

RESSALVA

Atendendo solicitação da autora,
o texto completo desta tese será
disponibilizado somente a partir
de 07/03/2026



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”

Câmpus de São José do Rio Preto

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma
família de corpos de números cujo grau é uma
potência de 2

São José do Rio Preto
2024

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma
família de corpos de números cujo grau é uma
potência de 2

Tese apresentada como parte dos requisitos para obtenção do título de Doutor em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto
2024

E79a

Esteves, Livea Cichito

Anel de inteiros algébricos e discriminante de uma família de corpos de números cujo grau é uma potência de 2 / Livea Cichito Esteves. -- São José do Rio Preto, 2024

187 p.

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto

Orientador: Antônio Aparecido de Andrade

1. Corpo de números. 2. Corpos puros. 3. Anel de inteiros algébricos. 4. Base integral. 5. Discriminante. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Livea Cichito Esteves

Anel de inteiros algébricos e discriminante de uma
família de corpos de números cujo grau é uma
potência de 2

Tese apresentada como parte dos requisitos para obtenção do título de Doutor em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Orientador

Prof. Dr. Agnaldo J. Ferrari
F. C. - Unesp, Bauru - SP

Prof. Dr. Trajano P. da Nóbrega Neto
Ibilce - Unesp, S. J. Rio Preto - SP

Prof. Dr. Edson D. de Carvalho
Feis - Unesp, Ilha Solteira - SP

Prof. Dr. Robson R. de Araujo
IFSP, Catanduva - SP

São José do Rio Preto
07 de março de 2024

*Às pessoas mais importantes da minha vida:
João Carlos, Maria Ines, Murilo e Rafael,
dedico.*

AGRADECIMENTOS

Durante os quatro anos em que realizei o curso de Doutorado e a elaboração desta tese, tive o apoio de várias pessoas que foram fundamentais para realização deste sonho e, por isso, quero expressar aqui a minha gratidão.

Agradeço primeiramente a Deus, por me dar saúde, força e sabedoria para superar os momentos de dificuldade.

Aos meus pais, João Carlos e Maria Ines, e ao meu irmão, Rafael, por todo amor, apoio e carinho em todos os momentos.

Ao meu namorado, Murilo, por todo amor e cuidado, por me incentivar e me encorajar a prosseguir nos estudos, além de toda paciência e ajuda nos mais diversos momentos.

À minha amiga e parceira de pesquisa, Linara, por todo o conhecimento compartilhado durante a realização deste trabalho e a todos os amigos com quem compartilhei momentos de aprendizado e de diversão.

Ao meu orientador, Toninho, por toda paciência e dedicação em me orientar e pelos valiosos ensinamentos.

Aos professores titulares da banca examinadora, Prof. Dr. Trajano Pires da Nóbrega Neto (Unesp - São José do Rio Preto), Prof. Dr. Robson Ricardo de Araujo (IFSP - Catanduva), Prof. Dr. Agnaldo José Ferrari (Unesp - Bauru), Prof. Dr. Edson Donizete de Carvalho (Unesp - Ilha Solteira), e aos professores suplentes da banca examinadora, Prof. Dr. Everton Luiz de Oliveira (UFMS - Campo Grande), Profa. Dra. Cintya Wink De Oliveira Benedito (Unesp - São João da Boa Vista) e Prof. Dr. Leandro Bezerra de Lima (UFMS - Campo Grande), por aceitarem o convite e pelas valiosas contribuições ao trabalho.

À Capes, pelo apoio financeiro.

A todos que direta ou indiretamente contribuíram na realização deste trabalho.

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

*A beleza da matemática só se mostra
aos seguidores mais pacientes.*

Maryam Mirzakhani

RESUMO

O objetivo deste trabalho é apresentar a estrutura do anel de inteiros algébricos e o discriminante do anel de inteiros algébricos de corpos de números do tipo $\mathbb{L} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[k]{d}$ e $d \neq 1$ é um inteiro livre de quadrados. Inicialmente, apresentamos a estrutura dos anéis de inteiros algébricos dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$ com $d \equiv 2, 3 \pmod{4}$ onde, nesse caso, $\mathbb{L}$ é monogênico. Na sequência, apresentamos bases integrais e os respectivos discriminantes para alguns corpos da forma $\mathbb{Q}(\sqrt[k]{d})$, para $k = 2, 3, 4, 5$, onde exploramos as estruturas dos anéis de inteiros algébricos de acordo com os valores de d . Posteriormente, como resultados principais desta tese, generalizamos essas bases e, com isso, também determinamos uma fórmula para o discriminante do anel de inteiros algébricos desses corpos $\mathbb{L}$. Nessa linha, apresentamos essas generalizações da seguinte forma: quando $d \equiv 5 \pmod{8}$, quando $d \equiv 9 \pmod{16}$ e, por fim, englobando todos os casos, apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos puros $\mathbb{Q}(\sqrt[k]{d})$ para $d \equiv 2^l + 1 \pmod{2^{l+1}}$ onde $2 \leq l \leq k - 1$ e para $d \equiv 1 \pmod{2^{k+1}}$.

Palavras-chave: Corpo de números. Corpos puros. Anel de inteiros algébricos. Base integral. Discriminante.

ABSTRACT

The objective of this work is to present an integral basis and the discriminant of algebraic number fields of the type $\mathbb{L} = \mathbb{Q}(\theta)$, where $\theta = \sqrt[k]{d}$ and $d \neq 1$ is a square-free integer. Initially, we present the rings of algebraic integers of fields $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$ with $d \equiv 2, 3 \pmod{4}$ where, in this case, $\mathbb{L}$ is monogenic. Afterwards, we present integral bases and the respective discriminants for some fields of the form $\mathbb{Q}(\sqrt[k]{d})$, for $k = 2, 3, 4, 5$, exploring their algebraic integer rings according to the values of d . Subsequently, as the main results of this thesis, comprising the main part of this work, we generalize these bases and, with this, we also determine a formula for the discriminant of these fields $\mathbb{L}$. Along these lines, we present these generalizations as follows: when $d \equiv 5 \pmod{8}$, when $d \equiv 9 \pmod{16}$, and finally, encompassing all cases, we present an integral basis and the discriminant of pure fields $\mathbb{Q}(\sqrt[k]{d})$ for $d \equiv 2^l + 1 \pmod{2^{l+1}}$ where $2 \leq l \leq k - 1$ and for $d \equiv 1 \pmod{2^{k+1}}$.

Keywords: Number field. Pure fields. Ring of algebraic integers. Integral bases. Discriminant.

Lista de Símbolos

$\equiv$	Equivalência
$\mathbb{N}$	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
$\mathbb{L}$	Corpo de números $\mathbb{L}$
$\mathcal{O}_{\mathbb{L}}$	anel de inteiros algébricos do corpo $\mathbb{L}$
$Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$	Traço do elemento $\alpha \in \mathbb{L}$ na extensão $\mathbb{L}/\mathbb{K}$
$N_{\mathbb{L}/\mathbb{K}}(\alpha)$	Norma do elemento $\alpha \in \mathbb{L}$ na extensão $\mathbb{L}/\mathbb{K}$
$N_{\mathbb{L}}(I)$	Norma do ideal $I \subset \mathcal{O}_{\mathbb{L}}$
$D(\mathbb{L})$	discriminante do anel de inteiros algébricos do corpo $\mathbb{L}$
$\det[A]$	Determinante da matriz A

Sumário

Introdução	19
1 Resultados básicos de teoria algébrica dos números	23
1.1 Traço e norma	23
1.2 Anel de inteiros algébricos	24
1.3 Base integral	25
1.4 Anel de Dedekind	26
1.5 Discriminante	28
1.6 O corpo $\mathbb{Q}(\sqrt[n]{d})$, com $d \neq 1$ um inteiro livre de quadrados	30
1.7 Considerações finais	31
2 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $d \equiv 2, 3 \pmod{4}$	33
2.1 Anel de inteiros algébricos	34
2.2 Discriminante	35
2.3 Considerações finais	36
3 Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[2^k]{d})$, onde $2 \leq k \leq 5$	37
3.1 Base integral e discriminante do corpo puro de grau 4	37
3.1.1 Anel de inteiros algébricos	38
3.1.2 Discriminante	44
3.2 Base integral e discriminante do corpo puro de grau 8	46
3.2.1 Anel de inteiros algébricos	46
3.2.2 Discriminante	58
3.3 Base integral e discriminante do corpo puro de grau 16	60
3.3.1 Anel de inteiros algébricos	60
3.3.2 Discriminante	84
3.4 Base integral e discriminante do corpo puro de grau 32	85
3.5 Considerações finais	86

4	Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[k]{d})$, onde $d \equiv 5 \pmod{8}$	87
4.1	Anel de inteiros algébricos	87
4.2	Discriminante	101
4.3	Considerações finais	108
5	Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[k]{d})$, onde $d \equiv 9 \pmod{16}$	109
5.1	Anel de inteiros algébricos	109
5.2	Discriminante	122
5.3	Considerações finais	123
6	Base integral e discriminante do corpo $\mathbb{Q}(\sqrt[k]{d})$	125
6.1	Anel de inteiros algébricos	125
6.2	Discriminante	171
6.3	Exemplos	176
6.4	Considerações finais	177
7	Conclusão e perspectivas futuras	179
	Referências	183
	Índice Remissivo	187

Introdução

A Teoria dos Números é uma das clássicas linhas de pesquisas da matemática na qual o estudo está centrado no conceito de números inteiros e objetos relacionados como, por exemplo, a quantidade de números primos contidos no conjunto dos números inteiros, além da resolução de equações diofantinas. Podemos citar como um clássico problema dessa área o Último Teorema de Fermat, cujas tentativas de demonstrá-lo, que perduraram mais de três séculos, trouxeram diversos avanços em linhas de pesquisas distintas da matemática.

Um dos ramos dentro da Teoria dos Números é a Teoria Algébrica dos Números, cujo foco é a expansão do conceito de número inteiro. Mais precisamente, consiste no estudo de números complexos que são raízes de polinômios cujos coeficientes são racionais, os quais são chamados números algébricos. Além disso, se os polinômios em questão são mônicos e seus coeficientes são inteiros, suas raízes são conhecidas como inteiros algébricos e o conjunto formado por esses elementos de um corpo $\mathbb{L}$ de extensão finita sobre $\mathbb{Q}$ formam um anel, o qual recebe o nome de anel de inteiros algébricos do corpo $\mathbb{L}$.

O estudo desses anéis de inteiros algébricos de um corpo $\mathbb{L}$ possui grande relevância na Álgebra, principalmente na parte de aplicações. Dentre elas, destacam-se as construções de reticulados algébricos de boa densidade de centro, os quais são muito utilizados no estudo de códigos e criptografia, como pode ser visto, por exemplo, em [1] e [2]. De forma geral, essas construções são realizadas a partir do chamado Homomorfismo de Minkowski (canônico), o qual consiste em uma função aplicada sobre um $\mathbb{Z}$ -módulo do anel de inteiros algébricos de um corpo de números de dimensão n sobre $\mathbb{Q}$ que resulta em um reticulado no espaço $\mathbb{R}^n$. Quando falamos na densidade de centro de um reticulado algébrico, no caso do homomorfismo canônico, um dos parâmetros necessários para seu cálculo é o discriminante do anel de inteiros algébricos do corpo $\mathbb{L}$, que destaca-se por sua dificuldade.

Além dos reticulados de alta densidade, outro tipo tem sido muito relevante nos últimos anos: os reticulados bem arredondados (*well-rounded*), que são aqueles em que o conjunto de vetores de norma mínima do reticulado gera o $\mathbb{R}^n$ (para mais detalhes, veja, por

exemplo, [3]). As aplicações envolvendo esses tipos de reticulados incluem problemas referentes ao número de contato (*kissing number*) e à diversidade de reticulados (para detalhes veja, por exemplo, [4] e [5]). A vantagem de obter reticulados desse modo reside na possibilidade de identificar os pontos do reticulado no $\mathbb{R}^n$ com os elementos do corpo de números $\mathbb{L}$. Com isso em vista, determinar quais reticulados algébricos são bem arredondados tem sido tópico de estudo de vários pesquisadores e, para determiná-los, também se faz necessário o conhecimento do anel de inteiros algébricos do corpo. Inclusive, em [6] foi provado que a imagem do anel de inteiros algébricos de um corpo quadrático via homomorfismo de Minkowski é um reticulado bem arredondado para apenas dois corpos imaginários, $\mathbb{L} = \mathbb{Q}(i)$ e $\mathbb{L} = \mathbb{Q}(\sqrt{-3})$. Nesse sentido, é de grande importância conhecer o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos de um corpo de números (veja as Definições 1.14 e 1.35) para a utilização dessas ferramentas. Além disso, esses fatores também podem ser úteis no estudo recente de Criptografia pós-quântica, cujos detalhes podem ser vistos em [7].

A procura do anel de inteiros algébricos de corpos de números tem sido objeto de estudo de vários matemáticos nos últimos anos, e resultados significativos têm surgido acerca desse assunto, principalmente abordando os corpos monogênicos, isto é, os corpos cuja base integral é potente (veja [8], por exemplo). Em particular, no início de 2015, Hameed [9] publicou um trabalho no qual apresentou um resultado onde analisou valores de d tais que os corpos do tipo $\mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados e $k \in \mathbb{N}$ são monogênicos. Para isso, o autor utilizou o conceito de índice de um inteiro algébrico (para mais detalhes veja Capítulo 2).

Também em 2015, Hameed [10] publicou um outro trabalho que consiste em determinar mais bases integrais além das potentes para o corpo de grau $2^k = 8$. A estratégia adotada por Hameed foi a de utilizar uma base integral do corpo de grau 4 conhecida de outros trabalhos como, por exemplo, [11] e [12], e explorar a extensão $\mathbb{Q}(\sqrt[4]{d}) \subset \mathbb{Q}(\sqrt[8]{d})$, a qual possui grau 2. Vale destacar que determinar uma base integral de um corpo não monogênico é um trabalho complexo, justificando assim a escolha do autor em restringir-se ao corpo de grau $2^k = 8$ nesses trabalhos. Os resultados presentes nos artigos [9] e [10] também podem ser encontrados em [13], sua tese de doutorado.

Dentro do mesmo escopo, outros trabalhos também foram publicados recentemente. Em fevereiro de 2021, Yakkou e Fadil exploraram os corpos cujo grau é uma potência de 3, no trabalho "On power integral bases of certain pure number fields defined by $x^{3^r} - m$ ", encontrado em [14]. Também em 2021, tivemos a contribuição de Facini em sua dissertação de mestrado [15] "Uma introdução aos corpos não abelianos de grau menor ou igual a 6", onde usando o polinômio característico, foi dado o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos dos corpos do tipo $\mathbb{Q}(\sqrt[n]{d})$, onde $2 \leq n \leq 6$.

e $d \neq 1$ é um inteiro livre de quadrados. Em 2022, Yakkou publicou um trabalho focado em corpos não monogênicos [16], onde dado um corpo de números gerado pelo trinômio $x^n + ax^m + b$, o autor estabelece condições para a, b e n de modo que a base não seja a potente. Mais recentemente, em 2023, Fadil e Kchital no trabalho [17], intitulado "On monogeneity of certain pure number fields defined by $x^{2^r 7^s} - m$ ", analisam em quais casos os corpos de grau $2^r 7^s$ e $m \neq 1$ livre de quadrados são monogênicos utilizando a teoria de polígonos de Newton. Fugindo um pouco dos casos tradicionais em que são considerados m livre de quadrados, o trabalho [18] explora os corpos cúbicos do tipo $\mathbb{Q}(\sqrt[3]{m})$ tal que $m \neq 1$ é livre de cubos e não livre de quadrados, apresentando uma base integral e o discriminante do anel de inteiros algébricos para esses corpos.

Embora os corpos monogênicos sejam muito importantes para as aplicações, principalmente devido à sua simplicidade, os anéis de inteiros algébricos dos demais corpos também podem ser aplicados a diversos contextos e, contudo, têm sido bem menos explorados, de modo que seu estudo, geralmente, se limita em abordar apenas casos particulares, como, por exemplo, em [19] e [20]. Um dos motivos que justificam esse fato é a falta de uma ferramenta imediata para facilitar este trabalho, como o índice de um inteiro algébrico que favorece esse estudo para os corpos monogênicos. Tendo em vista os avanços realizados nos últimos anos, a importância para algumas aplicações e a menor exploração para os casos não monogênicos, o presente trabalho tem como principal objetivo determinar o anel de inteiros algébricos e o discriminante do anel de inteiros algébricos associado aos corpos de números do tipo $\mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e $k \in \mathbb{N}$, os quais são chamados de corpos puros (*pure fields*) de grau 2^k , explorando o caso monogênico, já apresentado por Hameed, mas também as demais bases possíveis. Para isso, o texto está organizado em seis capítulos, sendo o primeiro dedicado aos conceitos preliminares da teoria algébrica dos números e os demais, que em conjunto abordam casos particulares e gerais, constituem o nosso resultado principal.

No Capítulo 1 retomamos alguns conceitos básicos da Teoria dos Números, como traço e norma de elementos do corpo, anel de inteiros algébricos, base integral e discriminante do anel de inteiros algébricos do corpo de números, que constituem uma base da teoria aqui desenvolvida. Além disso, também foi retomada algumas definições e propriedades envolvendo anel de Dedekind e ramificação de ideais, pois esses conceitos serão necessários para provar uma das proposições fundamentais para o desenvolvimento do trabalho. Na última seção, também exploramos alguns fatos a respeito do corpo $\mathbb{Q}(\sqrt[n]{d})$, o qual será nosso principal objeto de estudo.

No Capítulo 2, baseado no artigo de Hameed, [9], apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[k]{d})$, com $d \neq 1$ um inteiro livre de quadrados e $d \equiv 2, 3 \pmod{4}$, por meio do conceito de índice

de um inteiro algébrico. Esse tipo de corpo tem uma importância particular, pois, como veremos no decorrer do capítulo, o mesmo é monogênico, ou seja, uma base de seu anel de inteiros algébricos é potente.

No Capítulo 3, apresentamos as bases integrais e os discriminantes do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[k]{d})$, para $k = 2, 3, 4, 5$, com $d \neq 1$ um inteiro e livre de quadrados. O objetivo desse capítulo é apresentar a estrutura dos anéis de inteiros algébricos explicitamente além de apresentar as demonstrações em detalhes, a fim de que o leitor possa criar familiaridade com os passos e estratégias utilizados, pois os mesmos serão generalizados posteriormente. Além disso, embora esse capítulo trate apenas de casos particulares, o mesmo será essencial para a conclusão do resultado final da presente tese.

Nos Capítulos 4 e 5, damos os primeiros passos rumo à generalização dos resultados apresentados no Capítulo 3, onde, no Capítulo 4 o estudo se centraliza no caso em que $d \equiv 5 \pmod{8}$ ou, equivalentemente, $d \equiv 1 \pmod{4}$ e 4 é a maior potência de 2 que divide $d - 1$. Fixando essa família de valores de $d \neq 1$, apresentamos uma base integral e o discriminante do anel de inteiros algébricos do corpo $\mathbb{Q}(\sqrt[k]{d})$, para todo $k \geq 1$. Já no Capítulo 5, nos concentramos no caso em que $d \equiv 9 \pmod{16}$ ou, equivalentemente, $d \equiv 1 \pmod{8}$ e 8 é a maior potência de 2 que divide $d - 1$ e, utilizando de raciocínio análogo, apresentamos uma base e o discriminante do anel de inteiros algébricos dos corpos de números da forma $\mathbb{Q}(\sqrt[k]{d})$, para todo $k \geq 2$, destacando as semelhanças e diferenças entre as duas demonstrações.

No Capítulo 6, que contém nossa principal contribuição deste trabalho, apresentamos as bases integrais dos corpos de números da forma $\mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é inteiro livre de quadrados. Para isso, levamos em consideração o grau do corpo em questão e também o valor de d , pois as potências de 2 em que vale $d \equiv 1 \pmod{2^l}$ também são cruciais para a determinação da base integral. Analisando esses dois fatores foi possível determinar as estruturas das bases que geram estruturas de anéis de inteiros algébricos distintas para cada corpo de acordo com o grau e o valor de d e descrevê-las explicitamente. Para isso, enunciamos e demonstramos um teorema que descreve uma base integral de $\mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e $d \equiv 1 \pmod{2^l}$, para todo $k \geq 1$ e $l \geq 2$. Uma vez que o anel de inteiros algébricos é conhecido, também calculamos todos os discriminantes associados a essas bases.

Vale destacar ainda que os resultados obtidos na Seção 3.3 do Capítulo 3 assim como os resultados apresentados nos Capítulos 4, 5 e 6 são originais deste trabalho.

7 Conclusão e perspectivas futuras

Neste trabalho, apresentamos uma base integral e o discriminante do anel de inteiros algébricos dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Provamos que o corpo $\mathbb{L}$ de grau $n = 2^k$ possui $k + 1$ estruturas de bases integrais distintas, a qual é determinada pelo valor de d , sendo uma quando $d \not\equiv 1 \pmod{4}$, e k possibilidades quando $d \equiv 1 \pmod{2^l}$, uma para cada valor de l , onde $2 \leq l \leq k + 1$, sendo 2^l a maior potência de 2 que divide $d - 1$, exceto quando $l = k + 1$, pois este corresponde ao maior valor de l que altera a estrutura da base. Desse modo, conhecendo o valor do grau $n = 2^k$ e o valor de d , é possível estabelecer uma base integral e o discriminante a ela associado para qualquer corpo $\mathbb{L}$ desse tipo.

No primeiro capítulo fizemos uma breve revisão de alguns conceitos da Teoria Algébrica dos Números, onde destacamos a Proposição 1.39, cuja importância no desenvolvimento das demonstrações ficou evidente em cada caso.

O segundo capítulo foi totalmente voltado aos corpos monogênicos, onde utilizando o conceito de índice e baseando-se em [10], descrevemos valores de d tais que o anel de inteiros algébricos do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$ possui base potente. Esse tipo de abordagem tem sido muito utilizada e dentro deste escopo é possível desenvolver vários trabalhos distintos, fixando alguma família de corpos de números e buscando os valores tal que uma base do anel de inteiros algébricos é uma base potente, por exemplo, podemos determinar os valores de d que tornam o corpo de números $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, onde $n = 3 \cdot 5^k \cdot 2^r$, monogênico. Ainda dentro dessa perspectiva, é possível analisar os valores de d tal que uma base do anel de inteiros algébricos é potente, não necessariamente sobre o conjunto dos números inteiros, mas sobre outros corpos intermediários. Observando os resultados apresentados neste trabalho, podemos constatar que dado $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$, tal que $d \equiv 2^l + 1 \pmod{2^{l+1}}$ para todo $2 \leq l \leq k - 1$, então $\mathbb{L}$ é monogênico sobre $\mathbb{K} = \mathbb{Q}(\sqrt[k-1]{d})$, já que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}}[\theta]$. Uma análise similar pode ser feita para diversos corpos em que é conhecida uma base integral sobre $\mathbb{Z}$.

No terceiro capítulo, em cada seção, apresentamos as bases integrais e os discriminantes a elas associados dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$ para algum caso particular, ou seja, especificando

o valor de k . Para cada valor de k analisado, designadamente, 4, 8, 16 e 32, percorremos todos os valores inteiros de $d \neq 1$ livre de quadrados e explicitamos tanto uma base do anel de inteiros algébricos como o discriminante, ambos em função do valor de d . Dessa forma, foi possível identificar o padrão que as bases seguem para cada valor de d , as quais se repetem periodicamente modulo 2^{k+1} , além de adquirir familiaridade com a técnica utilizada nas demonstrações, já que todos os casos foram detalhadamente demonstrados (exceto grau 32 por ser similar aos demais). Seguindo nessa linha, existem vários trabalhos na literatura que fixam um determinado grau e exploram os valores e congruências de d a fim de obter bases integrais para esses tipos de corpos, como por exemplo no artigo [31], onde dado o corpo $\mathbb{L} = \mathbb{Q}(\sqrt[6]{d})$, com $d \neq 1$ um inteiro livre de quadrados, foram apresentadas 6 estruturas de bases integrais distintas conforme a variação do valor de d . Nesse contexto, podemos considerar, por exemplo, o corpo de grau 10, ou seja, $\mathbb{L} = \mathbb{Q}(\sqrt[10]{d})$, com $d \neq 1$ um inteiro livre de quadrados e apresentar uma base integral de $\mathbb{L} = \mathbb{Q}(\sqrt[10]{d})$ para certos valores de d . Além disso, é possível analisar casos onde d não é livre de quadrados, como foi realizado, por exemplo, no artigo [18], onde foram determinadas bases integrais do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[3]{d})$, onde $d \neq 1$ não é livre de quadrados e é livre de cubos. Nesse sentido, considerando graus maiores, existem vários casos a serem explorados.

No quarto capítulo, focamos em determinar uma base integral do corpo $\mathbb{L} = \mathbb{Q}(\sqrt[2^k]{d})$ para uma família de valores de d formada pelos elementos tais que $d \equiv 5 \pmod{8}$, a qual é englobada em todos os corpos cujo grau é uma potência de 2, exceto no caso de grau 2. Além de explicitar uma base integral, também fornecemos uma fórmula que permite o cálculo do discriminante do anel de inteiros algébricos de $\mathbb{L}$ conhecendo-se apenas os valores de k e d . O quinto capítulo segue o mesmo raciocínio, porém a família de valores de d que analisamos são as formadas pelos elementos tal que $d \equiv 9 \pmod{16}$. Dentro dessa linha outros trabalhos podem ser analisados e generalizados. Podemos considerar, por exemplo, os corpos cujo grau é uma potência de 3 do tipo $\mathbb{L} = \mathbb{Q}(\sqrt[3^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, pois através de uma análise de suas bases integrais é visível que seu anel de inteiros algébricos também possui um certo padrão em sua formação, onde o valor que determina a estrutura da base é o resto da divisão de d por 9 e de d por outras potências de 3. Assim, uma possibilidade de iniciar o estudo dos corpos cujo grau é uma potência de 3, é fixando, por exemplo, os corpos $\mathbb{L} = \mathbb{Q}(\sqrt[3^k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados e tal que $d \equiv 10 \pmod{27}$ determinando uma base do anel de inteiros algébricos restrito a esse caso. Uma vez que se tenha respondido a essa questão, pode-se avançar para a família de valores de $d \neq 1$ tal que $d \equiv 28 \pmod{81}$, e assim, sucessivamente.

Agora, no sexto capítulo, estendemos os resultados feitos nos capítulos anteriores

apresentando uma base integral e o discriminante do anel de inteiros algébricos para qualquer corpo puro da forma $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados. Partindo desse mesmo raciocínio, outras famílias de corpos podem ser analisadas a fim de encontrar uma base do anel de inteiros algébricos e o seu discriminante, como por exemplo, os corpos $\mathbb{L} = \mathbb{Q}(\sqrt[k]{d})$, onde $d \neq 1$ não é livre de quadrados ou os corpos puros de grau $3 \cdot 2^k$, com $k \in \mathbb{N}$, da forma $\mathbb{L} = \mathbb{Q}(\sqrt[3 \cdot 2^k]{d})$, uma vez que o grau da extensão $\mathbb{K} \subset \mathbb{L}$ para $\mathbb{K} = \mathbb{Q}(\sqrt[3 \cdot 2^{k-1}]{d})$ também é 2, possibilitando utilizar o mesmo raciocínio utilizado nesse trabalho. Analisar famílias de corpos desta natureza é pertinente, já que existem vários artigos explorando os corpos de grau 6 e, neste caso, o estudo dos corpos $\mathbb{L} = \mathbb{Q}(\sqrt[3 \cdot 2^k]{d})$ representa uma generalização.

Finalmente, vale ressaltar também, que a presente tese foi desenvolvida sempre direcionando a análise da parte teórica. Neste sentido, existem várias possibilidades de estudos de corpos puros da forma $\mathbb{L} = \mathbb{Q}(\sqrt[n]{d})$, onde $d \neq 1$ é um inteiro livre de quadrados, tanto na parte teórica quanto na parte de aplicações. Nesta linha, encaminhando-se agora para a parte das aplicações, utilizando os resultados aqui apresentados, é possível analisar a teoria de reticulados algébricos via o homomorfismo canônico tanto na busca de reticulados em relação à densidade de centro, quanto na busca de reticulados bem arredondados cujo grau é uma potência de 2, ou seja, buscar reticulados de grau 2^k que possuem boas propriedades. Entretanto, como nesse caso o corpo $\mathbb{L}$ é misto, ou seja, possui monomorfismos reais e complexos, existe a necessidade de explorar uma forma traço para o seu cálculo, uma vez que a forma traço conhecida é dada para corpos totalmente imaginários ou corpos totalmente reais. Assim, determinar essa fórmula é mais um dos possíveis trabalhos que podem ser desenvolvidos futuramente.

Referências

- [1] ANDRADE, A. A. et al. Constructions of dense lattices over number fields. *TEMA Tend. Mat. Apl. Comput.*, v. 21, n. 1, p. 57–63, 2020. ISSN 1677-1966,2179-8451. Disponível em: <<https://doi.org/10.5540/tema.2020.021.01.57>>.
- [2] ARAUJO, R. R. de. *Reticulados algébricos e aplicações a códigos e criptografia*. Tese (Doutorado) — Unicamp, 2018.
- [3] SICUTI, P. G. *Um estudo sobre reticulados algébricos bem arredondados*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho”-IBILCE, 2020.
- [4] MUSIN, O. R. The kissing number in four dimensions. *Ann. of Math. (2)*, v. 168, n. 1, p. 1–32, 2008. ISSN 0003-486X,1939-8980. Disponível em: <<https://doi.org/10.4007/annals.2008.168.1>>.
- [5] FERRARI, A. J.; SOUZA, T. M. R. Rotated A_n -lattice codes of full diversity. *Adv. Math. Commun.*, v. 16, n. 3, p. 439–447, 2022. ISSN 1930-5346,1930-5338. Disponível em: <<https://doi.org/10.3934/amc.2020118>>.
- [6] FUKSHANSKY, L.; PETERSEN, K. On well-rounded ideal lattices. *Int. J. Number Theory*, v. 8, n. 1, p. 189–206, 2012. ISSN 1793-0421,1793-7310. Disponível em: <<https://doi.org/10.1142/S179304211250011X>>.
- [7] LANGE, T.; STEINWANDT, R. (Ed.). *Post-quantum cryptography. 9th international conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018. Proceedings*. [S.l.]: Cham: Springer, 2018. v. 10786. (Lect. Notes Comput. Sci., v. 10786). ISSN 0302-9743. ISBN 978-3-319-79062-6; 978-3-319-79063-3.
- [8] YAKKOU, H. B.; FADIL, L. E. On monogeneity of certain pure number fields defined by $x^{p^r} - m$. *Int. J. Number Theory*, v. 17, n. 10, p. 2235–2242, 2021. ISSN 1793-0421,1793-7310. Disponível em: <<https://doi.org/10.1142/S1793042121500858>>.

-
- [9] HAMEED, A. et al. On existence of canonical number system in certain classes of pure algebraic number fields. *J. Prime Res. Math.*, v. 7, p. 19–24, 2011. ISSN 1817-2725.
- [10] HAMEED, A.; NAKAHARA, T. Integral bases and relative monogeneity of pure octic fields. *Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér.*, v. 58, n. 4, p. 419–433, 2015. ISSN 1220-3874.
- [11] FUNAKURA, T. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, v. 26, p. 27–41, 1984. ISSN 0030-1566.
- [12] ANDRADE, A. A.; FACINI, L. S.; ESTEVES, L. C. Algebraic intergers of pure quartic extensions. *International Journal of Apllied Mathematics*, v. 36, n. 1, p. 99–106, 2023. ISSN 1314-8060.
- [13] HAMEED, A. *On Pure Octic Fields Related to a Problem of Hasse*. Tese (Doutorado) — National University of Computer and Emerging Sciences, 2015.
- [14] YAKKOU, H. B.; KCHIT, O. On power integral bases of certain pure number fields defined by $x^{3^r} - m$. *São Paulo J. Math. Sci.*, v. 16, n. 2, p. 1072–1079, 2022. ISSN 1982-6907,2316-9028. Disponível em: <<https://doi.org/10.1007/s40863-021-00251-2>>.
- [15] FACINI, L. S. *Uma introdução aos corpos não abelianos de grau menor ou igual a 6*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho”-IBILCE, 2021.
- [16] YAKKOU, H. B. On nonmonogenic number fields defined by trinomials of type $x^n + ax^m + b$. *Rocky Mountain J. Math.*, v. 53, n. 3, p. 685–699, 2023. ISSN 0035-7596,1945-3795. Disponível em: <<https://doi.org/10.1216/rmj.2023.53.685>>.
- [17] FADIL, L. E.; KCHIT, O. On monogeneity of certain pure number fields defined by $x^{2^r \cdot 7^s} - m$. *Bol. Soc. Parana. Mat. (3)*, v. 41, p. 1–9, 2023. ISSN 0037-8712,2175-1188. Disponível em: <<https://doi.org/10.5269/bspm.62352>>.
- [18] ANDRADE, A.; FACINI, L.; ESTEVES, L. Algebraic integers of certain cubic extensions: Inteiros algébricos de certas extensões cúbicas. *Brazilian Journal of Development*, v. 8, n. 8, p. 56768–56786, 2022.
- [19] GAÁL, I.; REMETE, L. Non-monogeneity in a family of octic fields. *Rocky Mountain J. Math.*, v. 47, n. 3, p. 817–824, 2017. ISSN 0035-7596,1945-3795. Disponível em: <<https://doi.org/10.1216/RMJ-2017-47-3-817>>.

-
- [20] CHANG, M.-L. Non-monogeneity in a family of sextic fields. *J. Number Theory*, v. 97, n. 2, p. 252–268, 2002. ISSN 0022-314X,1096-1658. Disponível em: <[https://doi.org/10.1016/S0022-314X\(02\)00004-5](https://doi.org/10.1016/S0022-314X(02)00004-5)>.
- [21] MARCUS, D. A. *Number theory*. 1. ed. New York: Springer-Verlag, 1977.
- [22] SAMUEL, P. *Algebraic theory of numbers*. 1. ed. Paris: Hermann, 1970.
- [23] ALACA, S.; WILLIAMS, K. S. *Introductory algebraic number theory*. 1. ed. New York: Cambridge University Press, 2004.
- [24] ANDRADE, A. A. de. *Uma introdução a teoria algébrica dos números*. 1. ed. São José do Rio Preto - SP: Amazon.com, 2021.
- [25] ARAUJO, R. R. de. *Anéis de inteiros de corpos de números e aplicações*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho” - IBILCE, 2015.
- [26] NARKIEWICS, W. *Elementary and analytic theory of algebraic numbers*. 3. ed. Brasília: Springer-Verlag, 2004.
- [27] VICENTE, J. P. G. *Reticulados de posto 3 em corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho”-IBILCE, 2000.
- [28] RODRIGUES, V. C. da S. *Reticulados de posto 4 em corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho”-IBILCE, 2001.
- [29] RIBEIRO, A. C. *Reticulados sobre corpos de números*. Dissertação (Mestrado) — Universidade Estadual Paulista “Júlio de Mesquita Filho”-IBILCE, 2003.
- [30] REMETE, L. Integral bases of pure fields with square-free parameter. *Studia Sci. Math. Hungar.*, v. 57, n. 1, p. 91–115, 2020. ISSN 0081-6906,1588-2896. Disponível em: <<https://doi.org/10.1556/012.2020.57.1.1450>>.
- [31] ANDRADE, A. A.; FACINI, L. S.; ESTEVES, L. C. Algebraic intergers of pure sextic extensions. *Journal of Prime Reaserch in Mathematics*, v. 18, n. 2, p. 112–124, 2022.