

RESSALVA

Atendendo solicitação do autor,
o texto completo desta tese será
disponibilizado somente a partir
de 16/06/2027



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Câmpus de São José do Rio Preto

PLÍNIO GABRIEL SICUTI

**Reticulados via álgebras dos quatérnios sobre corpos
quadráticos imaginários e certos corpos ciclotômicos de grau
potência de dois sobre os racionais**

São José do Rio Preto

2025

Plínio Gabriel Sicuti

Reticulados via álgebras dos quatérnios sobre corpos quadráticos imaginários e certos corpos ciclotômicos de grau potência de dois sobre os racionais

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

Área de Concentração: Álgebra

Orientadora: Profa. Dra. Carina Alves
(UNESP)

Coorientador: Prof. Dr. Agnaldo José Ferrari
(UNESP)

São José do Rio Preto

2025

S567r

Sicuti, Plínio Gabriel

Reticulados via álgebras dos quatérnios sobre corpos quadráticos
imaginários e certos corpos ciclotômicos de grau potência de dois sobre os
racionais / Plínio Gabriel Sicuti. -- São José do Rio Preto, 2025
180 p.

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

Orientadora: Carina Alves

Coorientador: Agnaldo José Ferrari

1. Álgebras dos quatérnios. 2. Teoria algébrica dos números. 3. Corpos
ciclotômicos. 4. Reticulados algébricos. 5. Ordens maximais. I. Título.

PLÍNIO GABRIEL SICUTI

**RETICULADOS VIA ÁLGEBRAS DOS QUATÉRNIOS SOBRE CORPOS
QUADRÁTICOS IMAGINÁRIOS E CERTOS CORPOS CICLOTÔMICOS DE GRAU
POTÊNCIA DE DOIS SOBRE OS RACIONAIS :**

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

Área de Concentração: Álgebra

Data de defesa: 16/06/2025

BANCA EXAMINADORA

Profa. Dra. Carina Alves
Universidade Estadual Paulista (UNESP) – Câmpus de Rio Claro

Prof. Dr. Antônio Aparecido de Andrade
Universidade Estadual Paulista (UNESP) – Câmpus de São José do Rio Preto

Prof. Dr. Edson Donizete de Carvalho
Universidade Estadual Paulista (UNESP) – Câmpus de Ilha Solteira

Prof. Dr. Leandro Bezerra de Lima
Universidade Federal de Mato Grosso do Sul (UFMS)

Prof. Dr. Robson Ricardo de Araujo
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP)

À minha esposa, Cecília,
à minha filha, Sophie,
aos meus pais, Alcides e Ivani,
dedico.

AGRADECIMENTOS

À minha esposa, Cecília Ártico Banho, minha companheira de vida, deixo meu agradecimento mais profundo e emocionado. Em cada etapa desta longa jornada, estive ao meu lado com amor, paciência, generosidade e uma escuta sempre atenta. Nos momentos difíceis, foi apoio e tranquilidade; nos momentos felizes, compartilhou comigo cada conquista. Sem dúvida, foi a pessoa mais importante nesta caminhada, e saber que eu podia contar com sua presença deu sentido a cada esforço. Sou grato por ter compreendido meus silêncios, respeitado meu tempo de estudo e me incentivado com carinho e constância.

À minha filha, Sophie Ártico Sicuti, que chegou durante o doutorado e transformou completamente o meu mundo: o teu sorriso, as tuas risadas inocentes e a tua forma simples de enxergar a vida foram um alívio nas horas difíceis e uma fonte inesgotável de alegria. Mesmo sem saber, você esteve presente em cada linha desta tese. O amor que sinto por ti é infinito.

A vocês duas, minhas razões de viver, o meu amor eterno e minha gratidão sem fim.

Aos meus pais, Alcides Sidinei Sicuti e Ivani Ferreira Sicuti, agradeço pelo amor incondicional, pela educação que me deram e pelos valores que me ensinaram. Obrigado por sempre incentivarem meus estudos. Saibam que dar-lhes orgulho é, e sempre será, uma das maiores motivações da minha vida.

Aos amigos que a vida universitária me presenteou ao longo dos anos de graduação, mestrado e doutorado na UNESP, deixo meu sincero agradecimento. Compartilhar essa trajetória com pessoas tão generosas tornou o caminho mais leve e enriquecedor. Em especial, agradeço à minha amiga Isabela Mendes Cassio, cuja amizade ultrapassou os muros da universidade e permanece como uma das maiores conquistas que levo deste percurso. Sua presença, companheirismo e apoio foram fundamentais em muitos momentos.

Agradeço também aos alunos que tive o privilégio de acompanhar nos últimos anos. Compartilhar conhecimento com vocês deu sentido ao meu trabalho e renovou, dia após dia, a motivação para seguir ensinando e aprendendo. Ver o crescimento de cada um, suas descobertas e conquistas, reafirma minha convicção de que a educação transforma e de que ensinar é, acima de tudo, um ato de esperança.

Agradeço à minha orientadora, Profa. Dra. Carina Alves, e ao meu co-orientador, Prof. Dr. Agnaldo Ferrari, por toda confiança que depositaram em mim para o desenvolvimento deste trabalho e disponibilidade. Sou grato pelo aceite em integrar este projeto e, principalmente, pelas valiosas discussões, sugestões e ensinamentos que enriqueceram minha formação.

Aos membros da comissão examinadora por aceitarem o convite de compor a comissão e pelas valorosas contribuições ao trabalho.

Finalmente, à Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto, IBILCE, que me permitiu a realização deste sonho. E a todos que durante esses anos cruzaram meu caminho e acrescentaram conhecimentos e experiências.

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

“Believe in your heart.”
Ayumi Miyazaki, 1999, Brave Heart.

RESUMO

Esta tese apresenta construções algébricas do reticulado E_8 por meio da técnica que denominamos construção via representação matricial de módulos. Essa abordagem fundamenta-se no uso de ideais principais contidos em ordens maximais de álgebras de divisão dos quatérnios definidas sobre corpos quadráticos imaginários com número de classe 1, restringindo-se àquelas que minimizam o volume de Tamagawa, parâmetro diretamente relacionado ao desempenho de códigos espaço-tempo em sistemas MIMO. Em continuidade, investigamos álgebras de divisão dos quatérnios sobre corpos da forma $\mathbb{K} = \mathbb{Q}(\zeta_n)$, com $n = 2^r$ e $r \geq 2$, e caracterizamos o volume de reticulados de dimensão $4n$ por meio do homomorfismo canônico $\sigma_{\mathcal{A}}$, que associa elementos da álgebra a $\mathbb{R}^{4n}$. Essa construção permitiu desenvolver reticulados associados a ordens maximais e a ideais à esquerda nessas ordens. Por fim, apresentamos uma construção explícita de um reticulado a partir de um $\mathbb{Z}$ -módulo contido em uma ordem maximal de uma álgebra dos quatérnios sobre $\mathbb{K} = \mathbb{Q}(\zeta_8)$. As técnicas propostas ampliam as possibilidades de aplicação em criptografia e teoria dos códigos.

Palavras-Chave: álgebras dos quatérnios; teoria algébrica dos números; corpos ciclotômicos; reticulados algébricos; ordens maximais.

ABSTRACT

This thesis presents algebraic constructions of the E_8 lattice through a technique we refer to as the matrix representation of modules. This approach is based on the use of principal ideals contained in maximal orders of quaternion division algebras defined over imaginary quadratic fields with class number 1, restricted to those that minimize the Tamagawa volume, a parameter directly related to the performance of space-time codes in MIMO systems. Subsequently, we investigate quaternion division algebras over fields of the form $\mathbb{K} = \mathbb{Q}(\zeta_n)$, with $n = 2^r$ and $r \geq 2$, and characterize the volume of $4n$ -dimensional lattices via the canonical homomorphism $\sigma_{\mathcal{A}}$, which maps elements of the algebra to $\mathbb{R}^{4n}$. This construction enabled the development of lattices associated with maximal orders and left ideals in such orders. Finally, we provide an explicit construction of a lattice from a $\mathbb{Z}$ -module contained in a maximal order of a quaternion algebra over $\mathbb{K} = \mathbb{Q}(\zeta_8)$. The techniques introduced in this work broaden the range of potential applications in coding theory and cryptography.

Keywords: quaternion algebra; algebraic number theory; cyclotomic fields; algebraic lattices; maximal orders.

LISTA DE ILUSTRAÇÕES

Figura 1	Reticulado $\Lambda = \mathbb{Z}^2$	31
Figura 2	Região fundamental de $\Lambda = \mathbb{Z}^2$	32
Figura 3	Cadeia de extensões envolvendo a álgebra $\mathcal{A}$ e os corpos $\mathbb{L}$ e $\mathbb{K}$	42
Figura 4	Torre de corpos da álgebra $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$	51
Figura 5	Estrutura da álgebra $\mathcal{A} = (-p, -1)_{\mathbb{K}}$ definida sobre o corpo $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$	70
Figura 6	Álgebra $\mathcal{A} = (-3, -1)_{\mathbb{K}}$ definida sobre $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$	71
Figura 7	Álgebra $\mathcal{A} = (-7, -1)_{\mathbb{K}}$ definida sobre $\mathbb{K} = \mathbb{Q}(\sqrt{-19})$	75
Figura 8	Álgebra $\mathcal{A} = (-23, -1)_{\mathbb{K}}$ definida sobre $\mathbb{K} = \mathbb{Q}(\sqrt{-43})$	78
Figura 9	Álgebra $\mathcal{A} = (-19, -1)_{\mathbb{K}}$ definida sobre $\mathbb{K} = \mathbb{Q}(\sqrt{-67})$	81
Figura 10	Álgebra $\mathcal{A} = (-43, -1)_{\mathbb{K}}$ definida sobre $\mathbb{K} = \mathbb{Q}(\sqrt{-163})$	84
Figura 11	Torre de extensões	94
Figura 12	Subcorpos cíclicos entre $\mathbb{M}$ e $\mathbb{K}$ descritos pela correspondência de Galois e seus respectivos graus. $\mathbb{L}_s$ denota o subcorpo associado ao grupo $\langle \sigma^{p^s} \rangle$ para todo $s = 1, \dots, r - 1$	97
Figura 13	Correspondência entre corpos intermediários de $\mathbb{Q}(\zeta_q)$ e extensões de $\mathbb{K}$, com destaque para as extensões de grau 2 sob as condições do Teorema 4.8	101
Figura 14	Diagrama entre os corpos intermediários e as extensões associadas à álgebra cíclica $\mathcal{A}$	102

LISTA DE TABELAS

Tabela 1 – Pares (p, d) que satisfazem as condições da Proposição 3.11 para alguns valores fixos de d	67
Tabela 2 – Parâmetros e cálculo do volume de Tamagawa	69

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
Σ	Somatório
Π	Produtório
$\#A$	Cardinalidade do conjunto A
$\bar{x}$	Conjugado complexo de x
$\mathbb{K}, \mathbb{L}, \mathbb{M}, \mathbb{F}$	Corpos
$\mathbb{L} \mathbb{K}$	Extensão de corpos $\mathbb{L}$ sobre $\mathbb{K}$
$Gal(\mathbb{L} \mathbb{K})$	Grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$m_\alpha(x)$	Polinômio minimal de α
$Tr_{\mathbb{L} \mathbb{K}}(\alpha)$	Traço de α em relação à $\mathbb{L} \mathbb{K}$
$N_{\mathbb{L} \mathbb{K}}(\alpha)$	Norma de α em relação à $\mathbb{L} \mathbb{K}$
$D_{\mathbb{K}}$	Discriminante do corpo $\mathbb{K}$
$\sigma_{\mathbb{K}}$	Homomorfismo canônico de um corpo de números
ζ_n	Raiz primitiva n -ésima da unidade
$\varphi(n)$	Função de Euler aplicada a n
$\mathbb{Q}(\zeta_n)$	n -ésimo corpo ciclotômico
$M_n(\mathbb{K})$	Conjunto de matrizes de ordem n com entradas no corpo $\mathbb{K}$
$\det(M)$	Determinante da matriz M
Id_n	Matriz identidade de ordem n
$a \mid b$	a divide b

$a \equiv b \pmod{m}$ a congruente a b módulo m

$\Re(z)$ Parte real do número complexo z

$\Im(z)$ Parte imaginária do número complexo z

$\mathcal{I}, \mathcal{J}, \mathfrak{p}, \mathfrak{B}$ Ideais

$\langle \alpha \rangle$ Ideal principal gerado por α

SUMÁRIO

1	INTRODUÇÃO	16
2	PRELIMINARES	20
2.1	TEORIA ALGÉBRICA DOS NÚMEROS	20
2.2	CORPOS QUADRÁTICOS E CICLOTÔMICOS	23
2.3	RAMIFICAÇÃO DE IDEAIS	27
2.4	RETICULADOS E RETICULADOS ALGÉBRICOS	30
2.5	VALORAÇÃO p -ÁDICA	36
2.6	ÁLGEBRAS CÍCLICAS	38
2.7	ÁLGEBRAS DOS QUATÉRNIOS	43
2.8	ORDENS E DISCRIMINANTES	46
3	RETICULADOS VIA ORDENS MAXIMAIS DE ÁLGEBRAS DOS QUATÉRNIOS DEFINIDAS SOBRE CORPOS QUADRÁTICOS IMAGINÁRIOS	50
3.1	RETICULADOS OBTIDOS ATRAVÉS DA REPRESENTAÇÃO MATRICIAL DE MÓDULOS	51
3.2	PARÂMETROS PARA A CONSTRUÇÃO DE RETICULADOS E A FÓRMULA DO VOLUME DE TAMAGAWA	54
3.3	CARACTERIZAÇÃO DE IDEAIS EM ORDENS MAXIMAIS DE ÁLGEBRAS DOS QUATÉRNIOS	56
3.3.1	Escolha do ideal $\mathcal{I}$ para construção do reticulado E_8	58
3.3.1.1	Método para determinar $\mathcal{I}_1$	60
3.3.1.2	Método para determinar $\mathcal{I}_2$	61
3.4	CONSTRUÇÃO DE E_8 VIA $\mathcal{A} = (-p, -1)_{\mathbb{Q}(\sqrt{-d})}$, COM $d = 11, 19, 43, 67, 163$	62
3.4.1	Construção de E_8 via $\mathcal{A} = (-3, -1)_{\mathbb{Q}(\sqrt{-11})}$	71
3.4.2	Construção de E_8 via $\mathcal{A} = (-7, -1)_{\mathbb{Q}(\sqrt{-19})}$	74
3.4.3	Construção de E_8 via $\mathcal{A} = (-23, -1)_{\mathbb{Q}(\sqrt{-43})}$	77
3.4.4	Construção de E_8 via $\mathcal{A} = (-19, -1)_{\mathbb{Q}(\sqrt{-67})}$	80
3.4.5	Construção de E_8 via $\mathcal{A} = (-43, -1)_{\mathbb{Q}(\sqrt{-163})}$	83
3.5	CONSIDERAÇÕES FINAIS	87
4	CARACTERIZAÇÃO DO VOLUME DE RETICULADOS VIA ÁLGEBRAS DOS QUATÉRNIOS	88
4.1	HOMOMORFISMO CANÔNICO $\sigma_{\mathcal{A}}$	89

4.2	FAMÍLIAS DE ÁLGEBRAS DE DIVISÃO CÍCLICAS	92
4.3	CONSTRUÇÃO DE UMA FAMÍLIA DE ÁLGEBRA DOS QUATÉRNIOS	100
4.4	CARACTERIZAÇÃO DO VOLUME DE RETICULADOS VIA σ_A	102
4.5	CONSIDERAÇÕES FINAIS	130
5	CONSTRUÇÕES DE RETICULADOS VIA ORDENS MAXIMAIS, IDEAIS PRINCIPAIS E MÓDULOS DEFINIDOS EM ÁLGEBRAS DOS QUATÉRNIOS	131
5.1	VOLUME DE RETICULADOS VIA IDEAIS PRINCIPAIS EM ORDENS MAXIMAIS	132
5.2	CONSTRUÇÃO DE RETICULADOS VIA IDEAIS PRINCIPAIS EM ORDENS MAXIMAIS	136
5.2.1	Construção do reticulado $\mathbb{Z}^8$	136
5.2.2	Construção do reticulado E_8	142
5.2.3	Construção do reticulado $\mathbb{Z}^8 \oplus \sqrt{2} \cdot \mathbb{Z}^8$	145
5.2.4	Construção do reticulado $D_4 \oplus D_4 \oplus D_4 \oplus D_4$	151
5.3	CONSTRUÇÕES DE $\sqrt{2^{r-3}} \cdot \mathbb{Z}^{2^{r+1}}$ POR MEIO DE ORDENS MAXIMAIS	153
5.4	CONSTRUÇÃO DE RETICULADOS VIA $\mathbb{Z}$ -MÓDULOS EM ORDENS MAXIMAIS	169
5.4.1	Construção de um reticulado equivalente ao reticulado Λ_{16}	170
5.5	CONSIDERAÇÕES FINAIS	174
6	CONCLUSÃO E PERSPECTIVAS FUTURAS	175
	REFERÊNCIAS	177

1 INTRODUÇÃO

Reticulados são subgrupos aditivos discretos de $\mathbb{R}^n$, gerados por combinações lineares com coeficientes inteiros de vetores linearmente independentes. Essas estruturas desempenham papel central em diversas áreas da matemática, especialmente na teoria algébrica dos números, [1], [2] e [3], na codificação de informações e em sistemas de telecomunicações, sendo utilizados na construção de códigos corretores de erros eficientes [4].

A relevância dos reticulados estende-se à criptografia pós-quântica, [5] e [6], que explora problemas como LWE (Learning With Errors) e suas variantes RLWE (Ring-LWE) e CLWE (Cyclic Algebra LWE), que atuam como base para sistemas criptográficos seguros contra ataques de computadores quânticos, como descrito em [7]. Obras clássicas, como [8], estabeleceram uma base teórica sólida para essa área em crescimento.

Trabalhos recentes, como [4] e [9], têm explorado a relação entre propriedades de reticulados estudados na teoria algébrica dos números e sua eficácia como códigos corretores de erros. Tais estudos demonstram como construções com origem algébrica impactam diretamente tecnologias atuais em segurança digital e comunicação.

Na teoria da codificação para comunicações sem fio, reticulados são amplamente empregados em códigos de bloco espaço-tempo (Space-Time Block Codes), aplicados à transmissão de sinais em sistemas com múltiplas antenas, conhecidos como sistemas MIMO (Multiple Input Multiple Output), [10], [11], [12] e [13]. Nesses sistemas, a escolha de reticulados com boa densidade de empacotamento e simetria apropriada é decisiva para garantir robustez frente a ruídos e interferências.

Estruturas algébricas, como os anéis de inteiros de corpos de números e ordens maximais em álgebras dos quatérnios, fornecem uma base para construções de reticulados. Abordagens desse tipo, discutidas em [8] e [14], revelam como propriedades de ordens se refletem em propriedades dos reticulados. Em [9], os autores abordam o papel da teoria algébrica dos números no mundo das comunicações sem fio.

Álgebras de divisão cíclicas, em particular, as álgebras de divisão dos quatérnios, oferecem uma estrutura algébrica rica, adequada para representar transformações geométricas e resolver equações diofantinas. Tais estruturas são fundamentais em codificação e criptografia, devido à sua capacidade de combinar eficiência computacional com segurança, [15].

Em comunicações sem fio, álgebras cíclicas têm sido utilizadas com sucesso na construção de códigos espaço-tempo para sistemas MIMO, [10] e [16]. Essas construções se beneficiam das propriedades de ortogonalidade e alta taxa de transmissão oferecidas pelas álgebras dos quatérnios, resultando em códigos com bom desempenho em ambientes ruidosos, [17].

Em criptografia moderna, a segurança de muitos esquemas está fundamentada na dificuldade computacional de problemas matemáticos, como fatoração de inteiros, cálculo do logaritmo discreto, ou problemas em reticulados, cujas melhores soluções conhecidas requerem tempo

exponencial. Como mencionado, problemas como LWE e suas variantes sustentam sistemas seguros contra ataques quânticos, [5], [6] e [7]. Além disso, álgebras cíclicas têm sido aplicadas com êxito na construção de criptossistemas baseados em reticulados, conciliando segurança e viabilidade algorítmica.

A interação entre reticulados e álgebras de divisão cíclicas permite a construção de reticulados com propriedades ideais para aplicações em codificação e segurança da informação. Quando essas álgebras são definidas sobre corpos de números, é possível obter reticulados densos e bem estruturados. Reticulados construídos a partir de álgebras cíclicas, por exemplo, têm sido estudados em códigos espaço-tempo e esquemas criptográficos baseados em reticulados [9], [10] e [16].

O estudo dessas construções aprofunda a compreensão teórica e, simultaneamente, contribui para aplicações práticas relevantes, como transmissão segura de dados e otimização de desempenho em canais de comunicação.

Esta tese desenvolve construções algébricas de reticulados a partir de ordens maximais em álgebras dos quatérnios definidas sobre corpos quadráticos imaginários e certos corpos ciclotômicos, motivadas por aplicações potenciais em comunicação e criptografia, embora o foco esteja na análise teórica dessas estruturas.

Apresentamos novas construções de reticulados de dimensão 2^r , com $r > 2$, a partir de ideais principais e $\mathbb{Z}$ -módulos contidos em ordens maximais. Entre os principais resultados, destacamos a caracterização do volume de reticulados obtidos via o homomorfismo canônico associado a uma álgebra dos quatérnios definida sobre uma ordem maximal.

O Capítulo 2 apresenta os principais conceitos teóricos utilizados ao longo da tese, reunindo resultados da teoria algébrica dos números, da teoria dos reticulados e das álgebras dos quatérnios. Iniciamos com uma revisão da estrutura de corpos de números, seus anéis de inteiros, traço, norma, discriminante e extensões de Galois. Em seguida, abordamos de forma mais detalhada os corpos quadráticos e ciclotômicos, com ênfase na decomposição de ideais, na estrutura dos anéis $\mathcal{O}_{\mathbb{K}}$ e na análise de extensões ciclotômicas do tipo $\mathbb{Q}(\zeta_{2^r})$, com $r \geq 2$.

Na sequência, tratamos da teoria de ramificação de ideais, apresentando os conceitos de norma de um ideal, fatoração de primos em extensões, índice de ramificação, grau de inércia e a igualdade fundamental. Esses elementos serão importantes nas análises envolvendo ordens maximais em álgebras dos quatérnios. Na parte dedicada à teoria dos reticulados, introduzimos definições e propriedades básicas, como matriz geradora, matriz de Gram, volume, densidade de empacotamento e região fundamental. Em seguida, discutimos a construção de reticulados algébricos via $\mathbb{Z}$ -módulos, utilizando o homomorfismo canônico de um corpo de números $\mathbb{K}$. Também abordamos o conceito de equivalência de reticulados e a ação de matrizes unimodulares.

Ainda neste capítulo, introduzimos as valorações p -ádicas e os corpos locais $\mathbb{Q}_p$, com destaque para os critérios que permitem determinar a existência de quadrados e de soluções de equações em $\mathbb{Q}_p$. Esses resultados serão úteis na investigação de elementos que não são normas em certas extensões.

A segunda metade do capítulo é dedicada à teoria das álgebras cíclicas, com especial atenção às álgebras dos quatérnios. Apresentamos os critérios para que uma álgebra dos quatérnios seja de divisão e discutimos a condição de não ser norma. Por fim, abordamos a noção de ordem em álgebras dos quatérnios, com foco nas ordens maximais, e discutimos o conceito de discriminante de uma ordem, ferramenta central para a análise que será desenvolvida nos capítulos seguintes.

O Capítulo 3 é dedicado à construção do reticulado E_8 por meio de ordens maximais em álgebras dos quatérnios definidas sobre corpos quadráticos imaginários com número de classe 1. Inicialmente, retomamos a técnica de representação matricial de módulos para a obtenção de reticulados a partir de ideais em ordens maximais. Essa abordagem, além de reinterpretar construções já conhecidas, é generalizada ao contexto de diferentes álgebras de divisão, destacando sua aplicabilidade na construção de reticulados densos.

Na sequência, são discutidos os parâmetros que influenciam diretamente a construção, com ênfase na minimização do volume de Tamagawa. Um dos principais avanços deste capítulo está na formulação de um critério algébrico que orienta a escolha de ordens e ideais de forma a otimizar esse volume, garantindo propriedades geométricas desejáveis nos reticulados obtidos.

O capítulo também traz uma análise detalhada das condições sob as quais determinados ideais em ordens maximais podem ser usados para gerar reticulados equivalentes ao reticulado E_8 . Desenvolvemos, nesse contexto, um critério explícito, baseado em propriedades de norma e nos coeficientes da álgebra, que assegura a construção de E_8 em diferentes contextos algébricos.

Na parte central do capítulo, são apresentadas construções do reticulado E_8 a partir de diferentes álgebras dos quatérnios da forma $\mathcal{A} = (-p, -1)_{\mathbb{Q}(\sqrt{-d})}$, com p e d escolhidos de forma criteriosa para garantir que a álgebra seja de divisão e que a ordem considerada seja maximal. Um resultado inédito estabelecido neste capítulo demonstra que, para os valores de $d = 11, 19, 43, 67$ e 163 , e para os respectivos p escolhidos, as álgebras $\mathcal{A}$ são de fato álgebras de divisão, utilizando técnicas de não representabilidade de normas em $\mathbb{Q}_p$. Cada exemplo inclui a definição explícita do ideal, a escolha da base da ordem, a matriz associada via representação matricial e a verificação do volume, mostrando que o reticulado obtido é, de fato, equivalente ao reticulado E_8 . O capítulo é concluído com uma análise sobre as álgebras escolhidas.

O Capítulo 4 é dedicado à caracterização do volume de reticulados construídos a partir de ordens maximais em álgebras dos quatérnios, com foco na aplicação do homomorfismo canônico $\sigma_{\mathcal{A}}$. Inicialmente, é feita a definição formal desse homomorfismo para álgebras da forma $\mathcal{A} = (\alpha, \beta)_{\mathbb{K}}$, com $\mathbb{K}$ um corpo de números, generalizando o caso clássico de reticulados ideais associados a corpos de números. O objetivo central do capítulo é estender essa construção para o caso de reticulados obtidos a partir de ordens em álgebras dos quatérnios, com uma análise precisa de seu volume.

Em seguida, são estabelecidos os fundamentos para a construção de famílias de álgebras de divisão cíclicas, definidas sobre corpos ciclotômicos da forma $\mathbb{K} = \mathbb{Q}(\zeta_m)$, com $m = p^r$ e p primo. A partir de resultados clássicos da literatura, mostra-se que existem extensões quadráticas cíclicas $\mathbb{L}|\mathbb{K}$ para as quais ζ_m não é norma de $\mathbb{L}$ sobre $\mathbb{K}$, o que assegura que a

álgebra $\mathcal{A} = (\mathbb{L}|\mathbb{K}, \sigma, \zeta_m)$ seja uma álgebra de divisão e mostra-se também que para essa álgebra, a ordem natural é maximal. Essa propriedade é crucial, pois permite utilizar diretamente a base da ordem natural na construção de reticulados via homomorfismo canônico, simplificando os cálculos e assegurando boas propriedades estruturais.

O resultado principal do capítulo é a dedução de uma fórmula para o volume de reticulados construídos a partir de $\mathbb{Z}$ -módulos livres ou ideais contidos em ordens maximais dessas álgebras, porém sobre o corpo $\mathbb{Q}(\zeta_{2^r})$, com $r \geq 2$. Essa fórmula generaliza o teorema do volume clássico do caso comutativo, para o contexto não comutativo das álgebras dos quatérnios definidas sobre $\mathbb{Q}(\zeta_{2^r})$. A prova envolve a análise da matriz $M_{\mathcal{W}}$ obtida pelas imagens dos elementos do módulo via $\sigma_{\mathcal{A}}$, cuja estrutura matricial em blocos permite um cálculo eficiente do determinante e, portanto, do volume do reticulado. Além disso, o capítulo apresenta um estudo detalhado da ação de $\sigma_{\mathcal{A}}$ sobre os elementos da álgebra e de sua compatibilidade com automorfismos do grupo de Galois, decomposições modulares, normas, traços e discriminantes. Os resultados obtidos fornecem a base algébrica necessária para as construções exploradas no Capítulo 5, em que reticulados são explicitamente obtidos a partir das ordens analisadas neste capítulo.

O Capítulo 5 é dedicado à aplicação das ferramentas teóricas desenvolvidas nos capítulos anteriores à construção de reticulados via ordens maximais em álgebras dos quatérnios, com ênfase especial na utilização de ideais principais e $\mathbb{Z}$ -módulos em ordens maximais. As construções desse capítulo representam resultados originais. O capítulo inicia com uma análise refinada do volume dos reticulados associados a ideais principais à esquerda de ordens maximais, utilizando a fórmula do volume deduzida no Capítulo 4. Essa abordagem permite avaliar de maneira precisa o impacto dos parâmetros algébricos na geometria dos reticulados construídos.

Na sequência, são apresentadas construções de reticulados em dimensão 8, por meio de ideais principais cuidadosamente escolhidos em ordens maximais das álgebras estudadas. Entre os reticulados obtidos, destacam-se o reticulado $\mathbb{Z}^8$, o reticulado E_8 , e versões escalonadas, como $\mathbb{Z}^8 \oplus \sqrt{2} \cdot \mathbb{Z}^8$, além de construções com simetrias envolvendo cópias do reticulado D_4 . Cada construção é acompanhada da análise detalhada dos parâmetros envolvidos. Um destaque importante do capítulo é a construção de reticulados com estrutura do tipo $\sqrt{2^{r-3}} \cdot \mathbb{Z}^{2^{r+1}}$, obtidos a partir de ordens maximais definidas sobre álgebras dos quatérnios com centro nos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$, com $r \geq 2$.

Por fim, o capítulo apresenta a construção de reticulados a partir de $\mathbb{Z}$ -módulos que não são necessariamente ideais, o que representa uma generalização relevante das abordagens clássicas. Em particular, é apresentada a construção de um reticulado equivalente ao reticulado Λ_{16} por meio de um $\mathbb{Z}$ -módulo livre contido em uma ordem maximal de uma álgebra dos quatérnios.

6 CONCLUSÃO E PERSPECTIVAS FUTURAS

Este trabalho apresentou construções de reticulados por meio de álgebras dos quatérnios definidas sobre corpos totalmente complexos, incluindo corpos quadráticos imaginários e corpos ciclotômicos. No caso específico das construções baseadas em corpos ciclotômicos de grau maior que dois sobre $\mathbb{Q}$, trata-se de uma direção que, até onde se tem conhecimento, ainda não havia sido explorada na literatura. Essas construções apresentam potencial para aplicações em codificação e criptografia.

No Capítulo 3, analisamos a construção de reticulados a partir de ordens maximais em álgebras dos quatérnios definidas sobre corpos quadráticos imaginários. Demonstramos que a utilização da representação matricial de módulos permite obter reticulados equivalentes ao reticulado E_8 , contribuindo para a ampliação das técnicas de construção de reticulados na literatura. Além disso, encontramos ideais em ordens maximais cujos reticulados associados possuem a melhor densidade em dimensão 8, e introduzimos novas álgebras associadas a códigos eficientes no contexto do método de redução algébrica, minimizando o volume de Tamagawa.

No Capítulo 4, estabelecemos as bases teóricas para a construção dos reticulados discutidos no Capítulo 5, explorando extensivamente a estrutura das álgebras dos quatérnios definidas sobre corpos ciclotômicos $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, com $r \geq 2$. Apresentamos resultados fundamentais para a caracterização de ordens maximais em álgebras dos quatérnios e para a definição de famílias específicas dessas álgebras, destacando a relevância do 2^r -ésimo corpos ciclotômicos. Dentre as contribuições mais relevantes desse capítulo, destacamos a caracterização do volume dos reticulados obtidos por meio de um módulo contido em uma ordem maximal.

No Capítulo 5, aplicamos os resultados obtidos no capítulo anterior, para construir novos reticulados, utilizando ideais principais e ordens maximais. Demonstramos que certas ordens maximais dão origem a uma família de reticulados equivalentes a $\sqrt{s_r} \cdot \mathbb{Z}^n$, com $s_r = 2^{r-3}$, $n = 2^{r+1}$ e $r \geq 2$, fornecendo uma caracterização precisa para o volume desses reticulados. Além disso, apresentamos uma construção alternativa do reticulado E_8 , bem como um $\mathbb{Z}$ -módulo contido em uma ordem maximal, que gera um reticulado equivalente ao reticulado Λ_{16} . Essas construções não apenas fortalecem o entendimento da interação entre álgebras dos quatérnios e reticulados, mas também fornecem ferramentas valiosas para a área de criptografia baseada em reticulados e comunicações eficientes.

Dessa forma, este trabalho não apenas amplia as construções clássicas de reticulados, mas também introduz novas técnicas e abordagens para sua construção, através de álgebras dos quatérnios. As contribuições apresentadas têm potencial para impactar significativamente a pesquisa em teoria dos reticulados, criptografia e códigos corretores de erro, além de problemas como LWE e suas variantes RLWE e CLWE, [5], [6] e [7], oferecendo novas perspectivas e avanços na compreensão das interseções entre teoria dos números algébricos, álgebras dos quatérnios e reticulados.

Os resultados obtidos neste trabalho abrem diversas direções para pesquisas futuras, tanto no aprofundamento das construções de reticulados, quanto na exploração de novas estruturas algébricas. Um dos caminhos mais promissores consiste no estudo de outras ordens maximais associadas às álgebras de divisão dos quatérnios e suas generalizações. Caracterizar famílias de ordens maximais tem sido um problema investigado devido à sua relevância em aplicações práticas, [7] e [16].

A extensão do estudo feito aqui para álgebras de divisão cíclicas de índice maior do que dois e álgebras mais gerais, representa outra perspectiva relevante. Em particular, as álgebras produto cruzado surgem como uma generalização natural das álgebras de divisão cíclicas, sendo obtidas a partir de extensões de corpos cujo grupo de Galois não é cíclico. O estudo de ordens maximais nessas álgebras pode levar à identificação de novas classes de reticulados com propriedades desejáveis, expandindo o escopo das construções exploradas neste trabalho. Além disso, essas estruturas podem oferecer novas abordagens para a formulação de problemas difíceis em teoria dos números e sua aplicação em protocolos criptográficos baseados em reticulados.

No contexto das aplicações práticas, uma linha de pesquisa futura envolve a análise computacional das construções propostas, com o objetivo de implementar algoritmos eficientes para a determinação de reticulados associados a ordens maximais específicas. Isso permitiria verificar empiricamente as propriedades teóricas dos reticulados e otimizar suas aplicações em áreas como codificação de canal e criptografia pós-quântica.

Outro aspecto a ser investigado é a relação entre a escolha da ordem maximal e a densidade dos reticulados obtidos. Conforme mencionado ao longo deste trabalho, reticulados com alta densidade são fundamentais para diversas aplicações, desde a comunicação eficiente até o design de códigos corretores de erros. Assim, explorar outras famílias de ordens maximais pode levar à obtenção de reticulados com densidade ainda maior em outras dimensões e propriedades mais favoráveis para aplicações específicas.

Outra direção importante envolve a análise de parâmetros associados ao desempenho de códigos espaço-tempo, especialmente no que se refere à probabilidade de erro em canais MIMO. Além disso, a investigação de parâmetros associados à criptografia baseada em reticulados, como a distância mínima normalizada, a norma do vetor mais curto e a densidade de empacotamento também é uma perspectiva futura. Essas perspectivas futuras destacam o potencial das abordagens aqui exploradas para influenciar avanços teóricos e práticos em codificação e criptografia.

REFERÊNCIAS

- [1] CASSELS, J. W. S.; FRÖHLICH, A. Algebraic Number Theory. London: Academic Press, 1967. Proceedings of an instructional conference organized by the London Mathematical Society. ISBN 978-0-12-163251-5.
- [2] SAMUEL, P. Algebraic Theory of Numbers. Paris: Hermann, 1970. Translated from the French by Allan J. Silberberger. ISBN 978-3-540-58657-9.
- [3] MOLLIN, R. A. Algebraic Number Theory. Boca Raton, FL: CRC Press, 1999. ISBN 978-1-58488-184-6.
- [4] EBELING, W. Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch. 3. ed. [s.l.]: Springer Fachmedien Wiesbaden, 2013. ISBN 978-3-8348-8542-2.
- [5] REGEV, O. The learning with errors problem (invited survey). In: Proceedings of the IEEE Conference on Computational Complexity. Cambridge, MA, USA: IEEE Computer Society, 2010. p. 191–204. ISBN 978-0-7695-4060-3.
- [6] LYUBASHEVSKY, V.; PEIKERT, C.; REGEV, O. On lattices, learning with errors, random linear codes, and cryptography II. Journal of Mathematical Cryptology, v. 5, n. 3, p. 213–239, 2011.
- [7] GROVER, C.; MENDELSON, A.; LING, C.; VEHKALAHTI, R. Non-commutative Ring Learning with Errors from Cyclic Algebras. Journal of Mathematical Cryptology, v. 16, n. 1, p. 55–93, 2022.
- [8] CONWAY, J. H.; SLOANE, N. J. A. Sphere Packings, Lattices and Groups. 3. ed. New York: Springer-Verlag, 1999. v. 290. (Grundlehren der mathematischen Wissenschaften, v. 290). ISBN 978-0-387-98585-5.
- [9] BERESNEVICH, V.; VELANI, S.; BURR, A.; NAZER, B. Number Theory Meets Wireless Communications. Springer. NY, Em: Mathematical Engineering. 2020.
- [10] VEHKALAHTI, R.; HOLLANTI, C.; LAHTONEN, J.; RANTO, K. On the densest MIMO lattices from cyclic division algebras. IEEE Transactions on Information Theory, [s. l.], v. 55, n. 6, p. 2764–2772, 2009.
- [11] OGGIER, F.; REKAYA, G.; BELFIORE, J. C.; VITERBO, E. Perfect space-time block codes. IEEE Transactions on Information Theory, IEEE Transactions on Information Theory, v. 52, n. 9, p. 3885–3902, 2006.

- [12] TAROKH, V.; SESHADRI, N.; CALDERBANK, A. R. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE Transactions on Information Theory*, v. 44, n. 2, p. 744–765, 1998.
- [13] KIRAN, T.; RAJAN, B. S. STBC-schemes with nonvanishing determinant for certain number of transmit antennas. *IEEE Transactions on Information Theory*, [s. l.], v. 51, n. 8, 2005.
- [14] COSTA, S.; OGGIER, F.; CAMPELLO, A.; BELFIORE, J.-C.; VITERBO, E. *Lattices Applied to Coding for Reliable and Secure Communications*. Cambridge: Cambridge University Press, 2021. ISBN 978-1-108-83540-3.
- [15] OGGIER, F. *Algebraic Methods for Channel Coding*. 2005. Tese (Doutorado em Matemática) - École Polytechnique Fédérale de Lausanne, Lausanne, 2005.
- [16] LAHTONEN, J.; MARKIN, N.; MCGUIRE, G. Construction of multiblock space-time codes from division algebras with roots of unity as nonnorm elements. *IEEE Transactions on Information Theory*, [s. l.], v. 54, n. 11, 2008.
- [17] OGGIER, F.; BELFIORE, J. C.; VITERBO, E. Cyclic division algebras: A tool for space-time coding. *Foundations and Trends in Communications and Information Theory*, [s. l.], v. 4, n. 1, 2007.
- [18] ALVES, C.; BELFIORE, J. C. Lattices from maximal orders into quaternion algebras. *Journal of Pure and Applied Algebra*, [s. l.], v. 219, n. 4, 2015.
- [19] STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem*. 3. ed. Natick, MA: A K Peters, 2001. ISBN 978-1-56881-119-2.
- [20] RIBENBOIM, P. *Classical theory of algebraic numbers*. Springer Science & Business Media, 2013. ISBN 978-1-4614-1249-1.
- [21] ALBERT, A. A. *Structure of Algebras*. Providence, RI: American Mathematical Society, 1961. v. 24. (American Mathematical Society Colloquium Publications, v. 24). ISBN 978-0-8218-1004-3.
- [22] ENDLER, O. *Teoria dos números algébricos*. 2. ed. Rio de Janeiro: Projeto Euclides, Instituto de Matemática Pura e Aplicada (IMPA), 2014.
- [23] STEWART, I. *Galois Theory*. 3. ed. Chapman & Hall CRC, 1945.
- [24] WASHINGTON, L. C. *Introduction to Cyclotomic Fields*. 2 ed. New York: Springer-Verlag, 1982.
- [25] GOUVÊA, F. *p-adic Numbers: An Introduction*. Third Edition. Springer, 2020.

- [26] STEWART, I. TALL, D. Algebraic Number Theory. 2. ed. New York: Chapman & Hall, 1987.
- [27] SICUTI, P. Um estudo sobre reticulados algébricos bem arredondados. 2019. 127 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, fev, 2020.
- [28] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.2.0). 2023. <https://www.sagemath.org>.
- [29] BOSMA, W.; CANNON, J.; PLAYOUST, C. The magma algebra system i: The user language. *Journal of Symbolic Computation*, v. 24, n. 3-4, p. 235–265, 1997.
- [30] Wolfram Research, Inc. Mathematica, Version 11.3. Champaign, IL: [s.n.], 2018.
- [31] WANG, G.; ZHANG, J. K.; AMIN, M. Space-time block code designs based on quadratic field extension for two-transmitter antennas. *IEEE Transactions on Information Theory*, [s. l.], v. 58, n. 6, 2012.
- [32] BERHUY, G.; OGGIER, F. An Introduction to Central Simple Algebras and Their Applications to Wireless Communication. Providence, Rhode Island: American Mathematical Society, 2013. v. 191 Disponível em: <<http://www.ams.org/surv/191>>
- [33] PIERCE, R. S. Associative Algebras. New York: Springer-Verlag, 1982. v. 88. (Graduate Texts in Mathematics, v. 88). ISBN 978-1-4612-5695-1.
- [34] GUO, X.; XIA, X. G. An elementary condition for non-norm elements. *IEEE Transactions on Information Theory*, [s. l.], v. 55, n. 3, 2009.
- [35] VOIGHT, J. Quaternion Algebras. Cham: Springer International Publishing, 2021. ISBN 978-3-030-56664-7.
- [36] REINER, I. Maximal Orders. Oxford: Oxford University Press, 2003. ISBN 978-019-850650-1.
- [37] VEHKALAHTI, R. Class Field Theoretic Methods in the Design of Lattice Signal Constellations Designs. Dissertação (Master's Thesis) - University of Turku, Turku, Finland, 2008.
- [38] LUZZI, L.; OTHMAN, G. R. Ben; BELFIORE, J. C. Algebraic reduction for the golden code. *Advances in Mathematics of Communications*, [s. l.], v. 6, n. 1, 2012.
- [39] MACLACHLAN, C.; REID, A. W. The Arithmetic of Hyperbolic 3-Manifolds. New York: Springer-Verlag, 2003. v. 219. (Graduate Texts in Mathematics, v. 219). ISBN 978-0-387-98386-8.

- [40] FEAVER, A. Imaginary multiquadratic fields of class number 1. *Rose-Hulman Undergraduate Mathematics Journal*, v. 18, n. 1, p. 1–14, 2017. Disponível em: <<https://scholar.rose-hulman.edu/rhumj/vol18/iss1/6>>.
- [41] REID, A. W. Classification of Quaternion Algebras, Chapter 5, Course Notes. 2017. Course Notes, Physical Sciences Center. Available upon request.
- [42] HORN, R. A.; JOHNSON, C. R. *Matrix Analysis*. 2. ed. Cambridge: Cambridge University Press, 2012. ISBN 978-1-107-60131-4.
- [43] BENEDITO, C. W. de O.; ALVES, C.; BRASIL, N. G.; COSTA, S. I. R. Algebraic construction of lattices via maximal quaternion orders. *Journal of Pure and Applied Algebra*, [s. l.], v. 224, n. 5, 2020.
- [44] CARVALHO, E. D. de; ANDRADE, A. A.; PALAZZO, R. Quaternion orders over quadratic integer rings from arithmetic Fuchsian groups. *Serdica Mathematical Journal*, v. 38, n. 3, p. 393–406, 2012.
- [45] TU, F.-T.; YANG, Y. Lattice packing from quaternion algebra. *RIMS Kôkyûroku Bessatsu*, v. B32, p. 229–237, 2012.
- [46] JR, N. Construção de Reticulados via Álgebras de Divisão e Métodos Eficientes para Solução de Sistemas Lineares de Redes Distribuídas. Tese (Doutorado) - Universidade Estadual de Campinas (UNICAMP), Campinas, SP, Brasil, 2020.
- [47] LI, C.; YUE, Q.; BAE, S. Cyclic division algebras with non-norm elements. *Algebra Colloquium*, [s. l.], v. 21, n. 2, 2014.
- [48] STRAPASSON, J. E.; FERRARI, A. J.; JORGE, G. C.; COSTA, S. I. R. Algebraic constructions of rotated unimodular lattices and direct sum of Barnes-Wall lattices. *Journal of Algebra and its Applications*, [s. l.], v. 20, n. 3, 2021.
- [49] AMORÓS, L; DAMIR, M. Taoufiq; HOLLANTI, Camilla. Even unimodular lattices from quaternion algebras. arXiv preprint, arXiv:2109.09993, 2021. Disponível em: <https://arxiv.org/abs/2109.09993>.
- [50] FERRARI, A. J.; DE ANDRADE, A. A. Constructions of rotated lattice constellations in dimensions power of 3. *Journal of Algebra and its Applications*, [s. l.], v. 17, n. 9, 2018.
- [51] DE ANDRADE, A. A.; INTERLANDO, C. Artigo Rotated $\mathbb{Z}^n$ -Lattices via Real Subfields of $\mathbb{Q}(\zeta_{2^r})$. *TEMA (São Carlos)*, v. 20, n. 2, p. 229–237, 2019.
- [52] MIYAZAKI, A. *Brave Heart*. Letra de Shoko Omori; música e arranjo de Michihiko Ohta. Tóquio: Toei Animation, 1999.