoria algébrica dos números, tais como discriminante de um corpo, norma de um ideal e a minimização de uma forma quadrática, oriunda da função traço.

Buscando minimizar a forma quadrática e, assim, obter o raio de empacotamento, observou-se a relação existente entre o raio do empacotamento e a função traço. A técnica aqui desenvolvida, para obter um resultado geral para a função traço, é inédita.

Neste capítulo introduziu-se o conceito de caracteres de Dirichlet, para serem usados no cálculo do discriminante do corpo, diferentemente de como foi feito anteriormente.

Para finalizar, foram feitos exemplos de reticulados algébricos nas extensões cúbicas e para estes foi calculada a densidade de centro, notando que a decomposição de ideais na extensão em destaque, ocorre apenas nos casos extremos.

3.1 Sobre a Função Traço no Corpo Ciclotômico $\mathbb{Q}(\zeta_n)$

O Teorema de Kronecker-Weber garante que todo corpo de números abeliano está contido em um corpo ciclotômico $K = \mathbb{Q}(\zeta_n)$, para algum n. Portanto, estudar corpos de números abelianos equivale a estudar os subcorpos dos corpos ciclotômicos.

Como foi visto anteriormente a representação geométrica de um ideal ordinário não nulo de $\mathcal{O}_K$ é um reticulado do $\mathbb{R}^n$.

Neste reticulado a distância entre seus pontos é medida pela função traço, como será visto

a seguir.

Proposição 3.1.1 ([16], pag. 225) *Sejam K um corpo de números e $x \in K$. Então*

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

onde

$$c_K = \begin{cases} 1, & se\ r_2 = 0; \\ 1/2, & se\ r_1 = 0. \end{cases}$$

Lema 3.1.1 *Sejam i, n inteiros, $i < n$. Se $(i, n) = d$ então,*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \frac{\phi(n)}{\phi(\frac{n}{d})} Tr_{\mathbb{Q}(\zeta_{n/d})/\mathbb{Q}}(\zeta_{n/d}^{i/d}).$$

Demonstração: Considera-se a seguinte extensão $\mathbb{Q} \subset \mathbb{Q}(\zeta_{n/d}^{i/d}) \subset \mathbb{Q}(\zeta_n)$. Por propriedade do traço tem-se

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/d}^{i/d})] Tr_{\mathbb{Q}(\zeta_{n/d}^{i/d})/\mathbb{Q}}(\zeta_{n/d}^{i/d}). \tag{3.1}$$

Como $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/d}^{i/d})] = \phi(n)/\phi(n/d)$, e substituindo na equação (3.1) conclui-se a demonstração. ∎

Lema 3.1.2 *Sejam j e $p_i^{a_i}$ inteiros e primos entre si. Então,*

$$Tr_{\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}}(\zeta_{p_i^{a_i}}^j) = \begin{cases} -1, & se\ a_i = 1 \\ 0, & se\ a_i > 1. \end{cases}$$

Teorema 3.1.1 *Sejam $n = p_1^{a_1} \dots p_s^{a_s}$, $a_k \geq 1$, $k = 1, \dots, s$, i um inteiro e $d = (i, n)$ então,*

$$Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \frac{\phi(n)}{\phi(\frac{n}{d})} \mu\left(\frac{n}{d}\right), \text{ onde } \mu \text{ é a função de Möbius.}$$

Demonstração: Para $n/d = 1$ segue pelo Lema 3.1.1 que $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = \frac{\phi(n)}{\phi(n/d)}$. Quando n é livre de quadrados a demonstração será feita por indução, sobre a quantidade de números primos da decomposição de n. Para $s = 1$, vale o Lema anterior e assim o resultado é válido. Supõe-se verdadeira a afirmação para $s = k$, isto é,

$$Tr_{\mathbb{Q}(\zeta_{p_1 \dots p_k})/\mathbb{Q}}(\zeta_{p_1 \dots p_k}^i) = (-1)^k.$$

Agora prova-se a afirmação para $s = k + 1$. Dado $n = p_1 \dots p_{k+1}$, sejam $a = p_1 \dots p_k$, $b = p_{k+1}$ e u, v inteiros tais que $au + bv = 1$, tem-se

$$\zeta_n^i = \zeta_n^{i(au+bv)} = \zeta_{ab}^{jua} \zeta_{ab}^{ivb} = \zeta_b^{iu} \zeta_a^{iv}$$

onde $(iu, b) = (iv, a) = 1$. Então, para $L = \mathbb{Q}(\zeta_n)$ e $M = \mathbb{Q}(\zeta_a)$ tem-se pelas propriedades do traço que

$$\begin{aligned} Tr_{L/\mathbb{Q}}(\zeta_n^i) &= Tr_{M/\mathbb{Q}}(Tr_{L/M}(\zeta_b^{ju}\zeta_a^{iv})) = Tr_{M/\mathbb{Q}}(\zeta_a^{iv}Tr_{L/M}(\zeta_b^{iu})) \\ &= Tr_{L/M}(\zeta_b^{iu})Tr_{M/\mathbb{Q}}(\zeta_a^{iv}) = Tr_{L/M}(\zeta_b^{iu})(-1)^k \\ &= Tr_{\mathbb{Q}(\zeta_b)/\mathbb{Q}}(\zeta_b^{iu})(-1)^k = (-1)(-1)^k = (-1)^{k+1}. \end{aligned}$$

Portanto, $Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^i) = (-1)^s$. Caso contrário, sejam $a = p_1^{a_1},\ b = p_2^{a_2}\dots p_s^{a_s}$, supondo $a_1 > 1$ e $l,\ r$ inteiros tais que $al + br = 1$, logo

$$\zeta_n^i = \zeta_{ab}^{i(al+br)} = \zeta_{ab}^{ial}\zeta_{ab}^{ibr} = \zeta_b^{il}\zeta_a^{ir},$$

onde $(il, b) = (ir, a) = 1$. Então para $L = \mathbb{Q}(\zeta_n)$ e $M = \mathbb{Q}(\zeta_a)$ tem-se:

$$\begin{aligned} Tr_{L/\mathbb{Q}}(\zeta_n^i) &= Tr_{M/\mathbb{Q}}(Tr_{L/M}(\zeta_b^{il}\zeta_a^{ir}) \\ &= Tr_{M/\mathbb{Q}}(\zeta_a^{ir}(Tr_{L/M}(\zeta_b^{il}))) = Tr_{L/M}(\zeta_b^{il})Tr_{M/\mathbb{Q}}(\zeta_a^{ir}) \\ &= Tr_{L/M}(\zeta_b^{il})\ 0 = 0. \end{aligned}$$

■

Exemplo 3.1.1 *Seja $K = \mathbb{Q}(\zeta_{12})$. Pelo Lema 3.1.1*

$$Tr_{K/\mathbb{Q}}(\zeta_{12}^2) = Tr_{K/\mathbb{Q}}(\zeta_{12}^4) = 2$$

e pelo Teorema 3.1.1 tem-se

$$Tr_{K/\mathbb{Q}}(\zeta_{12}) = 1.$$

Agora considere $L = \mathbb{Q}(\zeta_{91})$ então

$$Tr_{L/\mathbb{Q}}(\zeta_{91}^7) = \frac{\phi(91)}{\phi(13)}(-1) = -6.$$

e

$$Tr_{L/\mathbb{Q}}(\zeta_{91}^{13}) = \frac{\phi(91)}{\phi(7)}(-1) = -12.$$

3.2 Cúbicas Galoisianas

Uma extensão K de $\mathbb{Q}$ é dita Galoisiana se esta é normal e separável.

Um corpo de números K é dito abeliano se K é uma extensão galoisiana dos racionais e seu grupo de Galois é abeliano.

Adjuntando uma raiz primitiva n-ésima da unidade ao corpo dos racionais, obtém-se a extensão n-ésima ciclotômica. Tal raiz será denotada por ζ_n e o corpo ciclotômico por $\mathbb{Q}(\zeta_n)$.

Teorema 3.2.1 ([*15*], pag. 88) *Sejam K um corpo de números e $L = K(\zeta_n)$. O corpo L é uma extensão galoisiana de K e o grupo de Galois de L sobre K é isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demonstração: O polinômio minimal de ζ_n sobre K divide $X^n - 1$ e suas raízes são as raízes n-ésimas da unidade e, portanto, potências de ζ_n. Logo, L é extensão galoisiana de K. Todo automorfismo $\sigma \in G$ é definido pelo seu valor em $\sigma(\zeta_n)$ que, por construção, $\zeta_n^{j(\sigma)}$, onde $j(\sigma)$ é unicamente determinado módulo n. Para $\sigma,\ \lambda \in G$, vale:

$$\sigma\lambda(\zeta_n) = \sigma(\zeta_n^{j(\lambda)}) = \sigma(\zeta_n)^{j(\lambda)} = \zeta_n^{j(\sigma)j(\lambda)}.$$

Assim, $j(\sigma\lambda) \equiv j(\sigma)j(\lambda)(mod\ n)$ e isto implica que $\sigma \longrightarrow j(\sigma)$ define um homomorfismo de G em $(\mathbb{Z}/n\mathbb{Z})^*$. Como $j(\sigma)$ determina σ, este homomorfismo é injetor concluindo assim a demonstração. ■

Como $\mathbb{Q}(\zeta_n)$ é uma extensão galoisiana sobre $\mathbb{Q}$ e como foi visto no Teorema 3.2.1 $G = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$, o qual é abeliano, segue que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é uma extensão abeliana.

Todo subgrupo H de $(\mathbb{Z}/n\mathbb{Z})^*$ é normal e o quociente $(\mathbb{Z}/n\mathbb{Z})^*/H$ é abeliano, da Teoria de Galois segue que todo subcorpo de um corpo abeliano é abeliano, em particular todo subcorpo de $\mathbb{Q}(\zeta_n)$ é abeliano. A recíproca desta afirmação é assegurada pelo Teorema de Kronecker-Weber (Teorema 2.3.1).

Dada uma extensão cúbica galoisiana K dos racionais, o grupo de Galois $G = Gal(K/\mathbb{Q})$ tem ordem 3 e, portanto, é abeliano. Pelo Teorema de Kronecker-Weber, K está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_n)$. Visto que o grau de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é $\phi(n)$, onde ϕ é a função de Euler, segue que se K está contido em $\mathbb{Q}(\zeta_n)$, então 3 divide $\phi(n)$. A recíproca também é válida, ou seja, se 3 divide $\phi(n)$ então $\mathbb{Q}(\zeta_n)$ contém uma cúbica .

Lema 3.2.1 ([*18*], pag. 83) *Dados n um número inteiro e $L = \mathbb{Q}(\zeta_n)$, então L contém uma cúbica se, e somente se, 3 divide $\phi(n)$.*

Agora o objetivo é determinar a quantidade de cúbicas contidas em $\mathbb{Q}(\zeta_n)$. Para isto será necessário o Teorema Fundamental da Teoria de Galois, o qual estabelece uma relação entre grupos e corpos.

Teorema 3.2.2 ([*19*], pag. 26) *Dados um grupo abeliano finito G e H um subgrupo de G, então G contém um subgrupo isomorfo a G/H.*

Através do próximo Teorema é possível saber a quantidade de cúbicas em $\mathbb{Q}(\zeta_n)$.

Teorema 3.2.3 *Sejam $n = p_1^{a_1} \dots p_s^{a_s}$ a fatoração de n em fatores primos e*

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

Então existem $\dfrac{3^r - 1}{2}$ *cúbicas em* $\mathbb{Q}(\zeta_n)$.

Demonstração: Pelo Teorema Fundamental da Teoria de Galois ([14], pag.49) tem-se uma correspondência biunívoca entre corpos e grupos. Toma-se a extensão $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n)$. Pelo referido Teorema tem-se

$$[K : \mathbb{Q}] = (G : H), \quad \text{onde} \quad G = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

Logo, o objetivo é encontrar a quantidade de subgrupos de $(\mathbb{Z}/n\mathbb{Z})^*$ de índice 3, que pelo Teorema 3.2.2 equivale a determinar a quantidade de subgrupos de ordem 3. Seja $\overline{G}$ este subgrupo. Sendo $\overline{G} = \{e, x, x^2\}$, onde a ordem de x é 3, conseqüentemente a ordem de x^2 também é, assim $\overline{G}$ tem ordem 3. Então, tem-se que cada subgrupo é formado pelo elemento neutro mais um par de elementos de ordem 3 cada. Assim, existem $s/2$ subgrupos de ordem 3, onde s é a quantidade de elementos de ordem 3 que vão formar os subgrupos. Seja $n = 2^\delta p_i^{a_i} \dots p_s^{a_s}$, logo pelo Teorema Fundamental dos Grupos Abelianos Finitos tem-se que

$$(\frac{\mathbb{Z}}{n\mathbb{Z}})^* \simeq G \times (\frac{\mathbb{Z}}{p_1^{a_1}\mathbb{Z}})^* \times \dots \times (\frac{\mathbb{Z}}{p_s^{a_s}\mathbb{Z}})^*, \tag{3.2}$$

onde G é um grupo, cuja ordem é uma potência de 2. Toma-se um elemento g em $G \times (\frac{\mathbb{Z}}{p_1^{a_1}\mathbb{Z}})^* \times \dots \times (\frac{\mathbb{Z}}{p_s^{a_s}\mathbb{Z}})^*$. Este elemento é da forma $(g_0, g_1, \dots, g_s)$. Para que g tenha ordem 3 tem-se que $(g_0, g_1, \dots, g_s)^3 = (1, 1, \dots, 1) \Longleftrightarrow$

$$\begin{cases} g_0^3 &= 1, \\ g_1^3 &= 1, \\ \vdots & \vdots \quad \vdots \\ g_s^3 &= 1. \end{cases} \tag{3.3}$$

Encontrar quantas soluções para o sistema (3.3), equivale a resolver a equação $x_i^3 = 1, \forall\ i,\ i = 1, \dots, s$. Supondo que $3 \nmid |H_i|$, então $x_i^3 = 1$ possui somente a solução trivial, onde $H_i \simeq (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*, \forall\ i,\ i = 1, \dots, s$ e se $3 \mid |H_i|$ e H_i é cíclico, então existem 3 soluções para $x_i^3 = 1$. Por outro lado, $|H_i| = \phi(p_i^{a_i})$, logo $3 \mid \phi(p_i^{a_i})$. Portanto, a solução do sistema (3.3) é uma s-upla, onde cada coordenada pode ser 1 ou três elementos e estas possibilidades equivalem a quantidade de primos tais que $3 \mid \phi(p_i^{a_i})$. ∎

Observação 3.2.1 *Em particular, tome $n = p.q$, onde p e q são números primos distintos, tem-se $\phi(n) = (p-1)(q-1)$. Assim, se $3 \nmid (p-1)$ e $3 \nmid (q-1)$ tem-se que $r = 0$ e assim existem $\frac{3^0-1}{2} = 0$ cúbicas na extensão galoisiana $\mathbb{Q}(\zeta_{pq})$ sobre $\mathbb{Q}$. E se $3 \mid (p-1)$ e $3 \nmid (q-1)$*

tem-se que $r = 1$ *e assim existem* $\frac{3^1-1}{2} = 1$ *cúbica na extensão galoisiana* $\mathbb{Q}(\zeta_{pq})$ *sobre* $\mathbb{Q}$. *No caso se* $3 \mid (p-1) \quad e \quad 3 \mid (q-1)$ *tem-se que* $r = 2$ *e assim existem* $\frac{3^2-1}{2} = 4$ *cúbicas na extensão galoisiana* $\mathbb{Q}(\zeta_{pq})$ *sobre* $\mathbb{Q}$.

Observação 3.2.2 *Em função do Teorema Fundamental da Teoria de Galois que estabelece uma relação entre subgrupos de ordem 3 e subgrupos de índice 3, do Teorema 3.2.3 que determina a quantidade de subgrupos de ordem 3 e estimulados por simulações, conjectura-se que o número de subgrupos de índice 3 é o mesmo daqueles de ordem 3 e assim sendo a quantidade de cúbicas contidas em* $\mathbb{Q}(\zeta_n)$ *seria* $\dfrac{3^r-1}{2}$, *onde* $n = p_1^{a_1} \dots p_s^{a_s}$ *e* $r = \#\{p_i : 3 \mid \phi(p_i^{a_i}), i = 1, \dots, s\}$.

Exemplo 3.2.1 *Seja* $n = 65 = 13 \cdot 5$, $\phi(65) = \phi(13.5) = 12.4 = 48$ *e* $3 \mid 12, \ 3 \nmid 4$, *assim* $r = 1$, *logo existe somente uma cúbica em* $\mathbb{Q}(\zeta_{65})$ *a qual está contida em* $\mathbb{Q}(\zeta_{13})$ *pois,* $\phi(13) = 12$ *e* $3 \mid 12$. *Assim,* $\mathbb{Q}(\zeta_5)$ *não contribui na quantidade de cúbicas de* $\mathbb{Q}(\zeta_{65})$.

Exemplo 3.2.2 *Seja* $n = 91 = 13 \cdot 7$, $\phi(91) = \phi(13.7) = 12.6 = 72$ *e* $3 \mid 12, \ 3 \mid 6$, *assim* $r = 2$, *logo existem 4 cúbicas em* $\mathbb{Q}(\zeta_{91})$. *Aplicando novamente o Teorema tem-se que* $\mathbb{Q}(\zeta_7)$ *e* $\mathbb{Q}(\zeta_{13})$ *possuem somente uma cúbica cada, as quais serão denotadas por* K_1 *e* K_2. *As outras duas cúbicas, contidas em* $\mathbb{Q}(\zeta_{91})$, *serão denotadas por* K_3 *e* K_4. *Pelo Teorema 2.3.3 tem-se que a cúbica contida em* $\mathbb{Q}(\zeta_7), \ K_1, \ é \ \mathbb{Q}(\theta_1)$, *onde* $\theta_1 = Tr_{\mathbb{Q}(\zeta_7)/K_1}(\zeta_7)$. *Analogamente, tem-se que a cúbica contida em* $\mathbb{Q}(\zeta_{13}), \ K_2, \ é \ \mathbb{Q}(\theta_2)$, *onde* $\theta_2 = Tr_{\mathbb{Q}(\zeta_{13})/K_2}(\zeta_{13})$.

Agora, será introduzido o conceito de Caracteres de Dirichlet para ser calculado o discriminante de K sem usar o seu anel de inteiros algébricos.

3.3 Caracteres de Dirichlet

Um caracter de Dirichlet é basicamente um homomorfismo multiplicativo

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*.$$

Se $n \mid m$ então χ induz um homomorfismo $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ por composição com a aplicação natural $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. Assim, considera-se χ como sendo definido módulo m ou módulo n, se ambos são essencialmente a mesma aplicação. É conveniente escolher n mínimo e chamá-lo condutor de χ, denotado por f ou f_χ.

Exemplo 3.3.1 *Seja* $\chi : (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ *definido por* $\chi(1) = 1, \ \chi(3) = -1, \ \chi(5) = 1 \quad e$ $\chi(7) = -1$. *Sendo* $\chi(a+4) = \chi(a)$, *logo* χ *é definido módulo* 4 *por* $\chi(1) = 1, \ \chi(-3) = -1$. *Se 4 é mínimo, então* $f_\chi = 4$.

Exemplo 3.3.2 *Seja* $\chi : (\mathbb{Z}/6\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ *definido por* $\chi(1) = 1,\ \chi(5) = -1$. *Então* χ *é induzida pela aplicação* $(\mathbb{Z}/3\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ *a qual leva* $\chi(1) = 1,\ \chi(2) = -1$. *Assim* $f_\chi = 3$.

É conveniente classificar caracteres em dois tipos: se $\chi(-1) = 1$ então χ é chamado de par, se $\chi(-1) = -1$ então χ é chamado de ímpar. Os exemplos acima são de caracteres ímpares. Muitas vezes considera-se χ como uma aplicação de $\mathbb{Z}$ em $\mathbb{C}$ por $\chi(a) = 0$ se $(a, f_\chi) \neq 1$. Assim, é importante fazer uma convenção em relação ao módulo da definição de χ.

Será sempre considerado χ como sendo definido módulo seu condutor. Tais caracteres são chamados primitivos. Essencialmente, esta escolha faz $\chi(a) = 0$ como mínimo possível. Então χ é periódica de período f_χ.

Na seqüência, quando for falado de caracteres de $(\mathbb{Z}/n\mathbb{Z})^*$, ou de caracteres módulo n, tem-se que incluir caracteres de condutores dividindo n, por exemplo o caracter do condutor trivial 1.

A convenção que todos os caracteres são primitivos trabalha com uma parte dos caracteres multiplicativos. Seja χ e ψ caracteres de Dirichlet com condutores f_χ e f_ψ. Define-se $\chi\psi$ como se segue.

Considera-se o homomorfismo

$$\gamma : (\mathbb{Z}/mmc(f_\chi, f_\psi))^* \longrightarrow \mathbb{C}^*$$

definido por $\gamma(a) = \chi(a)\psi(a)$. Então $\chi\psi$ é o caracter primitivo associado a γ.

Exemplo 3.3.3 *Define-se* χ *módulo* 12 *por* $\chi(1) = 1,\ \chi(5) = -1,\ \chi(7) = -1,\ \chi(11) = 1$ *e define-se* ψ *módulo* 3 *por* $\psi(1) = 1$ *e* $\psi(2) = -1$. *Então* $\chi\psi$ *sobre* $(\mathbb{Z}/12\mathbb{Z})^*$ *tem os valores* $\chi\psi(1) = 1,\ \chi\psi(5) = 1,\ \chi\psi(7) = -1$ *e* $\chi\psi(11) = -1$. *Tem-se que* $\chi\psi$ *tem condutor 4 e satisfaz* $\chi\psi(1) = 1$ *e* $\chi\psi(3) = -1$. *Note que* $\chi\psi(3) = -1 \neq \chi(3)\psi(3)$.

Exemplo 3.3.4 *Seja* χ *um caracter e* $\psi = \overline{\chi}$, *seu conjugado complexo. Então,* $\psi(a) = \chi(a)^{-1}$ *se* $(a, f_\chi) = 1$. *Segue que* $\chi\overline{\chi}$ *é o caracter trivial:* $\chi\overline{\chi}(a) = 1$, *para todo a, inclusive a=0.*

Exemplo 3.3.5 *Se* $(f_\chi, f_\psi) = 1$ *então* $f_{\chi\psi} = f_\chi f_\psi$.

Algumas vezes é vantajoso pensar em caracteres de Dirichlet como sendo caracteres de Grupos de Galois dos corpos ciclotômicos. Ao ser identificado $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ com $(\mathbb{Z}/n\mathbb{Z})^*$ então um caracter de Dirichlet módulo n é um caracter de Galois.

Os Exemplos 3.3.1 e 3.3.2 devem ser interpretados como segue:

Exemplo 3.3.6 *O núcleo do Exemplo 3.3.1 é* 1 (*mod* 8) *e* 5 (*mod* 8). *O grupo de Galois desta forma é*

$$Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)),$$

então χ é um caracter do quociente de $(\mathbb{Z}/8\mathbb{Z})^*$ por este subgrupo. Conseqüentemente, χ é um caracter de $Gal(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^*$. No Exemplo 3.3.2 tem-se $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$ um caracter módulo 6 e um módulo 3 são caracteres do mesmo grupo de Galois.

Em geral, seja χ um caracter módulo n, assim um caracter do $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Seja K um corpo fixado pelo núcleo de χ. Então $K \subset \mathbb{Q}(\zeta_n)$ e se n é mínimo, então $n = f_\chi$. O corpo K depende somente de χ e é chamado corpo associado a χ.

Mais geralmente, seja X um grupo finito de caracteres de Dirichlet.

Seja n o mínimo múltiplo comum dos condutores dos caracteres de Dirichlet em X, então X é um subgrupo dos caracteres do $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Sejam H a intersecção dos núcleos destes caracteres e K um corpo fixo de H. Então X é o conjunto dos homomorfismos de $Gal(K/\mathbb{Q})$ em $\mathbb{C}^*$. O corpo K é chamado o corpo associado em X e tem-se que $deg(K/\mathbb{Q}) = [K : \mathbb{Q}] =$ ordem de X. Se X é cíclico, gerado por χ, então K é precisamente o mesmo corpo associado a X mencionado acima.

Exemplo 3.3.7 *Seja X o grupo dos caracteres de $(\mathbb{Z}/n\mathbb{Z})^*$ satisfazendo $\chi(-1) = 1$, então a conjugação complexa $(\zeta_n \longmapsto \zeta_n^{-1})$ está no núcleo de cada $\chi \in X$. Então o corpo associado a X é $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ o qual é o subcorpo maximal real de $\mathbb{Q}(\zeta_n)$. Analogamente, se χ é todo caracter então o corpo pertencendo a χ é real se, e somente se, $\chi(-1) = 1$.*

Exemplo 3.3.8 *O caracter χ do exemplo 3.3.3 deve corresponder a uma subextensão quadrática de*

$$\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-3})\mathbb{Q}(i).$$

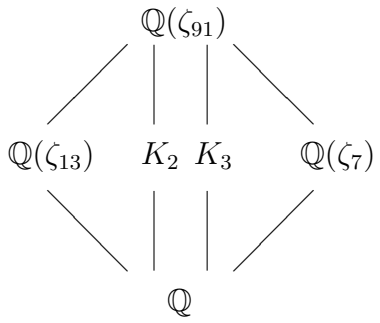
Os três subcorpos quadráticos são $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{3})$. As duas primeiras escolhas irão forçar χ a ter condutor 3 e 4, respectivamente, o que não é o caso. Assim, $\mathbb{Q}(\sqrt{3})$ é o corpo que pertence a χ. Alternativamente, se $\chi(-1) = 1$, o corpo que pertence a χ tem que ser real. O fato que o discriminante de $\mathbb{Q}(\sqrt{3})$ é 12 pode explicar o fato que χ tem condutor 12.

Teorema 3.3.1 ([*19*], pag. 27) *Seja K o corpo de números associado ao grupo X de caracteres de Dirichlet. Então o discriminante de K é dado por*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi.$$

Este Teorema será muito útil para calcular discriminantes de corpos de números abelianos. Por exemplo, considere o subcorpo real de $\mathbb{Q}(\zeta_p)$. O grupo de caracteres consiste do caracter trivial de condutor 1 e $(p-3)/2$ outros caracteres, todos do condutor p. Se $r_2 = 0$ tem-se que $d(\mathbb{Q}(\zeta_p + \zeta_p^{-1})) = p^{(p-3)/2}$. Este teorema será usado para calcular o discriminante de alguns reticulados sem utilizar o anel de inteiros algébricos do corpo de números considerado.

Exemplo 3.3.9 *Calcular o discriminante de* $\mathbb{Q}(\zeta_{91})$. *Pelo exemplo 3.2.2 tem-se o seguinte diagrama:*



E tem-se que existem 4 subgrupos de ordem 3, então pela Teoria de Galois existem 4 corpos fixados. Destes corpos conhece-se $\mathbb{Q}(\zeta_7)$ *e* $\mathbb{Q}(\zeta_{13})$, *os outros serão indicados por* K_2 *e* K_3. *Como* $\phi(91) = 72$ *então existem 72 caracteres de Dirichlet definidos sobre* $(\mathbb{Z}/91\mathbb{Z})^*$. *Assim para calcular o discriminante de* $\mathbb{Q}(\zeta_{91})$, *tem-se que encontrar os respectivos condutores dos caracteres. Dos 72 caracteres tem-se um condutor do caracter trivial, 5 condutores do caracter módulo* 7 *(pois* $\phi(7) = 6$ *e subtrai-se um, que representa o trivial), 11 condutores do caracter módulo* 13 *e* $72 - 5 - 11 - 1 = 55$ *condutores do caracter módulo* 91. *Portanto,*

$$d(\mathbb{Q}(\zeta_{91})) = (-1)^1.7^5.13^{11}.91^{55}.$$

Teorema 3.3.2 *([9]) : Seja* K *uma cúbica e* $K \subseteq \mathbb{Q}(\zeta_n)$, *de condutor* n. *Então,*

$$|D_K| = n^2.$$

3.4 Alguns Reticulados Algébricos

Dados $n = p_1^{a_1} \dots p_s^{a_s}$, $m = \phi(n)$, $L = \mathbb{Q}(\zeta_n)$, $\mathbb{Z}[\zeta_n]$ o anel dos inteiros algébricos de L, $P = p_1 \dots p_s$ e $K \subset L$ tal que $[K : \mathbb{Q}] = 3$, tem-se que:

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

Sendo K um corpo totalmente real e $c_K = 1$, vale a igualdade abaixo:

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

Pela propriedade **(c)** da função traço obtém-se:

$$|\sigma_L(x)|^2 = \frac{m}{3} c_L Tr_{K/\mathbb{Q}}(x\overline{x}) \quad \text{logo,} \quad Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{3}{m\ c_L}|\sigma_L(x)|^2.$$

Portanto,

$$|\sigma_K(x)|^2 = \frac{3}{m} Tr_{L/\mathbb{Q}}(x\overline{x}). \tag{3.4}$$

Dado $x = b_0 + b_1\zeta_n + \ldots + b_{m-1}\zeta_n^{m-1} \in \mathbb{Z}[\zeta_n]$ então $\overline{x} = b_0 + b_1\zeta_n^{-1} + \ldots + b_{m-1}\zeta_n^{-(m-1)}$. Tem-se que $x\overline{x} = \sum_{i=0}^{m-1} b_i^2 + 2\sum_{i=1}^{m-1} A_i\beta_i$, onde

$$A_i = b_0b_i + b_1b_{i+1} + \ldots + b_{m-1-i}b_{m-1},$$

e

$$\beta_i = \zeta_n^i + \zeta_n^{-i},\ \forall i,\ i = 1, \ldots, m-1,$$

logo,

$$Tr_{L/\mathbb{Q}}(x\overline{x}) = m\sum_{i=0}^{m-1} b_i^2 + 2\sum_{i=1}^{m-1} A_i Tr_{L/\mathbb{Q}}(\zeta_n^i). \tag{3.5}$$

Substituindo (3.5) em (3.4) tem-se

$$|\sigma_K(x)|^2 = \frac{3}{m}\left\{ m\sum_{i=0}^{m-1} b_i^2 + 2\sum_{i=1}^{m-1} A_i Tr_{L/\mathbb{Q}}(\zeta_n^i)\right\}.$$

Pelo Teorema 3.1.1 tem-se

$$Tr_{L/\mathbb{Q}}(x\overline{x}) = m\sum_{i=0}^{m-1} b_i^2 + 2\sum_{i=1}^{m-1} A_i\frac{\mu(n/d)}{\phi(n/d)}m. \tag{3.6}$$

onde $d = (n, i)$. O somatório $\sum_{i=1}^{m-1} A_i\frac{\mu(n/d)}{\phi(n/d)}m$ é não nulo quando $d = \frac{n}{P}.t_j$, onde $t_j = (j, P)$ para $j = 1, \ldots, \phi(P) - 1$. Logo, tem-se:

$$(*) \qquad \sum_{i=1}^{m-1} A_i\frac{\mu(n/d)}{\phi(n/d)}m = \frac{n}{P}\sum_{j=1}^{\phi(P)-1}\mu\left(\frac{P}{t_j}\right)\phi(t_j)A_{\frac{n}{P}j}.$$

Substituindo $(*)$ na equação 3.6, obtém-se

Teorema 3.4.1

$$(**) \qquad Tr_{L/\mathbb{Q}}(x\overline{x}) = \frac{n}{P}\left\{\phi(P)\sum_{i=0}^{m-1} b_i^2 + 2\sum_{j=1}^{\phi(P)-1}\mu\left(\frac{P}{t_j}\right)\phi(t_j)A_{\frac{n}{P}j}\right\}.$$

Corolário 3.4.1 *Sejam* $n = \prod_{i=1}^{s} p_i^{a_i}$ *e* $x \in \mathcal{O}_L = \mathbb{Z}[\zeta_n]$ *então,*

$$Tr_{L/\mathbb{Q}}(x\overline{x}) \equiv 0\ mod\ (2\ \frac{n}{P})$$

Exemplo 3.4.1 *Seja* $L = \mathbb{Q}(\zeta_{125})$ *e* $x \in \mathcal{O}_L$. *Pelo Corolário anterior, segue que* $Tr_{L/\mathbb{Q}}(x\overline{x})$ *é um múltiplo de* 50.

Por $(**)$ tem-se

$$\begin{aligned} |\sigma_L(x)|^2 &= c_L Tr_{L/\mathbb{Q}}(x\overline{x}) \\ &= c_L \frac{n}{P} \left\{ \phi(P) \sum_{i=0}^{m-1} b_i^2 + 2 \sum_{j=1}^{\phi(P)-1} \mu\left(\frac{P}{t_j}\right) \phi(t_j) A_{\frac{n}{P}j} \right\}. \end{aligned}$$

3.5 Exemplos de Reticulados Algébricos

Serão calculadas as densidades de centro para os casos particulares $n = p,\ p^r,\ r > 1$. Para isto, serão encontradas as formas quadráticas, para cada um destes casos.

Caso 1: Cúbicas em $\mathbb{Q}(\zeta_p)$

Primeiramente, quando $n = p$, pelo Teorema 2.3.3 tem-se que dados $K \subset \mathbb{Q}(\zeta_p),\ p$ primo, $p \equiv 1\ (mod\ 3)$ onde $[K : \mathbb{Q}] = 3,\ r = (p-1)/3,\ \theta = Tr_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)$ e $g \in \mathbb{Z}$ tal que σ_g gera $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Então $K = \mathbb{Q}(\theta)$ e $\mathcal{O}_K = \mathbb{Z}\theta + \mathbb{Z}\sigma(\theta) + \mathbb{Z}\sigma^2(\theta)$.

Seja $\alpha = a_0\theta + a_1\sigma(\theta) + a_2\sigma^2(\theta) \in \mathcal{O}_K$. Sendo K um corpo real e σ_K o homomorfismo canônico de K em $\mathbb{R}^3$, tem-se: $\sigma_K(\alpha) = (\alpha,\ \sigma(\alpha),\ \sigma^2(\alpha))$ e

$$|\sigma_K(\alpha)|^2 = (a_0^2 + a_1^2 + a_2^2) + \left(\frac{p-1}{3}\right)[(a_0 - a_1)^2 + (a_0 - a_2)^2 + (a_1 - a_2)^2].$$

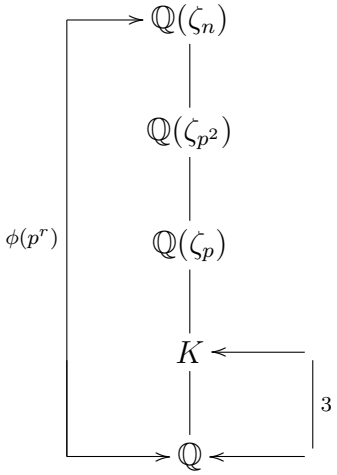
A forma quadrática acima assume valor mínimo 3 quando $a_0 = a_1 = a_2 = 1$. Logo $\rho = \dfrac{\sqrt{3}}{2}$ e novamente pelo Teorema 3.3.2, $D_K = \pm p^2$. Assim,

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{(\sqrt{3}/2)^3}{p} = \frac{3\sqrt{3}}{8p}.$$

No caso $p = 5$ tem-se $\delta(\sigma_K(\mathcal{O}_K)) = \dfrac{3\sqrt{3}}{40} \cong 0,1299$. E para $p = 7$, tem-se $\delta(\sigma_K(\mathcal{O}_K)) = \dfrac{3\sqrt{3}}{56} \cong 0,09279$. Lembrando que o recorde encontrado nesta dimensão, segundo [16] , é $0,17678$.

Caso 2: Cúbicas em $\mathbb{Q}(\zeta_{p^r})$

Para $L = \mathbb{Q}(\zeta_{p^r}),\ m = \phi(p^r) = p^{r-1}(p-1)$ tem-se $P = p$ e $j = 1, \ldots, \phi(P) - 1 = p - 2$ e segue o diagrama abaixo:



A partir disto, pelo Lema 3.2.1 tem-se que $\mathbb{Q}(\zeta_n)$ contém uma cúbica se, e somente se,

$$3 \mid p^{r-1}.(p-1) \Longleftrightarrow \begin{cases} 3 \mid (p-1) \\ \text{ ou} \\ 3 \mid p^{r-1} \end{cases}$$

Se $3 \mid p^{r-1} \Longrightarrow p = 3, \quad r > 1$, pelo Teorema 3.2.3, existe somente uma cúbica contida em $\mathbb{Q}(\zeta_{3^r})$, que é a mesma cúbica em $\mathbb{Q}(\zeta_9)$, que é o subcorpo maximal real $K = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Abaixo, será calculada a densidade de centro de $\sigma_K(\mathcal{O}_K)$, onde $\mathcal{O}_K = \mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$. Sendo $\theta = \zeta_9 + \zeta_9^{-1}$, então $f(x) = x^3 - 3x + 1 = irr(\theta, \mathbb{Q})$. Dado $\alpha = a + b\theta + c\theta^2 \in K$, tem-se que $\sigma_K(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \sigma_4(\alpha))$; logo

$$\begin{aligned} |\sigma_K(\alpha)|^2 &= Tr_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = Tr_{K/\mathbb{Q}}(\alpha^2) = Tr_{K/\mathbb{Q}}(a^2 + 2ab\theta + b^2\theta^2 + 2ac\theta^2 + 2bc\theta^3 + c^2\theta^4) \\ &= 3(a^2 + 2b^2 + 4ac - 2bc + 6c^2) \\ &= 3[(a+2c)^2 + (-b+c)^2 + b^2 + c^2]. \end{aligned}$$

A forma quadrática acima assume valor mínimo 3 quando $a = 1,\ b = c = 0$, assim $\rho = \frac{\sqrt{3}}{2}$; logo

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{(\sqrt{3}/2)^3}{9} = \frac{\sqrt{3}}{24} \cong 0,07217.$$

E se $3 \mid (p-1)$, tem-se que a única cúbica contida em $\mathbb{Q}(\zeta_{p^r}),\ r > 1$, é a cúbica contida em $\mathbb{Q}(\zeta_p)$, a qual foi analisada anteriormente.

Reticulados do tipo $\sigma_K(I)$

Seja $K/\mathbb{Q}$ uma extensão Galoisiana; como foi visto, a igualdade fundamental é dada por:

$$n = e.f.g,$$

onde e é o índice de ramificação, f é o grau residual de qualquer ideal primo $\mathfrak{p}_i \subset \mathcal{O}_K$ e g é chamado número de decomposição.

Observa-se que a partir da igualdade fundamental existem vários tipos de decomposição de $\mathfrak{p}$. Abaixo, serão indicados os casos extremos.

(a) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L,\ i = 1, \ldots, g$, é **totalmente decomposto** em L/K ou, equivalentemente, $\mathfrak{p}$ fatora-se completamente em L/K, se $g = n$, neste caso, $e_i = f_i = 1$.

(b) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L,\ i = 1, \ldots, g$, é **totalmente inerte** em L/K, quando $g_i = 1$ e $e_i = 1$, ou seja, $f_i = n$.

(c) O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L,\ i = 1, \ldots, g$, é **totalmente ramificado** em L/K, se $g = 1$ e $f_i = 1$, ou seja, $e_i = n$.

No caso de uma extensão cúbica galoisiana ocorrem somente os casos extremos. A seguir serão dados alguns exemplos sobre estes casos nas cúbicas $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ e $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

Exemplo 3.5.1 *Em $L = \mathbb{Q}(\zeta_7)$ existe apenas uma cúbica $K = \mathbb{Q}(\theta)$, onde $\theta = \zeta_7 + \zeta_7^{-1}$. Tem-se que $f(x) = x^3 + x^2 - 2x - 1 = irr(\theta, \mathbb{Q})$. Pelo Lema de Kummer, dado 7 como $7 \nmid 1 = [\mathcal{O}_K : \mathbb{Z}[\theta]]$ e $f(x)$ o polinômio irredutível de θ sobre $\mathbb{Q}$ então existem $p \in \mathbb{Z}[X]$, polinômio irredutível, $e \in \mathbb{N}^*$ tais que:*

$$x^3 + x^2 - 2x - 1 \equiv (x+5)^3 (mod\ 7\ \mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p} = \langle \theta + 5,\ 7 \rangle$ *é o ideal primo de $\mathcal{O}_K$ acima de $7\mathbb{Z}$;*

(2) $7\ \mathcal{O}_K = \mathfrak{p}^3$;

(3) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{7\mathbb{Z}} \right] = 1 = f.$

Logo, $N(\mathfrak{p}) = 7^1 = 7$. Dado $\alpha = a + b\theta + c\theta^2 \in \mathcal{O}_K$, sendo $\mathfrak{p}$ acima de $7\mathbb{Z}$ e $\theta \equiv -5\ (mod\ \mathfrak{p})$ então $\alpha \in \mathfrak{p} \iff a - 5b + 4c \in 7\mathbb{Z}$. Assim, como foi visto anteriormente tem-se:

$$|\sigma_K(\alpha)|^2 \ = \ (a^2 + b^2 + c^2) + \left(\frac{p-1}{3} \right) [(a-b)^2 + (a-c)^2 + (b-c)^2].$$

Logo, para $p = 7$ vale:

$$|\sigma_K(\alpha)|^2 \ = \ (a^2 + b^2 + c^2) + 2[(a-b)^2 + (a-c)^2 + (b-c)^2]. \tag{3.7}$$

A forma quadrática acima assume valor mínimo 3 quando $a = b = c = 1$ *satisfazendo* $a - 5b + 4c \in 7\mathbb{Z}$. *Logo* $\rho = \sqrt{3}/2$; *portanto,*

$$\delta(\sigma(\mathfrak{p})) = \frac{(\sqrt{3}/2)^3}{49} \cong 0,01326.$$

Como $e = 3 = n$, *o ideal primo* $\langle \theta + 5 \rangle$ *é totalmente ramificado na extensão* $K/\mathbb{Q}$.

Exemplo 3.5.2 *Sejam* $L = \mathbb{Q}(\zeta_7)$ *e* $K = \mathbb{Q}(\theta)$, *para* $\theta = \zeta_7 + \zeta_7^{-1}$ *aplicando o Lema de Kummer, tem-se que existem* $p_1,\ p_2,\ p_3 \in \mathbb{Z}[X]$, *polinômios irredutíveis, e* $e_1,\ e_2,\ e_3 \in \mathbb{N}^*$ *tais que:*

$$x^3 + x^2 - 2x - 1 \equiv (x + 11)(x + 26)(x + 22)(mod\ 29\ \mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p}_1 = \langle \theta + 11,\ 29 \rangle,\ \mathfrak{p}_2 = \langle \theta + 26,\ 29 \rangle,\ \mathfrak{p}_3 = \langle \theta + 22,\ 29 \rangle$ *são ideais primos de* $\mathcal{O}_K$ *acima de* $29\mathbb{Z}$;

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

(3) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}_i} : \dfrac{\mathbb{Z}}{29\mathbb{Z}}\right] = 1 = f.$

Logo, $N(\mathfrak{p}_i) = 29^1 = 29$. *Dado* $\alpha \in \mathcal{O}_K, \alpha = a + b\theta + c\theta^2$ *e sendo que* $\mathfrak{p}_1$ *está acima de* $29\mathbb{Z}$ *e* $\theta \equiv -11\ (mod\ \mathfrak{p})$ *então* $\alpha \in \mathfrak{p}_1 \Longleftrightarrow a - 11b + 5c \in 29\mathbb{Z}$. *A forma quadrática 3.7 é minimizada para* $a,\ b$ *e* c *inteiros, satisfazendo* $a - 11b + 5c \in 29\mathbb{Z}$, *assumindo assim o valor 10 quando* $a = b = 1$ *e* $c = 2$. *Logo* $\rho = \sqrt{10}/2$, *portanto,*

$$\delta(\sigma(\mathfrak{p}_1)) = \frac{(\sqrt{10}/2)^3}{7.29} = \frac{5\sqrt{10}}{4.7.29} \cong 0,01947.$$

Sendo $e_i = f_i = 1$ *segue que o ideal primo* $\langle \theta + 11 \rangle$ *é totalmente decomposto na extensão* $K/\mathbb{Q}$.

Exemplo 3.5.3 *Sejam* $L = \mathbb{Q}(\zeta_7)$ *e* $K = \mathbb{Q}(\theta)$, *para* $\theta = \zeta_7 + \zeta_7^{-1}$ *aplicando novamente o Lema de Kummer, tem-se que existe* $p \in \mathbb{Z}[X]$, *polinômio irredutível,* $e \in \mathbb{N}^*$ *tais que:*

$$x^3 + x^2 - 2x - 1 \equiv (x^3 + x^2 + 3x + 4)(mod\ 5\ \mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p} = \langle \theta^3 + \theta^2 + 3\theta + 4, 5 \rangle = \langle 5 \rangle = 5\mathcal{O}_K$;

(2) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{5\mathbb{Z}}\right] = 3 = f.$

Logo, $N(\mathfrak{p}) = 5^3$. *Dado* $\alpha \in \mathcal{O}_K,\ \alpha = a + b\theta + c\theta^2$ *e sendo que* $\mathfrak{p} = 5\mathcal{O}_K$ *tem-se* $\alpha \in \mathfrak{p} \Longleftrightarrow a,\ b,\ c$ *são múltiplos de* 5. *Neste caso, a forma quadrática 3.7 é minimizada para* $a = b = 5$ *e* $c = 0$, *assumindo assim valor 125. Logo* $\rho = 5\sqrt{5}/2$, *portanto,*

$$\delta(\sigma(\mathfrak{p})) = \frac{(5\sqrt{5}/2)^3}{5^3.7} = \frac{5\sqrt{5}}{8.7} \cong 0,1996.$$

Sendo $f = 3 = n$ *segue que o ideal primo* $\mathfrak{p}$ *é totalmente inerte na extensão* $K/\mathbb{Q}$.

Exemplo 3.5.4 *Em $L = \mathbb{Q}(\zeta_9)$ existe apenas uma cúbica, $K = \mathbb{Q}(\gamma)$, onde $\gamma = \zeta_9 + \zeta_9^{-1}$. Tem-se que $f(x) = x^3 - 3x + 1 = irr(\gamma, \mathbb{Q})$. Pelo Lema de Kummer, dado que $3 \nmid 1 = [\mathcal{O}_K : \mathbb{Z}[\gamma]]$ e $f(x)$ é o polinômio irredutível de γ sobre $\mathbb{Q}$, então existe $g \in \mathbb{Z}[X]$, polinômio irredutível, $e \in \mathbb{N}^*$ tais que:*

$$x^3 - 3x + 1 \equiv (x+1)^3 (mod\ 3\mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p} = \langle \gamma + 1,\ 3 \rangle$ *é o ideal primo de $\mathcal{O}_K$ acima de $3\mathbb{Z}$;*

(2) $3\ \mathcal{O}_K = \mathfrak{p}^3$;

(3) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{3\mathbb{Z}} \right] = 1 = f.$

Logo, $N(\mathfrak{p}) = 3^1 = 3$. Dado $\beta = a + b\gamma + c\gamma^2 \in \mathcal{O}_K$. Sendo que $\mathfrak{p}$ está acima de $3\mathbb{Z}$ e $\gamma \equiv -1\ (mod\ \mathfrak{p})$ então $\beta \in \mathfrak{p} \iff a - b + c \in 3\mathbb{Z}$. Assim, como foi visto anteriormente tem-se:

$$|\sigma_K(\beta)|^2 = 3[(a+2c)^2 + (-b+c)^2 + b^2 + c^2]. \tag{3.8}$$

é minimizada, para $a,\ b$ e c inteiros, os quais satisfazem $a - b + c \in 3\mathbb{Z}$, assumindo assim o valor 9 quando $a = b = 1$ e $c = 0$, logo $\rho = 3/2$, portanto,

$$\delta(\sigma(\mathfrak{p})) = \frac{(3/2)^3}{9 \cdot 3} = \frac{1}{8} = 0,125.$$

Como $e = 3 = n$, segue que o ideal primo $\langle \gamma + 1 \rangle$ é totalmente ramificado na extensão $K/\mathbb{Q}$.

Exemplo 3.5.5 *Sejam $L = \mathbb{Q}(\zeta_9)$ e $K = \mathbb{Q}(\gamma)$, onde $\gamma = \zeta_9 + \zeta_9^{-1}$. Aplicando o Lema de Kummer para $\gamma = \zeta_9 + \zeta_9^{-1}$, tem-se que existem $g_1, \quad g_2,\ g_3 \in \mathbb{Z}[X]$, polinômios irredutíveis, $e_1,\ e_2,\ e_3 \in \mathbb{N}^*$ tais que:*

$$x^3 - 3x + 1 \equiv (x+4)(x+3)(x+10) (mod\ 17\ \mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p}_1 = \langle \gamma + 4,\ 17 \rangle,\ \mathfrak{p}_2 = \langle \gamma + 3,\ 17 \rangle,\ \mathfrak{p}_3 = \langle \gamma + 10,\ 17 \rangle$ *são ideais primos de $\mathcal{O}_K$ acima de $17\mathbb{Z}$;*

(2) $\mathfrak{p}_1 = \mathfrak{p}_2 = \mathfrak{p}_3 = 17\mathcal{O}_K$;

(3) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}_i} : \dfrac{\mathbb{Z}}{17\mathbb{Z}} \right] = 1 = f.$

Logo, $N(\mathfrak{p}_i) = 17^1 = 17$. Dado $\beta \in \mathcal{O}_K, \beta = a + b\gamma + c\gamma^2$ e sendo $\mathfrak{p}_1$ acima de $17\mathbb{Z}$ e $\gamma \equiv -4\ (mod\ \mathfrak{p})$ então $\beta \in \mathfrak{p}_1 \iff a - 4b - c \in 17\mathbb{Z}$. A forma quadrática 3.8 é minimizada para a, b e c inteiros, os quais satisfazem $a - 4b - c \in 17\mathbb{Z}$, assumindo assim valor 33 quando $a = c = 1,\ b = 0$. Logo $\rho = \sqrt{33}/2$, portanto,

$$\delta(\sigma(\mathfrak{p}_1)) = \frac{(\sqrt{33}/2)^3}{17 \cdot 9} = \frac{11\sqrt{33}}{17 \cdot 3 \cdot 2^3} \cong 0,1549.$$

Sendo $e_i = f_i = 1$ segue que o ideal primo $\langle \gamma + 4 \rangle$ é totalmente decomposto na extensão $K/\mathbb{Q}$.

Exemplo 3.5.6 *Sejam* $L = \mathbb{Q}(\zeta_9)$ *e* $K = \mathbb{Q}(\gamma)$, *onde* $\gamma = \zeta_9 + \zeta_9^{-1}$. *Aplicando novamente o Lema de Kummer, tem-se que existe* $h \in \mathbb{Z}[X]$, *polinômio irredutível, e* $\in \mathbb{N}^*$ *tais que:*

$$x^3 + x^2 - 2x - 1 \equiv (x^3 + 2x + 1)(mod\ 5\ \mathbb{Z}[X]) \quad e$$

(1) $\mathfrak{p} = \langle \gamma^3 + 2\gamma + 1,\ 5\rangle = \langle 5\rangle = 5\mathcal{O}_K$;

(2) $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{5\mathbb{Z}}\right] = 3 = f.$

Logo, $N(\mathfrak{p}) = 5^3$. *Dado* $\beta \in \mathcal{O}_K$, $\alpha = a + b\gamma + c\gamma^2$ *e sendo que* $\mathfrak{p} = 5\mathcal{O}_K$ *tem-se* $\beta \in \mathfrak{p} \iff a,\ b,\ c$ *são múltiplos de* 5. *Neste caso, a forma quadrática 3.8 é minimizada para* $a = 5$ *e* $b = c = 0$, *assumindo assim valor 75. Logo* $\rho = 5\sqrt{3}/2$, *portanto,*

$$\delta(\sigma(\mathfrak{p})) = \frac{(5\sqrt{3}/2)^3}{5^3 \cdot 9} = \frac{\sqrt{3}}{2^3 \cdot 3} \cong 0,07217.$$

Sendo $f = 3 = n$, *segue que o ideal primo* $\mathfrak{p}$ *é totalmente inerte na extensão* $K/\mathbb{Q}$.

Referências Bibliográficas

[1] Boutros, J.; Viterbo, E.; *Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel*. IEEE Trans. Inform. Theory, V.44, n.4, 1998.

[2] Endler, O.; *Teoria dos Números Algébricos*. Projeto Euclides, 1986.

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

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

[5] Garcia, A.; Lequain, Y.; *Elementos de álgebra*. Projeto Euclides, 2002.

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

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

[8] Ireland, K.; Rosen, M.; *A Classical Introduction to Modern Number Theory*. Spring-Verlag, 1982.

[9] Lopes, J.O.D.; *Discriminante dos Corpos Abelianos*. Tese de Doutorado, IMECC/UNICAMP, 2003.

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

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

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

[13] Ribenboim, P.; *Classical Theory of Algebraic Numbers*. Spring-Verlag, 2000.

[14] Rotman, J.; *Galois Theory*. Springer-Verlag, 1990.

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

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

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

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

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