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

# Representação Geométrica em $\mathbb{Q}(\zeta_{pq})$

**Giovana Morali Ramos**

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

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

São José do Rio Preto, SP

Dezembro - 2005

# COMISSÃO JULGADORA

Titulares

Prof. Dr. Trajano Pires da Nóbrega Neto - Orientador

Prof. Dr. André Luíz Flores

Prof. Dr. José Othon Dantas Lopes

Suplentes

Prof. Dr. Ali Messaoudi

Prof. Dr. Marcelo Firer

“Jamais o fracasso me
surpreenderá se a minha
vontade de vencer for
suficientemente “forte”.”
(Autor desconhecido)

Aos meus pais,

Benedicto Oswaldo e Rita de

Cássia

Aos meus irmãos,

Danilo e Viviane

E ao meu namorado

Marcelo

*dedico.*

# Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus.

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

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

Aos professores do Departamento de Matemática da UNESP - São José do Rio Preto.

À minha família, pelo carinho, estímulo e paciência.

À minha amiga Fernanda, que trabalha comigo desde a graduação, pelo companheirismo e apoio.

Aos meus amigos Marcus, Elen, Cátia e Tatiane pela amizade, incentivo e apoio desde a graduação.

À todos os amigos da pós-graduação pelo companheirismo e pelos momentos de descontração.

À CAPES, pelo apoio financeiro.

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

# Sumário

# Índice de Símbolos

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

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

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

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

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

$\partial f$: grau do polinômio $f$

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

$\prod$: produtório

$\sum$: somatório

$det\ A$: determinante de $A$

$(a_{ij})$: matriz

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

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

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

$\#X$: cardinalidade do conjunto $X$

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

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

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

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

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

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

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

$\frac{R}{I}$: 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 $n$-ésima primitiva da unidade

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

$D_K$: discriminante absoluto do corpo $K$

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

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

$A$: conjunto dos números algébricos

$B$: conjunto dos inteiros algébricos

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

Ker $(f)$: núcleo do homomorfismo $f$

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

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

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

$K_p$: corpo de decomposição do primo $p$

# Resumo

O objetivo principal deste trabalho é estudar a densidade de centro de reticulados obtidos por meio do Método de Minkowski em subcorpos de $\mathbb{Q}(\zeta_{pq})$, com $p$ e $q$ primos ímpares distintos e satisfazendo a condição $o_q(p) \equiv o_p(q) \equiv 1 \ (mod\ 2)$.

O cálculo da densidade de centro é feito a partir do discriminante do corpo, da norma do ideal e da minimização da forma traço.

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

# Abstract

This work aims at studying the center density of the lattices got through the Minkowski's Method in subfields of $\mathbb{Q}(\zeta_{pq})$, $p$ and $q$ prime number and $o_q(p) \equiv o_p(q) \equiv 1 \ (mod\ 2)$.

The calcule of the center density is done using the discriminant of the field, the norm of the ideal and the minimization of trace form.

Keywords: Abelians Fields, Cyclotomic Fields, Lattices, Center Density.

# Introdução

A distribuição de esferas de mesmo raio no espaço euclidiano de tal modo que a intersecção entre duas delas tenha no máximo um ponto é chamada empacotamento esférico. A forma de dispor essas esferas de maneira que ocupem a maior parte desse espaço, ou seja, que esta distribuição tenha alta densidade, é um problema de grande importância e mereceu citação de Hilbert, que durante um Congresso em Paris, em 1900, relacionou-o como sendo o 18º numa lista de 23 problemas mais relevantes da época.

A partir daí, muitas teorias evoluíram, vários métodos matemáticos foram descritos com a finalidade de se obter empacotamentos esféricos com alta densidade.

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

Tudo ficou mais interessante quando Shannon, em 1948, publicou em um artigo [10] a estreita relação existente entre a eficiência dos códigos corretores de erro e a densidade de alguns reticulados. Com isto, passaram-se a associar o estudo dos códigos ao dos reticulados.

Diante disto, o interesse para esse problema aumentou consideravelmente, surgiram várias famílias de reticulados, cada uma dessas visando dar uma melhor contribuição no que diz respeito à densidade de empacotamento. Vários métodos foram desenvolvidos e dentre esses, destaca-se o descrito por Minkowski, que é baseado na Teoria Algébrica dos Números.

O método de Minkowski, que consiste na representação geométrica de ideais do anel dos inteiros algébricos de um corpo de números, despertou o interesse em um número maior de matemáticos e os avanços apareceram naturalmente. Um ponto de grande importância

foram os trabalhos desenvolvidos por Maurice Craig que reproduziu o reticulado de Leech ($\Lambda_{24}$) através da representação geométrica de um ideal do anel dos inteiros de $\mathbb{Q}(\zeta_{39})$, e com o mesmo método, obteve uma família, que denotou por $A_n^m$, que assume recordes em alguns dimensões da forma $p-1$, onde $p$ é um número primo.

Nos anos de 1994 e 1995, Joseph Boutros juntamente com a participação de outros três especialistas publicaram alguns resultados onde mostram que versões particulares de empacotamentos reticulados já conhecidos, construídos de corpos ciclotômicos, coincidem com os reticulados mais densos conhecidos e até assumem novos recordes. Apesar de existirem infinitos corpos ciclotômicos, a restrição ao estudo dos reticulados em tais corpos impõe limitações, com destaque para a dimensão. Esta restrição se justifica pela complexidade do problema quando este é tratado em outros corpos, mesmo nos corpos abelianos.

Estaremos interessados na densidade de centro dos reticulados, que para um ideal não nulo $I$ pode ser calculada pela expressão

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

onde $r_2$ é a metade do número de monomorfismos complexos de $K$ em $\mathbb{C}$, $n$ é o grau da extensão, $\rho$ é o chamado raio de empacotamento do reticulado, $D_K$ é o discriminante do corpo $K$, $N(I)$ é a norma do ideal $I$. Assim, podemos notar que o cálculo da densidade de centro de tais reticulados envolve o cálculo da norma do ideal $I$, que está relacionada com a teoria de decomposição de ideais em uma extensão ( veja Seção 2.5), o cálculo do discriminante do corpo $K$ (veja Seção 1.2) e o cálculo da menor distância do reticulado, o que equivale a minimizar uma forma quadrática como veremos no terceiro capítulo.

O Teorema de Kronecker-Weber ([16]) diz que todo corpo de números abeliano está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para algum $n$. Assim, estudar corpos abelianos equivale a estudar subcorpos de corpos ciclotômicos, que no caso geral já é considerado um estudo bastante abrangente.

Direcionamos nosso trabalho aos corpos abelianos, tendo em vista a possibilidade do uso propiciado pela Teoria de Galois. A fim de se aplicar alguns resultados aqui descorridos restringimos, ainda mais, o nosso interesse aos subcorpos de $\mathbb{Q}(\zeta_{pq})$, com $p$ e $q$ primos

ímpares distintos. Diante do fato de que os reticulados de maior interesse são aqueles com maior densidade de centro, e com o intuito de obter tais, consideramos ainda primos $p$ e $q$ que satisfazem a condição de que a ordem de $p$ módulo $q$ e a ordem de $q$ módulo $p$ sejam ímpares. Dessa forma, os primos $p$ e $q$ terão uma apropriada decomposição em $\mathcal{O}_K$. Considerando os corpos de decomposição do primo $p$ em $\mathbb{Q}(\zeta_q)$, $K_p$, e do primo $q$ em $\mathbb{Q}(\zeta_p)$, $K_q$, estamos interessados no subcorpo $K$ de $\mathbb{Q}(\zeta_{pq})$ obtido através do compositum de $K_p$ e $K_q$.

Assim, o objetivo principal deste trabalho consiste em estudar a densidade de centro dos reticulados obtidos através de ideais do anel dos inteiros algébricos do subcorpo $K$. Para isso, foi preciso estudar e compreender alguns conceitos que envolve a Teoria Algébrica dos Números como veremos adiante.

Este trabalho está dividido em três capítulos e, no início de cada um, mencionamos os principais resultados.

O primeiro Capítulo abrange aspectos gerais da Teoria Algébrica dos Números. Aqui introduzimos os conceitos de elemento algébrico, corpo de números, discriminante, inteiro algébrico, base integral, norma e traço de um elemento, entre outros. Os resultados aqui apresentados, bem como suas demonstrações, podem ser encontrados em [7] e [12].

No segundo Capítulo, apresentamos alguns resultados mais específicos que serão essenciais para o desenvolvimento e para uma melhor compreensão do próximo Capítulo, como os conceitos de corpos quadráticos, ciclotômicos e abelianos, a caracterização do anel dos inteiros algébricos de um corpo quadrático e do corpo ciclotômico, a decomposição de um ideal primo em uma extensão, com enfoque para extensões galoisianas, o cálculo do discriminante dos corpos ciclotômicos e dos subcorpos de $\mathbb{Q}(\zeta_p)$, entre outros. Apresentamos também um resultado onde mostra que todo ideal não nulo do anel dos inteiros algébricos pode ser fatorado unicamente em um produto de ideais primos. Enunciamos o Lema de Kummer que será de grande importância para o estudo da decomposição de um ideal primo em uma extensão. Neste capítulo optamos também por omitir as demonstrações, embora a cada resultado enunciado colocamos uma fonte do mesmo. No início desse Capítulo, mencionamos as referências utilizadas para o desenvolvimento de cada seção que compõe o mesmo.

Finalizando, no terceiro Capítulo, enfocamos a partir da teoria desenvolvida nos capítulos anteriores o objetivo principal deste trabalho. Iniciamos com as definições de reticulado, empacotamento esférico, densidade de centro e também o Método de Minkowski, para a obtenção de reticulados via representação geométrica de ideais dos anéis dos inteiros algébricos. Apresentamos uma expressão para a forma quadrática dos corpos ciclotômicos cuja aplicação se faz quando determinamos o raio de empacotamento de um reticulado.

Na última Seção estudamos os subcorpos de $\mathbb{Q}(\zeta_{pq})$, $p$ e $q$ primos ímpares distintos. Considerando que a ordem de $p$ módulo $q$ e a ordem de $q$ módulo $p$ sejam ímpares, existe um ideal que permite que todos os parâmetros para o cálculo da densidade de centro sejam desenvolvidos, e ainda, constatamos que essa assume recorde, por exemplo, na dimensão oito.

Por ser o Capítulo que contém os objetivos principais do nosso trabalho, achamos conveniente incluir algumas demonstrações dos resultados apresentados.

# Capítulo 1

# Teoria Algébrica dos Números

Neste capítulo introduzimos conceitos importantes da Teoria Algébrica do Números, tendo em vista fornecer uma base teórica para o desenvolvimento dos demais capítulos, além de fixar a notação. Admitimos que o leitor possua conhecimentos elementares de Álgebra, que pode ser encontrado nas referências ([3]) e ([5]).

Fizemos um breve estudo sobre os elementos algébricos sobre um corpo, inteiros sobre um anel e as relações entre eles. Definimos Corpo de Números e alguns de seus principais parâmetros, como: Anel dos Inteiros Algébricos, Discriminante, Base Integral, Norma e Traço de um elemento.

Optamos por omitir as demonstrações, embora a cada resultado enunciado é colocado uma fonte do mesmo, que de um modo geral, pode ser encontrado em [7] e [12].

Dentre os resultados centrais, destacamos o Teorema 1.1.1, que nos dá a caracterização de um corpo de números e o Teorema 1.4.1 onde mostra que $\mathcal{O}_K$ é um $\mathbb{Z}$ - módulo livre de posto $n$, ou seja, admite uma base integral.

## 1.1 Elementos Algébricos sobre um Corpo

Seja $K$ um subcorpo do corpo $L$, dizemos que $L$ é uma extensão do corpo $K$ e denotamos 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 denotamos por $[L : K]$. Dizemos que $L/K$ é uma extensão finita se $[L : K]$ é finito. Dados $K \subset L$ corpos e $\alpha$ um elemento de $L$, o

conjunto de todas as expressões polinomiais em $\alpha$ e coeficientes em $K$, denotaremos por $K[\alpha]$.

Dados um anel $R$ e $K$ um subcorpo de $R$, dizemos que $\alpha \in R$ é algébrico sobre $K$ se $\alpha$ é raiz de um polinômio não nulo com coeficientes em $K$. Caso contrário, $\alpha$ é transcedente sobre $K$. Se todo elemento de $R$ for algébrico sobre $K$, dizemos que $R$ é algébrico sobre $K$. No caso em que $R$ é um corpo e $R$ é algébrico sobre $K$, diz-se que $R$ é uma extensão algébrica sobre $K$.

Por exemplo, o elemento $\alpha = \sqrt{5} + \sqrt{-3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $X^4 - 4X^2 + 64 \in \mathbb{Q}[X]$.

Consideremos $\alpha \in L$ algébrico sobre $K$ e $J = \{p \in K[X] : p(\alpha) = 0\}$. O conjunto $J$ contém um único polinômio mônico $p_\alpha = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ de grau mínimo. Chamamos $p_\alpha$ de polinômio minimal de $\alpha$ sobre $K$, o seu grau, de grau de $\alpha$ sobre $K$ e mostra-se que é um polinômio irredutível.

Para $\alpha$ algébrico temos o seguinte resultado que pode ser encontrado em ([12], pag. 23) :

Sejam $L/K$ uma extensão e $\alpha \in L$, então $\alpha$ 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 $\alpha$ sobre $K$ e $K(\alpha) = K[\alpha]$.

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

Vale ressaltarmos um outro resultado muito útil de extensões algébricas que pode ser encontrado em ([12], pag. 22), onde mostra-se que sendo $H$ um corpo, $K$ uma extensão algébrica de $H$ e $L$ uma extensão algébrica de $K$, temos que $L$ é uma extensão algébrica de $H$ e vale $[L : H] = [L : K][K : H]$.

Denotamos por $A$ o conjunto dos números algébricos, que em ([12], pag. 39) mostra-se que é um subcorpo de $\mathbb{C}$.

Definimos um corpo de números como sendo um subcorpo $K$ de $\mathbb{C}$ tal que $[K : \mathbb{Q}]$ é finito. Isto implica que todo elemento de $K$ é algébrico sobre $\mathbb{Q}$ e assim $K \subseteq A$. Se $K$ é um corpo de números, então $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, para finitos números algébricos $\alpha_1, \ldots, \alpha_n$.

O seguinte teorema, conhecido com Teorema do Elemento Primitivo, nos mostra como se dá a caracterização de um corpo de números.

**Teorema 1.1.1** ([*12*], pag. 40) *Se $K$ é um corpo de números, então $K = \mathbb{Q}(\theta)$, para algum $\theta$ algébrico.* ∎

Considere, por exemplo, $K = \mathbb{Q}(\sqrt{5}, \sqrt[3]{7})$, então temos que $f(X) = X^2 - 5$ é o polinômio irredutível de $\sqrt{5}$ sobre $\mathbb{Q}$ e $g(X) = X^3 - 7$ é o polinômio irredutível de $\sqrt[3]{7}$ sobre $\mathbb{Q}$. As raízes de $f$ são $\alpha_1 = \sqrt{5}$ e $\alpha_2 = -\sqrt{5}$ e as de $g$ são $\beta_1 = \sqrt[3]{7}$, $\beta_2 = \sqrt[3]{7}\omega$ e $\beta_3 = \sqrt[3]{7}\omega^2$, onde $\omega = e^{\frac{2\pi i}{3}}$. Devemos encontrar $c \in \mathbb{Q}$ de modo que,

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

A equação acima vale para todo $c \in \mathbb{Q}^*$, em particular, para $c = 1$, assim $K = \mathbb{Q}(\sqrt{5} + \sqrt[3]{7})$.

A seguir enunciaremos uma proposição que será útil na próxima seção.

**Proposição 1.1.1** ([*7*], 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 $\varphi(\alpha) = \beta$.* ∎

## 1.2 Conjugados e Discriminantes

O discriminante de um corpo de números desempenha um papel fundamental na teoria dos reticulados algébricos, pois como veremos nos próximos capítulos, este se relaciona com o cálculo da densidade de centro de reticulados gerados a partir de ideais.

Em relação aos conjugados temos o seguinte resultado cuja demonstração usa-se a proposição 1.1.1, acima enunciado.

**Teorema 1.2.1** ([*12*], pag. 41) *Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau $n$. Então existem exatamente $n$ monomorfismos distintos*

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

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

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

$$f_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)) = X^n - \left(\sum_{i=1}^{n}\sigma_i(\alpha)\right)X^{n-1} + \ldots + (-1)^n\prod_{i=1}^{n}\sigma_i(\alpha). \qquad (1.2)$$

Em ([12], pag. 42), mostra-se que os coeficientes do polinômio característico são números racionais, ou seja, $f_\alpha(X) \in \mathbb{Q}(X)$.

Dessa forma, podemos concluir que $\sum_{i=1}^{n}\sigma_i(\alpha)$ e $\prod_{i=1}^{n}\sigma_i(\alpha)$ são números racionais.

Como consequências deste resultado temos que o polinômio característico $f_\alpha$ é uma potência do polinômio minimal $p$ e os $K-conjugados$ de $\alpha$ são as raízes de $p$ em $\mathbb{C}$, cada uma repetidas $n/m$ vezes, onde $m = \partial p$.

Vale lembrar que os $K$-conjugados de $\alpha$ são os elementos $\alpha_i$, para $i = 1, \ldots, n$. Embora os $\theta_i$ sejam distintos (e são os $K$-conjugados de $\theta$), nem sempre é verdade que os $K$-conjugados de $\alpha$ são distintos. Observe que os $K$-conjugados de $\alpha$ não são necessariamente elementos de $K$, como também, os $\theta_i$ não são necessariamente elementos de $K$. Por exemplo, seja $\theta$ a raiz real cúbica de 3, então $\mathbb{Q}(\theta)$ é um subcorpo de $\mathbb{R}$. Os $K$-conjugados de $\theta$ são $\theta$, $\omega\theta$ e $\omega^2\theta$ onde $\omega = e^{\frac{2\pi i}{3}} = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$. Observe que $\omega\theta$ e $\omega^2\theta$ não são reais, logo não estão em $\mathbb{Q}(\theta)$.

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

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

Considerando, por exemplo, $K = \mathbb{Q}(\sqrt{19})$ um corpo de números e $\{1, \sqrt{19}\} \subset K$. Então:

$$\Delta[1, \sqrt{19}] = \left(det\begin{pmatrix} 1 & \sqrt{19} \\ 1 & -\sqrt{19} \end{pmatrix}\right)^2 = (-2\sqrt{19})^2 = 76.$$

Tomando $\{\beta_1, \ldots, \beta_n\}$ uma outra $n$-upla de $K$, tais que $\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i$, com $c_{ik} \in \mathbb{Q},\ k = 1, \ldots, n$, temos que

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

$$= (det(c_{ik}))^2(det(\sigma_i(\alpha_j)))^2 = (det(c_{ik}))^2\Delta\left[\alpha_1,\ldots,\alpha_n\right].$$

No exemplo anterior vimos que $\Delta[1,\sqrt{19}] = 76$. Agora, considerando uma outra base de $K = \mathbb{Q}(\sqrt{19})$, por exemplo, $\{2-\sqrt{19}, 3+\sqrt{19}\}$, temos, pela observação acima que:

$$\Delta[2-\sqrt{19},3+\sqrt{19}] = \left(det\begin{pmatrix}2 & -1\\ 3 & 1\end{pmatrix}\right)^2.\Delta[1,\sqrt{19}] = 25.76 = 1900.$$

**Teorema 1.2.2** ([*12*], pag. 44) *O discriminante de qualquer base de $K = \mathbb{Q}(\theta)$ é racional e não nulo, e se todos os $K$-conjugados de $\theta$ são reais, então o discriminante de toda base é positivo.* ■

## 1.3 Inteiros Algébricos

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

Por exemplo, o elemento $\theta = \sqrt{-7}$ é inteiro algébrico sobre $\mathbb{Z}$, pois é raiz do polinômio mônico $f(X) = X^2 + 7$. O mesmo ocorre com o elemento $\alpha = \sqrt{3} + \sqrt{5}$, já que este é raiz do polinômio mônico $p(X) = X^4 - 4X^2 - 8$.

Segundo a definição, $\alpha$ 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 $a_n^{-1}$, temos:

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

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

**Observação 1.3.1** *Chamamos de $B$ o conjunto dos $\theta \in R$, tais que $\theta$ é um inteiro algébrico sobre $S$. Mostra-se em* ([12], pag. 47) *que os inteiros algébricos formam um subanel do corpo dos números algébricos $A$ e que se $\theta$ é um número complexo satisfazendo um polinômio mônico cujos coeficientes são inteiros algébricos, então $\theta$ é um inteiro algébrico.*

Assim podemos construir novos inteiros algébricos desconhecidos. Por exemplo, sabemos que $\sqrt{5}$ e $\sqrt{3}$ são inteiros algébricos, logo, temos que $\sqrt{5} + \sqrt{3}$, $2\sqrt{3} + 80\sqrt{5}$ e $(\sqrt{3})^3(2 + \sqrt{5})^2$, também são inteiros algébricos. E os zeros do polinômio

$$X^{15} - (2 + 5\sqrt{3})X^{10} + (\sqrt[3]{5})X^6 - 20\sqrt{5},$$

também são inteiros algébricos.

Dado um corpo de números $K$, definimos **o anel dos inteiros algébricos de $K$,** denotado por $\mathcal{O}_K$, como sendo $\mathcal{O}_K = K \cap B$.

Através do lema a seguir, mostra-se em ([12], pag. 49) que dado $K$ um corpo de números, então $K = \mathbb{Q}(\theta)$, onde $\theta$ é um inteiro algébrico.

**Lema 1.3.1** ([12], pag. 49) *Sejam $K$ um corpo de números e $\alpha$ um elemento não nulo de $K$. Então, para algum $c$ inteiro não nulo temos que $c\alpha \in \mathcal{O}_K$.* ∎

**Observação 1.3.2** *Se $K = \mathbb{Q}(\theta)$, onde $\theta$ é um inteiro algébrico, então certamente $\mathcal{O}_K$ contém $\mathbb{Z}[\theta]$, já que $\mathcal{O}_K$ é um anel contendo $\theta$, mas não é necessariamente igual a $\mathbb{Z}[\theta]$. Por exemplo, $\mathbb{Q}(\sqrt{21})$ é um corpo de número e $\sqrt{21}$ é um inteiro algébrico. Mas, $\frac{1+\sqrt{21}}{2}$ é um zero de $p(X) = X^2 - X - 5$, logo um inteiro algébrico contido em $\mathbb{Q}(\sqrt{21})$, então pertence a $\mathcal{O}_K$ e não pertence a $\mathbb{Z}[\sqrt{21}]$.*

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

**Lema 1.3.2** ([12], pag. 49) *Um número algébrico $\alpha$ é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.* ■

E para saber quando um inteiro algébrico é um número racional, temos o seguinte resultado:

**Lema 1.3.3** ([12], 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

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

$$a_1\alpha_1 + \ldots + a_n\alpha_n, \text{ com } a_i \in \mathbb{Z}.$$

É importante observarmos que $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma $\mathbb{Q}$ - base de $K$, constituída de inteiros algébricos, mas nem sempre é uma base integral de $\mathcal{O}_K$. Por exemplo, $\{1, \sqrt{13}\}$ é uma $\mathbb{Q}$ - base de $K = \mathbb{Q}(\sqrt{13})$, mas não é uma base integral.

**Lema 1.4.1** ([12], 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.* ■

O teorema a seguir nos mostra que $\mathcal{O}_K$ é um $\mathbb{Z}$ - módulo livre de posto $n$.

**Teorema 1.4.1** ([12], pag. 51) *Todo corpo de números $K$ possui uma base integral, ou seja, existem $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ com $n = [K : \mathbb{Q}]$ tal que $\mathcal{O}_K = \sum_{i=1}^{n} \mathbb{Z}\omega_i$.* ■

**Teorema 1.4.2** ([12], 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.* ■

Considere $K = \mathbb{Q}(\sqrt{5})$ e $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ uma base de $K$. Verifiquemos se esta é uma base integral. Os dois monomorfismos de $\mathbb{Q}(\sqrt{5})$ em $\mathbb{C}$ são dados por:

$$\sigma_1(p+q\sqrt{5}) = p+q\sqrt{5}, \qquad \sigma_2(p+q\sqrt{5}) = p-q\sqrt{5}.$$

Assim,

$$\Delta\left[1, \frac{1+\sqrt{5}}{2}\right] = \left( det \begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix} \right)^2 = (-\sqrt{5})^2 = 5$$

e sendo este livre de quadrados, temos que $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral.

**Observação 1.4.1** *A recíproca do teorema anterior é falsa, pois existe bases integrais cujo discriminante não é livre de quadrados, por exemplo, conideremos o corpo* $K = \mathbb{Q}(\sqrt{19})$, *que tem base integral* $\{1, \sqrt{19}\}$ *e discriminante* 76, *que não é livre de quadrados.*

Consideremos $K$ um corpo de números de grau $n$, $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ duas bases integrais de $\mathcal{O}_K$. Como existe uma matriz $C$ inversível, com entradas inteiras, tal que $\alpha_i = \sum_{j=1}^{n} c_{ij}\beta_j$, então, temos

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

pois a matriz mudança de base é unimodular.

Desta forma, podemos observar que o discriminante de uma base integral independe da escolha da base. Este valor comum, que denotamos por $D_K$, é chamado discrimante de $K$ e é sempre um inteiro não nulo. Vale lembrar que corpos de números isomorfos tem o mesmo discriminante.

## 1.5 Norma e Traço

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

$L/K$ como sendo, respectivamente:

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

Se $\alpha$ é um inteiro algébrico então a norma e o traço deste elemento são inteiros. No contexto em que estiver explícito, a norma e o traço de $\alpha$ serão abreviados por $N(\alpha)$ e $Tr(\alpha)$, respectivamente.

Sejam $K \subset L \subset M$ corpos de números, $\alpha,\ \beta \in M$ e $a \in K$. Então valem as seguintes propriedades:

**(1)** $Tr_{M/K}(\alpha + \beta) = Tr_{M/K}(\alpha) + Tr_{M/K}(\beta)$,

**(2)** $Tr_{M/K}(a\alpha) = aTr_{M/K}(\alpha)$,

**(3)** $Tr_{M/K}(a) = [M : K]a$,

**(4)** $N_{M/K}(\alpha\beta) = N_{M/K}(\alpha).N_{M/K}(\beta)$,

**(5)** $N_{M/K}(a) = a^{[M:K]}$,

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

**(7)** $Tr_{M/K}(\alpha) = Tr_{L/K}(Tr_{M/L}(\alpha))$.

Se $\alpha \in L$, temos:

**(8)** $Tr_{M/K}(\alpha) = [M : L]Tr_{L/K}(\alpha)$,

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

A seguir um resultado que relaciona o conceito de norma com o cálculo do discriminante.

**Proposição 1.5.1** ([*12*], pag. 53) *Seja $K = \mathbb{Q}(\theta)$ um corpo de números onde $\theta$ tem polinômio minimal $p$ de grau $n$. A $\mathbb{Q}$-base $\{1, \theta, \ldots, \theta^{n-1}\}$ tem discriminante*

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

*onde $p'$ é a derivada formal de $p$.* ∎

Como exemplo, considere $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{5}$ e $f(X) = X^3 - 5 = irr(\theta, \mathbb{Q})$. Então,

$$\Delta[1, \theta, \theta^2] = (-1)^{\frac{3.2}{2}} N_{K/\mathbb{Q}}(3\theta^2) = -(3\theta^2)^3 = -27.25 = -675.$$

# Capítulo 2

# Corpos Abelianos

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

Inicialmente caracterizamos resumidamente os corpos quadráticos, que serão úteis em exemplos posteriores e, em seguida, caracterizamos os corpos ciclotômicos. Aqui, optamos por omitir as demonstrações, dando assim uma visão geral desses conceitos. Embora, um estudo mais detalhado destes resultados podem ser vistos em ([7]) e ([12]).

Na seção 2.3 falamos um pouco dos Corpos Abelianos. Aqui podemos destacar os Teoremas 2.3.3 e 2.3.4 que serão de grande importância no terceiro capítulo.

Ainda neste capítulo, na seção 2.4, introduzimos os conceitos de decomposição de ideais em uma extensão e também em uma extensão galoisiana. Aqui, também omitimos as demonstrações, porém esses resultados, bem como suas demonstrações podem ser encontradas nas fontes citadas a cada resultado, de um modo geral, nas referências ([6]), ([9]) e ([12]), com exceção do Lema de Kummer que pode ser encontrado em ([1]). Dentre os resultados centrais desta seção podemos destacar o Teorema 2.4.1, que mostra a unicidade da fatoração de um ideal em ideais primos, assim como os resultados referentes a decomposição de um ideal em uma extensão galoisiana. Em relação ao Teorema 2.4.7, é valido observar que o enunciado está diferente, pois na referência citada ele se encontra dividido em dois teoremas.

Na seção 2.5, apresentamos o conceito de norma de ideal e algumas de suas caracterizações.

## 2.1 Corpos Quadráticos

Chamamos corpo quadrático a qualquer corpo de números de grau 2. Os corpos quadráticos são da forma $\mathbb{Q}(\sqrt{d})$ onde $d$ é um inteiro livre de quadrados.

Quanto ao anel de inteiros algébricos de $K = \mathbb{Q}(\sqrt{d})$, podemos dizer que $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $3(mod 4)$ e $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ se $d \equiv 1(mod 4)$.

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

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

E assim o valor do discriminante de $\mathbb{Q}(\sqrt{d})$ será $4d$ se $d \equiv 2$ ou $3(mod(4))$ e será $d$ se $d \equiv 1(mod 4)$

**Exemplo 2.1.1** *O primeiro corpo de números a ser estudado foi o corpo de números Gaussiano $K = \mathbb{Q}(\sqrt{-1})$. Assim, como $-1 \equiv 3(mod 4)$, o anel dos inteiros algébricos de $K$ é $\mathbb{Z}[\sqrt{-1}]$, também conhecido como anel dos inteiros algébricos Gaussianos, e temos que seu discriminante é $-4$. Neste caso, os monomorfismos de $K$ em $\mathbb{C}$ são dados pela inclusão e a conjugação complexa, isto é,*

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

*Assim,*

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

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

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

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

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

## 2.2 Corpos Ciclotômicos

Os corpos ciclotômicos desempenham papel fundamental na Teoria Algébrica dos Números. Como veremos a seguir é possível caracterizar o anel dos inteiros algébricos de um corpo ciclotômico e, consequentemente seu discriminante e demais parâmetros.

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 $\Phi_n$ é um polinômio mônico em $\mathbb{Z}[X]$ ($ver$[7], pag. 114), é irredutível sobre $\mathbb{Q}$ ($ver$[7], pag. 115) e de grau $\phi(n)$, onde $\phi$ é a função de Euler, a qual é caracterizada por

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

Mostra-se em ([7], pag. 110) que dado $n$ um inteiro positivo, então

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

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

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

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

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

*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* $\Phi_{21}$ *é obtido da igualdade:*

$$X^{21} - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_7 \cdot \Phi_{21} = (X^7 - 1)(X^2 + X + 1)\Phi_{21}$$

*ou seja,* $\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$.

### 2.2.1 O $p$-ésimo corpo ciclotômico.

Nesta seção veremos o traço, a norma e o discriminante de $\mathbb{Q}(\zeta_p)$, para qualquer $p$ primo. As potências $\zeta_p,\ \zeta_p^2, \ldots,\ \zeta_p^{p-1}$ também são raízes $p$-ésimas da unidade, distintas de 1, e também pelo mesmo argumento, tem $\Phi_p(X)$ como polinômio minimal.

Assim, temos que

$$\Phi_p(X) = X^{p-1} + \ldots + X + 1 = (X - \zeta_p)(X - \zeta_p^2)\ldots(X - \zeta_p{}^{p-1}) \tag{2.1}$$

logo os conjugados de $\zeta_p$ são $\zeta_p,\ \zeta_p^2, \ldots,\ \zeta_p^{p-1}$. Isto significa que os monomorfismos de $\mathbb{Q}(\zeta_p)$ em $\mathbb{C}$ são dados por

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

Considerando um elemento geral

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

temos

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

Caldulando a norma de $\zeta_p$ temos,

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

Sendo $\zeta_p$ e $\zeta_p{}^i$ $(1 \leq i \leq p-1)$ conjugados, então possuem a mesma norma, assim,

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

O traço de $\zeta_p$ 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

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

temos

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

Assim,

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

Sendo $\zeta_p{}^p = 1$, podemos usar esta fórmula para estender a equação 2.3 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:

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

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

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

a qual pode ser calculada colocando $X = 1$ na equação (2.1) para obter

$$N(1-\zeta_p) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = p \tag{2.6}$$

então, $N(1-\zeta_p) = p$.

**Observação 2.2.1** $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z} =< p >$ . *De fato: De (2.6) segue que :* $p = (1-\zeta_p)(1-\zeta_p{}^2)\ldots(1-\zeta_p{}^{p-1})$. *Assim temos que* $p \in (1-\zeta_p)\mathcal{O}_K$. *Portanto* $< p > \subset (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}$, *(pois* $< p >$ *é um ideal em* $\mathbb{Z}$*). Para mostrarmos a outra inclusão vamos supor que* $p\mathbb{Z} \subsetneq (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} \subseteq \mathbb{Z}$. *Como* $p\mathbb{Z}$ *é maximal*([4], pag. 24), *então* $(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$. *Como* $1 \in \mathbb{Z}$, *então* $1 = (1-\zeta_p)a, a \in \mathcal{O}_K$. *Então* $N(1) = N(1-\zeta_p).N(a)$, *donde segue que* $1 = p.N(a)$, *com* $N(a) \in \mathbb{Z}$,*o que é um absurdo.*

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

O seguinte teorema caracteriza o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_p)$ e consequentemente seu discriminante.

**Teorema 2.2.1** ([*12*], pag. 74) **(a)** *O anel dos inteiros algébricos de* $K = \mathbb{Q}(\zeta_p)$ *é* $\mathbb{Z}[\zeta_p]$. **(b)** *O discriminante de* $\mathbb{Q}(\zeta_p)$, *com* $p$ *um primo ímpar é*

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

■

Mostra-se também em ([16], pag. 11) que o anel dos inteiros algébricos de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}(\zeta_n)$, onde $n$ é um inteiro positivo qualquer. E também que o discriminante é:

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

**Exemplo 2.2.2** *Seja* $K = \mathbb{Q}(\zeta_5)$, *logo seu anel dos inteiros algébricos é* $\mathbb{Z}(\zeta_5)$ *e seu discriminante é* $D_K = (-1)^{(5-1)/2}.5^{5-2} = 5^3 = 125$

**Exemplo 2.2.3** *Seja* $K = \mathbb{Q}(\zeta_4)$, *logo seu anel dos inteiros algébricos é* $\mathbb{Z}(\zeta_4)$ *e seu discriminante é* $D_K = \pm \frac{4^{\phi(4)}}{\prod_{p|4} p^{\frac{\phi(4)}{(p-1)}}} = \frac{4^2}{2^{\frac{2}{1}}} = \frac{16}{2^2} = 4$

## 2.3 Corpos de Números Abelianos

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

Dizemos que uma extensão finita $L \supset K$ é uma extensão galoisiana se $\exists\ f(x) \in K[x]$ tal que $L = Gal(f, K)$, e dizemos que uma extensão algébrica $L \supset K$ é normal se $\forall\ g(x) \in K[x]$, irredutível sobre $K$ que possui uma raiz $\alpha \in L$ possui todas as suas raízes complexas em $L$. É fácil de ver que se $L \supset M \supset K$ são extensões tais que $L \supset K$ é galoisiana então $L \supset M$ é também galoisiana, porém $M \supset K$ não é necessariamente galoisiana como mostra o exemplo $L = Gal(X^3 - 2, \mathbb{Q})$, $M = \mathbb{Q}[\sqrt[3]{2}]$ e $K = \mathbb{Q}$.

Um dos principais resultados da Teoria de Galois que será utilizado é o Teorema Fundamental da Teoria de Galois. Seja $L/K$ uma extensão de corpos com grupo de

Galois $G$ que consiste de todos $K$ - automorfismos de $L$. Seja $C$ o conjunto dos corpos intermediários $M$, e $S$ o conjunto de todos subgrupos $H$ de $G$. Podemos definir duas funções

$$\varphi : C \longrightarrow S \qquad e \qquad \psi : S \longrightarrow C$$

assim, temos: se $M \in C$ então $\varphi(M)$ é o grupo de todos $M$ - automorfismos de $L$. Se $H \in S$ então $\psi(H)$ é o corpo fixado de $H$. Observemos que as funções $\varphi$ e $\psi$ são funções inversas, onde $M \subseteq \psi(\varphi(M))$, e $H \subseteq \varphi(\psi(H))$.

Com isso podemos enunciar o seguinte teorema:

**Teorema 2.3.1** *(Teorema Fundamental da Teoria de Galois)*([13], pag. 104) *Sejam $L/K$ uma extensão galoisiana de grau $n$, com grupo de Galois $G$; e $C$, $S$, $\varphi$ e $\psi$, definidas como acima, então:*

**(1)** *O grupo de Galois $G$ tem ordem $n$.*

**(2)** *As funções $\varphi$ e $\psi$ são inversas.*

**(3)** *Se $M$ é um corpo intermediário então $[L : M] = |\varphi(M)|$ e $[M : K] = |G|/|\varphi(M)|$.*

**(4)** *Um corpo intermediário $M$ é uma extensão normal de $K$ se, e somente se, $\varphi(M)$ é um subgrupo normal de $G$.*

**(5)** *Se um corpo intermediário $M$ é uma extensão normal de $K$ então o grupo de Galois de $M/K$ é isomorfo ao grupo quociente $G/\varphi(M)$.*

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

**Teorema 2.3.2** *(Teorema de Kronecker-Weber)*([16], pag. 319) *Se $K/\mathbb{Q}$ é uma extensão finita abeliana, então $K \subseteq \mathbb{Q}(\zeta_n)$, para algum $n \in \mathbb{N}$.*

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

Os dois resultados seguintes (Teoremas 2.3.3 e 2.3.4) são fortemente utilizados nas aplicações desenvolvidas do próximo capítulo, onde estudaremos os "Subcorpos de $\mathbb{Q}(\zeta_{pq})$".

**Teorema 2.3.3** ([8], pag. 64) *Sejam $p$ um número primo ímpar, $r$ um inteiro positivo e $K \subseteq \mathbb{Q}(\zeta_{p^r})$, $[K:\mathbb{Q}] = up^j$, $p$ não divide $u$. Então,*

$$D_K = \pm p^v$$

*onde*

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

■

O teorema a seguir é de grande importância, pois dado um subcorpo $K$ de $\mathbb{Q}(\zeta_p)$, ele nos mostra quem é $K$, quem é seu anel de inteiros algébricos e também o seu discriminante.

**Teorema 2.3.4** ([15], 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 $\sigma_g$ 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,*

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

■

## 2.4 Decomposição de Ideais

Kummer $(1810 - 1893)$ observou que em certos anéis a fatoração de ideais em ideais primos existe e é única. Estes anéis são chamados de anéis de Dedekind, que serão estudados a seguir.

Consideramos também a fatoração de ideais em uma extensão e em uma extensão galoisiana.

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

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

Um $M$-módulo é dito Noetheriano se satisfaz uma das seguintes condições equivalentes:

**(i)** Toda coleção não vazia de submódulos de $M$ contém um elemento maximal.

**(ii)** Toda cadeia crescente de submódulos de $M$ é estacionária.

**(iii)** Todo submódulo de $M$ é finitamente gerado.

Um anel $C$ é dito Noetheriano se, visto como $C$-módulo, for um módulo Noetheriano.

Um domínio $C$ é chamado de domínio de Dedekind se for integralmente fechado, Noetheriano e se todo ideal primo não nulo de $C$ for maximal.

A seguir, veremos algumas propriedades do anel dos inteiros algébricos de um corpo de números, cuja demonstração pode ser encontrada em ([12], pag. 115).

**(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.

Logo, podemos dizer que $\mathcal{O}_K$ é um Anel de Dedekind

De acordo com o seguinte resultado, podemos dizer que todo ideal não nulo de $\mathcal{O}_K$ se fatora de modo único em ideais primos.

**Teorema 2.4.1** ([9], pag. 50) *Sejam $C$ um anel de Dedekind e $\mathfrak{a}$ um ideal não nulo de $C$. Então existem ideais primos não nulos $\mathfrak{p}_i, \ldots, \mathfrak{p}_n$ de $C$ e inteiros positivos $e_i, \ldots, e_n$ tais que*

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

*e esta expressão é única, a menos da ordem dos fatores.*

Veremos agora como se dá a fatoração de ideais em uma extensão.

Consideraremos o problema de determinar como um dado primo se decompõe em um dado anel de inteiros. Mais geralmente, se $\mathfrak{p}$ é um ideal primo de algum anel de inteiros $\mathcal{O}_K = B \cap K$, $K$ um corpo de números, e se $L$ é um corpo de número contendo $K$, consideremos a decomposição prima do ideal gerado por $\mathfrak{p}$ no anel de inteiros $\mathcal{O}_L = B \cap L$.

**Proposição 2.4.1** ([9], pag. 71) *Sejam $K \subset L$ corpos de números, com $[L : K] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{2.7}$$

*a decomposição de $\mathfrak{p}\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$. Então os ideais $\mathfrak{p}_{i's}$ são necessariamente os ideais primos $\mathfrak{q}$ de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.* ∎

A partir da equação (2.7) $g$ é denominado número de decomposição de $\mathfrak{p}$ na extensão $L/K$. Notemos que, os ideais primos $\mathfrak{q}$ acima de um dado ideal primo $\mathfrak{p}$ são os únicos que ocorrem na decomposição prima de $\mathfrak{p}\mathcal{O}_L$. Os expoentes $e_i{}'s$ com os quais ocorrem são chamados de índices de ramificação e denotaremos por $e(\mathfrak{q} \mid \mathfrak{p})$. Dizemos que um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ é ramificado em $\mathcal{O}_L$ (ou em $L$) se, $e(\mathfrak{q} \mid \mathfrak{p}) > 1$ para algum ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$.

**Teorema 2.4.2** ([6], pag. 63) *Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$, $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$, então as seguintes condições são equivalentes:*

**(a)** $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$,

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

Quando ocorre as condições acima, dizemos que $\mathfrak{q}$ está acima de $\mathfrak{p}$, ou $\mathfrak{p}$ está abaixo de $\mathfrak{q}$. Mostra-se, em ([6], pag. 63) que todo ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$ está acima de um único ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ e todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ está abaixo de no mínimo um ideal primo $\mathfrak{q}$ de $\mathcal{O}_L$.

Há outros números importantes associados com um par de ideais primos $\mathfrak{p}$ e $\mathfrak{q}$, com $\mathfrak{q}$ acima de $\mathfrak{p}$. Sabemos que os anéis quocientes $\mathcal{O}_K/\mathfrak{p}$ e $\mathcal{O}_L/\mathfrak{q}$ são corpos já que $\mathfrak{p}$ e $\mathfrak{q}$ são ideais maximais. Além disso, existe uma maneira em que $\mathcal{O}_K/\mathfrak{p}$ pode ser visto como um subcorpo de $\mathcal{O}_L/\mathfrak{q}$. Como $\mathcal{O}_K \subset \mathcal{O}_L$, temos 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 $\mathcal{O}_K \cap \mathfrak{q}$. Sabemos que $\mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p}$ (pelo Teorema 2.4.2, item (d)), então obtemos a imersão $\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_L/\mathfrak{q}$. Esses são chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$. Esses corpos são finitos e assim, $\mathcal{O}_L/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_K/\mathfrak{p}$ e seja $f$ este grau. Então, $f$ é chamado de **grau de inércia** ou **grau residual** de $\mathfrak{q}$ sobre $\mathfrak{p}$ e denotaremos por $f(\mathfrak{q} \mid \mathfrak{p})$.

Notemos que se $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{u}$ são ideais primos nos respectivos anéis dos inteiros algébricos $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_U$, então

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

**Teorema 2.4.3** *(Igualdade Fundamental)*([6], pag. 65) *Sejam $n$ o grau de $L$ sobre $K$ e $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ os ideais primos de $\mathcal{O}_L$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Denotamos por $e_1, \ldots, e_g$ e $f_1, \ldots, f_g$ os correspondentes índices de ramificação e graus residuais. Então:*

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

■

**Lema 2.4.1** *(Lema de Kummer)*([1], pag. 39) *Sejam $K$ um corpo de números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Dados um número primo $p$ tal que $p$ não divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ e $f(X)$ o polinômio irredutível de $\theta$ sobre $\mathbb{Q}$, então existem $p_1(X), \ldots, p_g(X) \in \mathbb{Z}[X]$, polinômios irredutíveis, $e_1, \ldots, e_g \in \mathbb{N}^*$, tais que,*

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

**(i)** $\mathfrak{p}_i =< p, p_i(\theta) >= p\mathcal{O}_K + p_i(\theta)\mathcal{O}_K$ *são ideais primos de $\mathcal{O}_K$ acima de $p\mathbb{Z}, i = 1, \ldots, g$;*
**(ii)** $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$;
**(iii)** $\left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}}\right] = \partial p_i(X) = f_i$.

Veremos agora como se dá a fatoração de ideais em uma extensão galoisiana.

Aqui nós aplicaremos a Teoria de Galois para o problema geral de determinar como um ideal primo de um anel dos inteiros algébricos se fatora em um corpo de extensão.

**Teorema 2.4.4** *(Da Evidência)*([6], pag. 70) *Dados $L/K$ uma extensão galoisiana com grupo de Galois $G$ e, $\mathfrak{q}$ e $\mathfrak{q}'$ dois ideais primos de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{q}' \cap \mathcal{O}_K$. Então existe $\sigma \in G$, tal que $\sigma(\mathfrak{q}) = \mathfrak{q}'$.* ■

**Corolário 2.4.1** ([6], pag. 71) *Sejam $L$ galoisiana sobre $K$ e $\mathfrak{q}, \mathfrak{q}'$ são dois ideais primos acima de $\mathfrak{p}$, então $e(\mathfrak{q} \mid \mathfrak{p}) = e(\mathfrak{q}' \mid \mathfrak{p})$ e $f(\mathfrak{q} \mid \mathfrak{p}) = f(\mathfrak{q}' \mid \mathfrak{p})$.*

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

**Exemplo 2.4.1** *Considere $L = \mathbb{Q}(\zeta_8)$, assim $\mathcal{O}_L = \mathbb{Z}[\zeta_8]$. O polinômio minimal de $\zeta_8$ sobre $\mathbb{Q}$ é dado por $\Phi_8(X) = X^4 + 1$.*

*A decomposição do ideal $2\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$ satisfaz:*

$$\Phi_8(X) \equiv (p(X))^4 (mod\ 2\mathbb{Z}[X]),\ onde\ p(X) = X + 1$$

*Pelo lema de Kummer temos:*

**(i)** $\mathfrak{p} =< 2, p(\zeta_8) >=< 2, \zeta_8 + 1 >= 2\mathcal{O}_L + (\zeta_8 + 1)\mathcal{O}_L$; *são os ideais primos de $\mathcal{O}_L$ acima de $2\mathbb{Z}$,*

**(ii)** $2\mathcal{O}_L = \mathfrak{p}^4$,

**(iii)** $[\frac{\mathcal{O}_L}{\mathfrak{p}} : \frac{\mathbb{Z}}{2\mathbb{Z}}] = 1$.

*Assim temos $g = f = 1, e = 4, \quad e \quad 4 = g.e.f = 1.4.1$.*

*Agora considerando a decomposição do ideal $3\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$, temos :*

$$\Phi_8(X) \equiv p_1(X).p_2(X) (mod\ 3\mathbb{Z}[X]),\ onde\ p_1(X) = X^2 + 2X + 2\ e\ p_2(X) = X^2 + X + 2.$$

*Pelo Lema de Kummer temos:*

**(i)** $\mathfrak{p}_i =< 3, p_i(\zeta_8) >,\ i = 1, 2$ *são os ideais primos de $\mathcal{O}_L$ acima de $3\mathbb{Z}$,*

**(ii)** $3\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$,

**(iii)**$[\frac{\mathcal{O}_L}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{3\mathbb{Z}}] = 2$.

*Assim temos* $g = f = 2, e = 1, \quad e \quad 4 = g.e.f = 2.1.2$.

*Agora considerando a decomposição do ideal* $17\mathcal{O}_L$ *em ideais primos de* $\mathcal{O}_L$, *temos:*

$$\Phi_8(X) \equiv p_1(X).p_2(X).p_3(X).p_4(X)(mod\ 17\mathbb{Z}[X]),$$

$$onde\ p_1(X) = X + 15, p_2(X) = X + 8, p_3(X) = X + 9\ e\ p_4(X) = X + 2.$$

*Pelo Lema de Kummer temos:*

**(i)** $\mathfrak{p}_i =< 17, p_i(\zeta_8) >,\ i = 1, 2, 3, 4$ *são os ideais primos de* $\mathcal{O}_L$ *acima de* $17\mathbb{Z}$,

**(ii)** $17\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$,

**(iii)**$[\frac{\mathcal{O}_L}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{17\mathbb{Z}}] = 1$.

*Assim temos* $e = f = 1, g = 4, \quad e \quad 4 = g.e.f = 4.1.1$.

*Observe que o índice de ramificação* $e$ *e o grau residual* $f$ *dos ideais primos acima de* $3\mathbb{Z}$ *e acima de* $17\mathbb{Z}$ *são iguais, conforme o corolário acima.*

Seja $L$ uma extensão galoisiana de $K$ com grupo de Galois $G = Gal(L/K)$. Para cada ideal primo $\mathfrak{q}$ acima de $\mathfrak{p} \subseteq \mathcal{O}_K$ definimos o grupo de decomposição e o grupo inercial, que são, respectivamente:

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

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

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

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

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

Logo, se $D \lhd G$, para algum $\mathfrak{q}$ então $\quad D(\mathfrak{q} \mid \mathfrak{p}) = D(\mathfrak{p})$.

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

$$\#\ G = g \cdot \#\ D(\mathfrak{p}) \quad e, \quad portanto \quad \#\ D(\mathfrak{p}) = \frac{n}{g} = e.f.$$

Agora, olhamos para os corpos fixados de $D$ e $E$, denotados por $L_D$ e $L_E$, respectivamente. $L_D$ é chamado o corpo de decomposição e $L_E$ o corpo de inércia.

**Exemplo 2.4.2** *Considere $L = \mathbb{Q}(\zeta_{21})$, assim $\mathcal{O}_L = \mathbb{Z}(\zeta_{21})$. O polinômio minimal de $\zeta_{21}$ sobre $\mathbb{Q}$ é dado por*

$$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1.$$

*A decomposição do ideal $7\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$ satisfaz:*

$$\Phi_{21}(X) \equiv (p_1(X))^6 \cdot (p_2(X))^6 \ (mod\ 7\mathbb{Z}) \ onde\ p_1(X) = X + 3 \ e\ p_2(X) = X + 5,$$

*e do Lema de Kummer, segue que:*

**(a)** $\mathfrak{p}_i =< 7, p_i(\zeta_{21}) >,\ i = 1, 2$ *são os ideais primos de $\mathcal{O}_L$ acima de $7\mathbb{Z}$,*

**(b)** $7\mathcal{O}_L = {\mathfrak{p}_1}^6{\mathfrak{p}_2}^6$,

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

*Assim, temos $g = 2, e_1 = e_2 = 6, f_1 = f_2 = 1$.*

*O grupo dos $\mathbb{Q}$-automorfismos de L sobre $\mathbb{Q}$ é dado por:*

$$G = \{\sigma_i;\ (i, 21) = 1,\ i = 1, \ldots, 21;\ \sigma_i(\zeta_{21}) = {\zeta_{21}}^i\} =$$
$$= \{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_8, \sigma_{10}, \sigma_{11}, \sigma_{13}, \sigma_{16}, \sigma_{17}, \sigma_{19}, \sigma_{20}\}$$

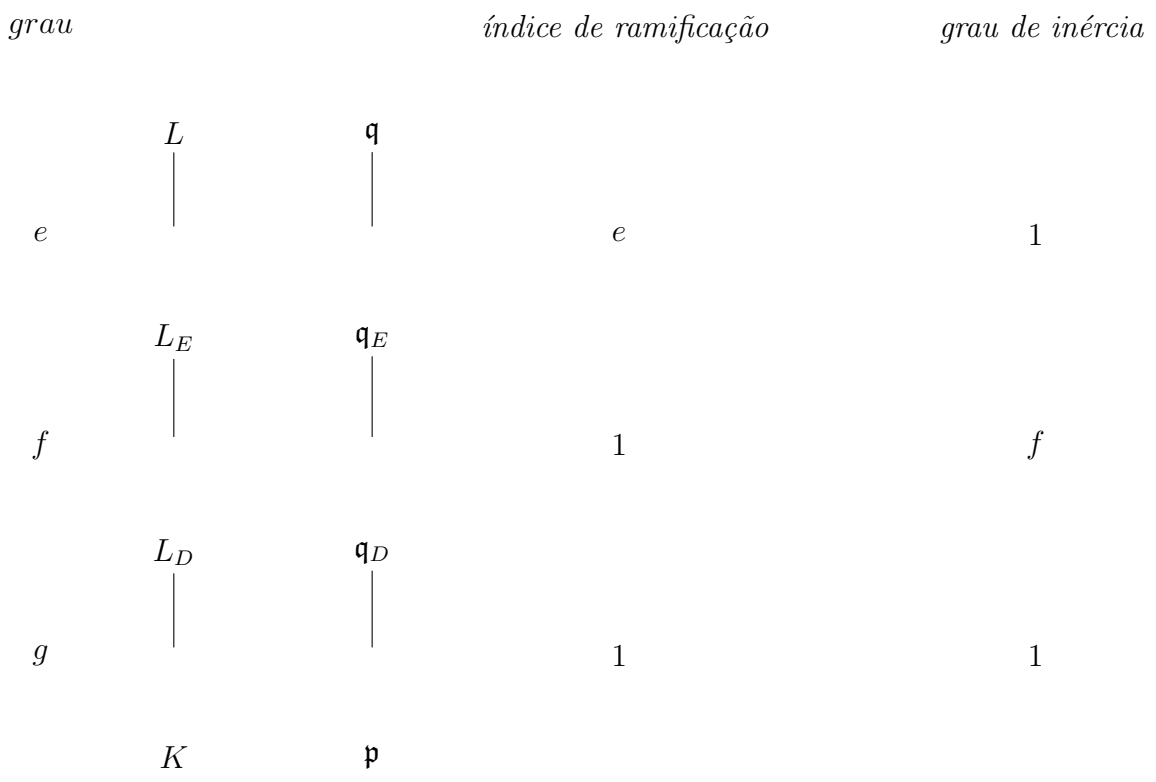
*O grupo de decomposição $D(7\mathbb{Z})$ é dado por*

$$D(7\mathbb{Z}) = \{\sigma \in G/\sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\sigma_1, \sigma_4, \sigma_{10}, \sigma_{13}, \sigma_{16}, \sigma_{19}\}.$$

*Da mesma forma o grupo de inércia é*

$$E(7\mathbb{Z}) = \{\sigma \in G/\sigma(x) \equiv x\ (mod\ \mathfrak{p}_1), x \in \mathcal{O}_L\} = \{\sigma_1, \sigma_4, \sigma_{10}, \sigma_{13}, \sigma_{16}, \sigma_{19}\}.$$

**Teorema 2.4.5** ([6], pag. 100) *Sejam L, K, $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathfrak{p}, \mathfrak{q}$, G, D, E, e, f e g como acima. Então temos o seguinte diagrama:*




■

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

**Teorema 2.4.6** ([6], pag. 104) *Com as notações acima, temos:*
**(a)** $L_D$ *é o maior corpo intermediário* $K^{'}$ *contendo* $K$ *tal que* $e(\mathfrak{p}^{'} \mid \mathfrak{p}) = f(\mathfrak{p}^{'} \mid \mathfrak{p}) = 1$;
**(b)** $L_D$ *é o menor subcorpo* $K^{'}$, *tal que* $\mathfrak{q}$ *é o único ideal primo de* $\mathcal{O}_L$ *acima de* $\mathfrak{p}^{'}$;
**(c)** $L_E$ *é o maior subcorpo* $K^{'}$, *tal que* $e(\mathfrak{p}^{'} \mid \mathfrak{p}) = 1$;
**(d)** $L_E$ *é o menor subcorpo* $K^{'}$, *tal que* $\mathfrak{q}$ *é totalmente ramificado sobre* $\mathfrak{p}^{'}$, *(isto é,* $e(\mathfrak{q} \mid \mathfrak{p}^{'}) = [L : K^{'}]$*).* ■

Seja $K/\mathbb{Q}$ uma extensão galoisiana de grau $n$, sabemos pelo Teorema da Igualdade Fundamental que $n = e.f.g$, onde $e$ é o índice de ramificação, $f$ é o grau residual de

qualquer ideal primo $\mathfrak{p}_i \subset \mathcal{O}_K$ e $g$ é dito número de decomposição do ideal primo $\mathfrak{p}$ em $K/\mathbb{Q}$.

Observamos que a partir do Teorema da Igualdade Fundamental existem vários tipos de decomposição de um ideal primo $\mathfrak{p}$. Indicaremos abaixo alguns casos:

**(a)** O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \ldots, g$, é totalmente ramificado em $L/K$, se $g = f_i = 1$ e $e_i = n$.

**(b)** O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \ldots, g$, é totalmente inerte em $L/K$, se $f_i = n$ e $g = e_i = 1$.

**(c)** O ideal primo $\mathfrak{p}_i$ de $\mathcal{O}_L$, $i = 1, \ldots, g$, é totalmente decomposto em $L/K$, se $g = n$ e $e_i = f_i = 1$.

**Exemplo 2.4.3** *Sejam $K = \mathbb{Q}(\zeta_7)$ e $\mathcal{O}_K = \mathbb{Z}[\zeta_7]$. O polinômio minimal de $\zeta_7$ sobre $\mathbb{Q}$ é dado por*

$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

*A decomposição do ideal $7\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ satisfaz*

$$\Phi_7(X) \equiv (X + 6)^6 \ (mod\ 7\mathbb{Z})$$

*Assim temos $g = f = 1$ e $e = 6$, ou seja, o ideal $7\mathcal{O}_K$ é totalmente ramificado. O ideal $3\mathcal{O}_K$ decompõem-se em ideais primos de $\mathcal{O}_K$ satisfazendo*

$$\Phi_7(X) \equiv X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \ (mod\ 3\mathbb{Z}).$$

*Logo, temos $g = e = 1$ e $f = 6$, logo o ideal $3\mathcal{O}_K$ é totalmente inerte. Agora tomando a decomposição do ideal $29\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$ temos:*

$$\Phi_7(X) \equiv p_1(X) \ldots p_6(X) \ (mod\ 29\mathbb{Z}),\ onde$$

$$p_1(X) = X + 9, \quad p_2(X) = X + 5, \quad p_3(X) = X + 6,$$
$$p_4(X) = X + 22, \quad p_5(X) = X + 4 \quad e \quad p_6(X) = X + 13.$$

*Logo temos $g = 6$, e $e = f = 1$, portanto o ideal $29\mathcal{O}_K$ é totalmente decomposto.*

Em relação a decomposição de ideais temos também o seguinte resultado:

**Teorema 2.4.7** ([6], pag. 72 e 112) *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 $D_K$.*

Vimos que o discriminante do corpo $K = \mathbb{Q}(\zeta_p)$ é $D_K = \pm p^{p-2}$, assim, pelo teorema anterior temos que o único ideal primo que se ramifica em $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ é $p\mathbb{Z}$.

O número de ideais acima de um primo em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$ é dado pelo seguinte resultado:

**Teorema 2.4.8** ([2], pag. 32) *Seja $p$ um primo que não divide $n$. Então o número $r_p$ de ideais primos distintos acima de $p$ em $\mathbb{Q}(\zeta_{p^s n})$ é $r_p = \frac{\phi(n)}{o_n(p)}$, onde $o_n(p)$ é a ordem de $p$ módulo $n$.*

## 2.5 Norma de um Ideal

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

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

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

Podemos caracterizar a norma também pelo seguinte resultado:

**Teorema 2.5.1** ([12], pag. 126) *Sejam $K$ um corpo de números de grau $n$ e $\mathcal{O}_K$ o seu anel dos inteiros algébricos. Então,*

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

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

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

*onde $D_K$ é o discriminante de $K$.* ∎

Veremos agora, através do seguinte resultado, que a norma de ideais é multiplicativa.

**Teorema 2.5.2** ([*12*], pag. 127) *Sejam $K$ um corpo de números e $\mathfrak{a}$ , $\mathfrak{b}$ ideais não nulos de $\mathcal{O}_K$. Então*

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

■

É conveniente introduzir ainda um 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 $\mathfrak{a} | < b >$, então escrevemos também $\mathfrak{a} \mid b$ e dizemos que $\mathfrak{a}$ divide $b$. É claro que $\mathfrak{a} \mid b$ se, e somente se, $b \in \mathfrak{a}$.

**Teorema 2.5.3** ([*12*], pag. 129) *Seja $\mathfrak{a}$ um ideal de $\mathcal{O}_K$, $\mathfrak{a} \neq 0$.*

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

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

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

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

*onde $m \leq n$, o grau de $K$.* ■

Em particular, o item (c) do Teorema 2.5.3, pode ser escrito do seguinte modo: para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$, temos que, $N(\mathfrak{p}) = p^f$, onde $f$ é o grau residual de $\mathfrak{p}$ e $p$ o único número primo de $\mathfrak{p}$. De fato, como $\left[\dfrac{\mathcal{O}_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{p\mathbb{Z}}\right] = f$, então resulta que $\mathcal{O}_K/\mathfrak{p}$ tem $p^f$ elementos.

# Capítulo 3

# Representação Geométrica de Ideais

Neste Capítulo definimos, primeiramente, o que é empacotamento esférico, reticulado, densidade de empacotamento, densidade de centro, entre outros. Estaremos interessados nos reticulados algébricos que são obtidos pelo Método de Minkowski, como veremos na Seção 3.2.

Veremos que a expressão da densidade de centro para esses reticulados envolve parâmetros importantes da Teoria Algébrica dos Números, tais como discriminante de um corpo, norma de um ideal e a forma traço.

Diante da dificuldade de minimizar a forma quadrática, optamos por restringir nossos estudos aos subcorpos de $\mathbb{Q}(\zeta_{pq})$, com $p$ e $q$ primos ímpares distintos. Para primos satisfazendo certas condições apresentamos cotas inferiores para a densidade de centro dos respectivos reticulados.

Por ser o Capítulo que contém o objetivo principal deste trabalho achamos conveniente incluir algumas demonstrações dos resultados aqui apresentados.

Neste Capítulo podemos destacar o Teorema 3.2.1, onde mostra que a representação geométrica de um ideal é um reticulado, a Proposição 3.2.1, para o cálculo de distâncias no reticulado gerado por um ideal e o Corolário 3.4.1, que será importante para a escolha de nosso ideal.

## 3.1 Reticulados

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 independente de V. Denominamos A-reticulado (ou simplesmente reticulado) com base $\{v_1, \ldots, v_r\}$ ao conjunto de elementos da forma

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

Em qualquer citação de reticulado, vamos supor que

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

A distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de tal modo que a intersecção entre duas delas tenha no máximo um ponto é denominada empacotamento esférico. Já um empacotamento reticulado é um empacotamento esférico em que o conjunto dos centros das esferas constituem um subgrupo discreto do $\mathbb{R}^n$, ou seja, formam um reticulado $\Lambda$ de $\mathbb{R}^n$. Definimos a densidade de um dado empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas.

Introduziremos agora os elementos básicos que possibilitarão obter uma expressão para a densidade de um empacotamento.

Denominamos

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

a Região Fundamental de um reticulado $\Lambda \subset \mathbb{R}^n$ associada a base $\beta = \{v_1, \ldots, v_n\}$. Podemos observar que a Região Fundamental depende da escolha da base do reticulado.

Fazendo

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

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

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

a qual é denominada matriz geradora para o reticulado $\Lambda$.

O volume da Região Fundamental, $R_\beta$, independe da base, pois a matriz mudança de base é invertível, com entradas inteiras, ou seja, tem determinante $\pm 1$. Logo, faz sentido definir o volume de $\Lambda$ como sendo o volume da Região Fundamental, e denotaremos por $v(\Lambda)$ e vale $|det(M_\beta)|$.

Temos interesse apenas pelo empacotamento associado ao reticulado $\Lambda$ cujas esferas tenham raio máximo. Assim, o maior raio possível para distribuir esferas centradas em cada ponto do reticulado $\Lambda$ e obter um empacotamento é denominado raio de empacotamento ($\rho$), o qual é dado por $\frac{\Lambda_{min}}{2}$, onde

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

Assim, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Denotamos a densidade de um reticulado $\Lambda$, ou seja, a densidade de empacotamento com esferas de raio $\rho$, associado a um reticulado $\Lambda$, por:

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

O volume de uma esfera $n$-dimensional de raio $\rho$ é

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

onde $v(B(1))$ é o volume de uma esfera de raio 1. Assim,

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

A densidade de centro dada por $\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)}$ é outro parâmetro importante em empacotamentos reticulados

## 3.2 O Homomorfismo Canônico

Sejam $K$ um corpo de números de grau $n$ e $\sigma_i : K \longrightarrow \mathbb{C}$, $i = 1, \ldots, n$, os monomorfismos de $K$ em $\mathbb{C}$. Dizemos que $\sigma_i$ é real, se $\sigma_i(K) \subseteq \mathbb{R}$, caso contrário, dizemos que $\sigma_i$ é imaginário.

Quando todos os monomorfismos de $K$ são reais, dizemos que o corpo é totalmente real e quando todos os monomorfismos de $K$ são imaginários dizemos que o corpo $K$ é totalmente imaginário.

Podemos definir o homomorfismo canônico, o qual é usado para descrever reticulados de posto $n$ em $\mathbb{R}^n$ originados de um ideal ordinário não nulo do anel dos inteiros algébricos de $K$, da seguinte maneira:

Dados $K$ um corpo de números de grau $n$, $r_1$ a quantidade de monomorfismos reais e $2r_2$ a quantidade de monomorfismos imaginários, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ do seguinte modo:

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

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

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

por

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

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

**Exemplo 3.2.1** *Sejam $K = \mathbb{Q}(\sqrt{11})$ com $\mathbb{Q}$-base $\{1, \sqrt{11}\}$ e os monomorfismos de $K$ em $\mathbb{C}$, $\sigma_1$ e $\sigma_2$, onde*

$$\sigma_1\left(a + b\sqrt{11}\right) = a + b\sqrt{11};\ a, b \in \mathbb{Q}.$$
$$\sigma_2\left(a + b\sqrt{11}\right) = a - b\sqrt{11};\ a, b \in \mathbb{Q}.$$

*Então para*

$$x = a + b\sqrt{11} \in K,\ a, b \in \mathbb{Q}$$

*temos*

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

**Exemplo 3.2.2** *Sejam* $K = \mathbb{Q}(\alpha)$ *onde* $\alpha \in \mathbb{R}$ *satisfaz* $\alpha^4 - 2 = 0$. *Os conjugados de* $\alpha = \sqrt[4]{2}$ *são* $\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3$ *onde* $\omega$ *é a raiz primitiva quarta da unidade. Um elemento de K, por exemplo* $x = a + b\alpha + c\alpha^2 + d\alpha^3$, *onde* $a, b, c, d \in \mathbb{Q}$, *é levado a* $\mathbb{R}^4$ *de acordo com*

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

**Teorema 3.2.1** ([9], 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* $(x_i)_{1 \le i \le n}$. *Então,* $\sigma_K(M)$ *é um reticulado em* $\mathbb{R}^n$ *com volume* $v(\sigma_K(M)) = 2^{-r_2} \left| det(\sigma_i(x_j)) \right|$.

**Demonstração:**

Sendo $\{x_1, \ldots, x_n\}$ uma base de $M$, mostraremos que $\{\sigma_K(x_1), \ldots, \sigma_K(x_n)\}$ é uma base de $\sigma_K(M)$. No caso em que K é totalmente real,

$$\sigma_K(x_i) = (\sigma_1(x_i), \ldots, \sigma_n(x_i)),\ i = 1, \ldots, n$$

Seja

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

Aplicando as propriedades de determinante em $D$, obtemos

$$detD = det(\sigma_i(x_j)).$$

Por outro lado, sabemos que

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

Logo

$$(detD)^2 = (det(\sigma_i(x_j)))^2 = \Delta[x_1, \ldots, x_n] \neq 0,\ \text{(ver Teorema 1.2.2)},$$

implicando que $\sigma_K(x_1), \ldots, \sigma_K(x_n)$ são vetores linearmente independentes sobre $\mathbb{R}$. Por construção $\sigma_K(x_1), \ldots, \sigma_K(x_n)$ geram $\sigma_K(M)$ logo $\{\sigma_K(x_1), \ldots, \sigma_K(x_n)\}$ é uma base de $\sigma_K(M)$ e, portanto, $\sigma_K(M)$ é um reticulado.

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

Mostremos agora que $v(\sigma_K(M)) = 2^{-r_2}|det(\sigma_i(x_j))|$, quando K é totalmente imaginário. Nesse caso

$$\sigma_K(x_i) = (Re\sigma_1(x_i), Im\sigma_1(x_i), \ldots, Re\sigma_{r_2}(x_i), Im\sigma_{r_2}(x_i)),\ i = 1, \ldots, n.$$

Seja

$$D = \begin{pmatrix} Re\sigma_1(x_1) & Im\sigma_1(x_1) & \ldots & Re\sigma_{r_2}(x_1) & Im\sigma_{r_2}(x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re\sigma_1(x_n) & Im\sigma_1(x_n) & \ldots & Re\sigma_{r_2}(x_n) & Im\sigma_{r_2}(x_n) \end{pmatrix}$$

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

$$D_1 = \begin{pmatrix} \sigma_1(x_1) & \overline{\sigma_1(x_1)} & \ldots & \sigma_{r_2}(x_1) & \overline{\sigma_{r_2}(x_1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(x_n) & \overline{\sigma_1(x_n)} & \ldots & \sigma_{r_2}(x_n) & \overline{\sigma_{r_2}(x_n)} \end{pmatrix}$$

Como $detD = (2i)^{-r_2}.detD_1$ e $\overline{\sigma_i} = \sigma_{r_2+i}$, então

$$v(\sigma_K(M)) = \mid detD \mid = \left|(2i)^{-r_2}\right| . |detD_1| = 2^{-r_2} . |det(\sigma_i(x_j))| .$$

■

Vimos anteriormente que $\mathcal{O}_K$ é um $\mathbb{Z}-$módulo livre de posto $n$ e que se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_K$ então $\mathfrak{a}$ é um $\mathbb{Z}-$módulo livre de posto menor ou igual a $n$. Como o índice de $\mathfrak{a}$ sobre $\mathcal{O}_K$ é finito, temos que $\mathfrak{a}$ é um $\mathbb{Z}-$módulo livre de posto $n$, também. Assim, pelo Teorema 3.2.1, $\sigma_K(\mathfrak{a})$ é uma reticulado, denominado *realização geométrica do ideal* $\mathfrak{a}$.

**Exemplo 3.2.3** *Sejam* $K = \mathbb{Q}(\sqrt{11})$ *e* $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$. *Sendo* $r_2 = 0$, *temos:*

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

**Exemplo 3.2.4** *Sejam* $K = \mathbb{Q}(\sqrt{-13})$ *e* $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$. *Sendo* $r_2 = 1$, *temos:*

$$v(\sigma_K(M)) = 2^{-1}\left|det\begin{pmatrix} 1 & \sqrt{-13} \\ 1 & -\sqrt{-13} \end{pmatrix}\right| = \frac{1}{2}\left|-2\sqrt{-13}\right| = \left|\sqrt{-13}\right| = \left|\sqrt{13}i\right| = \sqrt{13}$$

■

**Teorema 3.2.2** ([*9*], pag. 57) *Sejam* $K$ *um corpo de números de grau* $n$, *com discriminante* $D_K$ *e* $\mathfrak{a}$ *um ideal não nulo de* $\mathcal{O}_K$. *Então,*

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

**Demonstração:**

Seja $\{x_1, \ldots, x_n\}$ uma base do ideal $\mathfrak{a}$ e como $\mathcal{O}_K \subseteq K$, segue do Teorema 3.2.1 que $v(\sigma_K(\mathfrak{a})) = 2^{-r_2}.\left|det(\sigma_i(x_j))\right|$. Por outro lado, temos

$$|\Delta[x_1, \ldots, x_n]|^{\frac{1}{2}} = |D_K|^{\frac{1}{2}}.N(\mathfrak{a}) \quad e \quad \Delta[x_1, \ldots, x_n] = (det(\sigma_i(x_j)))^2$$

Logo

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

■

A expressão para a densidade de centro do reticulado $\sigma_K(\mathfrak{a})$, é dada por

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

■

Podemos medir distâncias em $\sigma_K(K) \subseteq \mathbb{R}^n$ da seguinte forma:

**Proposição 3.2.1** ([*11*], pag. 225) *Sejam* $K$ *um corpo de números e* $x \in K$. *Então*

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

*onde*

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

**Demonstração:**

No caso em que $r_2 = 0$, isto é, $K$ é totalmente real, para $x \in K$ e $\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_n(x))$, segue que :

$$|\sigma_K(x)|^2 = {\sigma_1}^2(x) + \ldots + {\sigma_n}^2(x) = \sigma_1(x^2) + \ldots + \sigma_n(x^2) = \sigma_1(x\overline{x}) + \ldots + \sigma_n(x\overline{x}) = Tr(x\overline{x})$$

Agora, suponhamos $r_1 = 0$, ou seja, $K$ totalmente imaginário. Então para $x \in K$, $n = 2r_2$ e $\sigma_K(x) = (Re\sigma_1(x), Im\sigma_1(x), \ldots, Re\sigma_{r_2}(x), Im\sigma_{r_2}(x))$, temos:

$$\begin{aligned} |\ \sigma_K(x)\ |^2 &= \sigma_1(x)\overline{\sigma_1(x)} + \ldots + \sigma_{\frac{n}{2}}(x)\overline{\sigma_{\frac{n}{2}}(x)} = \sigma_1(x)\overline{\sigma_1(x)} + \ldots + \sigma_{\frac{n}{2}}(x)\sigma_{\frac{n}{2}}(\overline{x}) = \\ &= \sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x}) \end{aligned}$$

Sendo

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

e

$$\overline{\sigma}_i(x\overline{x}) = \sigma_i(x\overline{x}), \quad \forall i = 1, \ldots, \frac{n}{2},$$

segue que

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = 2\left(\sigma_1(x\overline{x}) + \ldots + \sigma_{\frac{n}{2}}(x\overline{x})\right).$$

Portanto

$$|\sigma_K(x)|^2 = \frac{1}{2}.Tr_{K/\mathbb{Q}}(x\overline{x}).$$

■

A seguir apresentamos uma expressão para a função traço no corpo $\mathbb{Q}(\zeta_n)$, para $n$ qualquer, o qual é uma forma quadrática, e sua minimização, embora é o trabalho mais difícil, constitui um de nossos objetivos. Esta expressão será utilizada no momento em que calcularmos o parâmetro $t$ na fórmula da densidade de centro, como veremos na próxima seção.

**Teorema 3.2.3** ([*14*], pag. 60) *Dados*

$$n = \prod_{i=1}^{s} {p_i}^{a_i},\ P = \prod_{i=1}^{s} p_i, K = \mathbb{Q}(\zeta_n), \mathcal{O}_K = \mathbb{Z}[\zeta_n]\ e\ x = \sum_{j=0}^{\phi(n)-1} b_j {\zeta_n}^j,$$

*temos que:*

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{2n}{P}\left[\frac{\phi(P)}{2}\sum_{j=0}^{\phi(n)-1} b_j^2 + \mu(P)\sum_{i=1}^{\phi(P)-1} A_{\frac{n}{P}i}\phi((i,P))\mu((i,P))\right],$$

*onde* $\phi$ *é a função de Euler,* $\mu$ *é a função de Möbius e* $A_j = b_0b_j + b_1b_{j+1} + \ldots + b_{m-1-j}b_{m-1}, j = 1, \ldots, m-1$ ■

## 3.3 Os Reticulados Algébricos

Nesta seção, estudaremos a densidade de centro dos reticulados da forma $\sigma_K(I)$ onde $I$ satisfaz a seguinte propriedade:

**Propriedade 3.3.1** *$I$ é um ideal ordinário de $\mathcal{O}_K$, $I \neq 0$ e*

$$\sigma(I) = I,\ \forall\sigma \in G = Gal(K/\mathbb{Q}),\ \textit{ou seja},\ \sigma(x) \in I,\ \forall x \in I.$$

Uma consequência da propriedade acima é o seguinte

**Lema 3.3.1** *Sejam $I$ um ideal satisfazendo a Propriedade 3.3.1 e $x \in I$, então:*

$$Tr_{K/\mathbb{Q}}(x) \equiv 0\ (mod\ r),$$

*onde $r$é um gerador de $I \cap \mathbb{Z}$.*

**Demonstração:**

Seja $I \subset \mathcal{O}_K$ um ideal satisfazendo a Propriedade 3.3.1, então $\sigma(x) \in I, \quad \forall\ x \in I$. Assim,

$$Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n}\sigma_i(x) \in I, \quad \forall\ x \in I.$$

Logo $Tr_{K/\mathbb{Q}}(x) \equiv 0\ (mod \quad I)$. Por outro lado, $\quad Tr_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, deste modo

$$Tr_{K/\mathbb{Q}}(x) \in I \cap \mathbb{Z} = r\mathbb{Z}.$$

Portanto, $\quad Tr_{K/\mathbb{Q}}(x) \equiv 0\ (mod \quad r)$ onde $r$ é um gerador de $I \cap \mathbb{Z}$. ■

Notemos que se $I \neq \{0\}$, então $I \cap \mathbb{Z} \neq \{0\}$ e para $x \in I$ temos $N(x) \in I$.

**Exemplo 3.3.1** *Sejam $K/\mathbb{Q}$ uma extensão galoisiana com $G = Gal(K/\mathbb{Q})$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de $K$. Se $p$ é um número primo de $\mathbb{Z}$ tal que $p\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_s\overline{\mathfrak{p}}_1 \dots \overline{\mathfrak{p}}_s)^e$, tomando $I = \mathfrak{p}_1 \dots \mathfrak{p}_s$ então $\overline{I} = \overline{\mathfrak{p}}_1 \dots \overline{\mathfrak{p}}_s$ e o ideal $I\overline{I}$ tem a Propriedade 3.3.1, consequentemente*

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \in I\overline{I} \cap \mathbb{Z} = p\mathbb{Z}.$$

Vimos que a expressão para a densidade de centro dos reticulados $\sigma_K(I)$ é dada por

$$\delta(\sigma_K(I)) = \frac{2^{r_2}\rho^n}{|D_K|^{\frac{1}{2}}N(I)}. \tag{3.1}$$

Sabemos que $\rho = \frac{1}{2}min\{|\sigma_K(x)|\,;\ 0 \neq x \in I\}$ e da Proposição 3.2.1 segue que

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

Logo, tomando

$$t = min\{Tr_{K/\mathbb{Q}}(x\overline{x});\ 0 \neq x \in I,\} \tag{3.2}$$

temos

$$\rho^n = \frac{c_K^{\frac{n}{2}}}{2^n}t^{\frac{n}{2}}.$$

Substituindo a expressão encontrada para $\rho^n$ em (3.1), obtemos

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

Notemos que: $2^{r_2}c_K^{\frac{n}{2}} = 1$. Deste modo,

$$\delta(\sigma_K(I)) = \frac{1}{|D_K|^{\frac{1}{2}}}.\frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{N(I)} \tag{3.3}$$

Como vimos, um dos parâmetros que envolve o cálculo da densidade de centro de um reticulado $\sigma_K(I)$ é o parâmetro $t$, que consiste no menor valor não nulo que a forma quadrática assume. Diante da dificuldade em obtermos $t$, optamos por restringir os nossos estudos aos subcorpos de $\mathbb{Q}(\zeta_{pq})$ onde $p$ e $q$ são primos distintos.

## 3.4 Subcorpos de $\mathbb{Q}(\zeta_{pq})$

Nesta seção faremos uso de alguns resultados da Teoria de Galois, deste modo supomos que o leitor tenha um conhecimento prévio deste assunto, o qual pode ser encontrado nas referências ([4] e ([5]).

O resultado a seguir é muito importante para a construção dos nossos exemplos.

**Teorema 3.4.1** ([6], pag. 263) *Sejam $L$ uma extensão galoisiana de $K$ e $M$ uma extensão de $K$ em $\mathbb{C}$. Então $LM$ é galoisiana sobre $M$ e $H = Gal(LM/M)$ é imerso no $G = Gal(L/K)$ pelos automorfismos de $G$ restritos a $L$. Além disso, a imersão é um isomorfismo se, e somente se, $L \cap M = K$.*

**Demonstração:**

Seja $L = K[\alpha]$. Então $LM = M[\alpha]$ o qual é galoisiano sobre $M$, pois os conjugados de $\alpha$ sobre $M$ estão entre os conjugados de $\alpha$ sobre $K$, os quais estão todos em $L$.

Existe um homomorfismo $\varphi$ de $H$ em $G$, obtido pelos automorfismos $\sigma$ de $G$ restritos a $L$, e o núcleo é facilmente visto por ser trivial. Se $\sigma$ fixa $M$ e $L$ ponto-a-ponto, então ele fixa $LM$ ponto-a-ponto.

Finalmente consideremos $H^{'}$ a imagem de $H$ em $G$, $H^{'}$ fixa o corpo $L \cap M = K$, pois o corpo fixado por $H$ é $M$ e pelo Teorema da Correspondêcia de Galois $H^{'} = Gal(L/M \cap L)$. Então $H^{'} = Gal(L/K)$ se, e somente se, $L \cap M = K$. ∎

A seguir, mostraremos alguns resultados que possibilitarão uma melhor caracterização dos nossos ideais.

**Teorema 3.4.2** ([2], pag. 70) *Sejam $L = \mathbb{Q}(\zeta_{pq})$, $K$ um subcorpo de $L$, $\mathfrak{q}$ e $\mathfrak{q}^{'}$ ideais primos de $\mathcal{O}_K$ e $\mathcal{O}_L$, respectivamente, ambos acima de $q\mathbb{Z}$, $D_K(q)$ e $D_L(q)$ os respectivos grupos de decomposição de $\mathfrak{q}$ e $\mathfrak{q}^{'}$ e $\overline{\sigma}$ a conjugação complexa. Então,*

$$\overline{\sigma} \in D_L(q) \Longleftrightarrow \overline{\sigma} \in D_K(q).$$

**Demonstração:**

Seja $\sigma_i \in D_K(q)$ definido por $\sigma_i(\zeta_p) = \zeta_p^i$.

Para cada $\sigma_i \in D_K(q)$ existem $q-1$ extensões $\sigma_{i,j}$ de $D_L(q)$. Cada $\sigma_{i,j}$ é definido por seu valor em $\zeta_{pq}$. Sejam $u$ e $v$ tais que $1 = pu + qv$. Deste modo, segue que

$$\sigma_{i,j}(\zeta_{pq}) = \sigma_{i,j}(\zeta_{pq}^{pu+qv}) = \zeta_{pq}^{puj+qvi}.$$

Assim $\overline{\sigma} \in D_L(q)$ se, e somente se, existem $i, j$ tais que

$$puj + qvi \equiv \ -1 \ (mod\ pq),$$

que equivale a

$$\begin{cases} puj + qvi \equiv \ -1 \ (mod\ p); \\ \qquad\qquad \text{e} \\ puj + qvi \equiv \ -1 \ (mod\ q). \end{cases}$$

A segunda condição vale sempre, já que $j$ pode assumir qualquer valor não nulo módulo $q$. Quanto à primeira, esta equivale a $\overline{\sigma} \in D_K(q)$, o que conclui a prova. ∎

**Corolário 3.4.1** ([2], pag. 71) *Sejam $L = \mathbb{Q}(\zeta_{pq})$, $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$ acima de $q\mathbb{Z}$, $D_L(q)$ o grupo de decomposição de $\mathfrak{q}$, $\overline{\sigma}$ a conjugação complexa e $o_p(q)$ a ordem de $q$ módulo $p$. Então*

$$\overline{\sigma} \in D_L(q) \Longleftrightarrow o_p(q) \ \equiv \ 0 \ (mod\ 2).$$

∎

Quando $p$ e $q$ satisfazem às condições $o_q(p) \equiv o_p(q) \equiv 1 \ (mod\ 2)$, isto é, $\overline{\sigma} \notin D_L(q)$ *e* $\overline{\sigma} \notin D_L(p)$ então existem em $\mathbb{Z}[\zeta_{pq}]$ as decomposições em ideais primos

$$p\mathcal{O}_L = (p_1 p_2 \dots p_r \overline{p_1 p_2} \dots \overline{p_r})^{p-1} \quad \text{e} \quad q\mathcal{O}_L = (q_1 q_2 \dots q_s \overline{q_1 q_2} \dots \overline{q_s})^{q-1},$$

onde $s = \frac{q-1}{2(o_q(p))}$ e $r = \frac{p-1}{2(o_q(p))}$.

Temos particular interesse no ideal

$$I = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$$

Sejam $L = \mathbb{Q}(\zeta_{pq})$ com $p,\ q$ primos ímpares distintos onde $o_q(p) \equiv o_p(q) \equiv 1 \ (mod\ 2)$, $K_p \subseteq \mathbb{Q}(\zeta_q)$, $K_q \subseteq \mathbb{Q}(\zeta_p)$, com $l_1 = [\mathbb{Q}(\zeta_p) : K_q]$, $l_2 = [\mathbb{Q}(\zeta_q) : K_p]$. Visto que $[K_q : \mathbb{Q}] = 2r$, $[K_p : \mathbb{Q}] = 2s$ e $K_p \cap K_q = \mathbb{Q}$ então $[K : \mathbb{Q}] = 4rs$.

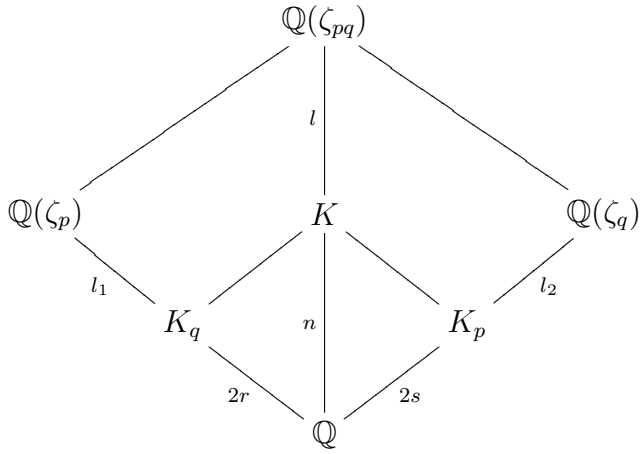



Figura 2: Diagrama dos subcorpos de $\mathbb{Q}(\zeta_{pq})$

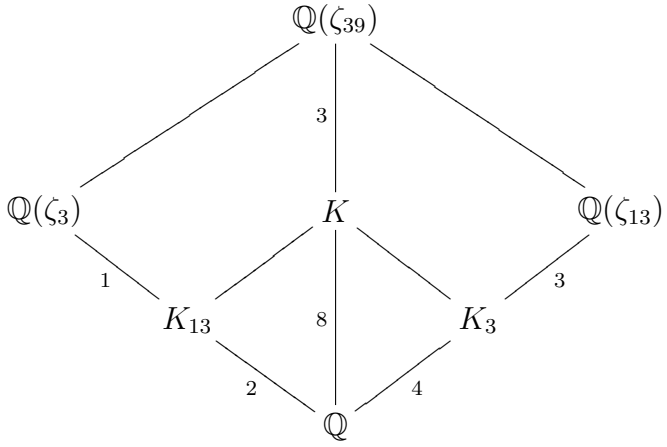
Devido ao fato de $o_q(p) \equiv o_p(q) \equiv 1 \ (mod\ 2)$, temos pelo Corolário 3.4.1 que a conjugação complexa $\overline{\sigma}$ não está contido no grupo de decomposição $D_L(p)$ e nem em $D_L(q)$. Assim, o ideal primo $p\mathbb{Z}$ se decompõe em $\mathcal{O}_{K_p}$ da forma $p\mathcal{O}_{K_p} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_s\overline{\mathfrak{p}_1\mathfrak{p}_2} \dots \overline{\mathfrak{p}_s}$, analogamente, $q\mathcal{O}_{K_q} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_r\overline{\mathfrak{q}_1\mathfrak{q}_2} \dots \overline{\mathfrak{q}_r}$. Agora, cada ideal $\mathfrak{p}_i$ e $\mathfrak{q}_j$, $i = 1, \dots, s$, $j = 1, \dots, r$, se decompõe em $\mathcal{O}_K$ da forma $\mathfrak{p}_i\mathcal{O}_K = P_i^{2r}$ e $\mathfrak{q}_j\mathcal{O}_K = Q_j^{2s}$;

Tomemos $I = P_1P_2 \dots P_sQ_1Q_2 \dots Q_r$. Como $I\overline{I}$ tem a Propriedade 3.3.1, temos que: se $x \in I$ então $Tr_{K/\mathbb{Q}}(x\overline{x}) \in I\overline{I} \cap \mathbb{Z} = pq\mathbb{Z}$, ou seja, $t = pq\tilde{h},\ \tilde{h} \in \mathbb{N}$. Sabemos, pelo Teorema 3.2.3, que $Tr_{L/\mathbb{Q}}(x\overline{x})$ é par. Sendo $Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{l}Tr_{L/\mathbb{Q}}(x\overline{x})$, e como $l$ é ímpar, então $Tr_{K/\mathbb{Q}}(x\overline{x})$ também é par, logo, $t = 2hpq,\ h \in \mathbb{N}$.

Do Teorema 2.3.4, temos que $D_{K_p} = q^{2s-1}$ e $D_{K_q} = p^{2r-1}$, como $K_p$ e $K_q$ são linearmente disjuntos (isto é, $K_p \cap K_q = \mathbb{Q}$ e possuem discriminantes relativamente primos) temos $D_K = q^{(2s-1)2r}p^{(2r-1)2s}$, ($ver$[16], pag. 11). Como a norma é multiplicativa temos que $N(I) = p^sq^r$. Para os valores de $t$, $N(I)$ $e$ $D_K$ acima obtidos, a expressão (3.3) da densidade de centro será dada por:

$$\delta(\sigma_K(I)) = \left(\frac{2h}{4}\right)^{\frac{[K:\mathbb{Q}]}{2}} = \left(\frac{h}{2}\right)^{2rs}$$

**Exemplo 3.4.1** *Sejam* $L = \mathbb{Q}(\zeta_{39})$, $K_{13} = \mathbb{Q}(\zeta_3)$, $K_3 \subset \mathbb{Q}(\zeta_{13})$ *tais que* $[K_3 : \mathbb{Q}] = 4$, $[K_{13} : \mathbb{Q}] = 2$ *e* $K = K_3K_{13}$, *logo* $[K : \mathbb{Q}] = 8$.




*Assim temos,* $3\mathcal{O}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_1\mathfrak{p}_2}$ *e* $13\mathcal{O}_{K_{13}} = \mathfrak{q}_1\overline{\mathfrak{q}_1}$, *pois* $\overline{\sigma} \notin D_L(3)$ *e* $\overline{\sigma} \notin D_L(13)$, *já que* $o_{13}(3) \equiv o_3(13) \equiv 1(mod 2)$. *Logo a decomposição de cada* $\mathfrak{p}_i$ *e* $\mathfrak{q}_j$ *em* $\mathcal{O}_K$ *é da forma* $\mathfrak{p}_i\mathcal{O}_K = P_i^2$, *ou seja,* $3\mathcal{O}_K = (P_1P_2\overline{P_1P_2})^2$. *Da mesma forma* $13\mathcal{O}_K = (Q_1\overline{Q_1})^4$.

*Tomemos o ideal* $I = P_1P_2Q_1 \subset \mathcal{O}_K$. *Sendo* $I\overline{I}$ *um ideal que satisfaz a Propriedade 3.3.1, temos que para* $x \in I$, $t = 39.h$; $h \in \mathbb{N}$. *Como a forma quadrática obtida para o* $Tr_{K/\mathbb{Q}}$ *no Teorema 3.2.3 é par, segue que* $t \geq 2.39$. *Tomando* $t = 2.39$ *segue que* $h = 1$, *assim*

$$\delta(\sigma_K(I)) = \left(\frac{1}{2}\right)^4 = 0,0625.$$

*Esta é o recorde para a dimensão 8.*

Podemos considerar outros corpos que satisfazem as condições acima citadas e obter reticulados com a mesma densidade de centro de $E_8$ (reticulado com maior densidade de centro na dimensão 8). Por exemplo:

Sejam $p = 7$ e $q = 29$, temos que $o_q(p) \equiv o_p(q) \equiv 1$ $(mod\ 2)$. Basta tomar $K_p$ o subcorpo de $\mathbb{Q}(\zeta_{29})$ de grau 4 e $K_q$ a extensão quadrática contida em $\mathbb{Q}(\zeta_7)$.

Sejam $p = 5$ e $q = 11$, temos que $o_q(p) \equiv o_p(q) \equiv 1$ $(mod\ 2)$. Basta tomar $K_p$ o subcorpo de $\mathbb{Q}(\zeta_{11})$ de grau 2 e $K_q$ o próprio $\mathbb{Q}(\zeta_5)$.

Sejam $p = 5$ e $q = 31$, temos que $o_q(p) \equiv o_p(q) \equiv 1$ $(mod\ 2)$. Basta tomar $K_p$ o subcorpo de $\mathbb{Q}(\zeta_{31})$ de grau 2 e $K_q$ o próprio $\mathbb{Q}(\zeta_5)$.

Em todos os casos, o corpo $K = K_pK_q$ tem grau 8. Resolvendo de modo análogo ao exemplo anterior, tomemos $h = 1$ e obtemos a densidade de $E_8$.

# Referências Bibliográficas


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

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

[3] Garcia, A.; Lequain, Y.; *Elementos de álgebra*. Projeto Euclides, 2002.

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

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

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

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

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

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

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

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

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

[13] Stewart, I.; *Galois Theory, Second edition*. Chapman & Hall, 1989.

[14] Rodrigues, T.M.; *Cúbicas Galoisianas*.Dissertação de Mestrado,IBILCE-UNESP, 2003.

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

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