UNIVERSIDADE ESTADUAL PAULISTA – UNESP
Instituto de Biociências, Letras e Ciências Exatas – São José do Rio Preto

João Pedro Galdino Pillar

CORPOS ABELIANOS E APLICAÇÕES

São José do Rio Preto
2025

JOÃO PEDRO GALDINO PILLAR

CORPOS ABELIANOS E APLICAÇÕES

Dissertação apresentada à Universidade Estadual Paulista (UNESP), Instituto de Biociência, Letras e Ciências Exatas, São José do Rio Preto, para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra.

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

Financiadora: Capes.

São José do Rio Preto

2025

P641c

Pillar, João Pedro Galdino
Corpos abelianos e aplicações / João Pedro Galdino Pillar. -- São José do Rio Preto, 2025
82 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Trajano Pires da Nóbrega Neto

1. Matemática. 2. Teoria Algébrica dos Números. 3. Corpos Abelianos. 4. Reticulados Algébricos. 5. Empacotamento Esférico. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

JOÃO PEDRO GALDINO PILLAR

CORPOS ABELIANOS E APLICAÇÕES

Dissertação apresentada à Universidade Estadual Paulista (UNESP), Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, para obtenção do título de Metre em Matemática.

Área de Concentração: Álgebra.

Financiadora: Capes.

Data da defesa: 11/04/2025.

Banca Examinadora:

_____

Prof. Dr. Trajano Pires da Nóbrega Neto (Orientador)
UNESP – Câmpus de São José do Rio Preto

_____

Prof. Dr. Antonio Aparecido de Andrade
UNESP – Câmpus de São José do Rio Preto

_____

Prof. Dr. Agnaldo José Ferrari
UNESP – Câmpus de Bauru

Aos meus pais e aos meus irmãos
dedico.

AGRADECIMENTOS

Primeiramente, agradeço à minha família, que apesar da distância sempre me deu força para seguir em frente. Ao meu pai, Nilton, que admiro profundamente por sua inteligência, dedicação, simplicidade e afeto. À minha mãe, Fernanda, que admiro pela sua amorosidade e tenacidade. Obrigado por, mesmo longe, estar ao meu lado nos momentos em que mais precisei. Aos meus irmãos, André Luiz e Fernando José, pelo apoio constante.

Ao meu orientador, Professor Trajano, pela sabedoria com que me guiou, pelos momentos de estudo e pelas conversas que tanto enriqueceram minha trajetória. Ele é, para mim, uma grande inspiração.

Aos membros titulares e suplentes da banca, Trajano, Agnaldo, Antonio, Grasiele e Robson pelo tempo dedicado e pelas valiosas contribuições.

Aos meus amigos Geo Maycow Galvan e Gustavo Reolon, que estiveram comigo desde o ensino médio, agradeço pela nossa sincera e duradoura amizade e por tudo que já fizemos juntos. Obrigado por estarem sempre comigo.

Aos meus amigos que fiz durante a graduação e que acompanharam minha trajetória até aqui: Débora Valadão, Eduardo Alves Ferreira, Géssica Eduarda Padilha, Luíza Perusso, Leonardo Zanardi, Luis Fernando Salla e Pedro Iseppi. Obrigado por todos os momentos que vivemos juntos.

Aos demais amigos que conquistei por meio da UTFPR, dentre estes, Alice Zucho, Everson Castoldi, Gileade Detogni e, principalmente, ao meu grande amigo Mateus Eduardo Salomão. Sem você, certamente eu não chegaria até aqui. Você foi primordial.

Aos professores do DAMAT da UTFPR: Adilson, André, Carlos, Cleonis, Divanete, Edinéia, Gilberto, Gilson, Ivan, Janecler, João, Luzia, Mariele, Mateus, Michael, Moises, Rodrigo e Waldir, pelo conhecimento compartilhado e pelo apoio ao longo da graduação.

Aos Programa de Pós-Graduação em Matemática da Unesp/São José do Rio Preto pela oportunidade, bem como aos professores do dos quais tive o prazer de ser aluno: Ali, Andréa, Danilo, Luci, Michele, Toninho e Vanderlei, pela dedicação e pelo ensino que tanto contribuíram para minha formação.

Aos amigos Gabriel Modolo e Lucas Pedro Martins, que ingressaram comigo no mestrado e cur-

saram muitas disciplinas ao meu lado, muito obrigado pelas diversas horas de estudo e discussões.

Aos meus grandes amigos Guilherme Zahra Cundari e Murillo Lozano Rubinho de Araujo, que foram os melhores companheiros que eu poderia ter nesses dois anos, vocês me ensinaram um novo significado para a palavra casa. Agradeço por todo o apoio e amizade.

Ao Diego Miloch, por todos os momentos de descontração, conversas, risadas e, principalmente, por ter me escutado falar de Teoria Algébrica dos Números em diversos momentos aleatórios do dia.

Aos demais amigos que fiz na matemática durante a pós-graduação: Carlos Augusto Seller, Eduardo Caramori, Eduardo Martins, Eduardo Scabora, Gabriela Assis, Isabela Pereira, João Brambila, José Luiz Tofanin Neto, Juliana Marques de Souza, Larissa Soilo, Leonardo Soria, Linara Facini, Livea Esteves, Maria Clara Taddone, Maria Fernanda Bonini, Milena Zacheo, Murilo Penteado, Rafael Araujo, Renan Antunes, Sérgio Rodrigues Verde Junior, Thiago Rodrigues e Vitor Gusson, pela companhia e pelos momentos de aprendizado e descontração. Ao restante dos amigos que fiz em São José do Rio Preto, que se fizeram presentes na minha vida durante esse período, seja em um jogo de vôlei, uma partida de xadrez, um café ou uma boa conversa.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Nada lhe pertence mais do que os seus sonhos.

Friedrich Nietzsche

RESUMO

Neste trabalho, serão estudados os Corpos Abelianos, com ênfase nos Corpos Ciclotômicos, visando a aplicação desses corpos no estudo de empacotamentos reticulados. Para tanto, serão apresentados conceitos fundamentais da Teoria Algébrica dos Números, tais como o anel dos inteiros algébricos, o traço e a norma relativos, além de explorar a Teoria de Galois e exibir o discriminante dos corpos ciclotômicos. Nesse contexto, esse estudo será utilizado para construção de reticulados algébricos do espaço euclidiano $\mathbb{R}^n$, onde $n = p - 1$ com p primo e na obtenção de resultados sobre a densidade de centro destes. A conexão entre as propriedades algébricas dos corpos ciclotômicos e a geometria dos empacotamentos esféricos será explorada, evidenciando a relevância desses corpos tanto no contexto teórico quanto em aplicações práticas.

Palavras-chave: corpos abelianos; anel dos inteiros algébricos; reticulados algébricos; empacotamento esférico; densidade de centro.

ABSTRACT

In this work, Abelian fields will be studied, with a particular focus on Cyclotomic Fields, aiming to apply these fields to the study of lattice packings. To this end, fundamental concepts from Algebraic Number Theory will be introduced, such as the ring of algebraic integers, the relative trace and norm, as well as an exploration of Galois Theory and the computation of the discriminant of cyclotomic fields. The study will then be applied to the construction of algebraic lattices in Euclidean space $\mathbb{R}^n$*, where* $n = p - 1$ *and* p *is a prime number, and to obtaining results on the center density of these lattices. The connection between the algebraic properties of cyclotomic fields and the geometry of sphere packings will be explored, highlighting the relevance of these fields in both theoretical contexts and practical applications.*

Keywords: abelian fields; ring of algebraic integers; algebraic lattices; sphere packing; center density.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}$	Conjunto dos Números Complexos
$\mathbb{L}$	Subcorpo dos Complexos
$\mathbb{Q}(\zeta_n)$	$n-$ésimo Corpo Ciclotômico
$\mathbb{Q}(\theta)$	Corpo de números com o elemento primitivo θ
$\mathcal{O}_B$	Anel de inteiros de A em B
$\mathcal{O}_{\mathbb{K}}$	Anel dos Inteiros Algébricos do Corpo $\mathbb{K}$
I	Ideal
$N(I)$	Norma do ideal I
$\langle a \rangle$	Ideal gerado por a
$\alpha\mathcal{O}_{\mathbb{K}}$	Ideal de $\mathcal{O}_{\mathbb{K}}$ gerado por α
$A[x]$	Conjunto dos polinômios na variável x e coeficientes em A
$p(x)$	Polinômio na variável x
$\mathrm{gr}(p(x))$	Grau do polinômio $p(x)$
$m_\alpha(x)$	Polinômio minimal de α
$p_\alpha(x)$	Polinômio característico de α
$\mathrm{gr}_{\mathbb{K}}(\alpha)$	Grau de α sobre $\mathbb{K}$

$D(\alpha_1, \ldots, \alpha_n)$	Discriminante do conjunto $\{\alpha_1, \ldots, \alpha_n\}$
$D(\alpha)$	Discriminante do elemento α
$D(f(x))$	Discriminante do polinômio f
$D(\mathbb{K})$	Discriminante do corpo $\mathbb{K}$
$v_{\mathfrak{p}}(\alpha)$	Valorização de α no ideal primo $\mathfrak{p}$
$v_p(a)$	Valorização do inteiro a no número primo p
$\sigma_{\mathbb{K}}$	Homomorfismo canônico de $\mathbb{K}$
$\det(M)$	Determinante da matriz M
$m \mid n$	m divide n
$m \nmid n$	m não divide n
$a \equiv b \ (mod\ m)$	a e b são congruentes módulo m
$a \not\equiv b \ (mod\ m)$	a e b não são congruentes módulo m

SUMÁRIO

1 INTRODUÇÃO

Os corpos são estruturas algébricas fundamentais na matemática e, entre eles, os corpos de números se destacam como extensões finitas dos números racionais. Esses corpos desempenham um papel essencial na Teoria dos Números, sendo um dos principais objetos de estudo nessa área. Um exemplo notável são os corpos ciclotômicos, que possuem a forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Além de serem corpos abelianos, os corpos ciclotômicos têm um papel central na Teoria dos Números, uma vez que todos os corpos abelianos podem ser considerados subcorpos de um corpo ciclotômico. Por essa razão, este trabalho dedica um capítulo específico aos corpos abelianos, com uma Seção dedicada aos corpos ciclotômicos.

O problema do empacotamento esférico visa cobrir o maior percentual do $\mathbb{R}^n$, com esferas $n-$dimensionais de mesmo raio, sem interseção a menos de um ponto, nesse contexto, uma forma interessante de construir um empacotamento esférico é por meio de reticulados, nesse caso, através da seguinte expressão podemos calcular a densidade de centro de um reticulado Λ:

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

onde ρ é o raio de empacotamento e $v(\Lambda)$ o volume do reticulado. Essa expressão é de extrema importância, visto que a partir dela, apenas multiplicando pelo volume da esfera $n-$dimensional de raio 1, conseguimos obter a densidade de empacotamento deste reticulado que indica a porção que o empacotamento cobre do $\mathbb{R}^n$. Vejamos que, para efetuar o cálculo precisamos identificar o raio ρ da esfera, que nem sempre é uma tarefa fácil e está ligada diretamente ao vetor de menor tamanho pertencente ao reticulado.

No prefácio da referência [1], mostram-se os recordes de densidade de centro para determinadas dimensões, sendo este por empacotamentos reticulados ou não, nosso objetivo é aplicar a Teoria dos Números ao estudo dos reticulados, com o intuito de investigar alguns empacotamentos reticulados fazendo um comparativo com o recorde de densidade para determinadas dimensões que será exibido de acordo com a referência citada, no último capítulo. Para organizar a abordagem, o trabalho é dividido em cinco capítulos.

No Capítulo 2, apresentamos uma série de conceitos e resultados fundamentais da Teoria dos Números, como extensões de corpos, corpos de números e o anel dos inteiros algébricos. O objetivo deste capítulo é relembrar ou introduzir ao leitor esses tópicos,

sem entrar em demonstrações, as quais estão disponíveis nas referências bibliográficas indicadas em cada resultado.

O Capítulo 3 aborda os corpos abelianos, começando pelos corpos quadráticos, que são corpos abelianos de grau 2. Em seguida, exploramos conceitos fundamentais sobre os corpos ciclotômicos, destacando sua relevância para o estudo dos corpos abelianos, além de discutirmos os corpos abelianos com condutor primo.

No Capítulo 4, apresentaremos o problema do empacotamento esférico, e falaremos dos reticulados, explorando como os conceitos discutidos nos capítulos anteriores podem ser aplicados a este estudo. Mostraremos, por exemplo, como gerar um reticulado a partir do anel dos inteiros algébricos de um corpo de números, utilizando o homomorfismo canônico. Além disso, discutiremos os conceitos essenciais que permitem calcular as densidades de centro e de empacotamento de um empacotamento reticulado, dando enfoque a alguns reticulados que surgiram a partir do ideal principal do anel dos inteiros algébricos de um $p-$ésimo corpo ciclotômico gerado por $(1-\zeta_p)^m$, com m inteiro positivo, os quais são conhecidos por "Família de Craig", sendo estes de devida importância já que são os recordes nas dimensões, 150, 180 e 192, por exemplo.

Finalmente, no Capítulo 5, faremos as considerações finais sobre o trabalho, onde comentaremos sobre os principais temas abordados e suas aplicações no estudo dos reticulados algébricos, como por exemplo no cálculo da densidade de centro. Por fim, daremos algumas informações sobre a Família de Craig.

2 PRELIMINARES

Neste capítulo trataremos dos conceitos preliminares para o estudo da Teoria Algébrica dos Números, as principais referências utilizadas foram [2], [3], [4] e [5] tendo em vista que esta Seção tem por objetivo apresentar ou relembrar conceitos, que serão utilizados posteriormente, optaremos por apenas exibir os resultados, sem fazer as demonstrações contudo, em cada enunciado deixaremos explícito onde estas podem ser encontradas. A Seção 2.1 trata de extensões algébricas, polinômio minimal e os conjugados de um elemento algébrico sobre um corpo, e extensões múltiplas. Em seguida, na Seção 2.2 apresentaremos o conceito de corpo de números, neste veremos os $\mathbb{K}-$conjugados e o polinômio característico de um elemento. Dando continuidade, na Seção 2.3, veremos conceitos básicos da Teoria de Galois, como o grupo de Galois de uma extensão, extensões galoisianas, corpo fixo por um subgrupo e o Teorema Fundamental da Teoria de Galois, além disso, definimos o traço e a norma relativos de um elemento, exibiremos algumas propriedades destes, definiremos o discriminante e apresentaremos um resultado que envolve esse conceito. Seguindo para a Seção 2.4, exploraremos os $A-$módulos, desde a definição e exemplos até os homomorfismos de módulos. Em seguida, na Seção 2.5, introduziremos o conceito de elemento inteiro sobre um anel, inteiro algébrico, anel dos inteiros algébricos de um corpo de números, relações destes com módulos, anel integralmente fechado e alguns resultados básicos sobre estes tópicos. Prosseguindo, na Seção 2.6 trabalharemos com a fatoração de ideais, definiremos domínio Noetheriano, domínio de Dedekind, ideal fracionário, número de decomposição, índices de ramificação e alguns resultados importantes. Por fim, na Seção 2.7 trataremos sobre valorização $p-$ádica, com definição e exemplos. Veremos esse conceito no contexto de ideais primos, que utilizaremos posteriormente para demonstrar um teorema que envolve o anel dos inteiros algébricos.

2.1 EXTENSÕES ALGÉBRICAS

Neste capítulo, a não ser que seja mencionado o contrário, consideraremos $\mathbb{L}$ um subcorpo de $\mathbb{C}$. Seja $\mathbb{K}$ um subcorpo de $\mathbb{L}$, neste caso, diremos que $\mathbb{L}$ é uma **extensão** de $\mathbb{K}$ e denotaremos por $\mathbb{L}/\mathbb{K}$, sob estas condições $\mathbb{L}$ é um espaço vetorial sobre $\mathbb{K}$ e a dimensão deste é chamado **grau da extensão**, e denotaremos por $[\mathbb{L} : \mathbb{K}]$, em particular,

neste capítulo falaremos sobre extensões algébricas. Uma extensão $\mathbb{L}/\mathbb{K}$ é dita **finita** se, $\mathbb{L}$ é um espaço vetorial de dimensão finita sobre $\mathbb{K}$, caso contrário a extensão é dita **infinita**.

Um elemento de $\mathbb{L}$ é dito **algébrico** sobre $\mathbb{K}$ se for raiz de um polinômio não nulo com coeficientes em $\mathbb{K}$, caso contrário, diremos que este é **transcendente** sobre $\mathbb{K}$. Em particular, quando $\mathbb{K} = \mathbb{Q}$, diremos simplesmente que o elemento é algébrico/transcendente. Uma extensão de corpos $\mathbb{L}/\mathbb{K}$ é dita **algébrica** se todo elemento de $\mathbb{L}$ for algébrico sobre $\mathbb{K}$.

Um exemplo de extensão algébrica é a extensão $\mathbb{R}/\mathbb{C}$ que tem grau 2, um resultado mais geral é que toda extensão finita é algébrica, mas não vale a recíproca. Dado um elemento α algébrico, a seguir definiremos o polinômio minimal e os conjugados de α. Para isso, consideremos nesta seção $\mathbb{K} \subseteq \mathbb{L}$ subcorpos de $\mathbb{C}$.

Dado um elemento α de $\mathbb{L}$ algébrico sobre $\mathbb{K}$, o polinômio mônico $m_\alpha(x)$ de grau mínimo tal que $m_\alpha(\alpha) = 0$ é chamado **polinômio minimal** de α sobre $\mathbb{K}$. Além disso, diremos que o **grau de** α **sobre** $\mathbb{K}$ é o grau do polinômio minimal de α sobre $\mathbb{K}$. Denotamos por $\mathrm{gr}_{\mathbb{K}}(\alpha)$.

Exemplo 2.1. Considere $\mathbb{K} = \mathbb{Q}$, $\sqrt{3}$ é algébrico sobre $\mathbb{Q}$, e seu polinômio minimal é $x^2 - 3$, portanto, o grau de $\sqrt{3}$ sobre $\mathbb{Q}$ é 2. Por outro lado, se $\mathbb{K} = \mathbb{R}$, então o polinômio minimal de $\sqrt{3}$ é $x - \sqrt{3}$, logo, o grau de $\sqrt{3}$ sobre $\mathbb{R}$ é 1.

Proposição 2.2. *([2], p. 89) Considere a extensão $\mathbb{L}/\mathbb{K}$ e α um elemento de $\mathbb{L}$. Se α é algébrico sobre $\mathbb{K}$, então $m_\alpha(x)$ é irredutível em $\mathbb{K}[x]$.*

Um corpo $\mathbb{F}$ é dito **algebricamente fechado**, quando todo polinômio de uma variável de grau maior ou igual a 1, com coeficientes em $\mathbb{F}$, tem pelo menos uma raiz em $\mathbb{F}$. Por exemplo, $\mathbb{C}$ é um corpo algebricamente fechado, enquanto que $\mathbb{R}$ não o é, uma vez que o polinômio $x^2 + 1$ não tem raízes reais.

Seja $\mathbb{K}$ um corpo. Diremos $\mathbb{L}$ é o **fecho algébrico** de $\mathbb{K}$ se $\mathbb{L}$ é um corpo algebricamente fechado e $\mathbb{L}/\mathbb{K}$ é algébrica. Sendo assim, temos que, $\mathbb{C}$ é o fecho algébrico de $\mathbb{R}$. Diremos que $\mathbb{L}$ é uma **extensão simples** de $\mathbb{K}$, quando existe um elemento α de $\mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.

Exemplo 2.3. A extensão $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ é simples pois $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ pode ser escrita da forma $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Por outro lado, se considerando $\mathbb{F}$ o fecho algébrico de $\mathbb{Q}$, a extensão $\mathbb{F}/\mathbb{Q}$ não é simples (justificativa após a Proposição 2.4).

Proposição 2.4. *([6], p. 47) Seja α um número complexo, se α é algébrico sobre $\mathbb{K}$ então $gr_{\mathbb{K}}(\alpha) = [\mathbb{K}(\alpha) : \mathbb{K}]$. Se α não é algébrico sobre $\mathbb{K}$, a extensão $\mathbb{K}(\alpha)/\mathbb{K}$ é infinita.*

Agora, justificaremos o fato de que a extensão $\mathbb{F}/\mathbb{Q}$, mencionada no Exemplo 2.3, não é simples. Suponhamos por absurdo que $\mathbb{F} = \mathbb{Q}(\alpha)$. Como $\mathbb{F}/\mathbb{Q}$ é algébrica, em particular,

segue que α é algébrico sobre $\mathbb{Q}$. Pela Proposição 2.4, $[\mathbb{F} : \mathbb{Q}] = gr_{\mathbb{F}}(\alpha) < \infty$, o que é um absurdo, uma vez que $\mathbb{F}/\mathbb{Q}$ é infinita.

Seja α em $\mathbb{L}$ algébrico sobre $\mathbb{K}$. Os **conjugados** de α sobre $\mathbb{K}$ são as raízes de $m_\alpha(x)$ em $\mathbb{L}$. Podemos exemplificar que, os conjugados de $\sqrt{3}$ sobre $\mathbb{Q}$ são $\sqrt{3}$ e $-\sqrt{3}$.

Proposição 2.5. *([2], p. 100) Seja α um número complexo, se α é algébrico sobre $\mathbb{K}$ e $gr(m_\alpha(x)) = n$, então $\mathbb{K}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}; a_0, a_1, \ldots, a_{n-1} \in \mathbb{K}\}$.*

Sejam $\alpha_1, \alpha_2, \ldots, \alpha_k$ números complexos e algébricos sobre o corpo $\mathbb{K}$. O corpo $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_k)$ é chamado **extensão múltipla** de $\mathbb{K}$ e é obtido através de uma sucessão de k junções simples:

$$\begin{aligned} \mathbb{K}(\alpha_1, \alpha_2) &= \mathbb{K}(\alpha_1)(\alpha_2) \\ \mathbb{K}(\alpha_1, \alpha_2, \alpha_3) &= \mathbb{K}(\alpha_1, \alpha_2)(\alpha_3) \\ &\vdots \\ \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_k) &= \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})(\alpha_k) \end{aligned}$$

Proposição 2.6. *([2], p. 102) Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos e α, β em $\mathbb{L}$ algébricos sobre $\mathbb{K}$, então existe um elemento γ de $\mathbb{L}$ algébrico sobre $\mathbb{K}$ tal que $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$.*

Considerando ainda a extensão $\mathbb{L}/\mathbb{K}$, sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementos de $\mathbb{L}$ algébricos sobre $\mathbb{K}$, utilizando a Proposição 2.6 de forma sucessiva, concluímos que existe α em $\mathbb{L}$ algébrico sobre $\mathbb{K}$ tal que $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}(\alpha)$.

Proposição 2.7. *([2], p. 106) Seja α um número complexo e algébrico sobre o corpo $\mathbb{K}$, então todo elemento β de $\mathbb{K}(\alpha)$ é algébrico sobre $\mathbb{K}$ e o grau de β sobre $\mathbb{K}$ é menor ou igual ao grau de α sobre $\mathbb{K}$.*

2.2 CORPOS DE NÚMEROS

Nesta Seção, trabalharemos com casos específicos de extensões algébricas, as extensões finitas dos racionais, denominaremos por corpos de números. Neste contexto, vamos explorar sobre elemento primitivo de um corpo de números, as imersões nos complexos, os conjugados e alguns resultados relacionados aos conceitos mencionados.

Um subcorpo de $\mathbb{C}$ que é uma extensão finita dos racionais é chamado de **corpo de números**, isto é, um corpo $\mathbb{K}$ é um corpo de números se $\mathbb{K}/\mathbb{Q}$ é finita, além disso quando o grau da extensão $\mathbb{K}/\mathbb{Q}$ for n, diremos que $\mathbb{K}$ é um **corpo de números de grau** n.

Proposição 2.8. *([2], p. 109) Se $\mathbb{K}$ é um corpo de números, então existe um número algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$.*

Nas condições da Proposição 2.8, chamaremos θ de **elemento primitivo** do corpo $\mathbb{K}$. Vale ressaltar que o mesmo corpo de números tem infinitos elementos primitivos.

Teorema 2.9. *([2], p. 112) Se $\mathbb{K}$ é um corpo de números de grau n, então existem exatamente n monomorfismos $\sigma_k : \mathbb{K} \to \mathbb{C}, k = 1, \ldots, n$.*

Diremos que σ_k é um **monomorfismo real**, quando $\sigma_k(\mathbb{K}) \subset \mathbb{R}$, caso contrário, chamaremos σ_k de **monomorfismo imaginário**. Neste contexto um corpo de números $\mathbb{K}$ é dito **totalmente real** quando todos os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são reais. Analogamente, $\mathbb{K}$ é dito **totalmente imaginário** quando todos os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são imaginários.

Note que, não necessariamente um corpo de números é totalmente real ou totalmente imaginário, como é o caso de $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$, que tem 2 monomorfismos imaginários e um real. Mais geralmente, dado um corpo de números de grau n, a quantidade de monomorfismos imaginários é sempre par, uma vez que dado σ_k um monomorfismo imaginário, ao compormos a conjugação complexa com σ_k, obtemos outro monomorfismo imaginário. Sendo assim, $n = r + 2s$, onde r é o número de monomorfismos reais e $2s$ o número de monomorfismos imaginários.

Sejam $\mathbb{K}$ um corpo de números de grau n sobre $\mathbb{Q}$ e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Dado α em $\mathbb{K}$, os elementos $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ são chamados de $\mathbb{K}-$**conjugados de** α ou conjugados de α **relativos** à $\mathbb{Q}$. Nestas condições, o **polinômio característico** de α sobre $\mathbb{K}$ é definido como o polinômio:

$$p_\alpha(x) = \prod_{k=1}^{n} (x - \alpha_k).$$

Proposição 2.10. *([2], p. 118) Seja $\mathbb{K}$ um corpo de números de grau n. Se α é um elemento de $\mathbb{K}$, então $p_\alpha(x) \in \mathbb{Q}[x]$.*

Na Proposição 2.10, vimos que o polinômio característico de um elemento de um corpo de números $\mathbb{K}$ está em $\mathbb{Q}[x]$, então o próximo resultado nos permite expressar o polinômio característico deste elemento como o produto do seu polinômio minimal.

Proposição 2.11. *([2], p. 120) Seja $\mathbb{K}$ um corpo de números de grau n. Se α é um elemento de $\mathbb{K}$, então $p_\alpha(x) = (m_\alpha(x))^s$, onde $s = \frac{n}{gr(m_\alpha(x))}$ é um número inteiro positivo.*

2.3 TEORIA DE GALOIS

Nesta Seção, consideraremos sempre $\mathbb{K}$ e $\mathbb{L}$ corpos de números. Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos, o conjunto de todos os automorfismos de $\mathbb{L}$, denotado por $Aut(\mathbb{L})$ é um grupo com a operação de composição. Vamos iniciar, esta Seção enunciando conceitos básicos da teoria de Galois, como o grupo de Galois de uma extensão, extensões galoisianas e o

corpo fixo associado a um subconjunto de $Aut(\mathbb{L})$, com objetivo finalizá-lo enunciando o teorema fundamental da teoria de Galois.

Diremos que $\varphi : \mathbb{L} \to \mathbb{L}$, é um **$\mathbb{K}$-automorfismo de $\mathbb{L}$** se φ é um homomorfismo bijetor e $\varphi(\alpha) = \alpha,\ \forall\ \alpha \in \mathbb{K}$. Isto é, $\varphi_{|\mathbb{K}} = Id$.

Sendo assim, podemos afirmar que o conjunto $G(\mathbb{L} : \mathbb{K}) = \{\sigma : \mathbb{L} \to \mathbb{L};\ \sigma$ é um $\mathbb{K}$-automorfismo de $\mathbb{L}\} \subseteq Aut(\mathbb{L})$. A proposição a seguir nos garante algo a mais do que isso.

Proposição 2.12. *([6], p. 103) $G(\mathbb{L} : \mathbb{K})$ é um subgrupo de $Aut(\mathbb{L})$.*

Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos. Quando $\mathbb{L}/\mathbb{K}$ é uma extensão finita de corpos e $[\mathbb{L} : \mathbb{K}] = o(G(\mathbb{L} : \mathbb{K}))$, diremos que esta extensão é **de Galois** ou **galoisiana**. Além disso, chamaremos $G(\mathbb{L} : \mathbb{K})$ de **grupo de Galois** da extensão $\mathbb{L}$ sobre $\mathbb{K}$ e, quando $\mathbb{L}/\mathbb{K}$ é galoisiana, denotamos por $Gal(\mathbb{L} : \mathbb{K})$.

Exemplo 2.13. A extensão $\mathbb{Q}(i)/\mathbb{Q}$ é galoisiana, visto que é uma extensão de grau 2 e $G(\mathbb{Q}(i) : \mathbb{Q}) = \{\sigma_1, \sigma_2\}$ onde σ_1 é a identidade e σ_2 a conjugação complexa. Por outro lado, a extensão $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ não é galoisiana, já que é de grau 3 e $o(G(\mathbb{Q}(\sqrt[3]{3}) : 1)) = 1$.

Diremos que uma extensão de corpos é **abeliana** quando a extensão é galoisiana e o grupo de Galois é abeliano. Um exemplo de extensão abeliana é $\mathbb{C}/\mathbb{R}$. Em contrapartida, para uma extensão não ser abeliana, é suficiente que esta não seja galoisiana, mas esta não é uma condição necessária, visto que a extensão $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ é galoisiana, mas não é abeliana.

Teorema 2.14. *([6], p. 143.) Se $\mathbb{K}$ é um corpo de números de grau 2, então a extensão $\mathbb{K}/\mathbb{Q}$ é galoisiana.*

Uma consequência do Teorema 2.14 é que todo corpo de números de grau 2 é uma extensão abeliana. Uma vez que o Teorema garante que a extensão é galoisiana e, neste caso, o grupo de Galois da extensão tem ordem 2, e portanto, é abeliano.

Proposição 2.15. *([6], p. 105) Se $H \subseteq Aut(\mathbb{L})$ é um subconjunto não vazio, então $\mathbb{L}^H = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha$ para todo $\sigma \in H\} \subseteq \mathbb{L}$ é um subcorpo.*

O subcorpo $\mathbb{L}^H$ referido na Proposição 2.15 é nomeado **corpo fixo associado a H**.

Proposição 2.16. *([6], p. 106) Se G é um grupo finito de automorfismos de $\mathbb{L}$, então $o(G) = [\mathbb{L} : \mathbb{L}^G]$, e assim, $G = G(\mathbb{L} : \mathbb{L}^G)$.*

Teorema 2.17 (Teorema Fundamental da Teoria de Galois)**.** *([6], p. 160) Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita de Galois e $G = Gal(\mathbb{L} : \mathbb{K})$. Então existe uma correspondência biunívoca entre os corpos intermediários entre $\mathbb{K}$ e $\mathbb{L}$ e os subgrupos de G, dados por $\mathbb{M} \to G(\mathbb{L} : \mathbb{M})$ e $H \to \mathbb{L}^H$, onde $\mathbb{M}$ é um corpo intermediário entre $\mathbb{K}$ e $\mathbb{L}$, e H é subgrupo de G. Mais ainda, se $\mathbb{M} \longleftrightarrow H$, então $[\mathbb{L} : \mathbb{M}] = o(H)$ e $[\mathbb{M} : \mathbb{K}] = [G : H]$. Além disso, H é subgrupo normal de G se, e somente se, a extensão $\mathbb{L}/\mathbb{K}$ é de Galois. Quando isso acontece, temos $Gal(\mathbb{L} : \mathbb{K}) \cong G/H$.*

2.3.1 Norma, traço e discriminante

Dada uma extensão de corpos $\mathbb{L}/\mathbb{K}$ de números de grau n, existem n $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$, dados por $\sigma_1, \ldots, \sigma_n$. A seguir definiremos, conceitos que dependem destes monomorfismos, e posteriormente, a partir destes obteremos resultados. Dado α em $\mathbb{L}$, definimos a **norma** e o **traço** de $\mathbb{L}$ sobre $\mathbb{K}$ respectivamente, por:

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

$$Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Por simplicidade, quando ficar claro a extensão referida, denotaremos apenas por $N(\alpha)$ e $Tr(\alpha)$.

Na referência ([4], p. 36) podemos encontrar as seguintes propriedades do traço e da norma relativos. Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, em que $[\mathbb{L} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{L}$ e $k \in \mathbb{K}$, então valem as seguintes propriedades:

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$
2. $Tr_{\mathbb{L}/\mathbb{K}}(k\alpha) = kTr_{\mathbb{L}/\mathbb{K}}(\alpha)$;
3. $Tr_{\mathbb{L}/\mathbb{K}}(k) = nk$;
4. $N_{\mathbb{L}/\mathbb{K}}(k) = k^n$;
5. $N_{\mathbb{L}/\mathbb{K}}(k\alpha) = k^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$
6. $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta)$;

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

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

Introduziremos agora, o conceito de discriminante, que será muito relevante para os próximos capítulos, porque temos aplicações deste conceito para efetuar alguns cálculos essenciais neste tema. Sejam $\mathbb{K}$ um corpo de números e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Considere $B = \{a_0, a_1, \ldots, a_{n-1}\}$ um conjunto de $\mathbb{K}/\mathbb{Q}$. O **discriminante** desse conjunto é dado por:

$$\mathcal{D}_{\mathbb{K}}(a_0, a_1, \ldots, a_{n-1}) = [det[\sigma_i(a_j)]]^2.$$

Proposição 2.18. *([3], p. 53.) Sejam $\mathbb{K} = \mathbb{Q}(\alpha)$ um corpo de números e $p(x)$ o polinômio minimal de α sobre $\mathbb{K}$, onde $p(x)$ tem grau n. Uma $\mathbb{Q}$-base de $\mathbb{K}$ $\{1, \alpha, \dots \alpha^{n-1}\}$ tem discriminante*

$$D_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \dots \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{K}/\mathbb{Q}}(p'(\alpha)),$$

onde $p'(x)$ é a derivada de $p(x)$.

Teorema 2.19. *([7], p. 41.) Sejam $\mathbb{L}/\mathbb{K}$ uma extensão finita, com $\mathbb{K}$ um corpo finito ou de característica zero, $[\mathbb{L} : \mathbb{K}] = n$ e α um elemento de $\mathbb{L}$. Se $\alpha_1, \alpha_2, \cdots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$ vezes, então:*

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$.
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i$.
3. $p_\alpha(x) = \prod_{i=1}^{n} (x - \alpha_i)$.

2.4 MÓDULOS

Nesta seção, o objetivo é apresentar o conceito de módulo sobre um anel com unidade, tendo em vista que no decorrer do trabalho falaremos sobre esta estrutura algébrica. Para isso, utilizaremos a Referência [8]. Seja A um anel com unidade. Um conjunto não vazio $\mathcal{M}$ é dito um **módulo sobre** A (ou um A**-módulo**) se $\mathcal{M}$ é um grupo abeliano em relação a uma operação, que indicaremos por $+$, e está definida uma lei de composição externa que cada par $(\alpha, m) \in A \times \mathcal{M}$ associa um elemento $\alpha m \in \mathcal{M}$ e, tal que, para todos $\alpha_1, \alpha_2 \in A$ e todos $m_1, m_2 \in \mathcal{M}$, verifica:

i) $\alpha_1(\alpha_2 m_1) = (\alpha_1 \alpha_2) m_1$;

ii) $\alpha_1(m_1 + m_2) = \alpha_1 m_1 + \alpha_1 m_2$;

iii) $(\alpha_1 + \alpha_2) m_1 = \alpha_1 m_1 + \alpha_2 m_1$;

iv) $1_A m_1 = m_1$.

Exemplo 2.20. Abaixo, citamos alguns exemplos de A-módulos:

- Todo espaço vetorial sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo;
- Todo grupo abeliano G pode ser considerado como um módulo sobre o anel $\mathbb{Z}$, definindo o produto de um número inteiro por um elemento de G convenientemente; (Vide [8], p. 19.)

- Todo anel A é um $A-$módulo.

Seja $\mathcal{M}$ um $A-$módulo. Um subconjunto $N \subset \mathcal{M}$ diz-se um $A-$**submódulo**, ou simplesmente, um **submódulo** se:

i) N é um subgrupo aditivo de $\mathcal{M}$.

ii) N é fechado em relação à multiplicação por escalares, isto é, para todo $a \in A$ e todo $n \in N$, tem-se que $an \in N$.

Sejam $\mathcal{M}$ e $\mathcal{N}$ $A-$módulos. Uma função $f : \mathcal{M} \to \mathcal{N}$ é dita um **homomorfismo de** $A-$**módulos** (ou A-homomorfismo) se para todos $m_1, m_2 \in \mathcal{M}$ e todo $a \in A$ se verifica:

i) $f(m_1 + m_2) = f(m_1) + f(m_2)$;

ii) $f(am_1) = af(m_1)$.

Dado um $A-$homomorfismo $f : \mathcal{M} \to \mathcal{N}$ chamamos **imagem** de f e **núcleo** (ou **kernel)** de f, os respectivos conjuntos:

$$Im(f) = \{n \in \mathcal{N}; f(m) = n, \text{ para algum } m \in \mathcal{M}\},$$

$$Ker(f) = \{m \in \mathcal{M}; f(m) = 0\}.$$

É possível verificar que $Im(f)$ e $Ker(f)$ são submódulos de $\mathcal{N}$ e $\mathcal{M}$ respectivamente.

Um $A-$homomorfismo é dito um $A-$**monomorfismo** ou um $A-$**epimorfismo** se for injetor ou sobrejetor, respectivamente. Dado $f : M \to N$ um homomorfismo de módulos. Como consequência das definições acima, temos que f é um A-epimorfismo de módulos se, e somente se, $Im(f) = N$. Assim como, f é um $A-$monomorfismo de módulos se, e somente se, $Ker(f) = (0)$.

Dado um anel A, denotaremos por $A^{(J)}$ o conjunto de todas as famílias quase-nulas $(\lambda_j)_{j\in J}$ onde $\lambda_j \in A$, para todo $j \in J$. Assim, dada uma família $\{x_j\}_{j\in J}$ de elementos de um $A-$módulo $\mathcal{M}$, dizemos que um elemento $x \in \mathcal{M}$ é uma **combinação linear** dos elementos da família, se existe $(\lambda_j)_{j\in J} \in A^{(J)}$ tal que

$$x = \sum_{j\in J} \lambda_j x_j.$$

Note que, a soma acima está bem definida, uma vez que só um número finito de parcelas somadas é diferente de zero. Dizemos que um $A-$módulo $\mathcal{M}$ é **finitamente gerado**, quando existe uma família $\{x_1, \ldots, x_n\}$ de elementos de $\mathcal{M}$, tal que todo $x \in \mathcal{M}$ é da forma

$$x = \sum_{j=1}^{n} \lambda_j x_j, \text{ com } \lambda_i \in A, \ 1 \leq j \leq n.$$

Dizemos que uma família $\{x_j\}_{j\in J}$ de elementos de um $A-$módulo $\mathcal{M}$ é **linearmente independente**, se para toda $(\lambda_j) \in A^{(J)}$ tem-se que

$$\sum_{j\in J} \lambda_j x_j = 0 \Rightarrow \lambda_j = 0 \text{ para todo } j \in J.$$

Uma família $\{x_j\}_{j\in J}$ de elementos de um $A-$módulo $\mathcal{M}$ é dita uma **base** de $\mathcal{M}$ se é uma família linearmente independente e gera $\mathcal{M}$. Dizemos que um $A-$módulo é **livre** se ele contém uma base.

Proposição 2.21. *([8], p.71) Sejam A um anel de integridade e $\mathcal{M}$ um $A-$módulo. Se $\{x_i\}_{1\leq i\leq n}$ é um conjunto linearmente independente de elementos de $\mathcal{M}$ e $\{y_j\}_{1\leq j\leq m}$ é um conjunto gerador, então $n \leq m$.*

Nesse contexto, segue da Proposição 2.21 que se A é um anel de integridade e $\mathcal{M}$ é um $A-$módulo livre, finitamente gerado, então toda base de $\mathcal{M}$ é finita. Além disso, nessas condições todas as bases de $\mathcal{M}$ têm o mesmo número de elementos. Sendo assim, dado A um anel de integridade e $\mathcal{M}$ um $A-$módulo livre finitamente gerado, o número de elementos de qualquer base de $\mathcal{M}$ é chamado **posto** de $\mathcal{M}$.

2.5 ANEL DOS INTEIROS ALGÉBRICOS

Consideremos $A \subseteq B \subseteq C$ anéis. Nesta Seção vamos introduzir alguns conceitos da teoria algébrica dos números, visando definir anel dos inteiros algébricos de um corpo de números e explorar alguns resultados envolvendo ambos. Um elemento de B é dito **inteiro sobre** A se é raiz de um polinômio mônico com coeficientes em A. Quando todo elemento de B for inteiro sobre A o anel B é dito **inteiro sobre** A. Um número complexo α é dito um **inteiro algébrico**, se α é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$.

Um resultado imediato dessas definições é que se B é inteiro sobre A e c em C é inteiro sobre B, então c é inteiro sobre A, visto que $A[x] \subseteq B[x]$. Por consequência, se C é inteiro sobre A, então C é inteiro sobre B.

Teorema 2.22. *([2], p. 77) Sejam A, B domínios de integridade tal que $A \subseteq B$. O elemento b de B é inteiro sobre A se, e somente se, $A[b]$ é um A-módulo finitamente gerado.*

Teorema 2.23. *([2], p. 78) Seja $b \in B$. Se existe D um subanel de B, tal que $A[b] \subseteq D \subseteq B$ e D é um A-módulo finitamente gerado, então b é inteiro sobre A e $A[b]$ é um A-módulo finitamente gerado.*

Este Teorema, nos faz concluir que quando B é um A-módulo finitamente gerado, então B é inteiro sobre A.

Proposição 2.24. *([2], p. 79) Se B é um A-módulo finitamente gerado e C é um B-módulo finitamente gerado, então C é um A-módulo finitamente gerado.*

Proposição 2.25. *([2], p. 80) Se $b_1, b_2 \in B$ são elementos inteiros sobre A, então $b_1 + b_2, b_1 - b_2$ e $b_1 b_2$ são elementos inteiros sobre A.*

Corolário 2.26. *([2], p. 80) O conjunto dos elementos de B que são inteiros sobre A é um subanel de B contendo A.*

Sendo assim, o último resultado nos garante que o conjunto dos elementos de B que são inteiros sobre A é um anel, e este é chamado de **anel de inteiros** de A em B denotado por $\mathcal{O}_B$. Isto é,

$$\mathcal{O}_B = \{\alpha \in B; \alpha \text{ é inteiro sobre } A\}.$$

Com essa notação, segue que B é inteiro sobre A se, e somente se $\mathcal{O}_B = B$. Além disso, em particular quando $A = \mathbb{Z}$, chamamos $\mathcal{O}_{\mathbb{B}}$ de **anel dos inteiros algébricos**.

Proposição 2.27. *([2], p. 80) Se $b_1, \ldots, b_n \in B$ são elementos inteiros sobre A, então $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado.*

Proposição 2.28. *([2], p. 80) Se $b_1, \ldots, b_n \in B$ são elementos inteiros sobre A então $A[b_1, \ldots, b_n]$ é inteiro sobre A.*

Um domínio de integridade A é dito **domínio de fatoração única** (DFU) quando todo elemento a em A, com $a \neq 0$ não inversível pode ser escrito como:

$$a = p_1 p_2 \cdots p_n,$$

onde cada p_i é irredutível em A para todo $i = 1, \ldots, n$ e esta fatoração é única no sentido de que se:

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_k,$$

tal que p_i, q_j são todos irredutíveis, então $n = k$ e cada fator q_j pode ser reindexado da forma:

$$q_j = \alpha_j p_j,$$

onde α_i é um elemento inversível de A, para todo $i = 1, \ldots, n$. Nessas condições, dizemos que q_j e p_j são associados.

Exemplo 2.29. O anel dos números inteiros é um domínio de fatoração única. Em contrapartida, o anel $\mathbb{Z}[\sqrt{-5}]$ não é um DFU. Pois, 6 é um elemento de $\mathbb{Z}[\sqrt{-5}]$, que tem as seguintes fatorações:

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

onde, $2, 3, 1 \pm \sqrt{-5}$ são irredutíveis e não são associados, uma vez que os elementos inversíveis de $\mathbb{Z}[\sqrt{-5}]$ são ± 1.

Proposição 2.30. *([2], p. 83) Sejam A um domínio de fatoração única e $\mathbb{K}$ o seu corpo de frações. Assim, $c \in \mathbb{K}$ é inteiro sobre A se, e somente se, $c \in A$.*

Uma vez que $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, por consequência da Proposição 2.30, o anel dos inteiros algébricos de $\mathbb{Q}$, denotado por $\mathcal{O}_{\mathbb{Q}}$ é $\mathbb{Z}$.

Proposição 2.31. *([2], p. 110) Se $\mathbb{K}$ é um corpo de números, então $\mathcal{O}_{\mathbb{K}}$ é um anel.*

O anel A é dito **integralmente fechado** em B quando $\mathcal{O}_B = A$. Em particular, se A é um domínio e $\mathbb{K}$ o seu corpo de frações, o anel A é chamado integralmente fechado se $\mathcal{O}_{\mathbb{K}} = A$. Sob essas condições, segue da Proposição 2.30 que A é integralmente fechado.

Proposição 2.32. *([2], p. 111) Se $\mathbb{K}$ é um corpo de números, então o corpo de frações de $\mathcal{O}_{\mathbb{K}}$ é $\mathbb{K}$.*

Proposição 2.33. *([2], p. 111) Se $\mathbb{K}$ é um corpo de números, então $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado.*

Proposição 2.34. *([2], p. 111) Se $\mathbb{K}$ é um corpo de números, então todo ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ contém um número $b \in \mathbb{Z}$ não nulo.*

Proposição 2.35. *([2], p. 112) Seja $\mathbb{K}$ um corpo de números. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existe $\gamma \in I$ tal que $\mathbb{K} = \mathbb{Q}(\gamma)$.*

Deste fato, podemos concluir que se um número complexo α é algébrico, então $\alpha = \frac{a}{b}$, com a um inteiro algébrico e $b \in \mathbb{Z}$ não nulo.

Proposição 2.36. *([2], p. 121) Sejam $\mathbb{K}$ um corpo de números. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então os $\mathbb{K}$-conjugados de α são inteiros algébricos.*

Proposição 2.37. *([2], p. 129) Seja $\mathbb{K}$ um corpo de números de grau n. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existem $\eta_1, \ldots, \eta_n$ em I tais que:*

$$D_{\mathbb{K}}(\eta_1, \ldots, \eta_n) \neq 0.$$

Teorema 2.38. *([2], p. 129) Seja $\mathbb{K}$ um corpo de números de grau n. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então existem $\eta_1, \ldots, \eta_n$ em I tal que para todo α em I, existem únicos números inteiros $a_1, \ldots, a_n$, tal que $\alpha = a_1\eta_1 + \cdots + a_n\eta_n$.*

Em outras palavras, nas hipóteses do Teorema 2.38 podemos concluir que o ideal I de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}-$módulo livre de posto n, visto que $\{\eta_1, \ldots, \eta_n\}$ forma uma base para I sobre $\mathbb{Z}$. Em particular, podemos tomar $I = \mathcal{O}_{\mathbb{K}}$ e assim, obteremos a mesma conclusão para $\mathcal{O}_{\mathbb{K}}$. Sendo assim, diremos que um conjunto $\{v_1, \ldots, v_n\}$ é uma **base integral** para o corpo $\mathbb{K}$ quando este conjunto for uma base para $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$.

Teorema 2.39. *([2], p. 131) Seja $\mathbb{K}$ um corpo de números de grau n e I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Se $\{v_1, \cdots, v_n\}$ e $\{u_1, \cdots u_n\}$ são bases de I. Então $D_{\mathbb{K}/\mathbb{Q}}(v_1, \cdots, v_n) = D_{\mathbb{K}/\mathbb{Q}}(u_1, \cdots, u_n)$.*

Portanto, tomando $I = \mathcal{O}_{\mathbb{K}}$ no Teorema 2.39, concluímos que o discriminante de duas bases integrais para $\mathbb{K}$ são iguais. Assim, definimos o **discriminante do corpo** $\mathbb{K}$ como o discriminante de uma base integral de $\mathbb{K}$ e denotaremos por $D(\mathbb{K})$.

Proposição 2.40. *([7], p. 43) Sejam A um domínio e $\mathbb{K}$ o seu corpo de frações, onde $\mathbb{K}$ tem característica zero. Se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e α é um elemento de $\mathbb{L}$ que é inteiro sobre A, então os coeficientes do polinômio característico de α são inteiros sobre A. Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são inteiros sobre A.*

Supondo que A é integralmente fechado, uma consequência da Proposição 2.40 é que $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A.

2.6 FATORAÇÃO DE IDEAIS

Um domínio é dito **domínio Noetheriano** quando todos os seus ideais são finitamente gerados. A seguir, apresentamos duas condições equivalentes a essa definição.

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

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

   então existe algum m tal que $\mathcal{I}_k = \mathcal{I}_m$, para todo $k > m$, isto é toda cadeia ascendente é estacionária.

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

Para as duas próximas definições, consideremos A um anel comutativo com unidade. Dizemos que um ideal $P \subsetneq A$ é um **ideal primo** de A quando para todo $a, b \in A$ tal que $ab \in I$, $a \in P$ ou $b \in P$.

Exemplo 2.41. Considere $A = \mathbb{Z}$. O ideal $n\mathbb{Z}$ é um ideal primo de A se, e somente se, n é um número inteiro primo.

Dizemos que um ideal $M \subsetneq A$ é um **ideal maximal** de A, quando para todo ideal I tal que $M \subseteq I \subseteq A$, temos que $I = M$ ou $I = A$. Todo ideal maximal é primo, porém a recíproca não é verdadeira. Considere o contraexemplo em que $A = \mathbb{Z}$ e I é o ideal nulo.

I é um ideal primo, uma vez que $\mathbb{Z}$ não tem divisores de zero, porém não é maximal, já que $I \subsetneq 2\mathbb{Z}$, por exemplo.

Um anel A é chamado um **anel (ou domínio) de Dedekind** se A é um domínio Noetheriano, integralmente fechado e se todo ideal primo não nulo de A é um ideal maximal.

Teorema 2.42. *([3], p. 115) Seja $\mathbb{K}$ um corpo de números. O anel $\mathcal{O}_\mathbb{K}$ tem as seguintes propriedades:*

- *$\mathcal{O}_\mathbb{K}$ é um domínio;*
- *$\mathcal{O}_\mathbb{K}$ é Noetheriano;*
- *Se $\alpha \in \mathbb{K}$ é raiz de um polinômio mônico com coeficientes em $\mathcal{O}_\mathbb{K}$, então $\alpha \in \mathcal{O}_\mathbb{K}$;*
- *Todo ideal primo não nulo de $\mathcal{O}_\mathbb{K}$ é maximal.*

Com a justificativa de que estamos interessados nos $\mathcal{O}_\mathbb{K}$-submódulos de $\mathbb{K}$, que tem estrutura de grupo sob a multiplicação, a próxima definição caracteriza estes pela seguinte propriedade.

Seja $\mathfrak{a}$ um $\mathcal{O}_\mathbb{K}$-submódulo de $\mathbb{K}$. Nessas condições, $\mathfrak{a}$ é dito um **ideal fracionário** de $\mathcal{O}_\mathbb{K}$ se existe algum c em $\mathcal{O}_\mathbb{K}$ não nulo tal que $c\mathfrak{a}$ é um ideal de $\mathcal{O}_\mathbb{K}$. Em outras palavras, o conjunto $\mathfrak{b} = c\mathfrak{a}$ é um ideal de $\mathcal{O}_\mathbb{K}$ e $\mathfrak{a} = c^{-1}\mathfrak{b}$. Portanto, cada ideal fracionário de $\mathcal{O}_\mathbb{K}$ é um subconjunto de $\mathbb{K}$ da forma $c^{-1}\mathfrak{b}$, onde $\mathfrak{b}$ é um ideal de $\mathcal{O}_\mathbb{K}$ e c é um elemento não nulo de $\mathcal{O}_\mathbb{K}$.

Teorema 2.43. *([3], p. 117) Os ideais fracionários não nulos de $\mathcal{O}_\mathbb{K}$ formam um grupo abeliano multiplicativo.*

Teorema 2.44. *([3], p. 117) Todo ideal não nulo de $\mathcal{O}_\mathbb{K}$ pode ser escrito como produto de ideais primos unicamente determinados, a menos da ordem dos fatores.*

Devido a esse último Teorema, considerando A um Anel de Dedekind e $\mathfrak{a}$ um ideal não nulo de A, então existem $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideais primos e $e_1, \ldots, e_n$ inteiros positivos tal que:

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

Mais do que isso, de acordo com ([4], p. 50), tal expressão é única a menos da ordem dos fatores.

Proposição 2.45. *([4], p. 71) Sejam $\mathbb{K} \subseteq L$ corpos de números, com $[\mathbb{L} : \mathbb{K}] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_\mathbb{K}$ e*

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{2.1}$$

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

Nas condições da Proposição 2.45, diremos que os ideais $\mathfrak{p}_{i's}$ **estão acima do ideal** $\mathfrak{p}$. Ainda, g é denominado **número de decomposição** de $\mathfrak{p}$ na extensão $\mathbb{L}/\mathbb{K}$ e os expoentes $e_{i's}$ são chamados de **índices de ramificação** que denotaremos por $e(\mathfrak{q}|\mathfrak{p})$. Diremos que um ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ é ramificado em $\mathcal{O}_{\mathbb{L}}$ (ou em $\mathbb{L}$) se $e(\mathfrak{q}|\mathfrak{p}) > 1$ para algum ideal primo de $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$.

Teorema 2.46. *([5], p. 63) Sejam* $\mathfrak{p}$ *um ideal primo de* $\mathcal{O}_{\mathbb{K}}$*,* $\mathfrak{q}$ *um ideal primo de* $\mathcal{O}_{\mathbb{L}}$*, então as seguintes condições são equivalentes:*

1. $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_{\mathbb{L}}$*;*
2. $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}_{\mathbb{L}}$*;*
3. $\mathfrak{q} \supset \mathfrak{p}$*;*
4. $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$*;*
5. $\mathfrak{q} \cap \mathbb{K} = \mathfrak{p}$*.*

Quando ocorre uma das condições acima, diremos que $\mathfrak{q}$ está acima de $\mathfrak{p}$, ou $\mathfrak{p}$ está abaixo de $\mathfrak{q}$. Mostra-se, em ([5], p. 63) que todo ideal primo $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ está acima de um único ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ e todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ está abaixo de no mínimo um ideal primo $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$.

Há outro número importante associado ao par de ideais primos $\mathfrak{p}$ e $\mathfrak{q}$, com $\mathfrak{q}$ acima de $\mathfrak{p}$. Sabemos que os anéis quocientes $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ e $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$ são corpos já que $\mathfrak{p}$ e $\mathfrak{q}$ são ideais maximais e ainda existe uma maneira em que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ pode ser visto como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{K}}$ em $\mathcal{O}_{\mathbb{L}}$ induz um homomorfismo de anéis $\mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{q}$, e o núcleo é $\mathcal{O}_{\mathbb{K}} \cap \mathfrak{q}$. Pelo item 4. do Teorema 2.46, se $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$, então obtemos a imersão $\mathcal{O}_{\mathbb{K}}/\mathfrak{p} \to \mathcal{O}_{\mathbb{L}}/\mathfrak{q}$. Esses são chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$, os quais são finitos, e portanto, $\mathcal{O}_{\mathbb{L}}/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$, com f sendo esse grau e nessas condições, f é chamado **grau residual** ou **grau de inércia** de $\mathfrak{q}$ sobre $\mathfrak{p}$, e denotaremos por $f(\mathfrak{q}|\mathfrak{p})$.

Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ corpos, por ([5], p. 64.), temos que se $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{m}$ são ideais primos nos respectivos anéis dos inteiros algébricos $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{M}}$, então:

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

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

Teorema 2.47. *(Igualdade Fundamental)([5], p. 65) Sejam n o grau de $\mathbb{L}$ sobre $\mathbb{K}$ e $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ os ideais primos de $\mathcal{O}_\mathbb{L}$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$. Se $e_1, \ldots, e_g$ e $f_1, \ldots f_g$ são os correspondentes índices de ramificação e graus residuais, então:*

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

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

Teorema 2.48. *([4], p. 74) Seja $\mathbb{K}$ um corpo de números. Uma condição necessária e suficiente para que um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifique em $\mathcal{O}_\mathbb{K}$ é que p divida $D(\mathbb{K})$.*

Uma consequência do Teorema 2.48 é que existe apenas um número finito de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathcal{O}_\mathbb{K}$.

Lema 2.49. *([4], p. 71) Seja $\mathbb{K}$ um corpo de números, $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos e $\theta \in \mathcal{O}_\mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Se p é um primo tal que p não divide $[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\theta]]$ e $f(x)$ o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem $p_1(x), \ldots, p_g(x) \in \mathbb{Z}[x]$, polinômios irredutíveis, $e_1, \ldots, e_g \in \mathbb{N}^*$, tal que,*

$$f(x) \equiv p_1(x)^{e_1} \cdots p_g(x)^{e_g} (mod\ p\mathbb{Z}[x])\ e,$$

1. $\mathfrak{p}_i = (p, p_i(\theta)) = p\mathcal{O}_\mathbb{K} + p_i(\theta)\mathcal{O}_\mathbb{K}$ *são os ideais primos de* $\mathcal{O}_\mathbb{K}$ *acima de* $p\mathbb{Z}$, $i = 1, \ldots, g$;
2. $p\mathcal{O}_\mathbb{K} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$;
3. $\left[\frac{\mathcal{O}_\mathbb{K}}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}}\right] = \partial p_i(x) = f_i$.

2.6.1 Decomposição de ideais em extensões galoisianas

Sejam $\mathbb{L}$ uma extensão Galoisiana de $\mathbb{K}$ e $\mathfrak{q}$ e $\mathfrak{q}'$ ideais primos de $\mathcal{O}_\mathbb{L}$ acima do ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$, onde $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ são os anéis dos inteiros algébricos de $\mathbb{K}$ e $\mathbb{L}$ respectivamente. Veremos como se comporta o grau de inércia e o índice de ramificação dos ideais $\mathfrak{q}$ e $\mathfrak{q}'$ sobre o ideal $\mathfrak{p}$.

Teorema 2.50. *(Teorema da Evidência)([5], p. 70) Dado $\mathbb{L}/\mathbb{K}$ galoisiana com grupo de Galois G e, $\mathfrak{q}$ e $\mathfrak{q}'$ tais que $\mathfrak{q} \cap \mathcal{O}_\mathbb{K} = \mathfrak{q}' \cap \mathcal{O}_\mathbb{K}$. Então existe $\sigma \in G$, tal que $\sigma(\mathfrak{q}) = \mathfrak{q}'$.*

Corolário 2.51. *([5], p. 71) Sejam $\mathbb{L}$ uma extensão galoisiana sobre $\mathbb{K}$. Se $\mathfrak{q}$ e $\mathfrak{q}'$ são dois ideais primos acima de $\mathfrak{p}$, então $e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}'|\mathfrak{p})$ e $f(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{p})$.*

Pelo Corolário 2.51, podemos concluir que para a extensão $\mathbb{L}/\mathbb{K}$, o ideal primo $\mathfrak{p}$ fatora-se como $(\mathfrak{q}_1, \ldots, \mathfrak{q}_g)^e$ em $\mathcal{O}_\mathbb{L}$, onde os $\mathfrak{q}_{i's}$ são os ideais primos distintos acima de $\mathfrak{p}$, todos com o mesmo grau residual f sobre $\mathfrak{p}$. Dessa forma, pelo Teorema 2.47, $n = [\mathbb{L} : \mathbb{K}] = g \cdot e \cdot f$.

Conhecendo o índice de ramificação e o grau de inércia, podemos classificar os ideais primos, $\mathfrak{p}_{i's}$ com $i = 1, \ldots, g$, de $\mathcal{O}_\mathbb{L}$ em: **(a)** Totalmente ramificado se $g = f_i = 1$ e $e_i = n$;

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

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

Sejam $\mathbb{K}$ um corpo de números de grau n, $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos e $\mathfrak{a}$ um ideal de $\mathcal{O}_\mathbb{K}$. Definimos a **norma do ideal** $\mathfrak{a}$ como o número de classes laterais de $\mathfrak{a}$ em $\mathcal{O}_\mathbb{K}$, e denotaremos por $N(\mathfrak{a})$, isto é,

$$N(\mathfrak{a}) = \#(\mathcal{O}_\mathbb{K}/\mathfrak{a})$$

Sendo assim, concluímos que, $N(\mathfrak{a})$ é um inteiro positivo.

Teorema 2.52. *([3], p. 126) Sejam $\mathbb{K}$ um corpo de número de grau n e $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos. Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$, então:*

1. *O ideal $\mathfrak{a}$ tem uma $\mathbb{Z}-$base $\{\alpha_1, \ldots, \alpha_n\}$;*

2. *A norma de $\mathfrak{a}$ satisfaz:*

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

onde $D(\mathbb{K})$ é o discriminante de $\mathbb{K}$.

Corolário 2.53. *([3], p. 126) Se $\mathfrak{a} =< a >$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então:*

$$N(\mathfrak{a}) = |N(a)|$$

Teorema 2.54. *([3], p. 127) Seja $\mathbb{K}$ um corpo de números. Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathcal{O}_\mathbb{K}$, então:*

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

Sejam $\mathfrak{a}$ um ideal de $\mathcal{O}_\mathbb{K}$ e b um elemento de $\mathcal{O}_\mathbb{K}$, tal que $\mathfrak{a} \mid < b >$. Neste caso, denotaremos apenas $\mathfrak{a} \mid b$. Uma consequência imediata é que $\mathfrak{a} \mid b$ se e somente se, b é um elemento de $\mathfrak{a}$.

Teorema 2.55. *([3], p. 129) Sejam $\mathbb{K}$ um corpo de números e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_\mathbb{K}$.*

- *Se $N(\mathfrak{a})$ é um primo, então $\mathfrak{a}$ é um ideal primo;*
- *$N(\mathfrak{a})$ é um elemento de $\mathfrak{a}$, ou equivalentemente, $a \mid N(\mathfrak{a})$;*
- *Se $\mathfrak{a}$ é um ideal primo que divide um primo p, então,*

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

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

O último item deste Teorema, garante concluir que para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$, temos que, $N(\mathfrak{p}) = p^f$, onde f é o grau residual de $\mathfrak{p}$ e p é o único número primo de $\mathfrak{p}$. De fato, como $\left[\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} : \frac{\mathbb{Z}}{p\mathbb{Z}}\right] = f$, segue que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ tem p^f elementos.

2.7 VALORIZAÇÃO p-ÁDICA

Para esta Seção, vamos considerar $\mathbb{Z}^*$, o conjunto dos números inteiros sem o zero. Sejam p um número primo e $a \in \mathbb{Z}^*$. Definimos a **valorização p-ádica** de a, o maior expoente de p tal que essa potência divide a, e denotaremos por $v_p(a)$.

Sendo assim, dado $a \in \mathbb{Z}^*$, ao exibirmos a sua fatoração em potências de números primos, saberemos a sua valorização p-ádica para cada p primo.

Por exemplo, o número 45 pode ser reescrito como $3^2 \cdot 5$, e portanto,

- $v_3(45) = 2$;
- $v_5(45) = 1$;
- $v_p(45) = 0$ para todo p primo diferente de 3 e 5.

Podemos listar algumas propriedades da valorização p-ádica. Para isso, se $a, b \in \mathbb{Z}^*$ e p um número primo, então:

1. $v_p(ab) = v_p(a) + v_p(b)$;
2. $v_p(a+b) \geq min\{v_p(a), v_p(b)\}$, desde que $a + b \neq 0$, neste caso, se $v_p(a) \neq v_p(b)$, então vale a igualdade.

A recíproca não é verdadeira, pois se $v_p(a) = v_p(b)$, consideremos $a = p^n a'$ e $b = p^n b'$ segue que $a + b = p^n(a' + b')$ e, eventualmente é possível que $v_p(a' + b') = k$, com $k > 0$. Assim $v_p(a + b) = n + k \neq min\{v_p(a), v_p(b)\}$

Estudaremos a valorização $p-$ádica no contexto de ideais de anéis Noetherianos, para isso, considere R um anel Noetheriano e $\mathfrak{p}$ um ideal primo de R. A **valorização $\mathfrak{p}-$ádica** de x em R é definida por $v_{\mathfrak{p}}(x) = k$ quando:

$$x \in \mathfrak{p}^k \qquad \text{e} \qquad x \notin \mathfrak{p}^{k+1}, \qquad \text{com } k \geq 0.$$

Para exemplificar, consideremos o anel $\mathbb{Z}$ e o ideal primo $\mathfrak{p} = 2\mathbb{Z}$. Assim,

1. $v_{\mathfrak{p}}(7) = 0$;
2. $v_{\mathfrak{p}}(6) = 1$;
3. $v_{\mathfrak{p}}(12) = 2$;
4. $v_{\mathfrak{p}}(8) = 3$.

Neste contexto, também valem as propriedades citadas para os números inteiros, isto é, dado R um anel Noetheriano e $\mathfrak{p}$ um ideal primo de R, para quaisquer a, b em R, valem:

1. $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$;
2. $v_{\mathfrak{p}}(a + b) \geq min\{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)\}$.

Para o segundo item, analogamente ao caso dos números inteiros, podemos afirmar que quando $v_{\mathfrak{p}}(a) \neq v_{\mathfrak{p}}(b)$, vale a igualdade, caso contrário, mantém-se o maior ou igual. Vale a pena mencionar que o conceito de valorização $\mathfrak{p}-$ádica tem diversas aplicações em casos mais gerais. Nas seções posteriores utilizaremos no contexto de ideais do anel dos inteiros algébricos de um corpo ciclotômico.

3 CORPOS ABELIANOS

Dentre os corpos, iremos nos restringir a um caso específico de corpo de números, que são chamados de corpos abelianos. Na Seção 2.3 vimos que uma extensão de $\mathbb{Q}$ é dita abeliana quando é galoisiana e o seu grupo de Galois é abeliano, nesse contexto quando $\mathbb{K}$ é um corpo de números e a extensão $\mathbb{K}/\mathbb{Q}$ for abeliana, diremos que $\mathbb{K}$ é um **corpo abeliano**. Veremos que estes corpos tem uma vasta área de estudo e são de grande importância para a Teoria dos Números Algébricos, tendo em vista que os corpos ciclotômicos são corpos abelianos e dedicamos uma seção para eles, devido sua relevância para o assunto. Na Seção 3.1, trataremos de corpos quadráticos, que durante a seção provaremos que se encaixam na definição de corpos abelianos, além disso exibiremos o anel dos inteiros algébricos, a forma quadrática e o discriminante destes corpos. Em seguida, na Seção 3.2 trataremos dos corpos ciclotômicos, que por sua vez tem um elemento primitivo bem interessante, exploraremos os conceitos de, raiz $n-$ésima da unidade, $n-$ésimo polinômio ciclotômico, discriminante, anel de inteiros e demonstraremos alguns resultados de ideais que serão importantes no decorrer do trabalho. Consequentemente na Seção 3.3, estudaremos o grupo de Galois destas extensões, inclusive uma condição para que este seja cíclico e terminamos a seção enunciando o importante Teorema de Kronecker-Weber, que não será demonstrado, já que além de ser uma demonstração extensa, não faz parte do objetivo deste trabalho, mas uma demonstração é encontrada em ([9], p. 273). Na Seção 3.4, falaremos sobre os subcorpos reais maximais de um corpo ciclotômico e veremos que dado um corpo ciclotômico, podemos exibir um elemento primitivo para o subcorpo real maximal deste, e por fim a Seção **??**, trata sobre corpos abelianos com condutor primo, a qual o principal resultado é, dado um corpo abeliano $\mathbb{K}$ de condutor primo, sob algumas condições sobre o grau deste corpo, podemos exibir um elemento primitivo e uma base integral.

3.1 CORPOS QUADRÁTICOS

Os corpos quadráticos, que definiremos em seguida, valem a pena ser explorados porque exibiremos resultados que explicitam de maneira simples informações como o anel dos inteiros e o discriminante, e além disso, posteriormente veremos que em uma de suas

aplicações, os exemplos podem ser visualizados graficamente no plano real, o que é uma vantagem com relação a extensões de corpos com graus maiores. Consideremos α um número complexo, que é raiz de um polinômio irredutível x^2+ax+b de $\mathbb{Q}[x]$. Neste caso, o corpo $\mathbb{Q}(\alpha)$ é chamado de **corpo quadrático** de $\mathbb{Q}$. Em outras palavras, $\mathbb{K}$ é um corpo quadrático quando o grau da extensão $\mathbb{K}/\mathbb{Q}$ é 2. Para exemplificar, consideremos $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(i)$. Estes são corpos quadráticos, já que $\sqrt{2}$ e i, respectivamente, são raízes dos polinômios x^2-2 e x^2+1. Por outro lado, o corpo $\mathbb{Q}(\sqrt[3]{2})$ não é um corpo quadrático, visto que o polinômio mônico de menor grau com coeficientes racionais que anula $\sqrt[3]{2}$ é x^3-2. Já vimos, pela Proposição 2.8, que todo o corpo de números pode ser expresso da forma $\mathbb{Q}(\theta)$, onde θ é um elemento algébrico. Porém no caso dos corpos quadráticos temos mais informações sobre quem é um elemento primitivo como foi mencionado no início desta seção. Contudo dado um corpo quadrático podemos explicitar um elemento primitivo com certa característica, e esta é a motivação para o primeiro resultado da Seção.

Diremos que um número inteiro d é **livre de quadrados** se ele não é divisível pelo quadrado de nenhum número inteiro maior que 1, uma consequência disso é que $d \not\equiv 0\ (mod\ n^2)$ para qualquer n inteiro. Portanto quando d for livre de quadrados, ao dizer que $d \not\equiv 1\ (mod\ 4)$, fica implícito que estamos tratando apenas do casos $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$.

Teorema 3.1. *([2], p. 95) Se $\mathbb{K}$ é um corpo quadrático, então existe um único número inteiro d, livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.*

Demonstração. Seja α um número complexo que é uma raiz do polinômio x^2+ax+b, com a, b racionais. Pela fórmula resolutiva da equação de segundo grau, $\alpha = \frac{-a+\sqrt{a^2-4b}}{2}$ ou $\alpha = \frac{-a-\sqrt{a^2-4b}}{2}$, e em ambos casos concluímos que $\mathbb{K} = \mathbb{Q}(\sqrt{a^2-4b})$. Por outro lado, como a e b são números racionais, a^2-4b também é racional, que pode ser reescrito como fração irredutível de números inteiros. Consideremos que seja $\frac{j}{k}$, que por sua vez é igual $\frac{jk}{k^2}$, e assim, concluímos que $\mathbb{K} = \mathbb{Q}(\sqrt{jk})$, onde jk é um inteiro livre de quadrados, visto que a fração $\frac{j}{k}$ é irredutível.

Provaremos agora, que nestas condições o número inteiro d no enunciado do teorema é único. Seja u livre de quadrados tal que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{u})$. Sendo assim, podemos escrever $\sqrt{d} = a + b\sqrt{u}$ onde a e b são racionais. Da igualdade anterior, segue que $a = \sqrt{d} - b\sqrt{u}$, e assim,

$$\begin{aligned} a^2 &= d - 2b\sqrt{du} + b^2u \\ 2b\sqrt{du} &= -a^2 + d + b^2u \\ \sqrt{du} &= \frac{-a^2 + d + b^2u}{2b} \\ du &= \left(\frac{-a^2 + d + b^2u}{2b}\right)^2 \end{aligned}$$

Pela construção, sabemos que $-a^2 + d + b^2u$ e $2b$ são racionais, e portanto, podemos escrever $\frac{-a^2+d+b^2u}{2b}$ como fração irredutível, seja esta $\frac{x}{y}$. Dando continuidade, obtemos que $du = \left(\frac{x}{y}\right)^2$. Contudo, como du é inteiro, podemos concluir que $y = 1$, e portanto, $du = x^2$.

Note que, na decomposição em primos de x^2, cada número primo tem expoente pelo menos 2. Por outro lado, como d e u são livres de quadrado, segue que cada primo em suas respectivas fatorações em primos, aparece no máximo uma vez. Como $du = x^2$, podemos concluir do que foi exposto que a fatoração em primos de d e u são iguais, isto é, $d = u$, concluindo a demonstração. ■

Exemplo 3.2. Por exemplo, $\sqrt{8}$ é raiz de $x^2 - 8$, e assim, $\mathbb{Q}(\sqrt{8})$ é um corpo quadrático, apesar de 8 não ser livre de quadrados, uma vez que $\sqrt{8} = 2\sqrt{2}$, concluímos que $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$, e portanto, $\mathbb{Q}(\sqrt{8})$ pode ser escrito conforme o Teorema 3.1. Devido a este resultado, prosseguiremos nesta seção considerando sempre $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d está nas condições do Teorema 3.1.

Teorema 3.3. *([2], p. 95) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com d livre de quadrados. O anel $\mathcal{O}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K}$ é:*

i) $\mathbb{Z}[\sqrt{d}]$ quando $d \not\equiv 1 \ (mod\ 4)$;

ii) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ quando $d \equiv 1 \ (mod\ 4)$.

Demonstração. Consideremos

$$M = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{se } d \not\equiv 1 \ (mod\ 4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{se } d \equiv 1 \ (mod\ 4). \end{cases}$$

Seja α um elemento de M. Como $M \subset \mathbb{K}$, segue que:

i) Se $d \not\equiv 1 \ (mod\ 4)$, então $\alpha = a + b\sqrt{d}$, com a, b inteiros, e portanto:

$$\begin{aligned}\alpha^2 &= a^2 + 2ab\sqrt{d} + b^2d \\ &= a^2 + b^2d + 2ab\sqrt{d} + 2a^2 - 2a^2 \\ &= -a^2 + b^2d + 2a(b\sqrt{d} + a) \\ &= -a^2 + b^2d + 2a\alpha.\end{aligned}$$

Da igualdade acima, concluímos que $\alpha^2 - 2a\alpha + (a^2 - b^2d) = 0$, ou seja, α é raiz do polinômio mônico $x^2 - 2ax + (a^2 - b^2d)$ que pela construção tem coeficientes inteiros, e assim, α é um elemento de $\mathcal{O}_{\mathbb{K}}$.

ii) Se $d \equiv 1\ (mod\ 4)$, então $\alpha = a + b(\frac{1+\sqrt{d}}{2})$, com a, b inteiros. De modo análogo ao caso anterior, obtemos que α é raiz do polinômio mônico $x^2 - (2a+b)x - \left(a^2 + ab - b^2\left(\frac{d-1}{4}\right)\right)$, que por sua vez tem coeficientes inteiros, já que $d \equiv 1\ (mod\ 4)$ implica que 4 divide $d-1$, e portanto, $\frac{d-1}{4}$ é um número inteiro.

De i) e ii) concluímos que $M \subset \mathcal{O}_{\mathbb{K}}$. Agora, verificaremos a outra inclusão. Para isso, seja α um elemento de $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathbb{K}$, segue que $\alpha = a + b\sqrt{d}$, com a, b números racionais. De modo análogo a i), observamos que α é raiz do polinômio $x^2 - 2ax + (a^2 - b^2d)$, que neste caso tem coeficientes racionais. Assim, $\Delta = 4a^2 - 4(a^2 - db^2) = 4db^2$, e como d é livre de quadrados, segue que este polinômio é redutível em $\mathbb{Q}[x]$ quando $b = 0$ e irredutível caso contrário. Logo, o polinômio minimal de α em $\mathbb{Q}[x]$ é:

$$m_{\mathbb{Q}}(\alpha) = \begin{cases} x - a, & \text{se } b = 0 \\ x^2 - 2ax + (a^2 - b^2d), & \text{se } b \neq 0. \end{cases}$$

Por outro lado, como α é um elemento de $\mathcal{O}_{\mathbb{K}}$, segue que o polinômio minimal de α é um elemento de $\mathbb{Z}[x]$, e assim, concluímos que todos os coeficientes são inteiros, isto é:

$$\begin{cases} a \in \mathbb{Z}, & \text{se } b = 0 \\ 2a \in \mathbb{Z} \text{ e } (a^2 - b^2d) \in \mathbb{Z}, & \text{se } b \neq 0. \end{cases}$$

Para $b = 0$, temos que a é inteiro, e assim, $\alpha = a$, e portanto, pertence a M. Vejamos agora quando $b \neq 0$. Neste caso temos que $2a$ é um número inteiro.

- Se $2a$ é par, então a é inteiro, o que implica que a^2 também é inteiro. Além disso, por hipótese $a^2 - b^2d$ também é inteiro. Assim, $b^2d \in \mathbb{Z}$. Como b é racional, tomemos $b = \frac{j}{k}$, com j, k inteiros, $k \neq 0$ e $mdc(j, k) = 1$, segue que,

$$db^2 = d\left(\frac{j}{k}\right)^2 \in \mathbb{Z}.$$

Sendo assim, k^2 divide d. Como d é livre de quadrados, concluímos que $k = \pm 1$, e por sua vez $b = \pm j \in \mathbb{Z}$, e portanto $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, isto é, α é um elemento de M.

- Se $2a$ é ímpar, então $2a = 2k + 1$, para algum k inteiro. Logo, $a = k + \frac{1}{2}$. Assim,

$$a^2 = k^2 + k + \frac{1}{4} \notin \mathbb{Z}$$

Porém, como $(a^2 - b^2 d)$ é inteiro, segue que $4(a^2 - b^2 d)$ também é inteiro. Logo,

$$4\left(\left(k + \frac{1}{2}\right)^2 - b^2 d\right) = 4\left(k^2 + k + \frac{1}{4} - b^2 d\right) = 4k^2 + 4k + (1 - 4b^2 d) \in \mathbb{Z}.$$

Com isso, podemos concluir que $4b^2 d$ é inteiro. Reescrevendo $2b = \frac{m}{n}$, de modo que $m, n \in \mathbb{Z}$, $n \neq 0$ e $mdc(m, n) = 1$, obtemos

$$4b^2 d = d(2b)^2 = d\left(\frac{m}{n}\right)^2 \in \mathbb{Z}.$$

Portanto, concluímos que n^2 divide d que é livre de quadrados, e portanto, $n = \pm 1$, e assim, $2b = \pm m$ é inteiro. Se $2b$ for par, teremos que b é inteiro, e portanto, b^2 também, e consequentemente, o mesmo para db^2. Porém, neste caso, $a^2 = (a^2 - db^2) + db^2 \in \mathbb{Z}$, o que é um absurdo, portanto $2b$ é ímpar. Sendo assim, $2b = 2q + 1$, para algum q inteiro. Por fim, temos que $a = \frac{2k+1}{2}$ e $b = \frac{2q+1}{2}$ com k, q inteiros. Assim,

$$\begin{aligned} a^2 - b^2 d &= \left(\frac{2k+1}{2}\right)^2 - d\left(\frac{2q+1}{2}\right)^2 \\ &= \frac{1}{4}\left((2k+1)^2 - d(2q+1)^2\right) \\ &= k^2 + k - dq^2 + dq + \frac{1-d}{4} \in \mathbb{Z}. \end{aligned}$$

Logo,

$$\frac{d-1}{4} = k^2 + k - dq^2 + dq \in \mathbb{Z}.$$

Com isso, concluímos que $d \equiv 1 \ (mod\ 4)$. Assim,

$$\begin{aligned}\alpha = a + b\sqrt{d} &= \frac{2k+1}{2} + \frac{2q+1}{2}\sqrt{d} \\ &= a + b\sqrt{d} = \frac{2k+1}{2} + \frac{2q+1}{2}\sqrt{d} + \frac{2q+1}{2} - \frac{2q+1}{2} \\ &= (2q+1)\left(\frac{1+\sqrt{d}}{2}\right) + k - q \\ &= (k-q)(2q+1)\left(\frac{1+\sqrt{d}}{2}\right).\end{aligned}$$

Pela construção, temos que $(k-q)(2q+1)$ é inteiro, e portanto α é um elemento de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, isto é, $\alpha \in M$. Com isso concluímos que α é um elemento de M, provando que $\mathcal{O}_{\mathbb{K}} \subset M$. Sendo assim, $\mathcal{O}_{\mathbb{K}} = M$, como queríamos. ■

Corolário 3.4. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com d livre de quadrados. O conjunto $\{1, \sqrt{d}\}$ é uma base integral para $\mathbb{K}$ se $d \not\equiv 1 \ (mod\ 4)$, assim como $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma base integral para $\mathbb{K}$ se $d \equiv 1 \ (mod\ 4)$.*

Demonstração. Consequência imediata do Teorema 3.3. ■

Pelo Teorema 2.14, já sabemos que a extensão $\mathbb{K}/\mathbb{Q}$ é abeliana. O seguinte resultado, explicitará o grupo de Galois desta extensão, com a motivação de calcular o discriminante de $\mathbb{K}$, visto que no caso em que a extensão é galoisiana, os n monomorfismos coincidem com o grupo de Galois. A seguir, demonstraremos um resultado elementar da Teoria de Grupos.

Proposição 3.5. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com d livre de quadrados. O grupo de Galois da extensão $\mathbb{K}/\mathbb{Q}$, é:*

$$G(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \sigma_2\},$$

onde $\sigma_1, \sigma_2 : \mathbb{K} \to \mathbb{K}$ tais que $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ e $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$, para $a + b\sqrt{2}$ em $\mathbb{K}$.

Demonstração. Uma condição necessária para que $\sigma \in G(\mathbb{K} : \mathbb{Q})$ é que:

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

Por outro lado, note que $d = \sigma(d) = \sigma((\sqrt{d})^2) = \sigma(\sqrt{d})\sigma(\sqrt{d})$. Daí temos:

$$d = \left(\sigma(\sqrt{d})\right)^2, \text{ ou seja, } \sigma(\sqrt{d}) = \pm\sqrt{d}.$$

Assim os dois casos possíveis são, $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ e $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$. Além disso, σ_1 e σ_2 são $\mathbb{Q}-$automorfismos de $\mathbb{K}$, e portanto, concluímos que $G(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \sigma_2\}$. ■

Para exemplificar, uma consequência da Proposição 3.5 é que quando $\mathbb{K}$ for um corpo quadrático totalmente imaginário, seu grupo de Galois é o conjunto cujos elementos são a identidade e a conjugação complexa.

Teorema 3.6. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d inteiro livre de quadrados, então o discriminante do corpo $\mathbb{K}$ é dado por:*

$$D(\mathbb{K}) = \begin{cases} 4d, & se\ d \not\equiv 1\ (mod\ 4) \\ d, & se\ d \equiv 1\ (mod\ 4). \end{cases}$$

Demonstração. Seja $d \not\equiv 1\ (mod\ 4)$. Pelo Corolário 3.4, temos que $\{1, \sqrt{d}\}$ é uma base integral para $\mathbb{K}$, e portanto,

$$D(\mathbb{K}) = D(1, \sqrt{d}) = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

Para o outro caso, seja $d \equiv 1\ (mod\ 4)$. Pelo mesmo corolário obtemos:

$$D(\mathbb{K}) = D\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d,$$

o que prova o Teorema. ■

Exemplo 3.7. Consideremos $\mathbb{K} = \mathbb{Q}(\sqrt{15})$. Como $15 \equiv 3\ (mod\ 4)$, pelo Teorema 3.6 $D(\mathbb{K}) = 4 \cdot 15 = 60$.

Corolário 3.8. *Se $\mathbb{K}$ é um corpo quadrático, então $\mathbb{K} = \mathbb{Q}(\sqrt{D(\mathbb{K})})$.*

Demonstração. Segue diretamente do Teorema 3.6. ■

3.2 CORPOS CICLOTÔMICOS

Os corpos ciclotômicos, são de extrema importância quando falamos em extensões abelianas. Nesta seção, veremos resultados que relacionam tais conceitos, sendo o principal resultado o teorema de Kronecker-Weber, que garante que toda extensão abeliana finita está contida em um corpo ciclotômico. Além disso, temos outros resultados interessantes relacionados ao anel dos inteiros algébricos de um corpo ciclotômico, os quais nos permitem determinar este anel, onde tais resultados serão desenvolvidos no decorrer deste capítulo.

Consideremos $\mathbb{K} = \mathbb{C}$. Um elemento $\alpha \in \mathbb{K}$ é dito uma **raiz n-ésima da unidade** se $\alpha^n = 1$, para $n \geq 1$, inteiro. Sendo assim, temos que as raízes n-ésimas da unidade são as raízes do polinômio $p(x) = x^n - 1$. Consideremos então $U_n = \{\alpha \in \mathbb{K}; \alpha^n = 1\}$, o conjunto de todas as raízes de $p(x)$ em $\mathbb{K}$. O conjunto U_n é um grupo cíclico com a multiplicação, e podemos representá-lo por $\zeta, \zeta^2, \ldots, \zeta^n = 1$, onde ζ é um gerador do grupo U_n.

Diremos que ζ é uma **raiz n-ésima primitiva** da unidade, se ζ é um gerador do grupo U_n, isto é, são todos os elementos da forma ζ^k, com $mdc(k,n) = 1$, para $k = 1, \ldots, n$. Assim, podemos descobrir a quantidade de raízes n-ésimas primitivas da unidade para cada n natural, para isso, basta analisar quantos são os números primos com n, menores que n, o qual é dado por $\varphi(n)$, onde φ é a função de Euler.

Dado n um inteiro positivo, definimos $\zeta_n = e^{\frac{2\pi i}{n}}$. O corpo $\mathbb{Q}(\zeta_n)$ é chamado o **n-ésimo corpo ciclotômico**. O polinômio cujas raízes são as raízes n-ésimas primitivas da unidade é chamado **n-ésimo polinômio ciclotômico**, dado por:

$$\Phi_n(x) = \prod_{j=1, mdc(j,n)=1}^{n} (x - \zeta_n^j). \tag{3.1}$$

Uma identidade polinomial que será muito útil no decorrer do trabalho é a seguinte

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + ... + x + 1, \tag{3.2}$$

que segue diretamente da divisão de polinômios, utilizando o método da chave por exemplo.

Lema 3.9. *([10], p. 100) Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Observemos que se p é primo, então uma consequência deste Lema é que

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x).$$

Da igualdade acima, concluímos que se p é primo, então utilizando a Equação 3.2, o p-ésimo polinômio ciclotômico é

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

Mais geralmente, para qualquer $n \geq 1$ inteiro, do Lema podemos concluir que

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}.$$

Também podemos verificar que para $n \geq 1$ inteiro, $gr(\Phi_n) = \varphi(n)$.

Quando $n = p^r$, onde p é um número primo e r inteiro positivo, utilizando o Lema 3.9 e a Equação 3.2, concluímos que o p^r-ésimo polinômio ciclotômico é:

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

Uma consequência disso é que:

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}) = \begin{cases} -1, & \text{se } r = 1 \\ 0, & \text{caso contrário.} \end{cases} \tag{3.3}$$

Teorema 3.10. *Se ζ_n é uma raíz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Demonstração. Pela Equação 3.1, na definição do n-ésimo polinômio ciclotômico, temos que $\Phi_n(\zeta_n) = 0$, sendo este um polinômio mônico e irredutível nos racionais. Portanto $\Phi_n(x) = min_{\zeta_n}(x)$ sobre $\mathbb{Q}$, sendo assim, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = gr(\Phi_n) = \varphi(n)$. ■

Dado um corpo ciclotômico, o próximo objetivo desta Seção é identificar o anel dos inteiros algébricos deste, bem como uma base integral. Para isso, vamos considerar inicialmente, $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo. No decorrer do capítulo, veremos o caso geral. Para fazermos a demonstração, iremos utilizar o fato de que sob estas condições,

$$Tr_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_p^k) = p, \ \forall \ k = 1, \ldots, p-1. \tag{3.4}$$

Agora, enunciaremos e demonstraremos um lema já conhecido, pois é um resultado que utilizamos posteriormente para provar a igualdade da Equação 3.4.

Lema 3.11. *Seja $G = \{g_1, g_2, \ldots, g_n\}$ um grupo. Se g é um elemento de G, então $\{gg_1, gg_2, \ldots, gg_n\} = G$.*

Demonstração. De fato, sejam g_i, g_j elementos de G, então:

$$gg_i = gg_j \Rightarrow g_i = g_j$$

Uma vez que G é um grupo, multiplicamos à esquerda pelo elemento inverso de g. Assim, concluímos que $gg_i \neq gg_j$ quando $i \neq j$. Por outro lado, como $g_i, g \in G$, temos que $gg_i \in G$ para todo $i = 1, \ldots, n$. Sendo assim $\{gg_1, gg_2, \ldots, gg_n\} \subset G$, visto que tal conjunto tem a mesma quantidade n de elementos que G, concluímos que $G = \{gg_1, gg_2, \ldots, gg_n\}$. ■

Prosseguiremos para a demonstração da Equação 3.4. Para isso,

$$Tr(1) = \sum_{i=1}^{p-1} \sigma_i(1) = p - 1,$$

já que $\sigma_i(1) = 1$, para todo $i = 1, \ldots, p-1$, onde p é um número primo. Por outro lado, $Tr(\zeta_p^k) = \sum_{i=1}^{p-1} \sigma_i(\zeta_p^k) = -1, \ \forall \ k = 1, \ldots, p-1$, já que:

$$Tr(\zeta_p^k) = \zeta_p^k + (\zeta_p^k)^2 + \cdots + (\zeta_p^k)^{p-2} + (\zeta_p^k)^{p-1} = \zeta_p^k + \zeta_p^{2k} + \cdots + \zeta_p^{k(p-2)} + \zeta_p^{k(p-1)} = -1.$$

Uma vez que

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*,$$

é um grupo com a multiplicação. Como $1 \leq k \leq p-1$, segue que $\overline{k}$ é um elemento deste grupo, e além disso, sabemos que $\overline{k} \cdot \overline{j} = \overline{kj}$. Assim pelo Lema 3.11, segue que, $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{k}, \overline{2k}, \ldots, \overline{k(p-1)}\}$. Por outro lado, de acordo com a Equação 3.3, quando $r = 1$, temos que $\zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1$. Assim, a menos da ordem dos expoentes, segue que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\zeta_p^k) = \zeta_p^k + \zeta_p^{2k} + \cdots + \zeta_p^{k(p-2)} + \zeta_p^{k(p-1)} = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1. \tag{3.5}$$

Daí, $Tr(\zeta_p^k) = -1$. Agora, utilizando as propriedades do traço, segue que

$$Tr(1 - \zeta_p^k) = Tr(1) - Tr(\zeta_p^k) = p - 1 - (-1) = p,$$

como queríamos.

Teorema 3.12. *([4], p. 43) Seja p número primo. O anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ é $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_p]$ e $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathcal{O}_\mathbb{K}$ como um $\mathbb{Z}$-módulo.*

Demonstração. Mostremos que $\mathcal{O}_\mathbb{K} \subseteq \mathbb{Z}[\zeta_p]$. Para isso, considere $\alpha \in \mathcal{O}_\mathbb{K}$. Como $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2};\ a_i \in \mathbb{Q}, \forall\ i = 1, \ldots, p-2.$$

Multiplicando ambos lados da igualdade por $(1 - \zeta_p)$, temos:

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

Aplicando o traço, segue que

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

Visto que, quando $i = 1, \ldots, p-2$, pela igualdade 3.5, temos que

$$Tr(\zeta_p^i) = Tr(\zeta_p^{i+1}) = -1 \Rightarrow Tr(\zeta_p^i - \zeta_p^{i+1}) = 0,$$

donde concluímos que

$$Tr(\alpha(1 - \zeta_p)) = a_0 Tr(1 - \zeta_p) = a_0 p.$$

Por outro lado, sabemos que $Tr(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$. Logo, $a_o p = pb$, com $b \in \mathbb{Z}$. Assim, $a_0 \in \mathbb{Z}$.

Agora, como $\zeta_p^{-1} = \zeta_p^{p-1}$, segue que $\zeta_p^{-1} \in \mathcal{O}_{\mathbb{K}}$. Logo,

$$(\alpha - a_o)\zeta_p^{-1} = a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3} \in \mathcal{O}_{\mathbb{K}}.$$

Sendo assim, podemos repetir o processo anterior, para concluir que $a_1 \in \mathbb{Z}$. Fazendo-o sucessivamente, teremos que a_i é um número inteiro para todo $i = 1, \ldots, p-2$. E portanto, α é um elemento de $\mathbb{Z}[\zeta_p]$. Assim, $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$, e concluímos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Além disso, como $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é linearmente independente sobre $\mathbb{Q}$, também é sobre $\mathbb{Z}$, portanto este conjunto é uma base para $\mathbb{Z}[\zeta_p]$. ■

Lema 3.13. *([5], p. 30) Sejam p um número primo e r um número natural. Então, $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$ e, $D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, 1-\zeta_{p^r}, \ldots, 1-\zeta_{p^r}^{(p-1)p^{r-1}-1}) = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1})$, para todo $p^r \geq 3$.*

Demonstração. A primeira igualdade segue do fato que $\zeta_{p^r} = 1-(1-\zeta_{p^r})$. Para a segunda igualdade, sabemos que os conjugados de ζ_{p^r} são os elementos $\zeta_{p^r}^k$ com $k = 1, \ldots p^r - 1$, e $mdc(k, p^r) = 1$. Daí segue que os elementos $1 - \zeta_{p^r}^k$, com k nas condições mencionadas, são os conjugados de $1 - \zeta_{p^r}$. Além disso, como a matriz $\left(\sigma_j(\zeta_{p^r}^i)\right)_{ij}$ é uma matriz de Vandermonde, segue que o determinante é dado por:

$$\begin{aligned} D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) &= \prod_{t<k}(\zeta_{p^r}^k - \zeta_{p^r}^t)^2 \\ &= \prod_{t<k}((1 - \zeta_{p^r}^k) - (1 - \zeta_{p^r}^t))^2 \\ &= D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, 1 - \zeta_{p^r}, \ldots, 1 - \zeta_{p^r}^{(p-1)p^{r-1}-1}), \end{aligned}$$

o que prova o resultado. ■

Lema 3.14. *([5], p. 31) Seja p um número primo e r um número natural, então:*

$$\prod_k (1 - \zeta_{p^r}^k) = p,$$

com $1 \leq k \leq p^r$, tal que $p \nmid k$.

Demonstração. Pela Equação 3.2, segue que $\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$. Portanto, todos os $\zeta_{p^r}^k$, com $1 \leq k \leq p^r$, tal que $p \nmid k$ são raízes de $\Phi_{p^r}(x)$, visto que são raízes de $x^{p^r} - 1$ mas não são raízes de $x^{p^{r-1}} - 1$. Desse modo, $\Phi_{p^r}(x) = \prod_k (x - \zeta_{p^r}^k)$, e existem exatamente $\varphi(p^r) = (p-1)p^{r-1}$ valores de k, uma vez que este é o grau de $\Phi_{p^r}(x)$. Assim, tomando $x = 1$, concluímos que:

$$\Phi_{p^r}(1) = \prod_{k=1;\ p\not| k}^{p^r} (1 - \zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p,$$

o que prova o resultado. ■

Lema 3.15. *([5], p. 29) Sejam $\mathbb{K}$ uma extensão finita de grau n sobre $\mathbb{Q}$ e $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, onde $\alpha_i \in \mathcal{O}_\mathbb{K}$. Se $D(\alpha_1, \ldots, \alpha_n) = d$, então todo elemento de $\mathcal{O}_\mathbb{K}$ pode ser escrito na forma:*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d},$$

onde $m_j \in \mathbb{Z}$ é m_j^2 é divisível por d, para todo $j = 1, \ldots, n$.

Demonstração. Seja $\alpha \in \mathcal{O}_\mathbb{K}$ então $\alpha \in \mathbb{K}$. Sendo assim, como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que existem $a_1, \ldots, a_n \in \mathbb{Q}$, tal que:

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n.$$

Considerando $\sigma_1, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, obtemos um sistema de n equações:

$$\sigma_i(\alpha) = a_1\sigma_i(\alpha_1) + \cdots + a_n\sigma_i(\alpha_n), \text{com } i = 1, \ldots, n.$$

Resolvendo esse sistema pela regra de Cramer, obtemos que as n soluções são dadas por $a_j = \gamma_j\delta$, onde $\delta = det(\sigma_i(\alpha_j))$ e γ_j é o determinante obtido da mesma forma que δ, porém trocando a j-ésima coluna por $\sigma_i(\alpha)$. Note que $\gamma_j \in \mathcal{O}_\mathbb{K}$, para todo $j = 1, \ldots, n$, visto que cada um destes é obtido a partir de operações elementares a partir dos α_i's, que estão em $\mathcal{O}_\mathbb{K}$ por hipótese. Uma vez que o discriminante da base referida no enunciado é $det(\sigma_i(\alpha_j))^2$, concluímos que $d = \delta^2$. Logo, $da_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j \in \mathcal{O}_\mathbb{K}$. Mais do que isso, usando que $\mathbb{Z}$ é integralmente fechado, concluímos que $da_j \in \mathbb{Z}$, para $j = 1, \ldots, n$. Considere $m_j = da_j$, como m_j é inteiro, vamos mostrar que $\frac{m_j^2}{d} \in \mathbb{Z}$. Assim, teremos que m_j^2 é divisível por d. No entanto, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, basta mostrar que $\frac{m_j^2}{d}$ é um inteiro algébrico (de $\mathbb{Q}$). Temos que, $m_j = da_j = \delta\gamma_j$, e portanto, $m_j^2 = (da_j)^2 = (\delta\gamma_j)^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Desta igualdade, $\frac{m_j^2}{d} = \gamma_j^2$, e portanto $\frac{m_j^2}{d}$ é um inteiro algébrico, uma vez que γ_j o é. Sendo assim, $\frac{m_j^2}{d} \in \mathbb{Z}$. Logo, m_j^2 é divisível por d. Concluímos que,

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}, \text{com } m_j \in \mathbb{Z}, \text{e } d|m_j^2, \text{para } j = 1, \ldots, n,$$

o que prova o resultado. ■

Lema 3.16. *([5], p. 31) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um número natural não nulo. Se $D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$, então $d = p^s$, para algum $s \in \mathbb{N}$.*

Demonstração. O p^r-ésimo ciclotômico é dado por:

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}.$$

Sendo assim,

$$x^{p^r} - 1 = \Phi_{p^r}(x)g(x), \text{onde } g(x) = x^{p^{r-1}} - 1.$$

Derivando ambos os lados da equação, temos:

$$p^r x^{p^r-1} = \Phi'_{p^r}(x)g(x) + \Phi_{p^r}(x)g'(x).$$

Tomando $x = \zeta_{p^r}$, obtemos:

$$p^r \zeta_{p^r}^{p^r-1} = \Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}) + \Phi_{p^r}(\zeta_{p^r})g'(\zeta_{p^r}) = \Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}),$$

visto que, $\Phi_{p^r}(\zeta_{p^r}) = 0$. Usando que $\zeta_{p^r}^{p^r-1} = \zeta_{p^r}^{-1}$, da igualdade acima, segue que

$$p^r = \zeta_{p^r}\Phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}).$$

Aplicando a norma obtemos:

$$p^{r(p-1)p^{r-1}} = N(\Phi'_{p^r}(\zeta_{p^r}))N(\zeta_{p^r}g(\zeta_{p^r})).$$

Pela Proposição 2.18, segue que

$$p^{r(p-1)p^{r-1}} = \pm D_{\mathbb{K}/\mathbb{Q}}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1})N(\zeta_{p^r}g(\zeta_{p^r})).$$

Portanto, $d | p^{r(p-1)p^{r-1}}$, ou seja, $d = p^s; s \in \mathbb{N}$. ■

A seguir, provaremos dois resultados já conhecidos no estudo dos corpos ciclotômicos.

Lema 3.17. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r um inteiro positivo. Então, $p\mathcal{O}_{\mathbb{K}} = (1-\zeta_{p^r})^n\mathcal{O}_{\mathbb{K}}$, onde $n = (p-1)p^{r-1}$. Logo, $\mathfrak{p}$ se ramifica completamente em $\mathbb{K}$.*

Demonstração. Vamos provar que existe um elemento ε de $\mathcal{O}_{\mathbb{K}}$, invertível, tal que $p = (1-\zeta_{p^r})^n\varepsilon$. Consideremos $I = \{0 < i < p^r;\ mdc(i, p^r) = 1\}$. Pelo Lema 3.14, segue que

$$p = \prod_{i\in I}(1 - \zeta_{p^r}^i).$$

Para todo $i \in I$,

$$(1 - \zeta_{p^r}^i) = (1 - \zeta_{p^r})(1 + \zeta_{p^r} + \zeta_{p^r}^2 + \cdots + \zeta_{p^r}^{i-1}). \tag{3.6}$$

Portanto,

$$p = (1 - \zeta_{p^r})^n \prod_{i\in I}(1 + \zeta_{p^r} + \zeta_{p^r}^2 + \cdots + \zeta_{p^r}^{i-1}).$$

Para cada i, denotemos $\varepsilon_i = (1 + \zeta_{p^r} + \zeta_{p^r}^2 + \cdots + \zeta_{p^r}^{i-1})$. Agora, basta mostrar que ε_i é invertível para todo $i \in I$. Pela Equação 3.6, segue que $\varepsilon_i = \frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}}$. Pela definição do

conjunto de índices, segue que existe $j \in I$, tal que $ij \equiv 1 \ (mod\ p^r)$. Assim,

$$(1-\zeta_{p^r}) = (1-\zeta_{p^r}^{ij}) = (1-(\zeta_{p^r}^{i})^{j}) = (1-\zeta_{p^r}^{i})(1+\zeta_{p^r}^{i}+\zeta_{p^r}^{2i}+\cdots+\zeta_{p^r}^{(j-1)i}).$$

Portanto,

$$\varepsilon_i^{-1} = \frac{1-\zeta_{p^r}}{1-\zeta_{p^r}^{i}} = (1+\zeta_{p^r}^{i}+\zeta_{p^r}^{2i}+\cdots+\zeta_{p^r}^{(j-1)i}) \in \mathcal{O}_{\mathbb{K}}.$$

Tomando $\varepsilon = \prod_{i\in I} \varepsilon_i$, segue que $p = (1-\zeta_{p^r})^n \varepsilon$, onde ε é um elemento invertível de $\mathcal{O}_{\mathbb{K}}$, como queríamos. ■

Corolário 3.18. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r um inteiro positivo. Então,*

$$(1-\zeta_{p^r})^n \mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}, \tag{3.7}$$

onde $n = (p-1)p^{r-1}$.

Demonstração. Utilizando o Lema 3.17, provaremos que

$$p\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}.$$

Temos que:

$$p\mathbb{Z} \subset \mathbb{Z} \text{ e } p\mathbb{Z} \subset p\mathcal{O}_{\mathbb{K}} \Rightarrow p\mathbb{Z} \subset p\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}.$$

Por outro lado, seja α um elemento da interseção entre $p\mathcal{O}_{\mathbb{K}}$ e $\mathbb{Z}$. Assim, $\alpha = p\alpha'$, para algum α' em $\mathcal{O}_{\mathbb{K}}$. Deste modo,

$$\alpha' = \frac{\alpha}{p} \in \mathcal{O}_{\mathbb{K}}.$$

Uma vez que p e α são inteiros, concluímos que α' é racional. Como $\mathbb{Q} \cap \mathcal{O}_{\mathbb{K}} = \mathbb{Z}$, concluímos que α' pertence a $\mathbb{Z}$. Visto que $\alpha = p\alpha'$, segue que α é um elemento de $p\mathbb{Z}$.■

Uma observação importante é que para o caso em que $r = 1$, isto é, $\mathbb{K} = \mathbb{Q}(\zeta_p)$, podemos afirmar que

$$(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}. \tag{3.8}$$

De fato, uma vez que $(1-\zeta_p)^n \mathcal{O}_{\mathbb{K}}$, onde $n = (p-1)p^{r-1}$, está contido em $(1-\zeta_p)\mathcal{O}_{\mathbb{K}}$, pelo Corolário 3.18, segue a inclusão

$$p\mathbb{Z} \subset (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$$

Para a outra inclusão, vamos usar o fato de que $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$. Note que o elemento 1 pertence a $\mathbb{Z}$, por outro lado, 1 não pertence a $(1-\zeta_p)\mathcal{O}_{\mathbb{K}}$, já que $(1-\zeta_p)$

não é um elemento invertível de $\mathcal{O}_{\mathbb{K}}$. Daí, 1 não pertence a $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} \neq \mathbb{Z}$, e pela maximalidade do ideal $p\mathbb{Z}$, concluímos que $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

Teorema 3.19. *([5], p. 30) Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, com p primo e r inteiro positivo. Então, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ e $\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ como um $\mathbb{Z}$-módulo.*

Demonstração. Mostremos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}]$. Assim, temos a validade do resultado pelo Lema 3.13. Suponhamos que $\mathcal{O}_{\mathbb{K}} \neq \mathbb{Z}[1-\zeta_{p^r}]$. Visto que, $\mathbb{Z}[1-\zeta_{p^r}] \subset \mathcal{O}_{\mathbb{K}}$, vamos supor por absurdo que $\mathcal{O}_{\mathbb{K}} \not\subset \mathbb{Z}[1-\zeta_{p^r}]$. Assim, seja $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\alpha \notin \mathbb{Z}[1-\zeta_{p^r}]$. Considerando a base $\{1, 1-\zeta_{p^r}, \ldots, (1-\zeta_{p^r})^{n-1}\}$, onde $n = \varphi(p^r) = (p-1)p^{r-1}$ e d o discriminante, pelo Lema 3.15, podemos escrever α da seguinte maneira:

$$\alpha = \frac{m_0 + m_1(1-\zeta_{p^r}) + \cdots + m_{n-1}(1-\zeta_{p^r})^{n-1}}{d}.$$

Com $m_j \in \mathbb{Z}$, para todo $j = 0, \ldots, n$. Além disso, pelo Lema 3.16, $d = p^s$, para algum $s \in \mathbb{Z}$. Portanto,

$$\alpha p^s = m_0 + m_1(1-\zeta_{p^r}) + \cdots + m_{n-1}(1-\zeta_{p^r})^{n-1}.$$

Para cada $i = 1, \ldots, n-1$, podemos reecrever $m_i = p^{\lambda_i}.m_i'$ tal que $m_i' \in \mathbb{Z}$ e $p \nmid m_i'$. Por outro lado, pelo Lema 3.17, segue que existe $\varepsilon \in \mathcal{O}_{\mathbb{K}}$ de modo que $p = (1-\zeta_{p^r})^n\varepsilon$, e portanto, $\alpha((1-\zeta_{p^r})^n\varepsilon)^s$ é igual a:

$$((1-\zeta_{p^r})^n\varepsilon)^{\lambda_0}m_0' + ((1-\zeta_{p^r})^n\varepsilon)^{\lambda_1}m_1'(1-\zeta_{p^r}) + \cdots + ((1-\zeta_{p^r})^n\varepsilon)^{\lambda_{n-1}}m_{n-1}'(1-\zeta_{p^r})^{n-1},$$

que por sua vez é o mesmo que

$$(1-\zeta_{p^r})^{n\lambda_0}m_0^* + (1-\zeta_{p^r})^{n\lambda_1+1}m_1^* + \cdots + (1-\zeta_{p^r})^{n\lambda_{n-1}+n-1}m_{n-1}^*, \tag{3.9}$$

onde $m_i^* = m_i'\varepsilon^{\lambda_i} \in \mathcal{O}_{\mathbb{K}}$. Afirmamos que os expoentes de $(1-\zeta_{p^r})$ do lado direito da igualdade são todos distintos, isto é, $n\lambda_i + i = n\lambda_j + j$ se, e somente se, $i = j$. De fato,

$$n\lambda_i + i = n\lambda_j + j \Leftrightarrow n(\lambda_i - \lambda_j) = j - i.$$

Logo, $j-i$ é um múltiplo de n. Porém, $|j-i| \leq n-1$, visto que $i, j \in \{0, 1, \ldots, n-1\}$. Sendo assim, o único múltiplo nessas condições é $j-i = 0$, ou seja, $i = j$, verificando a afirmação. Neste contexto, denotaremos o ideal primo $(1-\zeta_{p^r})\mathcal{O}_{\mathbb{K}}$ por $\mathfrak{p}$. Desta afirmação, concluímos então que $v_{\mathfrak{p}}((1-\zeta_{p^r})^{n\lambda_0}m_0^* + (1-\zeta_{p^r})^{n\lambda_1+1}m_1^* + \cdots + (1-\zeta_{p^r})^{n\lambda_{n-1}+n-1}m_{n-1}^*) = min\{n\lambda_i + i; i = 0, \ldots, n-1\}$. Além disso, se $n\lambda_k + k = min\{n\lambda_i + i; i = 0, \ldots, n-1\}$, então $\lambda_k \leq \lambda_i$ para todo $i = 0, \ldots, n-1$, uma vez que

$$n\lambda_k + k < n\lambda_i + i \Leftrightarrow n(\lambda_k - \lambda_i) < k - i \Leftrightarrow (\lambda_k - \lambda_i) < \frac{k-i}{n} < 1 \Leftrightarrow \lambda_k \leq \lambda_i,$$

para todo $i = 0, \ldots, n-1$. Agora, vamos analisar a valorização $\mathfrak{p}$-ádica de ambos os lados da igualdade obtida na Equação 3.9. Por um lado,

$$v_{\mathfrak{p}}(\alpha((1-\zeta_{p^r})^n\varepsilon)^s) = v_{\mathfrak{p}}(\alpha\varepsilon^s) + v_{\mathfrak{p}}((1-\zeta_{p^r})^{ns}) = v_{\mathfrak{p}}(\alpha\varepsilon^s) + ns.$$

Pelo outro, do que foi mencionado anteriormente,

$$v_{\mathfrak{p}}((1-\zeta_{p^r})^{n\lambda_0}m_0^* + (1-\zeta_{p^r})^{n\lambda_1+1}m_1^* + \cdots + (1-\zeta_{p^r})^{n\lambda_{n-1}+n-1}m_{n-1}^*) \geq n\lambda_k + k.$$

Sendo assim,

$$n\lambda_k + k = v_{\mathfrak{p}}(\alpha\varepsilon^s) + ns \Leftrightarrow n(\lambda_k - s) + k = v_{\mathfrak{p}}(\alpha\varepsilon^s) > 0.$$

Note que, $k < n$, uma vez que se $\lambda_k - s < 0$ teríamos que $|n.(\lambda_k - s)| < k$, o que é um absurdo. Assim,

$$v_{\mathfrak{p}}(\alpha\varepsilon^s) + ns \Leftrightarrow n(\lambda_k - s) + k = v_{\mathfrak{p}}(\alpha\varepsilon^s) > 0 \Rightarrow \lambda_k - s \geq 0.$$

Logo, $\lambda_k \geq s$. Portanto, $s \leq \lambda_k \leq \lambda_i$ para todo $i = 0, \ldots, n-1$. Assim, $p^s | p^{\lambda_i}$. Logo, $p^s | m_i$ para todo $i = 0, \ldots, n-1$, como queríamos. ■

Teorema 3.20. *([11], p. 9) O discriminante de $\mathbb{Q}(\zeta_{p^r})$ é dado por*

$$\begin{cases} -p^{(pr-r-1)\cdot p^{(r-1)}}, & \text{se } p^r = 4 \text{ ou } p \equiv 3 \ mod(4) \\ p^{(pr-r-1)\cdot p^{(r-1)}}, & \text{caso contrário.} \end{cases}$$

Lema 3.21. *Sejam $\mathbb{L}$ e $\mathbb{K}$ corpos de números, tais que seus discriminantes são relativamente primos e que os corpos são linearmente disjuntos, isto é, se $\{w_1, \ldots, w_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ e $\{v_1, \ldots, v_m\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, então $\{w_i v_j\}$ é uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$. Então,*

$$\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} \text{ e } D_{\mathbb{KL}} = D_{\mathbb{K}}^m D_{\mathbb{L}}^n.$$

Teorema 3.22. *([11], p. 11) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_n]$.*

Demonstração. Seja $\mathbb{Q}(\zeta_n)$, onde $n = a_1 a_2 \cdots a_s$, sendo $a_i = p_i^{r_i}$, com p_i primo e r_i natural não nulo. Vamos provar por indução em s. Se $s = 1$, temos que $n = a_1 = p_1^{r_1}$, daí pelo Teorema 3.19, segue o resultado. Suponhamos por hipótese de indução que vale para s,

isto é, se $n = a_1 a_2 \cdots a_s$ então $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. Provemos para $s+1$. Seja $m = a_1 \cdots a_s a_{s+1}$. Note que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_{a_{s+1}})$. Pelo Lema 3.21, obtemos que

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}\mathcal{O}_{\mathbb{Q}(\zeta_{a_{s+1}})},$$

e portanto,

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_n]\mathbb{Z}[\zeta_{a_{s+1}}] = \mathbb{Z}[\zeta_m],$$

concluindo a demonstração. ■

Teorema 3.23. *([11], p. 12) O discriminante de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é dado por:*

$$D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Demonstração. Pelo Lema 3.21, dados dois corpos de números linearmente disjuntos, $\mathbb{K}$ e $\mathbb{L}$, tais que seus discriminantes são relativamente primos, segue que

$$D(\mathbb{K}\mathbb{L}) = D(\mathbb{K})^{[\mathbb{L}:\mathbb{Q}]} D(\mathbb{L})^{[\mathbb{K}:\mathbb{Q}]}.$$

Colocando o módulo e aplicando a função logaritmo em ambos os lados da igualdade, obtemos:

$$log|D(\mathbb{K}\mathbb{L})| = log|D(\mathbb{K})|^{[\mathbb{L}:\mathbb{Q}]}.|D(\mathbb{L})|^{[\mathbb{K}:\mathbb{Q}]} = [\mathbb{L}:\mathbb{Q}]log|D(\mathbb{K})| + [\mathbb{K}:\mathbb{Q}]log|D(\mathbb{L})|.$$

Dividindo ambos os lados por $[\mathbb{K}\mathbb{L}:\mathbb{Q}]$, obtemos:

$$\frac{log|D(\mathbb{K}\mathbb{L})|}{[\mathbb{K}\mathbb{L}:\mathbb{Q}]} = \frac{log|D(\mathbb{K})|}{[\mathbb{K}:\mathbb{Q}]} + \frac{log|D(\mathbb{L})|}{[\mathbb{L}:\mathbb{Q}]}.$$

Agora, basta decompor n em fatores primos. Considerando $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, observemos que $\mathbb{Q}(\zeta_{p_i^{\alpha_i}})$ e $\mathbb{Q}(\zeta_{p_j^{\alpha_j}})$, satisfazem as condições do Lema 3.21, para $i, j \in \{1, \ldots, s\}$ sempre que $i \neq j$. Uma vez que $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$, substituindo na igualdade anterior, obtemos:

$$\begin{aligned}
\frac{log|D(\mathbb{Q}(\zeta_n))|}{\varphi(n)} &= \frac{log|D(\mathbb{Q}(\zeta_{p_1^{\alpha_1}}))|}{\varphi(p_1^{\alpha_1})} + \cdots + \frac{log|D(\mathbb{Q}(\zeta_{p_s^{\alpha_s}}))|}{\varphi(p_s^{\alpha_s})} \\
&= \sum_{i=1}^{s} \frac{log\ p_i^{p_i^{\alpha_i-1}(p_i\alpha_i-\alpha_i-1)}}{p_i^{\alpha_i-1}(p_i-1)} = \sum_{i=1}^{s} \frac{p_i^{\alpha_i-1}(p_i\alpha_i-\alpha_i-1)(log\ p_i)}{p_i^{\alpha_i-1}(p_i-1)} \\
&= \sum_{i=1}^{s} \frac{(p_i\alpha_i-\alpha_i-1)(log\ p_i)}{(p_i-1)} = \sum_{i=1}^{s} \frac{(\alpha_i(p_i-1)-1)(log\ p_i)}{(p_i-1)} \\
&= \sum_{i=1}^{s} (\alpha_i - \frac{1}{(p_i-1)})(log\ p_i) = \sum_{i=1}^{s} \alpha_i log\ p_i - \sum_{i=1}^{s} \frac{log\ p_i}{(p_i-1)} \\
&= \sum_{i=1}^{s} log\ p_i^{\alpha_i} - \sum_{i=1}^{s} log\ p_i^{\frac{1}{p_i-1}} = log \prod_{i=1}^{s} p_i^{\alpha_i} - log \prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}} \\
&= log\ n - log \prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}} = log \frac{n}{\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}}.
\end{aligned}$$

Da igualdade acima, concluímos que:

$$log|D(\mathbb{Q}(\zeta_n))| = \varphi(n)\left(log \frac{n}{\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}}\right) = \left(log \frac{n}{\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}}\right)^{\varphi(n)}.$$

Pela injetividade da função logaritmo, segue que:

$$|D(\mathbb{Q}(\zeta_n))| = \left(\frac{n}{\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}}\right)^{\varphi(n)} \Rightarrow D(\mathbb{Q}(\zeta_n)) = (-1)^{\frac{\varphi(n)}{2}} \left(\frac{n}{\prod_{i=1}^{s} p_i^{\frac{1}{p_i-1}}}\right)^{\varphi(n)}.$$

Por fim, segue que

$$D(\mathbb{Q}(\zeta_n)) = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}},$$

o que prova o resultado. ■

3.3 O GRUPO DE GALOIS

Denotaremos o grupo de Galois de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ por G_n. Note que tomando σ qualquer em G_n, temos:

$$\sigma\left(\sum a_i\zeta_n^i\right) = \sum \sigma(a_i\zeta_n^i) = \sum \sigma(a_i)\sigma(\zeta_n^i) = \sum a_i\sigma(\zeta_n)^i.$$

Portanto, para determinarmos o automorfismo σ, basta verificar $\sigma(\zeta_n)$.

Teorema 3.24. *([9], p. 39) Se $n \in \mathbb{N}$, então o grupo de Galois G_n de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é $G_n \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.*

A demonstração do Teorema 3.24 pode ser feita considerando $f : \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \to G_n$, dada por $f(\overline{j}) = \sigma_j$, onde esta aplicação está bem definida e é um isomorfismo.

Teorema 3.25. *([9], p. 44) O grupo multiplicativo $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ é cíclico se, e somente se, $n = 2, 4, p^r$ ou $2p^r$, onde p é um primo ímpar e $r \geq 1$.*

Teorema 3.26. *([12], p. 28) Se G é um grupo cíclico de ordem n, então existe um único subgrupo de ordem d para cada divisor d de n.*

Demonstração. Seja $G =< a >$ tal que $a^n = 1$. Como $d|n$, segue que $\frac{n}{d} \in \mathbb{Z}$. Assim, considerando $H =< a^{\frac{n}{d}} >$, segue que H é um subgrupo de G, de ordem d, pois $(a^{\frac{n}{d}})^d = a^n = 1$. Suponhamos que exista $K =< b >$ subgrupo de G tal que $|K| = d$. Uma vez que K é subgrupo de G, segue que $b \in G$. Logo, $b = a^m$, para algum $m \in \mathbb{Z}$. Como a ordem de K é d, segue que $1 = b^d = (a^m)^d = a^{md}$. Por outro lado, $a^n = 1$, e portanto, segue que existe $k \in \mathbb{Z}$ tal que $md = nk$. Portanto, $b = a^m = (a^{\frac{n}{d}})^k$, ou seja, $b \in G$. Como ambos subgrupos têm a mesma ordem, e $b \in G$, podemos concluir que $H = K$. ■

A seguir, mostraremos um resultado conhecido da Teoria de Grupos.

Proposição 3.27. *Seja G um grupo cíclico gerado por a de ordem n. Se d é um divisor de n, então o subgrupo H de G de ordem $c = \frac{n}{d}$ é o conjunto de todos os elementos b de G tal que $b^c = 1$, isto é, $H = \langle a^d \rangle$.*

Demonstração. Seja $c = \frac{n}{d}$, assim $d = \frac{n}{c}$. Pelo Teorema 3.26, existe um único subgrupo H de G com ordem c. Seja $b \in G$ tal que $b^c = 1$. Como G é cíclico gerado por a, existe $m \in \mathbb{Z}$ tal que $b = a^m$. Logo,

$$b^c = (a^m)^c = a^{mc} = 1.$$

Como $o(a) = n$, temos que $a^{mc} = 1$ se, e somente se, $n \mid mc$. Ou seja, existe $k \in \mathbb{Z}$ tal que $mc = kn$, o que implica

$$m = k \cdot \frac{n}{c} = kd.$$

Portanto,

$$b = a^m = a^{kd} = (a^d)^k \in \langle a^d \rangle = H.$$

Isso mostra que todo elemento $b \in G$ tal que $b^c = 1$ pertence a H. Reciprocamente, qualquer elemento de $H = \langle a^d \rangle$ é da forma a^{kd} para algum $k \in \mathbb{Z}$, e então:

$$(a^{kd})^c = a^{kdc} = a^{kn} = 1.$$

Logo, $b^c = 1$ para todo $b \in H$. Segue que

$$\{b \in G \mid b^c = 1\} = \langle a^d \rangle = H.$$

O que prova o resultado. ■

Seja $\mathbb{K} = \mathbb{Q}(\zeta_n)$. Pelo Teorema 3.24, concluímos que $\mathbb{K}$ é um corpo abeliano, visto que $o(G_n) = \varphi(n) = [\mathbb{K} : \mathbb{Q}]$, e G_n é abeliano. Além disso, pelo Teorema 2.17 (Teorema fundamental da Teoria de Galois), concluímos que todo corpo intermediário de um corpo ciclotômico também é um corpo abeliano. Enfim, chegamos ao esperado teorema que fala sobre a recíproca dessa afirmação.

Teorema 3.28 (Kronecker-Weber)**.** *([9], p. 273.) Se $\mathbb{K}$ um corpo de números abeliano, então $\mathbb{K}$ está contido em um corpo ciclotômico.*

Este resultado é primordial para dar continuidade no estudo dos corpos abelianos, e devido a este teorema é que podemos tratar um corpo abeliano do ponto de vista onde este é um corpo intermediário de uma extensão ciclotômica, esse resultado permite utilizar de outras ferramentas já conhecidas sobre corpos intermediários.

3.4 SUBCORPOS DOS CORPOS CICLOTÔMICOS

Nesta seção, abordaremos alguns subcorpos dos corpos ciclotômicos, dando enfoque ao subcorpo real maximal e aos corpos abelianos com condutor primo. Considerando o $n-$ésimo corpo ciclotômico $\mathbb{Q}(\zeta_n)$, o maior subcorpo de $\mathbb{Q}(\zeta_n)$ contido nos reais é denotado por $\mathbb{Q}(\zeta_n)^+$, isto é, $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Sabemos que $\zeta_n^{n-1} = \zeta_n^{-1}$, visto que $\zeta_n^{n-1} \cdot \zeta_n = \zeta_n^n = 1$. Além disso, podemos verificar que ζ_n^{-1} é o conjugado de ζ_n. Uma vez que $\zeta_n^{-1} = (cos\frac{2\pi}{n} + isen\frac{2\pi}{n})^{-1} = cos\frac{2\pi}{n} - isen\frac{2\pi}{n} = \overline{\zeta_n}$. Sendo assim, consideremos σ_1 a identidade e σ_{n-1} a conjugação complexa, onde estas duas imersões sempre fixam qualquer subcorpo real. Pela Teoria de Galois obtemos a seguinte associação:

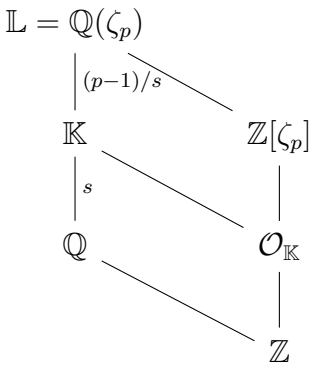
$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & \text{———} & \{\sigma_1\} \\ | & & | \\ \mathbb{Q}(\zeta_n)^+ & \text{——} & H = \{\sigma_1, \sigma_{n-1}\} \\ | & & | \\ \mathbb{Q} & \text{———} & G \end{array}$$

Por outro lado, sabemos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ e como $o(H) = 2$, pelo Teorema Fundamental da Teoria de Galois, concluímos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$. Sabendo disso, vamos determinar um elemento primitivo para $\mathbb{Q}(\zeta_n)^+$. Do que foi exposto anteriormente, temos que $\zeta_n + \zeta_n^{-1} \in \mathbb{R}$ e $\zeta_n + \zeta_n^{-1} \in \mathbb{Q}(\zeta_n)$. Note que ζ_n é raiz do polinômio mônico irredutível $p(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$, sendo este um polinômio com coeficientes em $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Afirmamos que $p(x)$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. De fato, se o polinômio $p(x)$ não fosse o minimal, como $p(x)$ é mônico e irredutível, segue que o minimal tem grau 1, o que é um absurdo já que $\zeta_n \notin \mathbb{R}$ e $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é totalmente real (pois $\zeta_n + \zeta_n^{-1} \in \mathbb{R}$). Sendo assim, concluímos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2 = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})]$.

Além disso, $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)^+$, já que por definição $\mathbb{Q}(\zeta_n)^+$ é o maior subcorpo de $\mathbb{Q}(\zeta_{\zeta_n})$ que contém os reais. Dos dois fatos mencionados anteriormente, podemos concluir que $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Proposição 3.29. *([11], p. 16) Se $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Seja $\mathbb{K}$ um corpo de números abeliano. Na Seção 3.3, vimos que de acordo com o Teorema de Kronecker-Weber, existe um corpo ciclotômico que contém $\mathbb{K}$. O menor número inteiro n tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ é chamado o **condutor** de $\mathbb{K}$. Estudaremos, nesta seção, corpos de números tal que o condutor é um número primo. Seja p o condutor de $\mathbb{K}$. Vimos também que $o(Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})) = p - 1$ e que este grupo é cíclico. Considerando σ_g um gerador de $Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, isto é, $\overline{g}$ é um gerador para o grupo $\left(\frac{\mathbb{Z}}{(p-1)\mathbb{Z}}\right)^*$. Assim, obtemos o subgrupo $H = \{\sigma_g^{(p-1)/d}, \sigma_g^{2(p-1)/d}, \ldots, \sigma_g^{d(p-1)/d} = Id\}$.



A seguir, provaremos um resultado da Teoria Algébrica dos Números.

Teorema 3.30. *Seja um corpo de números $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, tal que p é um primo ímpar e $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = d$, $t = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$. Se σ_g gera $G = Gal(\mathbb{Q}(\zeta_p) : \mathbb{Q})$, então, $\mathbb{K} = \mathbb{Q}(t)$ e o conjunto $\{t, \sigma_g(t), \sigma_g^2(t), \ldots, \sigma_g^{s-1}(t)\}$ é uma base integral para $\mathbb{K}$.*

Demonstração. Primeiramente, mostremos que $\mathbb{K} = \mathbb{Q}(t)$. Seja $s = (p-1)/d$. Uma vez que $t = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$ segue que $t \in \mathcal{O}_\mathbb{K}$. Portanto $\mathbb{Q}(t) \subset \mathbb{K}$. Sendo assim, obtemos a cadeia $\mathbb{Q} \subset \mathbb{Q}(t) \subset \mathbb{K} \subset \mathbb{Q}(\zeta_p)$. Vamos analisar o traço de ζ_p sobre $\mathbb{Q}$, usando suas propriedades. Assim, como $t = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p)$, segue que

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = Tr_{\mathbb{Q}(t)/\mathbb{Q}}(Tr_{\mathbb{K}/\mathbb{Q}(t)}(Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\zeta_p))) = Tr_{\mathbb{Q}(t)/\mathbb{Q}}(Tr_{\mathbb{K}/\mathbb{Q}(t)}(t)).$$

Como $t \in \mathbb{Q}(t)$, concluímos que $Tr_{\mathbb{K}/\mathbb{Q}(t)}(t) = [\mathbb{K} : \mathbb{Q}(t)] \cdot t$. Pela Equação 3.3, segue que $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$. Substituindo na igualdade acima, chegamos que

$$[\mathbb{K} : \mathbb{Q}(t)] \cdot Tr_{\mathbb{Q}(t)/\mathbb{Q}}(t) = -1$$

Por fim, como $s, Tr_{\mathbb{Q}(t)/\mathbb{Q}}(t) \in \mathbb{Z}$, concluímos que $[\mathbb{K} : \mathbb{Q}(t)] = \pm 1$. Como o grau da extensão é sempre positivo, concluímos que $[\mathbb{K} : \mathbb{Q}(t)] = 1$. Como $\mathbb{Q}(t) \subset \mathbb{K}$, concluímos que $\mathbb{K} = \mathbb{Q}(t)$.

Mostremos agora, que $\mathcal{O}_{\mathbb{K}} = \{a_1\theta(t) + \cdots + a_{(p-1)/d}\theta^{(p-1)/d}(t); a_i \in \mathbb{Z}\}$. Como $t \in \mathcal{O}_{\mathbb{K}}$, segue que $\theta^i(t) \in \mathbb{Z}[\zeta_p] \cap \mathbb{K}$, para todo $i = 1, \ldots, (p-1)/d$. Portanto, $\{a_1\theta(t) + \cdots + a_{(p-1)/d}\theta^{(p-1)/d}(t); a_i \in \mathbb{Z}\} \subset \mathcal{O}_{\mathbb{K}}$. Agora, seja $x \in \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$, segue que existem $a_1, \ldots, a_{p-1} \in \mathbb{Z}$ tal que:

$$x = \sum_{i=1}^{p-1} a_i \zeta_p^i.$$

Por outro lado, podemos reordenar os $\zeta_p^{i's}$ da seguinte maneira:

$$\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\} = \left\{ \begin{array}{ccccc} \sigma_g(\zeta_p), & \sigma_g^2(\zeta_p), & \ldots, & \sigma_g^s(\zeta_p), \\ \sigma_g^{s+1}(\zeta_p), & \sigma_g^{s+2}(\zeta_p), & \ldots, & \sigma_g^{2s}(\zeta_p), \\ & \vdots & & \\ \sigma_g^{(d-1)s+1}(\zeta_p), & \sigma_g^{(d-1)s+2}(\zeta_p), & \ldots, & \sigma_g^{ds}(\zeta_p) \end{array} \right\}$$

Note que a soma dos elementos na coluna s é exatamente t. Assim, a soma da $i-$ésima coluna é exatamente $\sigma_g^i(t)$. Podemos reescrever

$$\begin{aligned} x = \quad & b_1\sigma_g(\zeta_p) + \cdots + b_{(d-1)s+1}\sigma_g^{(d-1)s+1}(\zeta_p) + \\ & + b_2\sigma_g^2(\zeta_p) + \cdots + b_{(d-1)s+2}\sigma_g^{(d-1)s+2}(\zeta_p) + \\ & \vdots \\ & + b_s\sigma_g^s(\zeta_p) + \cdots + b_{ds}\sigma_g^{ds}(\zeta_p), \end{aligned}$$

onde para todo índice j, $b_j = a_i$ para algum $i \in \{1, \ldots, p-1\}$. Vamos mostrar que $b_k = b_j$ para todo $k \equiv j \ (mod\ s)$. Para isso, tomemos $\overline{k}$ uma classe de congruência módulo s. Visto que σ_g^s fixa os elementos de $\mathbb{K}$, segue que

$$\sigma_g^s(b_k\sigma_g^k(\zeta_p) + \cdots + b_{(d-1)s+k}\sigma_g^{(d-1)s+k}(\zeta_p)) = b_k\sigma_g^k(\zeta_p) + \cdots + b_{(d-1)s+k}\sigma_g^{(d-1)s+k}(\zeta_p).$$

Por outro lado,

$$\sigma_g^s(b_k\sigma_g^k(\zeta_p) + \cdots + b_{(d-1)s+k}\sigma_g^{(d-1)s+k}(\zeta_p)) = b_k\sigma_g^{s+k}(\zeta_p) + \cdots + b_{(d-1)s+k}\sigma_g^k(\zeta_p)).$$

Repetindo o mesmo processo d vezes, obtemos que:

$$b_k = b_{s+k} = \cdots = b_{(d-1)s+k}.$$

Portanto,

$$\begin{aligned} x &= b_1 \sum_{k=0}^{d-1} \sigma_g^{ks+1}(\zeta_p) + \cdots + b_s \sum_{k=0}^{d-1} \sigma_g^{ks}(\zeta_p) \\ &= b_1\sigma_g(t) + \cdots + b_{s-1}\sigma_g^{s-1}(t) + b_s t. \end{aligned}$$

Como $b_k \in \mathbb{Z}$, para todo $k = 1, \ldots, s$, concluímos que x é escrito como combinação linear de $\{t, \sigma_g(t), \sigma_g^2(t), \ldots, \sigma_g^{s-1}(t)\}$ com coeficientes inteiros, como queríamos. ■

4 RETICULADOS ALGÉBRICOS

Na matemática, existem vários problemas clássicos, que são estudados há muito tempo, onde um deles é chamado "o problema do empacotamento esférico". Acredita-se que a primeira aparição deste foi no início do século XVII, no manuscrito "The Six-Cornered Snowflake", de Johannes Kepler, inspirado por Thomas Harriot, com a motivação de qual seria a melhor forma de empilhar esferas. O problema consiste basicamente em buscar qual é a melhor maneira, em termos de densidade, de dispor esferas de mesmo raio que se intersectam em no máximo um ponto, para preencher um espaço. Para $\mathbb{R}$, o conjunto de todos os intervalos fechados de raio $1/2$ com centro nos números inteiros é um exemplo de empacotamento esférico neste espaço. Abaixo, exemplificamos um recorte de um empacotamento esférico para o $\mathbb{R}^2$.

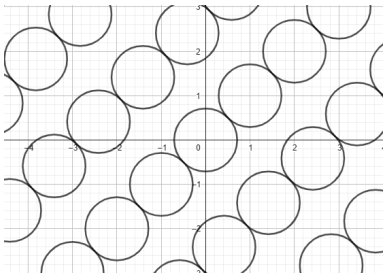


Figura 4.1: Exemplo de empacotamento esférico
Fonte: Autoria Própria

Contudo, podemos generalizar o problema para dimensões maiores, fazendo o mesmo questionamento para esferas $n-$dimensionais idênticas distribuídas no $\mathbb{R}^n$, de modo que a interseção entre quaisquer duas tenha no máximo um ponto. Temos diversas perguntas que podem ser feitas acerca deste problema. Algumas delas são, se o problema já foi resolvido para dimensões maiores e se é possível obter uma estimativa de quanto a melhor disposição cobre o espaço todo. Atualmente, tirando a dimensão 1 na qual é uma trivialidade, o problema está resolvido apenas para algumas dimensões. Além disso, em empacotamentos esféricos que seguem um determinado padrão é possível verificar a porcentagem do espaço todo que é coberto por este. A seguir, estudaremos alguns conceitos que irão ajudar a obter empacotamentos esféricos em várias dimensões, e no decorrer do capítulo explicaremos como é feito o cálculo de quanto cada um deles cobre do respectivo

espaço.

4.1 RETICULADOS

Existem diferentes maneiras de obtermos um empacotamento esférico. Uma é utilizando os reticulados, o qual se mostrou muito eficaz, tendo em vista que para a maioria das dimensões, o empacotamento esférico mais denso é obtido dessa forma. Nesta seção iremos formalizar alguns conceitos, e exibiremos alguns métodos que serão úteis neste contexto. Sejam n um inteiro positivo e $\{v_1, \ldots, v_m\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ sobre $\mathbb{R}$. Definimos o **reticulado** Λ de posto m e base $\{v_1, \ldots, v_m\}$ como sendo o conjunto

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

Estaremos interessados no caso em que $n = m$. Um reticulado que satisfaz essa condição é chamado **reticulado completo**. Daqui para frente trabalharemos apenas sob esta condição, e assim, por simplicidade chamaremos um reticulado completo apenas de reticulado.

Exemplo 4.1. Um dos exemplos mais triviais de reticulado é $\mathbb{Z}^2$. Isto é, considerando $\mathcal{B} = \{(1,0),(0,1)\}$, as combinações lineares com coeficientes inteiros destes vetores é exatamente o conjunto $\{(a,b); a,b \in \mathbb{Z}\}$, segue ilustrado um recorte:

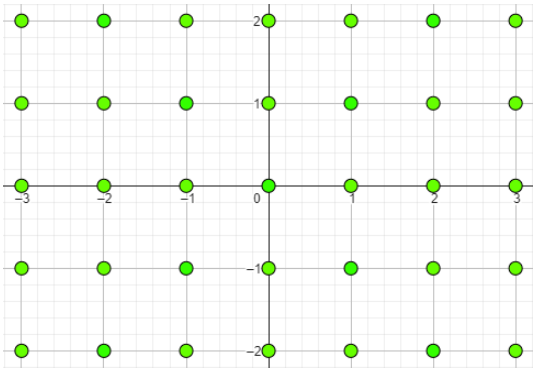


Figura 4.2: Ilustração de um reticulado no plano real.
Fonte: Autoria própria

Seja $H \subset \mathbb{R}^n$ um subgrupo aditivo. Diremos que H é um **subgrupo discreto** se para qualquer conjunto compacto $K \subset \mathbb{R}^n$, $H \cap K$ é um conjunto finito.

Teorema 4.2. *([4], p. 53) O conjunto $\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, Λ é um subgrupo aditivo discreto.*

Com essas informações, já podemos ter uma noção de como obter um empacotamento esférico por meio de reticulados. Conforme o Teorema 4.2, um reticulado Λ é um subgrupo

aditivo discreto do $\mathbb{R}^n$. O fato de ser discreto permite tomar uma vizinhança aberta V de um ponto deste reticulado, de modo que V não contém outro ponto de Λ. Por outro lado, como Λ é um subgrupo, ao tomarmos a norma do elemento de menor comprimento, saberemos que esta é a menor distância possível entre quaisquer dois pontos de Λ, o que torna possível tomar metade desta distância e torná-la o raio de esferas centradas em cada ponto deste reticulado. Assim, cada esfera não terá interseção a menos de um ponto. Neste contexto, diremos que um empacotamento esférico é um **empacotamento reticulado** quando o conjunto dos centros das esferas forma um reticulado em $\mathbb{R}^n$. No decorrer do capítulo, apresentaremos uma maneira interessante de construir empacotamentos reticulados.

Dado um reticulado Λ em $\mathbb{R}^n$, ao maior raio, para o qual seja possível definir um empacotamento de Λ, definimos o **raio de empacotamento** de Λ, denotado por ρ, e dado por:

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

Agora, considerando $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base de Λ, o conjunto

$$\mathcal{R}(\mathcal{B}) = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{n} \lambda_i v_i; 0 \leq \lambda_i < 1, \forall i = 1, \ldots, n \right\},$$

é chamado **região fundamental** de Λ com relação à base $\mathcal{B}$.

Para exemplificar esse conceito, consideremos o reticulado de $\mathbb{R}^2$ que é gerado pela $\mathbb{Z}$-base $\mathcal{B} = \{(1,1), (\sqrt{2}, -\sqrt{2})\}$. Na figura abaixo, destacado em azul temos uma região fundamental com relação a esta base.

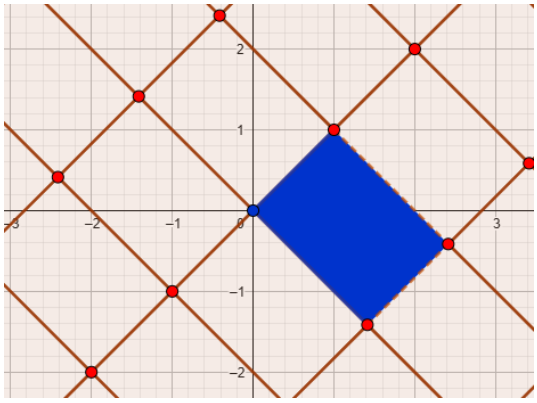


Figura 4.3: Região fundamental de um reticulado.
Fonte: Autoria própria

Seja $\Lambda \subset \mathbb{R}^n$ com base $\mathcal{B} = \{v_1, \ldots, v_n\}$. Seja $v_j = (v_{1j}, v_{2j}, \ldots, v_{nj})$ a expressão em coordenadas reais de cada vetor dessa base. A matriz $M = [v_{ij}]_{1 \leq i,j \leq n}$ é chamada **matriz geradora** de Λ.

Consideremos μ a medida de Lebesgue em $\mathbb{R}^n$. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com região fundamental $\mathcal{P}$. O **volume do reticulado** Λ é definido como sendo:

$$v(\Lambda) = v(\mathcal{P}) = \mu(\mathcal{P}) = \int_{\mathcal{P}} d\mu.$$

A seguir, nos próximos dois resultados mostraremos que $v(\mathcal{P})$ independe da base escolhida, e assim, não teremos problemas com essa definição, podendo assim denotar o volume do reticulado tanto por $v(\mathcal{P})$ quanto por $v(\Lambda)$.

Proposição 4.3. *([13], p. 186) Se M é uma matriz geradora de um reticulado Λ, então $v(\Lambda) = |det\ (M)|$.*

Corolário 4.4. *([4], p. 55) O volume da região fundamental $v(\mathcal{P})$ independe da base escolhida.*

Proposição 4.5. *([13], p. 184) Seja Λ um reticulado de $\mathbb{R}^n$. Se $\mathcal{P}$ é uma região fundamental de Λ, então todo elemento de $\mathbb{R}^n$ pertence a uma única região $\mathcal{P}+l$, em que $l \in \Lambda$, isto é, $\mathbb{R}^n = \dot{\bigcup}_{l\in\Lambda} \mathcal{P} + l$.*

Demonstração. Seja $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base geradora para Λ. Como $\mathcal{B}$ é um conjunto linearmente independente do $\mathbb{R}^n$, com n elementos, segue que é uma base para o espaço vetorial $\mathbb{R}^n$. Portanto, todo $x \in \mathbb{R}^n$, pode ser escrito da forma $x = \sum_{i=1}^{n} a_i v_i$, com $a_i \in \mathbb{R}$, para todo $i = 1, \ldots, n$. Podemos reescrever $a_i = b_i + \alpha_i$, onde b_i é o maior inteiro menor que a_i e $0 \leq \alpha_i < 1$. Assim,

$$x = \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} (b_i + \alpha_i) v_i = \sum_{i=1}^{n} b_i v_i + \sum_{i=1}^{n} \alpha_i v_i.$$

Como $\sum_{i=1}^{n} b_i v_i \in \Lambda$ e $\sum_{i=1}^{n} \alpha_i v_i \in \mathcal{P}$, segue que $x \in \mathcal{P} + l$, para algum $l \in \Lambda$. Agora, basta mostrar que esta região é a única. Para isso, suponhamos que exista $y \in \mathbb{R}^n$ tal que $y \in \mathcal{P} + l_1$ e $y \in \mathcal{P} + l_2$, onde $l_1 = \sum_{i=1}^{n} a_i v_i$ e $l_2 = \sum_{i=1}^{n} b_i v_i$ são distintos, com $a_i, b_i \in \mathbb{Z}$. Como y pertence as duas classes, segue que

$$y = \sum_{i=1}^{n} (a_i + \alpha_i) v_i \text{ e } y = \sum_{i=1}^{n} (b_i + \beta_i) v_i,$$

onde $0 \leq \alpha, \beta < 1$. Assim,

$$\sum_{i=1}^{n} (a_i - b_i) v_i = \sum_{i=1}^{n} (\beta_i - \alpha_i) v_i.$$

Como $\mathcal{B}$ é uma base, concluímos da igualdade anterior que $a_i - b_i = \beta_i - \alpha_i$ para cada i. Uma vez que $a_i - b_i \in \mathbb{Z}$, temos que $\beta_i - \alpha_i \in \mathbb{Z}$. Por outro lado, pela construção de α_i, β_i

sabemos que $-1 < \beta_i - \alpha_i < 1$. Logo, a única possibilidade é que $\alpha_i = \beta_i$, para todo i. Portanto, $l_1 = l_2$ o que contraria a suposição de que são distintos. ■

Em outras palavras, o $\mathbb{R}^n$ é coberto por completo pela união disjunta explicitada na Proposição. Neste caso diremos que esta união é uma **pavimentação** ou um **ladrilhamento** de $\mathbb{R}^n$. Abaixo segue um recorte do ladrilhamento de $\mathbb{R}^2$ com relação ao reticulado exibido anteriormente.

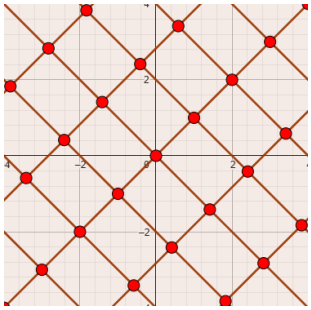


Figura 4.4: Um ladrilhamento para o plano real.
Fonte: Autoria própria

Visto que os centros de um reticulado formam um subgrupo aditivo do $\mathbb{R}^n$, podemos efetuar o cálculo de quanto o empacotamento esférico cobre o espaço todo, simplesmente verificando qual é a porcentagem da região fundamental que foi coberta, visto que o padrão se repete para todas as regiões fundamentais transladadas.

Por conseguinte, definimos a **densidade de empacotamento**, dada por

$$\Delta(\Lambda) = \frac{\text{volume de uma esfera de raio } \rho}{\text{volume da região fundamental}}.$$

Considerando $B(\rho)$ a esfera de centro na origem e raio ρ, podemos reescrever da seguinte maneira:

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

Uma vez que em cada dimensão o volume da esfera unitária é um valor constante, ao fixarmos a dimensão, podemos evitar que a notação fique carregada deixando de fora essa constante. Sendo assim, dado o reticulado Λ definimos a **densidade de centro**, que denotaremos $\delta(\Lambda)$, por:

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

4.1.1 O homomorfismo canônico

Mostraremos, nesta seção, uma forma de construir reticulados a partir do anel dos inteiros algébricos de um corpo de números, com o objetivo de obter empacotamentos

reticulados e, em seguida, veremos como calcular o volume dos reticulados obtidos a partir desta construção.

Conforme os comentários após o Teorema 2.9, seja $\mathbb{K}$ um corpo de números de grau n e $\sigma_1, \ldots, \sigma_n$ os n monomorfismos nos números complexos. Neste caso, $n = r + 2s$, onde r é o número de monomorfismos reais e $2s$ o número de monomorfismos imaginários. Mais do que isso, podemos considerar $\sigma_1, \ldots, \sigma_r$ os r monomorfismos reais, e $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ os monomorfismos imaginários, de modo que σ_{r+s+j} seja o conjugado de σ_{r+j}, para $j = 1, \ldots, s$.

Exemplo 4.6. Quando $\mathbb{K} = \mathbb{Q}(\alpha)$, onde $\alpha = \sqrt[8]{7}$, uma das maneiras de enumerar os monomorfismos da forma mencionada é:

i) $\sigma_1(a + b\alpha) = a + b \cdot \alpha$

ii) $\sigma_2(a + b\alpha) = a + b \cdot (-1)\alpha$

iii) $\sigma_3(a + b\alpha) = a + b \cdot i\alpha$

iv) $\sigma_4(a + b\alpha) = a + b \cdot \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\alpha$

v) $\sigma_5(a + b\alpha) = a + b \cdot \left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\alpha$

vi) $\sigma_6(a + b\alpha) = a + b \cdot (-i)\alpha$

vii) $\sigma_7(a + b\alpha) = a + b \cdot \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\alpha$

viii) $\sigma_8(a + b\alpha) = a + b \cdot \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\alpha.$

Existem inúmeras formas de enumerarmos, mas para definirmos o homomorfismo canônico o que nos interessa, principalmente, é que os monomorfismos σ_k sejam reais para $k < n$ e que não sejam conjugados entre si quando $r < k < s + 1$. Em seguida, ficará claro o porquê desse fato.

O homomorfismo injetivo de $\mathbb{Z}-$módulos $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^n$, definido por,

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_r(x), Re(\sigma_{r+1}(x)), Im(\sigma_{r+1}(x)), \ldots, Re(\sigma_s(x)), Im(\sigma_s(x))) \quad (4.1)$$

é chamado de **homomorfismo canônico**, onde $Re(z)$ e $Im(z)$ representam, respectivamente, a parte real e imaginária de um número complexo z.

Teorema 4.7. *([4], p. 56) Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathcal{M} \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $\{x_1, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{M}$, então $\sigma_{\mathbb{K}}(\mathcal{M})$ é um reticulado em $\mathbb{R}^n$, cujo volume é:*

$$v(\sigma_{\mathbb{K}}(\mathcal{M})) = 2^{-s}|det(\sigma_i(x_j)|,$$

onde s é metade do número de imersões imaginárias.

Conforme o comentário após o Teorema 2.38, vimos que se $\mathbb{K}$ é um corpo de números de grau n, então o anel dos inteiros algébricos deste corpo é um $\mathbb{Z}-$módulo livre de posto n. Portanto, o Teorema 4.7 garante que a imagem do anel dos inteiros algébricos de um corpo de números é um reticulado.

Exemplo 4.8. Consideremos o corpo quadrático $\mathbb{Q}(\sqrt{2})$ e o seu anel de inteiros $\mathbb{Z}[\sqrt{2}]$. Na figura a seguir, ilustramos o conjunto imagem de $\mathbb{Z}[\sqrt{2}]$ pelo Homomorfismo Canônico, que por sua vez, do que foi exposto, é um reticulado.

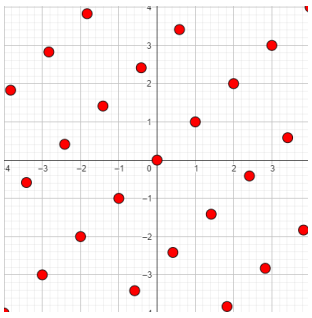


Figura 4.5: Conjunto imagem de $\mathbb{Z}[\sqrt{2}]$ pelo homomorfismo canônico.
Fonte: Autoria própria

Neste caso, podemos verificar que o raio de empacotamento é $\sqrt{2}/2$, já que pela imagem podemos visualizar que os vetores de menor comprimento são $(1,1)$ e $(-1,-1)$, os quais o módulo é $\sqrt{2}$. A seguir, ilustramos a figura do empacotamento esférico deste reticulado.

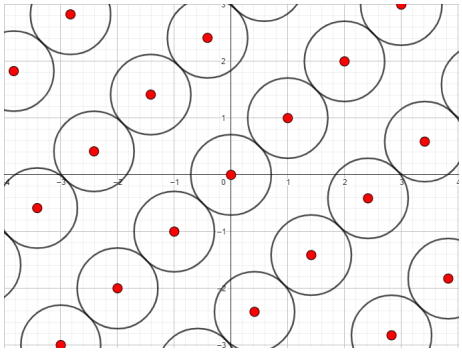


Figura 4.6: Empacotamento reticulado a partir de $\mathbb{Z}[\sqrt{2}]$.
Fonte: Autoria própria

Pelo Teorema 4.7 o volume deste reticulado é $2\sqrt{2}$. Portanto a densidade de centro $\frac{1}{4\sqrt{2}}$ e consequentemente densidade de empacotamento $\frac{\pi}{4\sqrt{2}} \approx 0,5553$ deste reticulado, o que nos permite afirmar que tal empacotamento esférico cobre aproximadamente $55,53\%$ do $\mathbb{R}^2$. Visualmente não é difícil perceber pela Figura 4.6 que existem empacotamentos esféricos que cobrem uma parcela maior do plano real, na Seção seguinte comentaremos sobre o melhor empacotamento esférico em termos de densidade, para o $\mathbb{R}^2$.

Proposição 4.9. *([4], p. 57) Se D é o discriminante de $\mathbb{K}$ e $\mathcal{I}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathcal{I})$ é um reticulado no $\mathbb{R}^n$, cujo volume é:*

$$v(\sigma_{\mathbb{K}}(\mathcal{I})) = 2^{-s}|D|^{1/2}N(\mathcal{I}),$$

onde s é metade do número de imersões imaginárias.

De acordo com o Teorema 4.9, dado um corpo de números $\mathbb{K}$, podemos obter um reticulado a partir de um ideal não nulo $\mathcal{I}$ de $\mathcal{O}_{\mathbb{K}}$. O reticulado $\sigma_{\mathbb{K}}(\mathcal{I})$ é denominado **Realização Geométrica** de $\mathcal{I}$.

4.2 DENSIDADES DE CENTRO

Como mencionado no início deste capítulo, atualmente é conhecida a solução do problema do empacotamento esférico para algumas dimensões. Nas páginas xix e xx do prefácio de [1], estão listados alguns dos recordes da densidade de centro para várias dimensões. Evidentemente, podemos obter empacotamentos esféricos de várias maneiras e não necessariamente por reticulados. Na referência citada, quando o recorde não é dado por um reticulado, é explicitado também qual a maior densidade utilizando reticulados. A seguir, veremos uma tabela com alguns destes dados. Nessa seção, o objetivo será conhecer alguns recordes e reticulados importantes.

Dimensão	**Densidade de centro**
1	$1/2 = 0,5$
2	$1/(2\sqrt{3}) \approx 0,28868$
3	$1/(4\sqrt{2}) \approx 0,17678$
4	$1/8 = 0,125$
5	$1/(8\sqrt{2}) \approx 0,08839$
6	$1/(4\sqrt{2}) \approx 0,07217$
7	$1/16 = 0,62650$
8	$1/16 = 0,62650$
$\vdots$	$\vdots$
24	1

Tabela 4.1: Densidades de centro

Um fato interessante é que, a partir da dimensão 6 o volume da bola unitária começa a diminuir com relação às anteriores. Sendo assim, em dimensões maiores é comum encontrarmos densidades de centro maiores que 1, visto que este número será multiplicado pelo volume que é cada vez menor. A seguir, exibimos a fórmula para o volume da bola em cada dimensão:

$$v(B(1)) = \begin{cases} \frac{\pi^{m/2}}{(m/2)!} & \text{, se m é par} \\ \frac{2^m \pi^{(m-1)/2}((m-1)/2)!)}{m!} & \text{, caso contrário.} \end{cases}$$

Quando se trata do empacotamento esférico, para a dimensão 1, o problema é trivial, uma vez que podemos cobrir a reta real com intervalos fechados de raio $1/2$ centrados nos números inteiros. Para a dimensão 2, a maior densidade de centro possível de acordo com a Tabela 4.1 é $1/(2\sqrt{3})$, mas, podemos obter esta densidade por meio do corpo quadrático $\mathbb{Q}(\sqrt{-3})$ e aplicando o homomorfismo canônico no anel de inteiros. A seguir, ilustra-se este empacotamento reticulado.

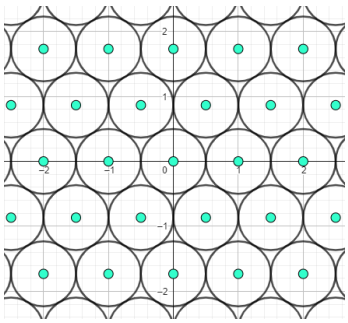


Figura 4.7: Empacotamento reticulado a partir de $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$
Fonte: Autoria própria

Utilizando o Teorema 4.7 podemos verificar que a densidade de centro deste reticulado é$1/(2\sqrt{3})$, e portanto, concluímos que a densidade de empacotamento é $\pi/(2\sqrt{3}) \approx 0,9067$. Assim podemos afirmar que este empacotamento esférico cobre aproximadamente $90,67\%$ do $\mathbb{R}^n$.

Para o caso da dimensão 3, é possível cobrir aproximadamente $74,05\%$ do espaço. Na dimensão 8, o volume da bola unitária é $\frac{\pi^4}{4!} \approx 4,0587$, enquanto que na dimensão 24 é $\frac{\pi^{12}}{12!} \approx 0,00192$. Daí os empacotamentos mais densos para as dimensões 8 e 24 nesta ordem, cobrem aproximadamente $25,36\%$ e $0,19\%$ de seus respectivos espaços.

4.3 MINIMIZANDO A FORMA QUADRÁTICA

Com os resultados obtidos nas Seções 4.1 e 4.2, dado um reticulado para efetuar o cálculo da densidade de centro, uma das informações necessárias é o raio de empacotamento, ou equivalentemente, encontrar qual é o vetor de menor norma neste reticulado, que por sua vez, geralmente não é uma tarefa trivial. Para isso, veremos nesta seção algumas formas que vão ajudar a obter esse dado. Dada uma extensão $\mathbb{K}/\mathbb{Q}$ galoisiana, segue $\mathbb{K}$ é totalmente real ou totalmente imaginária, visto que, neste caso todos os monomorfismos sob estas condições são automorfismos, sendo assim, dado σ_j um monomorfismo de $\mathbb{K}$, temos que $\sigma_j(\mathbb{K}) = \mathbb{K}$. Portanto, se $\mathbb{K} \subset \mathbb{R}$, a extensão será totalmente real, caso contrário, será totalmente imaginária. Assim, para o estudo dos corpos abelianos, podemos utilizar o próximo resultado.

Proposição 4.10. *Se $\mathbb{K}$ é um corpo abeliano, $x \in \mathbb{K}$ e $\sigma_{\mathbb{K}}$ é o homomorfismo canônico, então,*

$$|\sigma_{\mathbb{K}}(x)|^2 = c \cdot Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}), \text{ onde } c = \begin{cases} 1, & \text{se } \mathbb{K} \text{ for totalmente real;} \\ \frac{1}{2}, & \text{se } \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Demonstração.

i) Suponha que $\mathbb{K}$ seja totalmente real. Assim,

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

o que prova o resultado.

ii) Suponha que $\mathbb{K}$ seja totalmente imaginário. Temos que $n = 2s$, e portanto:

$$\begin{aligned} |\sigma_{\mathbb{K}}(x)|^2 &= |(Re(\sigma_1(x)), Im(\sigma_1(x)), \ldots, Re(\sigma_s(x)), Im(\sigma_s(x))|^2 \\ &= (Re(\sigma_1(x)))^2 + (Im(\sigma_1(x)))^2 + \cdots + (Re(\sigma_s(x)))^2 + (Im(\sigma_s(x)))^2 \\ &= \sigma_1(x)\overline{\sigma_1(x)} + \cdots + \sigma_n(x)\overline{\sigma_n(x)} \\ &= \sigma_1(x)\sigma_1(\overline{x}) + \cdots + \sigma_s(x)\sigma_s(\overline{x}) \\ &= \sigma_1(x\overline{x}) + \cdots + \sigma_s(x\overline{x}) \\ &= \frac{1}{2}(\sigma_1(x\overline{x}) + \cdots + \sigma_s(x\overline{x}) + \sigma_{s+1}(x\overline{x}) + \cdots + \sigma_n(x\overline{x})) \\ &= \frac{1}{2}Tr(x\overline{x}). \end{aligned}$$

■

Uma vez que $\mathbb{Q}(\zeta_n)$, é um corpo totalmente imaginário, para $n < 1$, o próximo resultado, já conhecido, é exposto com o objetivo de minimizar a forma quadrática de um corpo de um $p-$ésimo corpo ciclotômico, onde p é um número primo. Nesse contexto, consideraremos $\mathbb{L} = \mathbb{Q}(\zeta_p)$.

Teorema 4.11. *Se $\mathbb{L} = \mathbb{Q}(\zeta_p)$ e x é um elemento de $\mathcal{O}_{\mathbb{L}}$ escrito da forma $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, então:*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = p\sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2.$$

Demonstração. Considerando x conforme o enunciado, segue que

$$\overline{x} = a_0 + a_1\zeta_p^{-1} + a_2\zeta_p^{-2} + \cdots + a_{p-2}\zeta_p^{-(p-2)}.$$

Portanto,

$$\begin{aligned} x\overline{x} &= (a_0^2 + a_1^2 + \cdots + a_{p-2}^2) + (a_0a_1 + a_1a_2 + \cdots + a_{p-3}a_{p-2})(\zeta_p^{-1} + \zeta_p) + \\ &+ (a_0a_2 + a_1a_3 + \cdots + a_{p-4} + a_{p-2})(\zeta_p^{-2} + \zeta_p^2) + \cdots + (a_0a_{p-2})(\zeta_p^{p-2} + \zeta_p^{-(p-2)}) \\ &= \sum_{i=0}^{p-2} a_i^2 + \sum_{i=1}^{p-2}(a_0a_{0+i} + \cdots + a_{p-2-i}a_{p-2})(\zeta_p^i + \zeta_p^{-i}). \end{aligned}$$

Aplicando o traço na igualdade acima, obtemos:

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) &= Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=0}^{p-2} a_i^2 + \sum_{i=1}^{p-2}(a_0a_{0+i} + \cdots + a_{p-2-i}a_{p-2})(\zeta_p^i + \zeta_p^{-i})\right) \\ &= Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=0}^{p-2} a_i^2\right) + Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=1}^{p-2}(a_0a_{0+i} + \cdots + a_{p-2-i}a_{p-2})(\zeta_p^i + \zeta_p^{-i})\right) \\ &= (p-1)\sum_{i=0}^{p-2} a_i^2 + \sum_{i=1}^{p-2}(a_0a_{0+i} + \cdots + a_{p-2-i}a_{p-2})Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i + \zeta_p^{-i}). \end{aligned}$$

Por outro lado, note que $Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i + \zeta_p^{-i})) = 2Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i)$. Mais ainda, visto que $i = 1, \ldots, p-2$, segue que $\sum_{i=1}^{p-2} Tr_{\mathbb{L}/\mathbb{Q}}(\zeta_p^i) = -1$. Portanto, voltando na igualdade acima, concluímos que:

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) &= (p-1)\sum_{i=0}^{p-2} a_i^2 - 2\sum_{i=1}^{p-2} a_0a_{0+i} + \cdots + a_{p-2-i}a_{p-2} \\ &= (p-1)\sum_{i=0}^{p-2} a_i^2 - 2\sum_{0\le i<j\le p-2} a_ia_j \\ &= p\left(\sum_{i=0}^{p-2} a_i^2\right) - \left(\sum_{i=0}^{p-2} a_i^2 + 2\sum_{0\le i<j\le p-2} a_ia_j\right) \\ &= p\left(\sum_{i=0}^{p-2} a_i^2\right) - \left(\sum_{i=0}^{p-2} a_i\right)^2, \end{aligned}$$

o que prova o resultado. ■

Vejamos agora, uma forma de minimizar o traço de $x\overline{x}$. Pela definição de traço, sabemos que:

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = \sum_{i=1}^{p-1} \sigma_i(x\overline{x}), \tag{4.2}$$

onde $\sigma_1, \cdots, \sigma_{p-1}$ são os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Dividindo ambos os lados da Equação 4.2 por $p-1$, obtemos que

$$\frac{Tr(x\overline{x})}{p-1} = \frac{\sum_{i=1}^{p-1} \sigma_i(x\overline{x})}{p-1}. \tag{4.3}$$

Note que a expressão ao lado direito da igualdade acima representa a média aritmética dos elementos do conjunto $\{\sigma_1(x\overline{x}), \cdots, \sigma_{p-1}(x\overline{x})\}$. Utilizando o fato de que a média aritmética é maior ou igual que a média geométrica, concluímos que:

$$\frac{\sum_{i=1}^{p-1} \sigma_i(x\overline{x})}{p-1} \geq \left(\prod_{i=1}^{p-1} \sigma_i(x\overline{x})\right)^{1/(p-1)},$$

ou seja,

$$\sum_{i=1}^{p-1} \sigma_i(x\overline{x}) \geq (p-1) \cdot \left(\prod_{i=1}^{p-1} \sigma_i(x\overline{x})\right)^{1/(p-1)}. \tag{4.4}$$

Desenvolvendo o lado direito desta inequação, segue que:

$$\begin{aligned}
(p-1) \cdot \left(\prod_{i=1}^{p-1} \sigma_i(x\overline{x})\right)^{1/(p-1)} &= (p-1) \cdot \left(\prod_{i=1}^{p-1} \sigma_i(x)\sigma_i(\overline{x})\right)^{1/(p-1)} \\
&= (p-1) \cdot \left(\prod_{i=1}^{p-1} \sigma_i(x)\overline{\sigma_i(x)}\right)^{1/(p-1)} \\
&= (p-1) \cdot \left(\prod_{i=1}^{p-1} |\sigma_i(x)|^2\right)^{1/(p-1)}.
\end{aligned}$$

Logo, pelas Equações (4.2) e (4.4), concluímos que

$$Tr(x\overline{x}) \geq (p-1) \cdot \left(\prod_{i=1}^{p-1} |\sigma_i(x)|^2\right)^{1/(p-1)}.$$

Note que, $\prod_{i=1}^{p-1} \sigma_i(x) = N(x)$, uma vez que $\mathbb{Z}$ é integralmente fechado, pelo comentário após a Proposição 2.40, sabemos que $N(x)$ é um número inteiro, e portanto, $\prod_{i=1}^{p-1} |\sigma_i(x)|^2$ é um inteiro positivo. Uma vez que o menor inteiro positivo é 1, concluímos que:

$$Tr(x\overline{x}) \geq (p-1).$$

Note que para $x = 1$, isto é, $a_0 = 1$ e $a_i = 0$, para todo $i = 1, \ldots, p-1$, temos pela expressão dada no Teorema 4.11, que $Tr(x\overline{x}) = p.1 - (1)^2 = p-1$, e portanto, verificamos

que o menor traço possível é exatamente $p-1$, exibindo um elemento dessa forma. ■

Agora, o objetivo será minimizar a forma quadrática de um corpo de números com condutor primo. Portanto, consideraremos $\mathbb{K}$ um corpo abeliano, de condutor primo ímpar p, nesse contexto chamaremos $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Já sabemos que a extensão $\mathbb{K}/\mathbb{Q}$ é galoisiana, logo é totalmente real ou totalmente imaginária, sendo assim, de acordo com a Proposição 4.10, em ambos casos, dado y em $\mathcal{O}_{\mathbb{K}}$, basta minimizarmos $Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y})$. Para isso, vejamos alguns resultados já conhecidos que vão ajudar. De acordo com o Teorema 3.30, dado o corpo abeliano $\mathbb{K}$ de condutor primo p, podemos exibir uma base integral para $\mathbb{K}$ a partir do gerador do grupo de Galois da extensão $\mathbb{L}/\mathbb{Q}$. Tendo isso em vista, dado y um elemento de $\mathbb{K}$ escrito com relação a esta base, o próximo teorema é um resultado conhecido, que trata do traço de $y\overline{y}$.

Teorema 4.12. *([14], p. 50) Seja $\mathbb{K}$ um corpo abeliano de condutor p. Se $y \in \mathcal{O}_{\mathbb{K}}$ é escrito da forma $y = b_1 t + b_2\theta(t) + \cdots + b_s\theta^{(s-1)}(t)$, onde $s = (p-1)/d$, então:*

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

4.4 RETICULADOS VIA IDEAIS

Nesta seção, consideramos $\mathbb{Q}(\zeta_p)$ de $\mathbb{L}$, onde p é número primo ímpar, a não ser que seja mencionado o contrário. O objetivo é verificar a densidade de centro de alguns ideais de $\mathcal{O}_{\mathbb{L}}$. O passo inicial será verificar a densidade de centro de $\sigma_L(\mathcal{O}_{\mathbb{L}}) = \Lambda$.

Pelo Teorema 3.23, segue que

$$D_{\mathbb{L}/\mathbb{Q}} = (-1)^{(p-1)/2} \cdot \frac{p^{p-1}}{p} \Rightarrow |D_{\mathbb{L}/\mathbb{Q}}| = p^{p-2}.$$

Daí,

$$\delta(\Lambda) = \frac{\rho^{p-1}}{2^{-(p-1)/2} \cdot |D|^{1/2}} = \frac{2^{(p-1)/2}\rho^{p-1}}{p^{(p-2)/2}}.$$

Por outro lado, no comentário após o Teorema 4.11, vimos que:

$$min\{|\sigma_{\mathbb{L}}(x)|^2; x \in \mathcal{O}_{\mathbb{L}}\} = \frac{p-1}{2},$$

e portanto, $min\{|\sigma_{\mathbb{L}}(x)|; x \in \mathcal{O}_{\mathbb{L}}\} = \sqrt{\frac{p-1}{2}}$. Assim,

$$\rho = \frac{1}{2}\sqrt{\frac{p-1}{2}} = \frac{1}{2} \cdot \left(\frac{p-1}{2}\right)^{1/2} = \frac{1}{2^{3/2}} \cdot (p-1)^{1/2}.$$

Substituindo, na equação acima, obtemos:

$$\delta(\Lambda) = \frac{2^{(p-1)/2}\left(\frac{1}{2^{3/2}} \cdot (p-1)^{1/2}\right)^{p-1}}{p^{(p-2)/2}} = \frac{2^{(p-1)/2}}{2^{3(p-1)/2}} \cdot \frac{(p-1)^{(p-1)/2}}{p^{(p-2)/2}} = \frac{(p-1)^{(p-1)/2}}{2^{p-1}p^{(p-2)/2}}.$$

O próximo resultado indicará a densidade de centro de um reticulado gerado pelo ideal principal $a\mathcal{O}_{\mathbb{L}}$, onde a é um elemento de $\mathbb{Z}$.

Proposição 4.13. *Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$, com p primo. Se $\mathcal{I} = a\mathcal{O}_{\mathbb{L}}$ é um ideal principal de $\mathcal{O}_{\mathbb{L}}$ onde a é um número inteiro, então, $\delta(\sigma_{\mathbb{L}}(\mathcal{I})) = \delta(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}}))$.*

Demonstração. Se x é um elemento de $\mathcal{I}$, então $x = a(a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1})$, com $a_i \in \mathbb{Z}$, para todo $i = 1, \ldots, p-1$. Logo,

$$x\overline{x} = a^2\left(\sum_{i=1}^{p-1} a_i^2 + \sum_{i=1}^{p-1}(a_1a_{1+i} + \cdots + a_{p-1-i}a_{p-1})(\zeta_p^i + \zeta_p^{-i})\right).$$

Aplicando o traço em ambos lados, como a é inteiro, segue que

$$\begin{aligned} Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) &= a^2 \cdot Tr_{\mathbb{L}/\mathbb{Q}}\left(\sum_{i=1}^{p-1} a_i^2 + \sum_{i=1}^{p-1}(a_1a_{1+i} + \cdots + a_{p-1-i}a_{p-1})(\zeta_p^i + \zeta_p^{-i})\right) \\ &= a^2\left((p-1)\sum_{i=1}^{p-1} a_i^2 - 2\sum_{1\leq i<j\leq p-1} a_ia_j\right). \end{aligned}$$

Portanto, $min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}); x \in \mathcal{I}\} = \frac{a^2(p-1)}{2}$, e assim,

$$\rho = \left(\sqrt{\frac{a^2(p-1)}{2}}\right)/2 = \frac{|a|}{2} \cdot \left(\frac{(p-1)}{2}\right)^{\frac{1}{2}} \Rightarrow \rho^{p-1} = \frac{|a|^{p-1}}{2^{p-1}} \cdot \left(\frac{(p-1)}{2}\right)^{\frac{p-1}{2}}$$

Por outro lado, note que $N(\mathcal{I}) = N(a) = a^{p-1}$. Uma vez que $p-1$ é par, segue que $a^{p-1} = |a|^{p-1}$. Do que foi exposto, obtemos:

$$\delta(\sigma_{\mathbb{L}}(\mathcal{I})) = \frac{\frac{|a|^{p-1}}{2^{p-1}} \cdot \left(\frac{(p-1)}{2}\right)^{\frac{p-1}{2}}}{2^{-(p-1)/2} \cdot |D|^{1/2} \cdot |a|^{p-1}} = \frac{2^{(p-1)/2}\left(\frac{1}{2^{3/2}} \cdot (p-1)^{1/2}\right)^{p-1}}{p^{(p-2)/2}} = \delta(\Lambda),$$

como queríamos. ∎

Sendo assim, tomando um ideal da forma da Proposição 4.13 não obtivemos melhores resultados com relação à densidade de centro. Verificaremos, agora, o que acontece ao tomar $(1-\zeta_p)$ como o gerador do ideal. Chamaremos $\mathfrak{p} = (1-\zeta_p)\mathcal{O}_{\mathbb{L}}$.

Consideremos o conjunto $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$, que por sua vez não é uma base de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, visto que não é um conjunto linearmente independente. Porém, é um conjunto gerador, isto é, todo elemento de $x \in \mathbb{Q}(\zeta_p)$ pode ser escrito da forma:

$$x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1},$$

onde $a_1, \ldots, a_{p-1} \in \mathbb{Q}$.

Naturalmente, essa forma não é única. Com essa motivação, veremos, como pode ser útil esta escrita. Para isso, provemos dois resultados conhecidos.

Lema 4.14. *Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Se x é um elemento de $\mathcal{O}_\mathbb{L}$, então, x pode ser escrito da forma*

$$x = b_0 + b_1\zeta_p + \cdots + b_{p-1}\zeta_p^{p-1},$$

onde $b_0, \ldots, b_{p-1} \in \mathbb{Z}$. De modo que $0 \leq \sum_{i=0}^{p-1} b_i < p$. Neste caso, essa forma é única.

Demonstração. Seja $x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, com $a_0, \ldots, a_{p-1}$ inteiros. Uma vez que $\sum_{i=0}^{p-1} a_i$ é um número inteiro, pelo Algoritmo da Divisão de Euclides, segue que existem únicos q, r inteiros tal que

$$\sum_{i=0}^{p-1} a_i = qp + r,$$

com $0 \leq r < p$. Por outro lado, sabemos da Expressão 3.5, que:

$$\zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1 \Leftrightarrow 1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0.$$

Assim, basta tomarmos $b_i = (a_i - q)$, já que:

$$x + (-q \cdot (1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1})) = x + 0 = x.$$

Fazendo isso, concluímos que $x = b_0 + b_1\zeta_p + \cdots + b_{p-1}\zeta_p^{p-1}$ de modo que

$$\sum_{i=0}^{p-1} b_i = \sum_{i=0}^{p-1}(a_i - q) = \left(\sum_{i=0}^{p-1} a_i\right) - pq = (pq + r) - pq = r$$

onde pela construção $0 \leq r < p$. Para a unicidade, suponha que

$$x = c_0 + c_1\zeta_p + \cdots + c_{p-1}\zeta_p^{p-1}, \text{ com } 0 \leq \sum_{i=0}^{p-1} c_i < p,$$

onde $c_0, \ldots, c_{p-1}$ são inteiros. Assim,

$$\sum_{i=0}^{p-1}\left((c_i - b_i)\zeta_p^i\right) = x - x = \sum_{i=0}^{p-1}\left((b_i - c_i)\zeta_p^i\right).$$

Uma vez que, b_i e c_i são positivos e menores do que p para todo $i = 0, \ldots, p-1$, segue que $0 \leq \sum_{i=0}^{p-1} b_i - \sum_{i=0}^{p-1} c_i < p$ e $0 \leq \sum_{i=0}^{p-1} c_i - \sum_{i=0}^{p-1} b_i < p$. Portanto, $\sum_{i=0}^{p-1} b_i = \sum_{i=0}^{p-1} c_i$. ■

Corolário 4.15. *Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Se $x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta^{p-1}$, nas condições do Lema 4.14, então x é um elemento de $\mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-1} a_i = 0$ e é única.*

Demonstração. Afirmamos que $x \in \mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-1} a_i \in p\mathbb{Z}$. Provando isso, o resultado segue imediatamente do Lema 4.4. De fato, podemos reescrever x da seguinte maneira

$$\begin{aligned} x &= a_0 - a_0 + a_1\zeta_p - a_1 + a_2\zeta_p^2 - a_2 + \cdots + a_{p-1}\zeta_p^{p-1} - a_{p-1} + (a_0 + a_1 + a_2 + \cdots + a_{p-1}) \\ &= a_1(\zeta_p - 1) + a_2(\zeta_p^2 - 1) + \cdots + a_{p-1}(\zeta_p^{p-1} - 1) + \sum_{i=0}^{p-1} a_i. \end{aligned}$$

Suponhamos que $x \in \mathfrak{p}$. Assim,

$$x - (a_1(\zeta_p - 1) + a_2(\zeta_p^2 - 1) + \cdots + a_{p-2}(\zeta_p^{p-1} - 1)) = \sum_{i=0}^{p-1} a_i \in \mathfrak{p}.$$

Por outro lado, como $a_0, \ldots, a_{p-1}$ são inteiros, segue que $\sum_{i=0}^{p-1} a_i \in \mathbb{Z}$. Sendo assim, concluímos que $\sum_{i=0}^{p-1} a_i \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Analogamente, prova-se a recíproca.

Agora, dada a condição $\sum_{i=0}^{p-1} a_i = 0$, provaremos a unicidade dos coeficientes. Para isso, suponhamos que $x = \sum_{i=0}^{p-1} a_i\zeta_p^i = \sum_{i=0}^{p-1} b_i\zeta_p^i$ tal que $\sum_{i=0}^{p-1} a_i = \sum_{i=0}^{p-1} b_i = 0$. Logo,

$$0 = x - x = \sum_{i=0}^{p-1}(a_i - b_i)\zeta_p^i = \sum_{i=0}^{p-1} c_i\zeta_p^i, \text{ onde } c_i = a_i - b_i.$$

Por outro lado, novamente pela Expressão 3.5, sabemos que $(1 + \zeta_p + \cdots + \zeta_p^{p-1}) = 0$ e desse modo,

$$0 = c_0(1 + \zeta_p + \cdots + \zeta_p^{p-1}) = \sum_{i=0}^{p-1} c_0\zeta_p^i.$$

Assim,

$$0 = \sum_{i=0}^{p-1} c_i\zeta_p^i - \sum_{i=0}^{p-1} c_0\zeta_p^i = \sum_{i=0}^{p-1}(c_i - c_0)\zeta_p^i = \sum_{i=1}^{p-1}(c_i - c_0)\zeta_p^i.$$

Porém, como o conjunto $\{\zeta_p, \cdots, \zeta_p^{p-1}\}$ é base de $\mathcal{O}_{\mathbb{L}}$, concluímos que $c_0 = c_1 = \cdots = c_{p-1}$, e por conseguinte $a_0 - b_0 = a_1 - b_1 = \cdots = a_{p-1} - b_{p-1}$. Por fim, observemos que:

$$\sum_{i=0}^{p-1} a_i = \sum_{i=0}^{p-1} b_i = 0 \Rightarrow \sum_{i=0}^{p-1} a_i - b_i = 0.$$

Portanto, temos uma soma de termos iguais resultando em zero. Sendo assim, a única possibilidade é que todos os termos sejam zero, ou seja, $a_i - b_i = 0$. Logo, $a_i = b_i$, para $i = 0, 1, \ldots, p-1$. Assim, sob estas condições, x é escrito de forma única. ■

Uma propriedade importante do traço é que, independente do conjunto gerador para o anel dos inteiros algébricos de um número que seja escolhido, o traço de um elemento sempre é o mesmo, e isso decorre do seguinte fato.

Lema 4.16. *Seja $\mathbb{K}$ um corpo de números. Se α é um elemento de $\mathbb{K}$ e $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, o polinômio minimal de α, então $Tr(\alpha) = -a_{n-1}$ e $N(\alpha) = (-1)^n a_0$.*

Demonstração. Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ as raízes de $m_\alpha(x)$. Assim,

$$m_\alpha(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n).$$

Expandindo o produto, obtemos que:

$$m_\alpha(x) = x^n - (\alpha_1 + \alpha_2 + \cdots + \alpha_n)x^{n-1} + \cdots + (-1)^n\alpha_1\alpha_2\ldots\alpha_n.$$

Comparando com a forma geral do polinômio minimal:

$$m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

concluímos que $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$. Portanto,

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_{n-1}.$$

Por outro lado, como $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ é o traço de α, segue que

$$Tr(\alpha) = -a_{n-1}.$$

Do mesmo modo,

$$(-1)^n a_0 = \alpha_1\alpha_2\ldots\alpha_n.$$

Uma vez que $\alpha_1 \cdots \alpha_n$ é a norma de α, obtemos:

$$N(\alpha) = (-1)^n a_0,$$

o que prova o resultado. ■

Portanto, uma vez que o polinômio minimal de um elemento independe do conjunto gerador escolhido, concluímos que essa escolha não interfere no traço. Além disso, já vimos que:

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = p\sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2.$$

Agora, o objetivo é minimizar o traço de $x\overline{x}$, com x em $\mathfrak{p}$, sob certas condições.

Pelo Corolário 4.15, dado $x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$ em $\mathfrak{p}$, segue que $\sum_{i=0}^{p-1} a_i = 0$, e portanto,

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = p\sum_{i=0}^{p-1} a_i^2.$$

Como cada a_i^2 é um número inteiro positivo segue que, a soma $\sum_{i=0}^{p-1} a_i^2$ também é um inteiro positivo. Portanto, vejamos qual o menor inteiro positivo que podemos obter a partir de certas condições iniciais. Para que tal soma resulte em 1, a única possibilidade é que $a_j = \pm 1$ e $a_i = 0$, para todo $i \neq j$. Porém, neste caso $\sum_{i=0}^{p-1} a_i = \pm 1$, e consequentemente, o elemento inicial não estaria em $\mathfrak{p}$. Por outro lado, o elemento $y = 1 - \zeta_p$ é um elemento de $\mathfrak{p}$ e $Tr_{\mathbb{L}/\mathbb{Q}}(y\overline{y}) = 2p$. Assim,

$$min\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}); x \in \mathfrak{p}\} = 2p. \tag{4.5}$$

Finalmente, a densidade de centro é dada por

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{p^{(p-1)/2}}{2^{(p-1)/2}p^{(p-2)/2}\cdot p} = \frac{p^{-1/2}}{2^{(p-1)/2}} = \frac{1}{2^{(p-1)/2}\sqrt{p}}.$$

Afim de comparar as densidades de centro dos reticulados obtidos por esse processo com as densidades máximas conhecidas, observemos o seguinte exemplo.

Exemplo 4.17. Consideremos $p = 3$, isto é, $\mathbb{Q}(\zeta_3) = \mathbb{L}$ e $\mathfrak{p} = (1 - \zeta_3)\mathcal{O}_{\mathbb{L}}$. Utilizando o resultado que acabamos de obter, temos:

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{3^{-1/2}}{2^{(3-1)/2}} = \frac{1}{2\sqrt{3}} \approx 0,28868.$$

Observe que, $\mathbb{Q}(\zeta_3)$ é um corpo de números de grau dois, e por sua vez o resultado obtido é o recorde de densidade de centro para esta dimensão.

Sendo assim, podemos observar que esses reticulados mostram-se promissores. Vejamos, agora, o que acontece com as densidades de centro utilizando esse mesmo processo

para corpos ciclotômicos com graus maiores. Para isso, considerando $p = 19$, segue que

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{19^{-1/2}}{2^{(19-1)/2}} = \frac{1}{2^9\sqrt{19}} \approx 0,00044 \tag{4.6}$$

Uma vez que para dimensão 18 o recorde via reticulados é aproximadamente $0,07217$, o resultado obtido está muito distante do recorde, porém, vejamos se é possível aumentar a densidade de centro utilizando outro ideal principal. Para isso, o objetivo será generalizar a fórmula obtida para ideais da forma $(1-\zeta_p)^n$, com $n < \frac{p-1}{2}$ inteiro positivo. Antes disso, veremos alguns resultados importantes, que já são conhecidos.

Teorema 4.18. *Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Considere $\mathfrak{p}^{n+1} = (1-\zeta_p)^{n+1}\mathcal{O}_{\mathbb{L}}$, onde $1 \leq n+1 \leq p-1$ e $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, com $a_0, \ldots, a_{p-1} \in \mathbb{Z}$. Se $f(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$, então α é um elemento de $\mathfrak{p}^{n+1}$ se, e somente se,*

$$f(1) \equiv f'(1) \equiv \cdots = f^{(n)}(1) \equiv 0 \ (mod\ p),$$

onde $f^{(n)}(1)$ é a $n-$ésima derivada de f aplicada em 1.

Demonstração. Primeiramente, note que $\alpha = f(\zeta_p)$. Uma vez que $f(x) \in \mathbb{Z}[x]$ e tem grau no máximo $p-1$, utilizando o algoritmo da divisão sucessivamente, podemos fatorá-lo da seguinte maneira:

$$f(x) = (1-x)^{p-1}c_{p-1} + (1-x)^{p-2}c_{p-2} + \cdots + (1-x)c_1 + c_0,$$

onde $c_0, c_1, \ldots, c_{p-1}$ são números inteiros. Observemos que:

$$\begin{aligned} f(1) &= 0!\ c_0 \\ f'(1) &= -1!\ c_1 \\ f^{(2)}(1) &= 2!\ c_2 \\ &\vdots \\ f^{(n)}(1) &= (-1)^n\ n!\ c_n, \text{ para todo } n \leq p-2. \end{aligned}$$

Além disso, uma vez que $c_k \in \mathbb{Z}$ para todo $k = 0, \ldots, p-1$, segue da Equação (3.18) e do Lema 3.17 que

$$c_k \in \mathfrak{p} \Leftrightarrow c_k \in p\mathbb{Z} \Leftrightarrow c_k \in \mathfrak{p}^{p-1}.$$

Por outro lado,

$$\alpha = f(\zeta_p) = (1-\zeta_p)^{p-1}c_{p-1} + (1-\zeta_p)^{p-2}c_{p-2} + \cdots + (1-\zeta_p)c_1 + c_0.$$

Desse modo, note que $(1-\zeta_p)^{p-1}c_{p-1} + (1-\zeta_p)^{p-2}c_{p-2} + \cdots + (1-\zeta_p)c_1 \in \mathfrak{p}$. Assim, segue que $\alpha \in \mathfrak{p}$ se, e somente se, $c_0 \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Daí, concluímos que $\alpha \in \mathfrak{p}$ se, e

somente se, $c_0 = f(1) \equiv 0 \ (mod\ p)$. Uma vez que $\mathfrak{p}^2 \subset \mathfrak{p}$, consideremos $\alpha \in \mathfrak{p}$ e vejamos sob quais condições $\alpha \in \mathfrak{p}^2$. Desse modo, como $\alpha \in \mathfrak{p}$ segue que do caso anterior que $c_0 = f(1) \equiv 0 \ (mod\ p)$, e portanto, $c_0 \in \mathfrak{p}^{p-1}$. Daí, segue que

$$(1-\zeta_p)^{p-1}c_{p-1} + (1-\zeta_p)^{p-2}c_{p-2} + \cdots + (1-\zeta_p)^2 c_2 + c_0 \in \mathfrak{p}^2.$$

Assim, $\alpha \in \mathfrak{p}^2$, se e somente se, $(1-\zeta_p)c_1 \in \mathfrak{p}^2$, que é equivalente a $c_1 \in \mathfrak{p}$. Uma vez que $f'(1) = -2c_1$, segue que $\alpha \in \mathfrak{p}^2$ se, e somente se, $f(1) \equiv f'(1) \equiv 0 \ (mod\ p)$. Sabendo que $\mathfrak{p}^{n+1} \subset \mathfrak{p}^n \subset \cdots \subset \mathfrak{p}^2 \subset \mathfrak{p}$, fazendo sucessivamente o mesmo processo, prova-se o resultado para $n+1 \leq p-1$. ■

Vejamos se a partir destes ideais principais conseguimos aumentar a densidade de centro com relação à $\mathcal{O}_{\mathbb{K}}$. Pela Equação 4.5, quando $m = 1$ segue que o menor traço é $2p$. Para provarmos o caso em que $m = 2$, utilizaremos o seguinte resultado, já conhecido.

Lema 4.19. *Seja $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Se x em $\mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ é par.*

Demonstração. Pelo Teorema 4.11, basta provarmos que

$$p\sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2 \equiv 0 \ (mod\ 2).$$

Visto que p é um primo ímpar, tomando a congruência módulo 2, segue que

$$\begin{aligned} p\sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2 &\equiv \sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2 \pmod 2 \\ &\equiv \sum_{i=0}^{p-2} a_i^2 - \sum_{i=0}^{p-2} a_i \pmod 2 \\ &\equiv \sum_{i=0}^{p-2} a_i - \sum_{i=0}^{p-2} a_i \pmod 2 \\ &\equiv 0 \pmod 2. \end{aligned}$$

Logo, $p\sum_{i=0}^{p-2} a_i^2 - \left(\sum_{i=0}^{p-2} a_i\right)^2$ é par. ■

Agora, seja $x = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$ um elemento de $\mathfrak{p}^2$. Afirmamos que:

$$\min\{Tr(x\overline{x}); x \in \mathfrak{p}^2\} = 4p.$$

De fato, seja $t = \min\{Tr(x\overline{x}); x \in \mathfrak{p}^2\}$. Pelo Lema 4.19, concluímos que o $Tr(x\overline{x})$ é par e uma vez que $\mathfrak{p}^2 \subset \mathfrak{p}$, segue que t é par e múltiplo de p. Assim, justifiquemos que $t \neq 2p$. Para $t = 2$, pela forma quadrática, segue que obrigatoriamente $x = a_j\zeta_p^j + a_k\zeta_p^k$,

onde $a_j = \pm 1$ e $a_k = \pm 1$. Por outro lado, como $x \in \mathfrak{p}$, segue que $a_j + a_k = 0$. Logo, suponhamos sem perda de generalidade que $a_j = 1$ e $a_k = -1$. Assim, $x = \zeta_p^j - \zeta_p^k$, porém,

$$\zeta_p^j - \zeta_p^k \notin \mathfrak{p}^2.$$

Agora, supondo sem perda de generalidade que $j < k$ e supondo por absurdo que $x \in \mathfrak{p}^2$ segue que

$$\begin{cases} \zeta_p^j - \zeta_p^k = (1 - \zeta_p^{k-j})\zeta_p^j \\ \zeta_p^j - \zeta_p^k = (1 - \zeta_p)^2\epsilon, \quad \text{com} \quad \epsilon \in \mathcal{O}_{\mathbb{K}}. \end{cases}$$

Daí, $(1 - \zeta_p^{k-j})\zeta_p^j = (1 - \zeta_p)^2\epsilon$, e aplicando a norma em ambos os lados segue que

$$N\Big((1 - \zeta_p^{k-j})\zeta_p^j\Big) = N\Big((1 - \zeta_p)^2\epsilon\Big),$$

ou seja,

$$p - 1 = p^2 N(\epsilon).$$

O que é uma contradição, e assim $t \neq 2p$. De tudo que foi exposto, concluímos que $t \geq 4p$. Note que, pelo Teorema 4.18, podemos verificar que o elemento $y = \zeta_p - \zeta_p^2 - \zeta_p^3 + \zeta_p^4$ pertence a $\mathfrak{p}^2$. Além disso, $Tr(y\overline{y}) = 4p$. Portanto, $t = 4p$. Para o caso geral, não faremos a demonstração, uma vez que esta seção tem por objetivo falar sobre as aplicações, contudo o resultado é:

$$\min\{Tr(x\overline{x}); x \in \mathfrak{p}^m\} \geq 2pm.$$

Portanto, com essa informação, fixando p podemos verificar qual é a fórmula da densidade de centro para o reticulado $\sigma_{\mathbb{L}}(\mathfrak{p}^m)$. Para isso, utilizando a Proposição 4.9, segue que

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p}^m)) \geq \frac{2^{(p-1)/2} \cdot \left(\frac{\sqrt{pm}}{2}\right)^{p-1}}{p^{(p-2)/2} \cdot p^m} = \frac{2^{(p-1)/2} \cdot (pm)^{(p-1)/2}}{2^{(p-1)} \cdot p^{(p-2)/2} \cdot p^m} =$$

$$= \frac{m^{(p-1)/2} \cdot p^{(p-1)/2}}{2^{(p-1)/2} \cdot p^{(p-2)/2} \cdot p^m} = \frac{m^{(p-1)/2} \cdot p^{1/2}}{2^{(p-1)/2}} \cdot p^m =$$

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

Portanto, fixando p, vamos exibir uma fórmula da densidade de centro para o reticulado $\sigma_{\mathbb{L}}(\mathfrak{p}^m)$, com m inteiro positivo. Tal fórmula é válida para $m < \frac{p-1}{2}$:

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p}^m)) = \frac{m^{(p-1)/2}}{2^{(p-1)/2} \cdot p^{(2m-1)/2}}, \tag{4.7}$$

que podemos reescrever da seguinte forma:

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p}^m)) = c \cdot \frac{m^{(p-1)/2}}{p^m},$$

onde, $c = \left(\frac{p}{2^{(p-1)}}\right)^{1/2}$ que não depende de m. Sendo assim, para descobrirmos qual m fornece o ponto máximo, basta derivar a expressão com relação a m. Assim,

$$\frac{\partial(c \cdot \frac{m^{(p-1)/2}}{p^m})}{\partial m} = m^{(p-3)/2}\frac{\left(\frac{p-1}{2} - m\ ln\ p\right)}{p^m}.$$

Visto que $c \cdot m^{(p-3)/2} > 0$, concluímos que essa expressão é zero quando $m = \frac{p-1}{2ln\ p}$. Agora, voltando no Exemplo 4.6, segue que

$$m = \frac{19-1}{2ln\ 19} \approx 3,0566.$$

Sendo assim,

$$\sigma_{\mathbb{L}}(\mathfrak{p}^3) = \frac{3^9}{2^9 \cdot \sqrt{19^5}} \approx 0,02444,$$

onde, apesar de ainda não atingir o recorde para esta dimensão, tem uma densidade de centro maior que a do reticulado obtido a partir do ideal $\mathfrak{p}$.

5 CONCLUSÃO

Diante do que foi exposto, percebemos que a Teoria Algébrica dos Números pode servir como uma ferramenta muito eficaz para o estudo dos reticulados, visto que a imagem de um ideal do anel dos inteiros algébricos de um corpo de números pelo homomorfismo canônico é um reticulado. Verificamos também a importância dos conceitos de discriminante, forma quadrática e do traço relativo, que se mostraram informações essenciais para efetuar o cálculo da densidade de centro de reticulados algébricos. No Capítulo 4, vimos uma forma de obter reticulados a partir da imagem do ideal $\mathfrak{p}^m$, com m um número inteiro positivo, pelo homomorfismo canônico e calcular sua densidade de centro. Estes reticulados são chamados de família de Craig, que quando surgiram em 1978 bateram o recorde de densidade de centro para as dimensões $148 \leq p-1 \leq 3000$, onde p é um número primo.

Nesse contexto, as aplicações dadas no Capítulo 4 deste trabalho abordaram alguns reticulados de posto máximo no espaço euclidiano $p-1$ dimensional, onde p é um número primo. Uma vez que as densidades de centro da Família de Craig foram as maiores densidades conhecidas na época, e que atualmente nem todas essas densidades de centro continuam sendo o recorde, ainda tem muito do que se explorar nessas dimensões. A técnica abordada foi por meio dos ideais principais gerados por uma potência de $(1-\zeta_p)$. Então, pode-se dar continuidade nesse estudo, verificando para outros ideais do anel dos inteiros algébricos de $\mathbb{Q}(\zeta_p)$. Também, por consequência do Teorema de Kroneker-Weber e do que foi exposto no Capítulo 3, é possível explorar outras dimensões, a partir de um corpo de números com condutor p.

REFERÊNCIAS

[1] CONWAY J. H.; SLOANE, N. J. A. *Sphere packings, lattices and groups*. 3. ed. New York: Springer-Verlag, 1998.

[2] ALACA S.; WILLIAMS, K. S. *Intruductory Algebraic Number Theory*. 1. ed. New York: Cambridge University Press, 2004.

[3] STEWART I.; TALL, D. *Algebric Number Theory*. Londres: Champman Hall, 1987.

[4] SAMUEL, P. *Algebraic Theory of Numbers*. 1. ed. Paris: Hermann, 1970.

[5] MARCUS, D. A. *Number Fields*. 1. ed. New York: Springer-Verlag, 1977.

[6] ANDRADE, A. A. *Uma Introdução à Teoria de Corpos*. 1. ed. São José do Rio Preto: Amazon.com, 2021.

[7] FACINI, L. S. *Uma introdução aos corpos não abelianos de grau menor ou igual a 6*. Dissertação (Mestrado) — UNESP, 2021.

[8] MILIES, C. P. *Anéis e Módulos*. 1. ed. São Paulo: Editora Livraria da Física, 2018.

[9] RIBENBOIM, P. *Classical theory of algebraic numbers*. 2. ed. New York: Springer Science & Business Media, 2013.

[10] MONTEIRO, L. H. J. *Teoria de Galois*. 1. ed. Rio de Janeiro: Impa, 1969.

[11] WASHINGTON, L. C. *Introduction to Cyclotomic Fields*. New York: Spring-Verlang, 1982.

[12] ROTMAN, J. J. *An Introduction to the Theory of Groups*. 4. ed. New York: Springer-Verlag, 1934.

[13] ARAUJO, R. R. *Anéis de inteiros de corpos de números e aplicações*. Dissertação (Mestrado) — UNESP, 2015.

[14] MELO, F. D. *Uma Forma Quadrática no Corpo de Condutor Primo*. Dissertação (Mestrado) — UNESP, 2005.

Índice Remissivo