UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

ROBSON RICARDO DE ARAUJO

Reticulados algébricos e aplicações a códigos e criptografia

Campinas

2018

Robson Ricardo de Araujo

Reticulados algébricos e aplicações a códigos e criptografia

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Orientadora: Sueli Irene Rodrigues Costa

Este exemplar corresponde à versão final da Tese defendida pelo aluno Robson Ricardo de Araujo e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas

2018

Agência(s) de fomento e nº(s) de processo(s): CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Ar15r

Araujo, Robson Ricardo de, 1991-
Reticulados algébricos e aplicações a códigos e criptografia / Robson Ricardo de Araujo. – Campinas, SP : [s.n.], 2018.

Orientador: Sueli Irene Rodrigues Costa.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Reticulados algébricos. 2. Criptografia - Matemática. 3. Teoria dos números algébricos. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Algebraic lattices and applications to codes and cryptography
Palavras-chave em inglês:
Algebraic lattices
Cryptography - Mathematics
Algebraic number theory
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
José Carmelo Interlando
Antonio Aparecido de Andrade
Marcelo Muniz Silva Alves
João Eloir Strapasson
Data de defesa: 14-12-2018
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 14 de dezembro de 2018 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). JOSÉ CARMELO INTERLANDO

Prof(a). Dr(a). ANTONIO APARECIDO DE ANDRADE

Prof(a). Dr(a). MARCELO MUNIZ SILVA ALVES

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Aos meus pais,
dedico.

Agradecimento

Ao concluir este trabalho, agradeço:

A Deus, em primeiro lugar, que me deu luz, sabedoria e perseverança para a elaboração desta tese.

Aos meus pais, Nelson e Aparecida, que me deram apoio, sustento, incentivo, carinho, amor e educação em toda vida e, em especial, nesses anos de doutorado.

À minha esposa Beatriz, que, com muito amor, carinho e dedicação, me ajudou a superar grandes barreiras e me incentivou a persistir na pesquisa.

À minha tia Idalina, ao meu tio Eurípedes, ao meu tio Renato (*in memorian*), à minha tia Maria, ao meu avô Osvaldo, aos meus sogros José e Lurdes, aos meus avôs, avós, tios e parentes já falecidos e a todos os demais membros de minha família, pelo apoio, pelo incentivo, pela intercessão e pelos ensinamentos que me deram.

À minha orientadora, Profa. Dra. Sueli Irene Rodrigues Costa (Imecc/Unicamp), pelos conselhos, suportes e incentivos que me deu nos quatro anos de doutorado.

Aos professores titulares da banca examinadora, Prof. Dr. Antonio Aparecido de Andrade (Ibilce/Unesp), Prof. Dr. José Carmelo Interlando (San Diego State University), Prof. Dr. Marcelo Muniz Silva Alves (UFPR), Prof. Dr. João Eloir Strapasson (FCA/Unicamp), e aos professores suplentes da banca examinadora Prof. Dr. Marcelo Firer (Imecc/Unicamp), Profa. Dra. Grasiele Cristiane Jorge (Unifesp) e Prof. Dr. José Plínio de Oliveira Santos (Imecc/Unicamp).

Aos professores com quem trabalhei no Instituto de Matemática, Estatística e Computação Científica (Imecc/Unicamp), por todo aprendizado e experiência que me proporcionaram.

Aos meus amigos Altair, Jheyne, Monisse, Giane, Francisco e tantos outros com quem convivi no doutorado em Campinas, pelo apoio, pela amizade e pelas boas conversas.

Aos meus amigos Alex e Rodrigo, que continuaram sendo grandes companheiros, mesmo à distância.

Aos meus amigos da comunidade da Paróquia São Francisco de Assis, em especial ao padre Alexandre e ao frei Eliseo, pelo suporte espiritual imprescindível no caminho do doutorado.

A todos que direta ou indiretamente contribuíram para a 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.

Os conhecimentos que se repartem são como o andaime que ajuda a construir o edifício do amor e da sabedoria, edifício que há de durar para sempre, inclusive quando os conhecimentos forem esquecidos.

Santo Agostinho

Resumo

Neste trabalho estudamos a aplicação de reticulados algébricos a diferentes contextos. Ao todo, quatro objetivos norteiam esta tese. O primeiro objetivo consiste na construção de reticulados com boa densidade de centro via submódulos de anéis de inteiros de corpos de números algébricos. Nesse contexto, concluímos a construção algébrica do reticulado D_n, para qualquer n, e estudamos a sua distância produto mínima, bem como a de $\mathbb{Z}^n$. Além disso, calculamos a expressão da forma traço associada a corpos de números abelianos de grau primo ímpar ramificado, a qual está relacionada à densidade de centro de reticulados algébricos obtidos via o mergulho de Minkowski. O segundo objetivo se trata da análise de situações em que reticulados algébricos são bem arredondados. Provamos que em cada dimensão prima ímpar existem infinitos reticulados algébricos não equivalentes entre si que são bem arredondados. O terceiro objetivo é apresentar a aplicabilidade e a atualidade dos reticulados algébricos no contexto da criptografia pós-quântica. Além de resumir os avanços recentes da criptografia via reticulados, propomos a utilização de reticulados algébricos obtidos via o mergulho torcido a este contexto e provamos que a dificuldade de quebra da segurança do sistema proposto está associada à dificuldade de solucionar o problema anel-LWE. Por fim, o quarto objetivo trata do estudo dos reticulados logarítmicos, com especial destaque ao raio de cobertura através das unidades de qualquer corpo ciclotômico. Calculamos uma cota superior para o raio de cobertura de reticulados logarítmicos construídos através desses corpos. Nas abordagens dentro dos quatro propósitos acima fica ressaltado que ferramentas algébricas vêm contribuindo de forma eficaz para a produção de reticulados aplicáveis a diversos contextos em teoria de códigos e criptografia.

Palavras-chave: reticulados algébricos; reticulados bem arredondados; criptografia baseada em reticulados; forma traço de corpos de números.

Abstract

In this work we study applications of algebraic lattices in different contexts. Four goals guide this PhD thesis. The first goal is the construction of lattices with great center density via submodules of the ring of integers of algebraic number fields. In this approach, we obtain the algebraic construction of the lattice D_n, for all n, and study its minimum product distance, as well as of the lattice $\mathbb{Z}^n$. Besides, we calculate the expression of the trace form associated with abelian number fields of ramified odd prime degree, which is related to the center density of algebraic lattices obtained via the Minkowski embedding. The second goal is the analysis of cases which provide well rounded algebraic lattices. We prove that for each odd prime dimension there exist infinitely many non-equivalent algebraic lattices which are well rounded. The third goal is to present the application of algebraic lattices in the context of the so called post-quantum cryptography. We resume recent advances of lattice cryptography, propose the use of algebraic lattices coming from twisted embedding in this context and prove that the hardness of broking the security of the proposed system is related to the hardness to solve the ring-LWE problem. The fourth goal is the study of logarithmic lattices, specially the analysis of the covering radius of those obtained from units of cyclotomic number fields. We calculate an upper bound of the covering radius of the logarithmic lattices constructed from these fields. In the four objectives described above it is stressed that algebraic tools have good contributions to produce lattices used in coding theory and cryptography.

Keywords: algebraic lattices; well-rounded lattices; lattice-based cryptography; trace form of number fields.

Lista de ilustrações

Lista de tabelas

Lista de Abreviaturas e Siglas

$\mathbb{N}^*$	Números inteiros positivos
$\Lambda(B)$	Reticulado com base B
Λ	Idem
$span(\Lambda)$	Espaço gerado pelo reticulado Λ
M^T	Transposição da matriz ou do vetor M
det	Determinante
$\det(\Lambda)$	Determinante do reticulado Λ
$R(u)$	Região de Voronoi em u
$P(B)$	Polítopo fundamental associado à base B
$vol(\Lambda)$	Volume do reticulado Λ
$B_n(r)$	Bola n-dimensional centrada na origem e de raio r
$\Delta(\Lambda)$	Densidade do reticulado Λ
$\rho(\Lambda)$	Raio de empacotamento do reticulado Λ
$N_{min}(\Lambda)$	Norma mínima do reticulado Λ
$\delta(\Lambda)$	Densidade de centro do reticulado Λ
$\mu(\Lambda)$	Raio de cobertura do reticulado Λ
$\equiv$	Equivalência
$\simeq$	Aproximação ou isomorfismo
$\Lambda^\vee$	Reticulado dual de Λ
$\lfloor x \rceil$	Chão de x
$\mathbb{K}(\theta)$	Menor corpo que contém $\mathbb{K}$ e θ
xA	Ideal gerado por x num anel A
$\langle x \rangle_A$	Idem
$\langle x \rangle$	Idem
$Gal(\mathbb{L}/\mathbb{K})$	Grupo de Galois da extensão $\mathbb{L}/\mathbb{K}$.
$\mathcal{O}_\mathbb{K}$	Anel de inteiros do corpo $\mathbb{K}$
$Tr_{\mathbb{L}/\mathbb{K}}$	Traço na extensão $\mathbb{L}/\mathbb{K}$
$N_{\mathbb{L}/\mathbb{K}}$	Norma na extensão $\mathbb{L}/\mathbb{K}$
$N(I)$	Norma do ideal I
$D(\mathbb{K})$	Discriminante do corpo $\mathbb{K}$

i	Unidade imaginária
$\varphi(n)$	Função totiente de Euler
ζ_n	Raiz n-ésima primitiva da unidade
R_q	Notação para R/qR, em que R é um anel e $q \in R$.
$\mathbb{Z}_n^*$	Grupo dos elementos de $\mathbb{Z}/n\mathbb{Z}$ que são primos com n
$I \lhd A$	I é ideal de A
$\Im$	Parte imaginária de um número complexo
$\Re$	Parte real de um número complexo
$\overline{x}$	Conjugado complexo de x
$\lvert x \rvert$	Valor absoluto de $x \in \mathbb{R}$
$\lVert x \rVert$	Norma euclidiana de x
δ_{ij}	Delta de Kronecker
div	Diversidade
cos	Cosseno
sen	Seno
tg	Tangente
d_p	Distância produto
$d_{p,min}$	Distância produto mínima
lim	Limite
$\otimes$	Produto tensorial
I_n	Matriz identidade de ordem n
$f\lvert_A$	Função f restrita a um conjunto A
$cond(\mathbb{K})$	Condutor do corpo abeliano $\mathbb{K}$
mdc	Máximo divisor comum
$\lvert A \rvert$	Cardinalidade do conjunto A
$S(\Lambda)$	Conjunto dos vetores mínimos do reticulado Λ
$\lambda_k(\Lambda)$	k-ésimo mínimo sucessivo do reticulado Λ
λ_k	Idem
$\gamma(\Lambda)$	Invariante de Hermite associado ao reticulado Λ
γ_n	Constante de Hermite
$\mathbb{K}_\mathbb{R}$	Notação para $\mathbb{K} \otimes_\mathbb{Q} \mathbb{R}$
$I^\vee$	Ideal dual do ideal I

$D_{\Lambda,r}$	Distribuição Gaussiana Discreta de comprimento r sobre o reticulado Λ
ρ_r	Função gaussiana
exp	Exponencial
log	Logaritmo na base 10
$\min_A f$	Mínimo da função f sobre o conjunto A
R^*	Grupo das unidades do anel R
Log	Mergulho logarítmico

Sumário

Introdução

A teoria algébrica dos números é um dos mais antigos e intrigantes campos de estudo em matemática, tendo seus primórdios associados aos estudos de Diofanto de Alexandria, no século III d.C. O desenvolvimento dessa teoria ao longo dos séculos trouxe como contribuição grandes resultados teóricos, tais como o Teorema da Unidades de Dirichlet e o Último Teorema de Fermat [Sam70, ST02]. Nos últimos anos a teoria algébrica dos números tem ganhado notoriedade prática ao produzir aplicações importantes à teoria de códigos e à criptografia. Além das contribuições propiciadas pela fatoração de números inteiros e pelas curvas elípticas, hoje já reconhecidas pelo seu uso em criptografia, a associação de teoria algébrica dos números com a teoria de reticulados também tem ganhado cada vez mais destaque e aplicabilidade [BFOV04, McM05, LPR10, GBK+16, Goo16, CLB18].

Um reticulado é um subgrupo aditivo discreto do espaço euclidiano. Os reticulados aparecem vinculados ao estudo de difíceis problemas em matemática, como o problema do empacotamento esférico e o problema da cobertura esférica [CS98, LASC12, Mar03]. A partir de $\mathbb{Z}$-módulos e ideais de anéis de inteiros de corpos de números algébricos, que são estruturas algébricas estudadas pela teoria dos números, é possível produzir reticulados através do mergulho de Minkowski ou do mergulho torcido - os quais são chamados de reticulados algébricos. Essa via de obtenção de reticulados traz algumas vantagens, tais como a vinculação do problema de empacotamento esférico ao problema de minimização de uma forma quadrática, a obtenção de reticulados com diversidade máxima através de corpos de números totalmente reais e a produção de algoritmos mais rápidos para determinados sistemas criptográficos baseados em reticulados. Os conceitos básicos sobre reticulados e teoria algébrica dos números essenciais para a compreensão desta tese estão disponíveis no Capítulo 1.

Este trabalho apresenta uma pesquisa sobre reticulados algébricos pautada por quatro objetivos: construir reticulados algébricos densos com diversidade máxima, construir reticulados algébricos bem arredondados, pesquisar reticulados algébricos viáveis para esquemas na criptografia pós-quântica e analisar o raio de cobertura dos reticulados logarítmicos. Do ponto de vista das aplicações, obviamente um dos objetivos citados é voltado à criptografia, enquanto os outros três estão no escopo da teoria de códigos.

O primeiro objetivo deste trabalho é a construção de reticulados algébricos com boa densidade, a fim de serem disponibilizados para canais gaussianos, e com diversidade máxima, para que possam ser usados em canais do tipo Rayleigh com desvanecimento. Reticulados com boa densidade são aqueles que se aproximam da solução do problema do empacotamento esférico em uma dada dimensão, enquanto reticulados com diversidade máxima são aqueles que não possuem vetores com alguma coordenada nula, a não ser o vetor nulo. No Capítulo 2 utilizamos as construções conhecidas dos reticulados $\mathbb{Z}^n$ via corpos de números totalmente reais para obter versões algébricas com diversidade máxima dos reticulados D_n em dimensões n ainda não tratadas em trabalhos anteriores. Além disso, estudamos o parâmetro conhecido como distância produto mínima desses reticulados. Finalmente, comparamos o desempenho dos reticulados $\mathbb{Z}^n$ e D_n obtidos aqui do ponto de vista das suas densidades e distâncias produto mínimas. Resultados preliminares deste trabalho foram apresentados no Congresso Nacional de Matemática Aplicada e Computacional de 2017 [dA17] e o artigo conjunto com esses resultados foi submetido para publicação [dAJ17].

O Capítulo 3 também se enquadra no primeiro objetivo. Nele dedicamo-nos a encontrar a forma traço $Tr_{\mathbb{K}}(x^2)|_{\mathcal{O}_{\mathbb{K}}}$ associada a corpos de números cíclicos $\mathbb{K}$ de grau primo ímpar p tais que o ideal $p\mathcal{O}_{\mathbb{K}}$ seja ramificado, isto é, quando o corpo abeliano $\mathbb{K}$ tem condutor igual a p^2 multiplicado eventualmente por um produto de primos distintos congruentes a 1 módulo p. Também calculamos o mínimo dessa forma traço em casos particulares. Já é conhecida na literatura a expressão de $Tr_{\mathbb{K}}(x^2)|_{\mathcal{O}_{\mathbb{K}}}$ no caso em que $p\mathcal{O}_{\mathbb{K}}$ é um ideal não ramificado, ou seja, quando o condutor de $\mathbb{K}$ é um produto de primos distintos equivalentes a 1 módulo p. O mínimo da forma traço $Tr_{\mathbb{K}}(x^2)$, com $x \neq 0$ em algum $\mathbb{Z}$-módulo M, está associado à densidade do reticulado obtido por M através do mergulho de Minkowski. Versões preliminares desse trabalho foram apresentadas na Escola de Álgebra de 2016 [dA16] e no Congresso Nacional de Matemática Aplicada e Computacional de 2018 [dA18] e a versão final foi submetida para publicação no artigo conjunto [dACAN18].

O segundo objetivo, concentrado no Capítulo 4, consiste no estudo e na construção de reticulados algébricos bem arredondados, que são aqueles que têm um conjunto de vetores linearmente independentes com norma igual à norma mínima do reticulado tal que a cardinalidade desse conjunto seja igual ao posto do reticulado. Um teorema encontrado em [FP12] diz que um reticulado algébrico obtido pelo anel de inteiros de um corpo de números via o mergulho de Minkowski é bem arredondado se, e somente se, esse corpo de números é ciclotômico. No presente trabalho alertamos que esse teorema pode não ser verdade para qualquer corpo de números, mas provamos que é válido colocando a hipótese de que esse seja totalmente real ou totalmente complexo. Além disso, estendemos esse estudo para $\mathbb{Z}$-módulos e provamos que é possível obter infinitos reticulados algébricos bem arredondados não equivalentes entre si em toda dimensão prima ímpar. Do ponto de vista algébrico, mostramos que, contido no anel de inteiros de cada corpo de números

cíclico de grau primo ímpar, é possível encontrar um $\mathbb{Z}$-módulo de posto máximo cuja imagem pelo mergulho de Minkowski é um reticulado bem arredondado. Os resultados deste trabalho foram apresentados no Congresso Internacional de Matemáticos de 2018 [dAC18b] e aceitos para publicação no periódico Archiv der Mathematik [dAC18a].

No Capítulo 5 tratamos do terceiro objetivo deste trabalho, que é o estudo de reticulados algébricos visando o uso em criptografia. Uma necessidade que urge com a possibilidade do advento dos computadores quânticos é a obtenção de sistemas criptográficos que substituam os utilizados atualmente, os quais não são resistentes a ataques quânticos. Uma das propostas mais promissoras dessa chamada criptografia pós-quântica é baseada em reticulados. Propomos a extensão do mergulho de Minkowski para o mergulho torcido no problema criptográfico RLWE (problema α-RLWE) e demonstramos sua segurança. Essa nova proposta é um trabalho conjunto que foi apresentado na Semana Latino-Americana de Códigos e Informação [OdAD+18b] e está disponível no sítio eletrônico *Cryptology ePrint Archive* [OdAD+18a].

O quarto objetivo, tratado no Capítulo 6, é analisar o raio de cobertura do reticulado logarítmico em determinadas situações. O reticulado logarítmico é aquele obtido como imagem do grupo das unidades do anel de inteiros de um corpo de números através do mergulho logarítmico. Neste trabalho apresentamos um limitante superior para o raio de cobertura do reticulado logarítmico obtido via corpos ciclotômicos de qualquer ordem, generalizando o resultado anterior de [CDPR16] que trata apenas de corpos ciclotômicos de ordem igual a uma potência de um número primo.

Por fim, nesta tese, como um todo, utilizamos elementos e resultados teóricos da teoria algébrica dos números na construção de estruturas geométricas, os reticulados, visando aplicações a teoria de códigos corretores de erros e criptografia.

CAPÍTULO 1

Preliminares

O primeiro capítulo desta tese é dedicado ao estudo introdutório sobre reticulados e teoria algébrica dos números. Na Seção 1.1 são apresentados conceitos básicos envolvendo reticulados e algumas de suas propriedades. Na Seção 1.2 tratamos de dois grandes problemas, o do empacotamento esférico e o da cobertura esférica, os quais serão entendidos do ponto de vista da teoria de reticulados. Na Seção 1.3 são definidos reticulados equivalentes, duais, integrais e unimodulares e estudadas algumas de suas propriedades. Alguns reticulados famosos são caracterizados na Seção 1.4, tais como $\mathbb{Z}^n$, D_n, A_n e Λ_{24}. Por sua vez, na Seção 1.5 são introduzidos aspectos importantes da teoria algébrica dos números que são fundamentais em grande parte deste trabalho. Nas seções 1.6 e 1.7 são definidos monomorfismos que associam $\mathbb{Z}$-módulos em corpos de números a reticulados, produzindo os reticulados algébricos, que são os personagens principais desta tese. Nessas seções estudam-se algumas propriedades dos reticulados obtidos, bem como a associação desses com o problema do empacotamento esférico. Por fim, na Seção 1.8 são apresentados os conceitos de diversidade e de distância produto mínima e suas aplicações a canais do tipo Rayleigh com desvanecimento. As referências utilizadas neste capítulo incluem [CS98, COC+17, LASC12, Mar03, End14, End05, DI03, Jor12, Lan05, Mar95, Rib01, Sam70, Was95, dA15].

1.1 Reticulados

Nesta primeira seção vamos apresentar conceitos e resultados que são básicos para o estudo de reticulados.

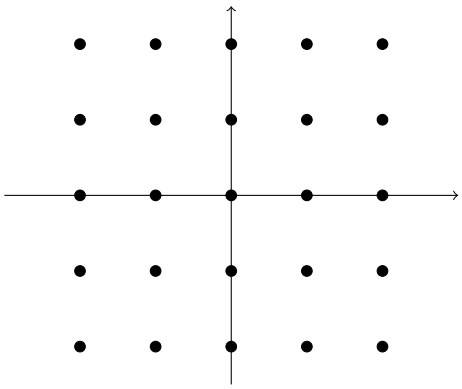
Definição 1.1.1. *Seja $\mathcal{B} = \{u_1, u_2, \ldots, u_m\} \subset \mathbb{R}^n$ uma coleção de $m \leqslant n$ vetores linearmente independentes. O conjunto*

$$\Lambda(\mathcal{B}) = \left\{ \sum_{i=1}^{m} a_i u_i \ : \ a_i \in \mathbb{Z}, 1 \leqslant i \leqslant m \right\} \tag{1.1}$$

é chamado reticulado m-dimensional *em* $\mathbb{R}^n$*, com* base $\mathcal{B}$*. Se* $m = n$*, dizemos que* $\Lambda(\mathcal{B})$ *é um* reticulado de posto completo*.*

Exemplo 1.1.1. *O exemplo mais trivial de reticulado é o conjunto* $\mathbb{Z}^n$ *em* $\mathbb{R}^n$*, o qual tem base* $\mathcal{B} = \{\mathbf{e}_i = (0, \ldots, 0, 1(\textit{posição } i), 0, \ldots, 0) : 1 \leqslant i \leqslant n\}$*. Por exemplo, na Figura 1 vemos a representação geométrica do reticulado* $\mathbb{Z}^2 \subset \mathbb{R}^2$*, que tem base* $\{(0,1),(1,0)\}$*.*

Figura 1 – Representação geométrica do reticulado $\mathbb{Z}^2$ em $\mathbb{R}^2$.



Uma característica dos elementos de um reticulado é que eles formam um conjunto discreto e um grupo abeliano aditivo no espaço euclidiano. O próximo resultado se usa disso para dar uma forma equivalente de caracterizar os reticulados, cuja demonstração pode ser encontrada, por exemplo, em [dA15, Corolário 7.1.1]:

Proposição 1.1.1. *Seja* Λ *um subgrupo aditivo de* $\mathbb{R}^n$*. O conjunto* Λ *é um reticulado se, e somente se,* Λ *é um subgrupo discreto de* $\mathbb{R}^n$*.*

Observamos, por exemplo, que o conjunto $\mathbb{Q}^n$ contido em $\mathbb{R}^n$ é um subgrupo aditivo, mas não é um reticulado, pois não é discreto.

Se $\Lambda \subset \mathbb{R}^n$ é um reticulado m-dimensional, com $m \leqslant n$, o subespaço vetorial de $\mathbb{R}^n$ gerado pelos vetores da base de Λ (sobre $\mathbb{R}$) é simplesmente chamado de *subespaço gerado* por Λ e denotado por $span(\Lambda)$. Notemos que se $m = n$, então $span(\Lambda) = \mathbb{R}^n$.

Todo reticulado m-dimensional Λ em $\mathbb{R}^n$ possui uma *matriz geradora* M de ordem $n \times m$ tal que um vetor v pertence ao reticulado Λ se, e somente se, existe $u \in \mathbb{Z}^m$ tal que $Mu^T = v^T$. A matriz M é definida colocando-se nas suas colunas as coordenadas dos m vetores de uma das bases do reticulado. Define-se a *matriz de Gram* desse reticulado como sendo a matriz quadrada $G = M^T M$ de ordem m. O determinante de G é frequentemente chamado de *determinante* do reticulado e é denotado por $\det(\Lambda)$.

Exemplo 1.1.2. *Em $\mathbb{R}^3$, consideremos os vetores $u = (1, 0, 0)$ e $v = (1, 2, 0)$. Se $\mathcal{B} = \{u, v\}$, o reticulado 2-dimensional $\Lambda(\mathcal{B}) \subset \mathbb{R}^3$ tem matriz geradora*

$$M = \begin{bmatrix} u & v \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 0 & 0 \end{bmatrix} \tag{1.2}$$

e matriz de Gram

$$G = M^T M = \begin{bmatrix} 1 & 1 \\ 1 & 5 \end{bmatrix}. \tag{1.3}$$

O determinante de $\Lambda(\mathcal{B})$ é igual a $\det(G) = 4$.

O reticulado $\Lambda(\mathcal{B})$ do Exemplo 1.1.2 também tem base formada pelos vetores $w = (2, 2, 0)$ e $v = (1, 2, 0)$. Isso significa que a matriz $M_2 = \begin{bmatrix} \mathrm{w} & \mathrm{v} \end{bmatrix}$ é uma matriz geradora de $\Lambda(\mathcal{B})$, obviamente diferente da matriz geradora M obtida no exemplo mencionado. Além disso, as matrizes de Gram obtidas via M e via M_2 são diferentes. No entanto, notemos que os determinantes dessas matrizes coincidem (são iguais a 4). Um reticulado tem infinitas bases, matrizes geradoras e matrizes de Gram distintas, mas o determinante obtido pelas matrizes de Gram é o mesmo:

Proposição 1.1.2. *[LASC12, Seção 2.4] Sejam $\mathcal{B}_1$ e $\mathcal{B}_2$ duas bases distintas de um mesmo reticulado Λ. Consideremos M_1 e M_2 as matrizes geradoras de Λ obtidas por cada uma dessas bases, respectivamente. Assim, existe uma matriz Q com entradas inteiras e determinante ± 1 (chamada unimodular) tal que $M_1 = M_2 Q$. Daí, $\det(M_1^T M_1) = \det(M_2^T M_2)$ e, consequentemente, o determinante de um reticulado é invariante sob mudanças de base.*

Seja Λ um reticulado em $\mathbb{R}^n$. Um conjunto $F \subset \mathbb{R}^n$ é chamado de *região fundamental* de Λ se ele ladrilha $\mathbb{R}^n$. Isso significa que a união de todos os ladrilhos $F + u$, com $u \in \Lambda$, cobre o $\mathbb{R}^n$ e que, se $u \neq v$, então $F + u$ e $F + v$ têm intersecção vazia ou apenas nas suas fronteiras. Duas regiões fundamentais importantes são a região de Voronoi na origem e o polítopo fundamental associado a uma base, que definimos abaixo. Lembramos antes que $\|.\|$ denota a norma euclidiana $\|.\|_2$.

Definição 1.1.2. *Sejam Λ um reticulado em $\mathbb{R}^n$ e $u \in \Lambda$. Definimos a* região de Voronoi *de u como sendo o conjunto dos pontos em $\mathbb{R}^n$ que estão mais próximos de u do que de qualquer outro ponto do reticulado, isto é, o conjunto*

$$R(u) = \{x \in \mathbb{R}^n \ : \ \|x - u\| \leqslant \|x - v\|, \ \forall v \in \Lambda\}. \tag{1.4}$$

Se $\mathcal{B} = \{u_1, \ldots, u_m\}$ é uma base do reticulado Λ, então o conjunto

$$P(\mathcal{B}) = \left\{ \sum_{i=1}^{m} a_i u_i \ : \ 0 \leqslant a_i < 1 \right\} \tag{1.5}$$

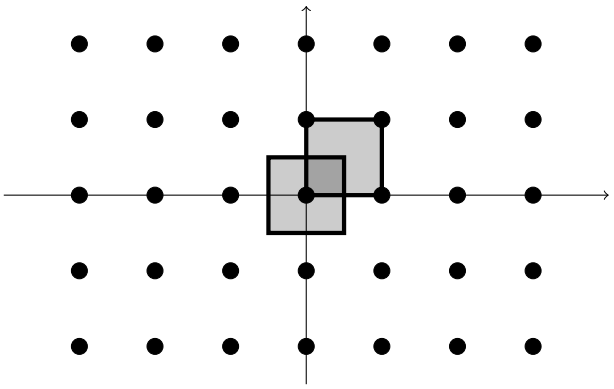
é chamado de polítopo fundamental associado à base $\mathcal{B}$.

A região de Voronoi $R(0)$ e os polítopos fundamentais são regiões fundamentais de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ [LASC12, Seção 2.3] e têm o mesmo volume. O volume de qualquer uma dessas regiões é chamado de *volume do reticulado* e denotado por $vol(\Lambda)$. Além disso, esse volume é dado por

$$vol(\Lambda) = \sqrt{\det(\Lambda)}. \tag{1.6}$$

Exemplo 1.1.3. *Consideremos o reticulado 2-dimensional $\mathbb{Z}^2$ em $\mathbb{R}^2$. Na Figura 2 estão destacados o polítopo fundamental associado à base canônica $\{(1,0),(0,1)\}$ e a região de Voronoi $R(0)$ de $\mathbb{Z}^2$. Um polítopo fundamental é o quadrado de vértices $(0,0)$, $(0,1)$, $(1,0)$ e $(1,1)$ e a região de Voronoi é o quadrado centrado na origem.*

Figura 2 – Um polítopo fundamental e a região de Voronoi $R(0)$ do reticulado $\mathbb{Z}^2$.



Se Λ é um reticulado em $\mathbb{R}^n$ e Λ' é um subgrupo aditivo contido em Λ, dizemos que Λ' é um *sub-reticulado* de Λ. Quando for finito, o índice do subgrupo Λ' em Λ é denotado por $[\Lambda : \Lambda']$, é dado pelo número de elementos do quociente Λ/Λ' e pode ser calculado pela razão $[\Lambda : \Lambda'] = \dfrac{vol(\Lambda')}{vol(\Lambda)}$.

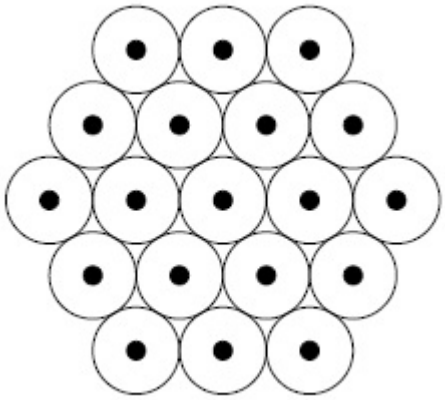
1.2 Empacotamento e cobertura de esferas

Nesta seção vamos apresentar dois problemas importantes tratados na teoria de reticulados: o problema do empacotamento esférico e o problema da cobertura esférica.

O problema do *empacotamento esférico* em $\mathbb{R}^n$ consiste em dispor esferas maciças n-dimensionais de mesmo raio nesse espaço de modo que elas se interceptem em no máximo um ponto e ocupem a maior porção possível do espaço, isto é, se distribuam com a maior densidade realizável. Se o conjunto dos centros das esferas de um determinado empacotamento esférico forma um reticulado, dizemos que este é um *empacotamento reticulado*.

O problema do empacotamento esférico intriga matemáticos já há muitos séculos. Ao dispor tubos cilíndricos em um caminhão, uma transportadora deve se interessar pela solução do mencionado problema em $\mathbb{R}^2$. Com efeito, a forma de dispor círculos não secantes em $\mathbb{R}^2$ ocupando o maior espaço possível indica a maneira mais eficiente de dispor os tubos no caminhão a fim de maximizar a quantidade transportada. A solução do problema do empacotamento esférico em $\mathbb{R}^2$ é dada pelo reticulado gerado pelos vetores $(1, 0)$ e $(1/2, \sqrt{3}/2)$, chamado de *reticulado hexagonal*. Os círculos de raio $1/2$ centrados nos pontos deste reticulado formam um empacotamento que ocupa mais de 90% do plano. A Figura 1.2 representa esse empacotamento.

Figura 3 – Empacotamento do reticulado hexagonal.



Para comparar o empacotamento produzido por reticulados utilizam-se os conceitos de densidade de empacotamento e de densidade de centro. A *densidade de empacotamento* (ou, simplesmente, densidade) de um reticulado $\Lambda \subset \mathbb{R}^n$ é definida por

$$\Delta(\Lambda) = \frac{V(B_n(\rho))}{vol(\Lambda)} = \frac{\rho^n V(B_n(1))}{\sqrt{\det(\Lambda)}} \tag{1.7}$$

em que $B_n(r)$ denota a bola n-dimensional de raio r centrada na origem e ρ é o *raio de empacotamento* de Λ, cujo valor corresponde a

$$\rho = \frac{N_{min}(\Lambda)}{2} \tag{1.8}$$

em que

$$N_{min}(\Lambda) = \min_{0 \neq u \in \Lambda} \|u\| \tag{1.9}$$

é a *norma mínima* do reticulado Λ. Expressões para o volume de $B_n(1)$ podem ser encontradas em [CS98, Capítulo 1].

Exemplo 1.2.1. *A norma mínima do reticulado $\mathbb{Z}^2$ é igual a 1, seu raio de empacotamento é igual $1/2$ e a sua densidade de empacotamento é*

$$\Delta(\mathbb{Z}^2) = \frac{\rho^n V(B_n(1))}{\sqrt{\det(\mathbb{Z}^2)}} = \frac{\pi}{4} \simeq 0,785. \tag{1.10}$$

Por sua vez, o reticulado hexagonal Λ_{hex}*, gerado por* $(1,0)$ *e* $(1/2, \sqrt{3}/2)$*, tem norma mínima* 1*, raio de empacotamento* $1/2$*, determinante* $3/4$ *e densidade de empacotamento*

$$\Delta(\Lambda_{hex}) = \frac{\rho^n V(B_n(1))}{\sqrt{\det(\Lambda_{hex})}} = \frac{\pi}{2 \cdot \sqrt{3}} \simeq 0,907, \tag{1.11}$$

que é a maior densidade possível de ser atingida em dimensão dois.

Para maximizar a densidade de empacotamento de um reticulado Λ, basta maximizar sua *densidade de centro*, que é definida pelo valor

$$\delta(\Lambda) = \frac{\Delta(\Lambda)}{V(B_n(1))}. \tag{1.12}$$

Com base no Exemplo 1.2.1, vemos que a densidade de centro de $\mathbb{Z}^2$ é $1/4$, enquanto a densidade de centro do reticulado hexagonal é $1/(2\sqrt{3})$.

Em terceira dimensão, Gauss provou que o reticulado chamado FCC, o qual conheceremos adiante, produz o empacotamento *reticulado* mais denso ($\Delta = 0.7405...$). O empacotamento esférico produzido pelo FCC assemelha-se à disposição de laranjas em uma banca de feira.

Vamos agora ao problema da cobertura esférica. Sejam Λ um reticulado em $\mathbb{R}^n$ e H o subespaço de $\mathbb{R}^n$ gerado por Λ. Chama-se de *raio de cobertura* de Λ ao valor

$$\mu(\Lambda) = \max_{x \in H} \min_{u \in \Lambda} \|x - u\|. \tag{1.13}$$

Geometricamente, o raio de cobertura $\mu(\Lambda)$ corresponde ao menor raio r tal que $\Lambda + B_n(r)$ cobre H. O *problema da cobertura esférica* consiste em encontrar a disposição de esferas n-dimensionais idênticas com menor raio possível cobrindo o espaço $\mathbb{R}^n$, permitindo sobreposição. Visto do ponto de vista dos reticulados, esse problema busca descobrir o reticulado de posto completo com determinante igual a 1 que tem menor raio de cobertura em cada dimensão. Em dimensão 2, a solução para o problema da cobertura esférica é dado pelo reticulado hexagonal. Em dimensão 3, o reticulado com melhor cobertura não é o que tem melhor empacotamento.

Um fato notável citado em [CS98, p. 33] é que, em um reticulado Λ com região de Voronoi congruente a um polítopo V, centrado na origem, o círculo de raio igual ao raio de empacotamento ρ e centro na origem é o círculo inscrito a V (isto é, o círculo de maior raio contido em V). Por sua vez, o círculo de raio igual ao raio de cobertura $\mu(\Lambda)$ e centro na origem é o círculo circunscrito a V (isto é, o círculo de menor raio contendo V).

1.3 Equivalência, dualidade, integralidade e unimodularidade

Dois reticulados são equivalentes quando um é obtido do outro por uma transformação ortogonal, uma translação e uma dilatação. Formalmente, temos a seguinte definição:

Definição 1.3.1. *Sejam Λ_1 e Λ_2 dois reticulados em $\mathbb{R}^n$ com matrizes geradoras M_1 e M_2, respectivamente. Dizemos que Λ_1 e Λ_2 são equivalentes se existem um número real $c > 0$, uma matriz H unimodular (isto é, com entradas inteiras e determinante ± 1) e uma matriz ortogonal U com entradas reais tais que $M_2 = cUM_1H$.*

Neste caso, c é chamado de *razão de semelhança* entre Λ_1 e Λ_2. Se Λ_1 e Λ_2 são reticulados equivalentes e G_1 e G_2 são suas matrizes de Gram, respectivamente, então é imediato o fato de que $G_2 = c^2H^TG_1H$. Portanto, Λ_1 e Λ_2 são reticulados equivalentes quando existem um número real positivo λ e uma aplicação ortogonal $U : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ tais que $\lambda U(\Lambda_1) = \Lambda_2$.

A proposição seguinte nos mostra importantes características geométricas que podem ser transferidas de um reticulado para uma versão equivalente dele:

Proposição 1.3.1. *[LASC12, Proposição 2.4] Sejam Λ_1 e Λ_2 reticulados equivalentes com razão de semelhança c. Então existem matrizes de Gram G_1 e G_2 de Λ_1 e Λ_2, respectivamente, tais que $G_2 = c^2G_1$. Além disso, se ρ_1 e ρ_2 são os raios de empacotamento e Δ_1 e Δ_2 são as densidades de Λ_1 e Λ_2, respectivamente, então $\rho_2 = c\rho_1$ e $\Delta_2 = \Delta_1$.*

Quando dois reticulados equivalentes têm razão de semelhança $c = 1$, dizemos que eles são *congruentes*. Segue da Proposição 1.3.1 que dois reticulados congruentes têm mesmo raio de empacotamento, têm mesma densidade e possuem matrizes de Gram iguais.

Proposição 1.3.2. *[Cos16] Dois reticulados que possuem mesma matriz de Gram são congruentes.*

Demonstração. Sejam M_1 e M_2 as matrizes geradoras de dois reticulados Λ_1 e Λ_2 que têm matrizes de Gram iguais. Assim, $M_1^TM_1 = M_2^TM_2$. Admitamos inicialmente que esses reticulados têm posto completo. Seja T a matriz da transformação linear que leva uma base do reticulado Λ_1 numa base do reticulado Λ_2, de modo que $M_2 = TM_1$. Isso implica $M_1^TM_1 = M_2^TM_2 = M_1^TT^TTM_1$, donde segue que $T^TT = I$ (matriz identidade), já que M_1 e M_1^T são invertíveis. Portanto, T é uma matriz ortogonal, implicando que Λ_1 e Λ_2 são congruentes. Agora suponhamos que Λ_1 e Λ_2 têm posto $m < n$ em $\mathbb{R}^n$ e consideremos U e V os subespaços gerados por Λ_1 e Λ_2, respectivamente. Consideremos matrizes ortogonais O_1 e O_2, $n \times n$, tais que $O_1(U) = O_2(V) = W$ é um subespaço de $\mathbb{R}^n$ com as $n - m$ últimas coordenadas nulas. Definamos $\Lambda_1' = O_1(\Lambda_1)$ e $\Lambda_2' = O_2(\Lambda_2)$. Assim, os reticulados

Λ_1' e Λ_2' podem ser identificados com reticulados-projeção em $\mathbb{R}^m$, os quais denotamos por Λ_1'' e Λ_2''. Sabendo que as matrizes de Gram são obtidas por produtos escalares das respectivas bases e que O_1 e O_2 são ortogonais, Λ_1'' e Λ_2'' têm a mesma matriz de Gram dos reticulados originais Λ_1 e Λ_2. Usando a primeira parte da demonstração concluímos que as matrizes geradoras M_1'' e M_2'' de Λ_1'' e Λ_2'', respectivamente, satisfazem $M_2'' = O_3 M_1''$ (matrizes $m \times m$), ou ainda que as matrizes geradoras de Λ_1' e Λ_2' satisfazem $M_2' = O_4 M_1'$, onde O_4 é uma matriz diagonal em blocos com partes O_4 e I_{n-m}. Portanto, sendo M_1 e M_2 as matrizes geradoras de Λ_1 e Λ_2, respectivamente, temos $M_2 = O_2^T M_2' = O_2^T O_4 O_1 M_1$, donde segue que $M_2 = OM_1$, em que O é uma matriz ortogonal. Logo, os reticulados M_1 e M_2 são congruentes. □

Corolário 1.3.1. *Se as matrizes de Gram G_1 e G_2 de dois reticulados Λ_1 e Λ_2, respectivamente, satisfazem $G_1 = \lambda G_2$, para algum número real $\lambda > 0$, então esses reticulados são equivalentes.*

Demonstração. Suponhamos $G_1 = M_1^T M_1$ e $G_2 = M_2^T M_2$, em que M_1 e M_2 são matrizes geradoras dos reticulados Λ_1 e Λ_2, respectivamente. Assim,

$$M_1^T M_1 = \left(\sqrt{\lambda} M_2\right)^T \left(\sqrt{\lambda} M_2\right), \tag{1.14}$$

donde segue que a matriz de Gram de Λ_1 é igual à matriz de Gram de $\sqrt{\lambda}\Lambda_2$. A Proposição 1.3.2 nos permite ver que Λ_1 e $\sqrt{\lambda}\Lambda_2$ são congruentes, o que nos faz concluir que Λ_1 e Λ_2 são equivalentes. □

Exemplo 1.3.1. *Consideremos o reticulado hexagonal em $\mathbb{R}^2$, denotado por Λ_{hex} e gerado pelos vetores $(1,0)$ e $(-1/2, -\sqrt{3}/2)$, o qual pode ser incluído naturalmente em $\mathbb{R}^3$. Por sua vez, denotemos por A_2 o reticulado dado pelos elementos (x,y,z) de $\mathbb{Z}^3$ tais que $x+y+z=0$, o qual tem posto 2 em $\mathbb{R}^3$ e base formada pelos vetores $(1,-1,0)$ e $(0,1,-1)$. Os reticulados Λ_{hex} e A_2 são equivalentes. De fato, a matriz de Gram de Λ_{hex} é*

$$G(\Lambda_{hex}) = \begin{bmatrix} 1 & -1/2 \\ -1/2 & 1 \end{bmatrix} \tag{1.15}$$

e a matriz de Gram de A_2 é

$$G(A_2) = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}. \tag{1.16}$$

Assim, $G(A_2) = 2G(\Lambda_{hex})$. Portanto, segue do Corolário 1.3.1 que A_2 e Λ_{hex} são equivalentes.

Definição 1.3.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado m-dimensional, com $m \leqslant n$. Se $H = span(\Lambda)$, definimos o* reticulado dual *de Λ como sendo*

$$\Lambda^\vee = \{x \in H \ : \ \langle x, y\rangle \in \mathbb{Z}, \ \forall y \in \Lambda\}. \tag{1.17}$$

Exemplo 1.3.2. *Vamos encontrar a base do reticulado dual $\Lambda^\vee$, sendo Λ o reticulado gerado por $\{(2,0),(0,1)\}$ em $\mathbb{R}^2$. Para qualquer par $(r,s) \in \mathbb{R}^2$ e para quaisquer $a,b \in \mathbb{Z}$ temos*

$$\langle (r,s), a(2,0)+b(0,1)\rangle = \langle (r,s),(2a,b)\rangle = 2ar+sb. \tag{1.18}$$

Como $2ar+sb$ deve pertencer a $\mathbb{Z}$ para quaisquer $a,b \in \mathbb{Z}$, tomando em particular $a=0$ e, depois, $b=0$, vê-se que $2ar+sb \in \mathbb{Z}$ se, e somente se, $(r,s) \in (1/2)\mathbb{Z}\times\mathbb{Z}$. Logo, $\Lambda^\vee$ tem base $\{(1/2,0),(0,1)\}$.

Proposição 1.3.3. *[COC+17] Seja Λ um reticulado de posto completo em $\mathbb{R}^n$. Se M é a matriz geradora de Λ, então M^{-T} é a matriz geradora do dual $\Lambda^\vee$. Se a matriz de Gram de Λ é G, então a matriz de Gram de $\Lambda^\vee$ é G^{-1}. Consequentemente,* $\det(\Lambda^\vee) = \dfrac{1}{\det(\Lambda)}$.

Definição 1.3.3. *Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito* integral *se $\Lambda \subset \Lambda^\vee$, ou seja, se o produto interno entre qualquer par de elementos de Λ é inteiro.*

Equivalentemente, um reticulado é integral quando sua matriz de Gram tem entradas inteiras. Se Λ é um reticulado integral, definimos o *grupo quociente dual* como sendo $\Lambda^\vee/\Lambda$, cuja ordem é $\det(\Lambda)^2$. Nesse caso, é provado em [CS98, p. 48] que

$$\Lambda \subset \Lambda^\vee \subset \frac{1}{\det(\Lambda)}\cdot\Lambda. \tag{1.19}$$

Notemos ainda que, sendo Λ integral, $\|x\|^2 = \langle x,x\rangle \in \mathbb{Z}$ para qualquer $x \in \Lambda$. Caso o produto interno $\langle x,x\rangle$ seja par para todo $x \in \Lambda$, dizemos que Λ é um reticulado (integral) *par*. Caso contrário, Λ é chamado reticulado (integral) *ímpar*.

Definição 1.3.4. *Um reticulado integral com determinante igual a ± 1 é chamado* unimodular.

Observação 1.3.1. *Um reticulado integral Λ é unimodular se, e somente se, $\Lambda = \Lambda^\vee$. Por isso, é comum chamar um reticulado unimodular de reticulado* autodual.

1.4 Reticulados notáveis

Nesta seção vamos apresentar algumas famílias de reticulados que merecem uma atenção especial, mencionando algumas de suas principais propriedades: $\mathbb{Z}^n$, A_n, D_n, E_8, Λ_{24} e BW_k. Mais informações sobre esses reticulados podem ser encontradas em [CS98, cap. 4], [NRS02] ou [COC+17].

O reticulado $\mathbb{Z}^n$ (para $n \geqslant 1$ inteiro), também chamado de *reticulado cúbico* ou *inteiro*, já foi utilizado no Exemplo 1.1.1. Uma matriz geradora desse reticulado é a matriz identidade de ordem n, I_n, que também é sua matriz de Gram. O reticulado inteiro tem determinante $\det(\mathbb{Z}^n)=1$, norma mínima $N_{min}(\mathbb{Z}^n)=1$, raio de empacotamento $\rho = 1/2$,

raio de cobertura $\mu = \sqrt{n}/2$, densidade $\Delta = V_n 2^{-n}$, onde V_n é o volume da bola de centro 0 e raio 1 em $\mathbb{Z}^n$, e densidade de centro $\delta = \Delta/V_n = 2^{-n}$. Além disso, $\mathbb{Z}^n$ é autodual.

A família de reticulados A_n, com $n \geqslant 1$ inteiro, é definida por

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} \ : \ x_0 + \ldots + x_n = 0\}, \tag{1.20}$$

o que mostra que A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$ em $\mathbb{R}^{n+1}$. Sendo $e_i \in \mathbb{R}^{n+1}$ o vetor contendo 1 na i-ésima entrada e 0 nas outras, $0 \leqslant i \leqslant n$, a base padrão de A_n é dada por

$$\beta = \{e_i - e_{i-1}\}_{i=1}^{n} = \{(-1, 1, 0, \ldots, 0), (0, -1, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, -1, 1)\}. \tag{1.21}$$

A matriz de Gram associada a β é dada por

$$\begin{pmatrix} 2 & -1 & 0 & 0 & \ldots & 0 & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 2 & -1 \\ 0 & 0 & 0 & 0 & \ldots & -1 & 2 \end{pmatrix}. \tag{1.22}$$

O reticulado A_n tem determinante $n+1$, norma mínima $\sqrt{2}$, raio de empacotamento $\rho = \sqrt{2}/2$, raio de cobertura $\mu = \rho \left(\dfrac{2a(n+1-a)}{n+1} \right)^{1/2}$, onde $a = \lfloor (n+1)/2 \rfloor$, e densidade de centro $\delta = \dfrac{1}{2^{n/2}\sqrt{n+1}}$. Os reticulados A_1 e $\mathbb{Z}$ são congruentes, enquanto A_2 é equivalente ao reticulado hexagonal (Exemplo 1.3.1), que é conhecido por ser o reticulado mais denso em dimensão 2, com densidade igual a $\Delta = \pi/\sqrt{12} = 0,9069....$ O reticulado dual de A_n é gerado pelos vetores $e_0 - e_i$, $1 \leqslant i \leqslant n-1$, e $\left(\dfrac{-n}{n+1}, \dfrac{1}{n+1}, \dfrac{1}{n+1}, \ldots, \dfrac{1}{n+1} \right)$. O determinante de $A_n^{\vee}$ é $1/(n+1)$, sua norma mínima é $\sqrt{n/(n+1)}$, seu raio de empacotamento é $\rho = \dfrac{1}{2}\sqrt{\dfrac{n}{n+1}}$, seu raio de cobertura é $\mu = \sqrt{\dfrac{n(n+2)}{12(n+1)}}$ e sua densidade de centro é $\delta = \dfrac{n^{n/2}}{2^n (n+1)^{(n-1)/2}}$. Os reticulados A_1 e A_2 são autoduais. O reticulado $A_3^{\vee}$ é conhecido como *BCC* (em inglês, *body-centered cubic lattice*).

Para $n \geqslant 3$, o reticulado n-dimensional D_n é definido como sendo

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \ : \ x_1 + \ldots + x_n \in 2\mathbb{Z}\}. \tag{1.23}$$

O reticulado D_n tem matriz geradora dada por

$$\begin{pmatrix} -1 & 1 & 0 & \dots & 0 \\ -1 & -1 & 1 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}, \tag{1.24}$$

determinante igual a 4, norma mínima igual a $\sqrt{2}$, raio de empacotamento $\rho = 1/\sqrt{2}$, raio de cobertura $\mu = \rho\sqrt{2}$ $(n = 3)$ ou $\mu = \rho\sqrt{n/2}$ $(n \geqslant 4)$ e densidade de centro $\delta = 2^{-(n+2)/2}$. O reticulado D_3 é conhecido como *FCC* (em inglês, *face-centered cubic lattice*), é equivalente ao reticulado A_3 e é o que possui maior densidade em terceira dimensão, ocupando aproximadamente 74% do espaço. O reticulado dual de D_n tem matriz geradora

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 1/2 \\ 0 & 1 & \dots & 0 & 1/2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 1/2 \\ 0 & 0 & \dots & 0 & 1/2 \end{pmatrix}, \tag{1.25}$$

determinante igual a $1/4$, norma mínima igual a $\sqrt{3}/2$ $(n = 3)$ ou 1 $(n \geqslant 4)$ e densidade de centro $\delta = 3^{1,5}2^{-5}$ $(n = 3)$ ou $2^{-(n-1)}$ $(n \geqslant 4)$.

O reticulado E_8, o mais denso em oitava dimensão, é definido por

$$E_8 = \left\{ (x_1, x_2, \dots, x_8) \in \mathbb{R}^8 \ : \ \forall i, x_i \in \mathbb{Z} \cup (\mathbb{Z} + 1/2) \ e \ \sum_{i=1}^{8} x_i \equiv 0 \ (mod\ 2) \right\}. \tag{1.26}$$

O reticulado E_8 tem matriz geradora

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}, \tag{1.27}$$

tem determinante igual a 1, norma mínima igual a $\sqrt{2}$, raio de empacotamento $\rho = 1/\sqrt{2}$, raio de cobertura $\mu = 1$, densidade $\Delta = 0,2537...$ e densidade de centro $\delta = 1/16$. Além disso, E_8 é o único reticulado unimodular par em $\mathbb{R}^8$. A partir do reticulado E_8 é possível definir outros reticulados conhecidos como E_7 e E_6, que são os mais densos nas dimensões sete e seis, respectivamente [CS98, cap. 4].

Tabela 1 – Reticulados mais densos conhecidos em $\mathbb{R}^n$, para alguns valores de n.

n	δ	Reticulado
1	$1/2$	$A_1 = \mathbb{Z}$
2	$1/(2\sqrt{3})$	A_2
3	$1/(4\sqrt{2})$	$A_3 \simeq D_3$
4	$1/8$	D_4
5	$1/(8\sqrt{2})$	D_5
6	$1/(8\sqrt{3})$	E_6
7	$1/16$	E_7
8	$1/16$	E_8
16	$1/16$	$\Lambda_{16} = BW_4$
24	1	Λ_{24}

Outro importante reticulado é o *reticulado de Leech*, que é o mais denso em dimensão 24. Para defini-lo, definimos antes o código de Golay $\mathcal{C}_{24} \subset \mathbb{F}_2^{24}$, que é um subespaço de dimensão 12 formado por todas as palavras de 24 bits que diferem em pelo menos 8 coordenadas. O reticulado de Leech Λ_{24} é o conjunto de todos os vetores da forma $\sqrt{8^{-1}}(0^{24} + 2c + 4x)$ ou da forma $\sqrt{8^{-1}}(1^{24} + 2c + 4y)$, em que $c \in \mathcal{C}_{24}$ e $x, y \in \mathbb{Z}^{24}$ satisfazem $\sum x_i \equiv 0 \ (mod\ 2)$ e $\sum y_i \equiv 1 \ (mod\ 2)$. O reticulado de Leech é unimodular par, tem determinante igual a 1, norma mínima igual a 2, raio de empacotamento $\rho = 1$, raio de cobertura $\mu = \sqrt{2}$, densidade $\Delta = \pi^{12}/12! = 0,001930...$ e densidade de centro $\delta = 1$.

Por fim, apresentamos a família de reticulados Barnes-Wall, que ocorre em dimensões 2^k, $k \geqslant 2$. Uma das construções conhecidas para os reticulados Barnes-Wall, denotados por BW_k, pode ser encontrada em [NRS02]. Em dimensão 4 ($k = 2$) o reticulado Barnes-Wall coincide com D_4, enquanto em dimensão 8 ($k = 3$) o reticulado Barnes-Wall coincide com E_8. Assim como esses últimos dois, o reticulado Barnes-Wall em dimensão 16 ($k = 4$), também denotado por Λ_{16}, é o que tem empacotamento mais denso conhecido em sua dimensão. Sobre o $BW_4 = \Lambda_{16} \subset \mathbb{R}^{16}$ sabemos que seu determinante é igual a 256, sua norma mínima é 4, seu raio de empacotamento é $\rho = 1$, seu raio de cobertura é $\mu = \sqrt{3}$, sua densidade é $\Delta = \pi^8/(16.8!) = 0,01471...$ e sua densidade de centro é $\delta = 1/16$.

Na Tabela 1.4 apresentamos de forma resumida os reticulados mais densos conhecidos nas dimensões de 1 a 8, 16 e 24 e os valores da densidade de centro deles.

1.5 Conceitos básicos em teoria algébrica dos números

Nesta tese iremos assumir que o leitor tenha conhecimento básico em álgebra, admitindo sabidos os principais conceitos, resultados e propriedades envolvendo grupos,

anéis, ideais, corpos e extensões, espaços vetoriais, A-módulos (sendo A um anel) e teoria de Galois. Sobre esses assuntos, pode-se consultar [DI03, Mil72, Hun74, HK71, End05, Lan05]. Na presente seção iremos apresentar concisamente conceitos elementares da teoria algébrica dos números. Um aprofundamento dos assuntos aqui mencionados pode ser feito a partir das referências [Sam70, Mar95, Rib01, ST02, End14, dA15].

Um corpo $\mathbb{K}$ é chamado de *corpo de números* se a extensão de corpos $\mathbb{K}/\mathbb{Q}$ for finita. Neste caso, denotamos por $[\mathbb{K} : \mathbb{Q}]$ o grau desta extensão. Segundo o Teorema do Elemento Primitivo, em todo corpo de números $\mathbb{K}$ existe θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$ (a notação $\mathbb{Q}(\theta)$ denota o menor corpo que contém os números racionais e θ concomitantemente), o que leva θ a ser chamado de *elemento primitivo* de $\mathbb{K}$. O *polinômio minimal* de θ é o polinômio mônico de menor grau com coeficientes racionais que tem θ como raiz. Denotando o polinômio minimal de θ por $p(x) \in \mathbb{Q}[x]$, temos

$$\mathbb{K} \simeq \frac{\mathbb{Q}[x]}{\langle p(x) \rangle}, \tag{1.28}$$

em que $\simeq$ denota um isomorfismo (de corpos) e $\langle p(x) \rangle$ denota o ideal gerado por $p(x)$ em $\mathbb{Q}[x]$. Se $[\mathbb{K} : \mathbb{Q}] = n$ então o *grau* de $p(x)$ é n.

Se $\mathbb{L}/\mathbb{K}$ é uma extensão de corpos de números, denotamos por $Gal(\mathbb{L}/\mathbb{K})$ o *grupo de Galois* desta extensão, que é o conjunto de todos os $\mathbb{K}$-automorfismos de $\mathbb{L}$. Essa extensão de corpos é dita *galoisiana* quando $|Gal(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$ e é dita *abeliana* quando é galoisiana e quando $Gal(\mathbb{L}/\mathbb{K})$ é um grupo abeliano. É comum chamarmos um corpo de números $\mathbb{K}$ de galoisiano (abeliano) se a extensão $\mathbb{K}/\mathbb{Q}$ é galoisiana (abeliana, respectivamente).

Se $\mathbb{K}$ é um corpo de números e $\alpha \in \mathbb{K}$ é um número tal que $p(\alpha) = 0$ para algum polinômio mônico $p(x) \in \mathbb{Z}[x]$, dizemos que α é um *inteiro algébrico*. O polinômio $p(x)$ é o polinômio minimal de α, isto é, o polinômio mônico de menor grau com coeficientes inteiros que tem α como raiz. O conjunto composto por todos os inteiros algébricos de $\mathbb{K}$ forma um anel chamado *anel de inteiros* de $\mathbb{K}$ e é denotado por $\mathcal{O}_{\mathbb{K}}$. Se $\mathbb{K} = \mathbb{Q}$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$. Se $\mathbb{K}$ é um corpo de números de grau n, então $\mathcal{O}_{\mathbb{K}}$ admite uma $\mathbb{Z}$-base com n elementos, chamada *base integral* de $\mathbb{K}$. Isto significa que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre finitamente gerado de posto n, assim como os ideais de $\mathcal{O}_{\mathbb{K}}$.

Sendo A um anel e α um elemento não pertencente a A, a notação $A[\alpha]$ denota o menor anel que contém A e α concomitantemente, o qual é dado por $A[\alpha] = \{p(\alpha) \ : \ p(x) \in A[x]\}$. Assim, se $\mathbb{K}$ é um corpo de números e $\alpha \in \mathcal{O}_{\mathbb{K}}$ tem polinômio minimal $p(x) \in \mathbb{Z}[x]$ de grau n, então o anel $\mathbb{Z}[\alpha]$ é formado por todas as combinações lineares de $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ com coeficientes inteiros. Claramente $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$. Quando $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$ para algum inteiro algébrico α, dizemos que $\mathcal{O}_{\mathbb{K}}$ é um anel de inteiros *monogênico* e que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma *base integral de potências* de $\mathbb{K}$, o que é equivalente a dizer que $\mathcal{O}_{\mathbb{K}}$ é isomorfo, como anel, a $\mathbb{Z}[x]/\langle p(x) \rangle$, em que $p(x)$ é o polinômio minimal de α.

Consideremos $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de números de grau n. Existem exatamente n $\mathbb{K}$-monomorfismos $\sigma_i : \mathbb{L} \longrightarrow \mathbb{C}$, $1 \leqslant i \leqslant n$. Por isso, se $x \in \mathbb{L}$, podemos definir o *traço* de x na extensão $\mathbb{L}/\mathbb{K}$ como sendo

$$Tr_{\mathbb{L}/\mathbb{K}}(x) = \sum_{i=1}^{n} \sigma_i(x) \tag{1.29}$$

e a *norma* de x na extensão $\mathbb{L}/\mathbb{K}$ por

$$N_{\mathbb{L}/\mathbb{K}}(x) = \prod_{i=1}^{n} \sigma_i(x). \tag{1.30}$$

Se $\mathbb{K} = \mathbb{Q}$, denotamos o traço apenas por $Tr_{\mathbb{L}}(x)$ e a norma apenas por $N_{\mathbb{L}}(x)$. Se $\mathbb{M}/\mathbb{L}/\mathbb{K}$ é uma extensão de corpos de números, então $Tr_{\mathbb{M}/\mathbb{K}}(x) = Tr_{\mathbb{L}/\mathbb{K}}\left(Tr_{\mathbb{M}/\mathbb{L}}(x)\right)$ (transitividade do traço) e $N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}\left(N_{\mathbb{M}/\mathbb{L}}(x)\right)$ (transitividade da norma). Outras propriedades importantes do traço e da norma dizem que o traço preserva a soma enquanto a norma preserva o produto entre elementos do corpo. Ademais, se $x \in \mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}/\mathbb{K}}(x) \in \mathcal{O}_{\mathbb{K}}$ e $N_{\mathbb{L}/\mathbb{K}}(x) \in \mathcal{O}_{\mathbb{K}}$.

Se I é um ideal do anel de inteiros de $\mathbb{K}$, podemos definir a *norma do ideal* I como sendo o número de elementos (finito) do quociente $\mathcal{O}_{\mathbb{K}}/I$, denotando-a por $N(I)$. Se I e J são ideais do anel de inteiros de $\mathbb{K}$, então $N(IJ) = N(I)N(J)$. Quando I for um ideal principal gerado por x, $I = \langle x \rangle$, então $N(I) = |N_{\mathbb{K}}(x)|$.

Dado qualquer conjunto $\mathcal{B} = \{u_1, u_2 \ldots, u_n\} \subset \mathcal{O}_{\mathbb{K}}$, em que $\mathbb{K}$ é um corpo de números, definimos o discriminante de $\mathbb{K}$ em relação a $\mathcal{B}$ por

$$D_{\mathbb{K}}(\mathcal{B}) = \det(Tr_{\mathbb{K}}(u_i u_j))_{1 \leqslant i,j \leqslant n} \in \mathbb{Z}. \tag{1.31}$$

Se $\mathcal{B}$ e $\mathcal{B}'$ são bases integrais de $\mathbb{K}$, então $D_{\mathbb{K}}(\mathcal{B}) = D_{\mathbb{K}}(\mathcal{B}')$. Logo, podemos definir o *discriminante de* $\mathbb{K}$ como sendo $D(\mathbb{K}) = D_{\mathbb{K}}(\mathcal{B})$, para qualquer base integral $\mathcal{B}$ de $\mathbb{K}$. Se um conjunto U é uma $\mathbb{Q}$-base de $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{K}}$ então U será uma base integral de $\mathbb{K}$ quando $D_{\mathbb{K}}(U)$ for livre de quadrados.

Os exemplos mais importantes de corpos de números envolvem os corpos quadráticos, os corpos ciclotômicos e seus subcorpos:

Exemplo 1.5.1. *Todo corpo de números* $\mathbb{K}$ *de grau* 2 *é chamado* corpo quadrático *e pode ser descrito como* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*, em que* d *é um número inteiro livre de quadrados. Se* $d \not\equiv 1 \pmod 4$ *então* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$ *e* $D(\mathbb{Q}(\sqrt{d})) = 4d$*. Por sua vez, se* $d \equiv 1 \pmod 4$*, então* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[(1+\sqrt{d})/2]$ *e* $D(\mathbb{Q}(\sqrt{d})) = d$*. Em particular, o corpo de números gaussiano* $\mathbb{Q}(i)$*, em que* $i = \sqrt{-1}$*, é um corpo quadrático com discriminante* -4 *e anel de inteiros formado por todos os elementos da forma* $a + bi$*, com* $a, b \in \mathbb{Z}$*, já que* $-1 \not\equiv 1 \pmod 4$*. Por sua vez, como* $5 \equiv 1 \pmod 4$*, o corpo de números quadrático* $\mathbb{Q}(\sqrt{5})$ *tem anel de inteiros composto pelos elementos da forma* $a + b\theta$*, em que* $\theta = (1+\sqrt{5})/2$ *é o número de ouro, e discriminante igual a* 5*.*

Exemplo 1.5.2. *Seja $\zeta_n = e^{\frac{2\pi i}{n}}$ uma raiz n-ésima primitiva da unidade, isto é, $x = \zeta_n$ é raiz de $x^n - 1 = 0$, mas não é raiz de $x^m - 1 = 0$ para $0 < m < n$. O corpo de números $\mathbb{Q}(\zeta_n)$ é chamado n-ésimo* corpo ciclotômico*, o qual tem grau igual à função totiente de Euler $\varphi(n)$. Vale observar que para $n = p$ o polinômio minimal de ζ_p é $x^{p-1} + \ldots + x + 1$. Para qualquer n, o anel de inteiros de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$, ou seja, o anel de inteiros do corpo ciclotômico é monogênico. O discriminante de $\mathbb{Q}(\zeta_n)$ é dado por $(-1)^{s\varphi(n)/2} n^{\varphi(n)} / \left(\prod_{q|n} q^{\varphi(n)/(q-1)} \right)$, em que s é o número de fatores primos distintos de n e os números q que aparecem na expressão devem ser tomados apenas entre esses primos. Vale mencionar ainda que o grupo de Galois $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é isomorfo a $\mathbb{Z}_n^* = \{\alpha \in \mathbb{Z} \ : \ 1 \leqslant \alpha < n, \ mdc(\alpha, n) = 1\}$.*

Exemplo 1.5.3. *Qualquer corpo contido em um corpo ciclotômico é chamado* subcorpo ciclotômico*. O caso mais notável é o* subcorpo maximal real *$\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, que é o maior corpo contido em $\mathbb{R} \cap \mathbb{Q}(\zeta_n)$, o qual tem anel de inteiros $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. O grupo de Galois de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q}$ é isomorfo a $\mathbb{Z}_n^*/\{\pm 1\}$.*

Observação 1.5.1. *Ao contrário do que os exemplos anteriores podem sugerir, nem todo anel de inteiros de um corpo de números é monogênico. Em [dA15, Capítulo 4] há exemplo e discussão sobre o assunto.*

Os pilares da teoria algébrica dos números estão assentados, entre outras coisas, num fato muito importante: o anel de inteiros de um corpo de números é um domínio de Dedekind. Isso implica que, se $\mathbb{K}$ é um corpo de números, todo ideal I de $\mathcal{O}_\mathbb{K}$ pode ser fatorado (ou melhor, *ramificado*) como produto de ideais primos $\mathfrak{P}_i$'s:

$$I = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \ldots \mathfrak{P}_g^{e_g}. \tag{1.32}$$

Em particular, consideremos uma extensão de corpos de números $\mathbb{L}/\mathbb{K}$ de grau n e P um ideal primo em $\mathcal{O}_\mathbb{K}$. Assim, o ideal $I = P\mathcal{O}_\mathbb{L}$ pode não ser primo em $\mathcal{O}_\mathbb{L}$, mas pode ser fatorado como em (1.32). Cada $\mathfrak{P}_i$ desta fatoração é chamado de *ideal primo acima* de P, enquanto P é um *ideal primo abaixo* de $\mathfrak{P}_i$. Isso implica que, para i satisfazendo $1 \leqslant i \leqslant g$, vale a igualdade $\mathfrak{P}_i \cap \mathcal{O}_\mathbb{K} = P$. O expoente e_i na fatoração de $P\mathcal{O}_\mathbb{L}$ é chamado de *índice de ramificação* de $\mathfrak{P}_i$ sobre $\mathcal{O}_\mathbb{K}$ e a dimensão do espaço vetorial $\mathcal{O}_L/\mathfrak{P}_i$ sobre o corpo $\mathcal{O}_\mathbb{K}/P$ é chamada de *grau residual* (ou grau inercial) de $\mathfrak{P}_i$ sobre $\mathcal{O}_\mathbb{K}$ e denotada por f_i. A *Igualdade Fundamental* garante que $\sum_{i=1}^{g} e_i f_i = n$. Se $\mathbb{L}/\mathbb{K}$ é uma extensão galoisiana, então todos os graus residuais são iguais e denotados por f, e todos os índices de ramificação são iguais e denotados por e, o que ocorre porque todos os ideais primos acima de P são conjugados com relação aos automorfismos do grupo de Galois $Gal(\mathbb{L}/\mathbb{K})$. Assim, a Igualdade Fundamental diz que $n = efg$. Com relação à fatoração de um ideal primo $P \lhd \mathcal{O}_\mathbb{K}$ em $\mathcal{O}_\mathbb{L}$ segundo a expressão em (1.32), temos ainda as seguintes classificações:[1]

[1] Neste texto utilizamos o símbolo $I \lhd A$ para indicar que I é um ideal do anel A.

- Dizemos que P *se ramifica* em $\mathcal{O}_{\mathbb{L}}$ se $e_i > 1$ para algum $i \in \{1, 2, \ldots, g\}$. Caso contrário, P é chamado *não ramificado* em $\mathcal{O}_{\mathbb{L}}$.
- P é dito *totalmente decomposto* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = f_i = 1$, para todo $i \in \{1, 2, \ldots, g\}$.
- P é dito *totalmente inerte* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = 1$ e $f_i = n$, para algum $i \in \{1, 2, \ldots, g\}$.
- P é dito *totalmente ramificado* em $\mathcal{O}_{\mathbb{L}}$ se $e_i = n$ e $f_i = 1$, para algum $i \in \{1, 2, \ldots, g\}$.

Exemplo 1.5.4. *Sejam $p \in \mathbb{Z}$ um número primo ímpar e $\mathbb{Q}(\zeta_p)$ o p-ésimo corpo ciclotômico, de grau $n = \varphi(p) = p - 1$. O único ideal primo acima de p é $\langle 1 - \zeta_p \rangle \lhd \mathbb{Z}[\zeta_p]$, de modo que $p\mathbb{Z}[\zeta_p] = \langle 1 - \zeta_p \rangle^{p-1}$. Neste caso, $e = p - 1$, $f = 1$ e $g = 1$.*

1.6 Mergulho de Minkowski

Nesta e na próxima seção vamos estabelecer relações entre os reticulados e a teoria algébrica dos números. Como veremos, é possível tratar os elementos de um corpo de números do ponto de vista geométrico. Uma via para obter uma representação geométrica de um corpo de números é através do mergulho de Minkowski, sobre o qual falaremos nesta seção, enquanto outra, mais geral, se dá pelo mergulho torcido, que será tratado na seção seguinte. Por meio de qualquer um desses mergulhos veremos que a imagem de um $\mathbb{Z}$-módulo de posto máximo contido em um anel de inteiros constitui-se em um reticulado no espaço euclidiano.

Definição 1.6.1. *Sejam $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de números de grau n e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os n $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Assim:*
a) Se um monomorfismo σ_i satisfaz $\sigma_i(\mathbb{L}) \subset \mathbb{R}$, ele é dito real. *Caso contrário, ele é chamado* complexo.
b) Se σ_i é real para todo $i = 1, 2, \ldots, n$, dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão totalmente real. *Quando $\mathbb{K} = \mathbb{Q}$, dizemos que $\mathbb{L}$ é um* corpo de números totalmente real.
c) Se σ_i é complexo para todo $i = 1, 2, \ldots, n$, dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão totalmente complexa. *Quando $\mathbb{K} = \mathbb{Q}$, dizemos que $\mathbb{L}$ é um* corpo de números totalmente complexo.

Proposição 1.6.1. *Se $\mathbb{K}$ é um corpo de números galoisiano, então $\mathbb{K}$ é totalmente real ou totalmente complexo.*

A demonstração da proposição acima pode ser encontrada, por exemplo, em [dA15, Proposição 7.3.1].

Consideremos $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de um corpo de números $\mathbb{K}$ em $\mathbb{C}$. Seja $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ a conjugação complexa, isto é, $\alpha(a + bi) = a - bi$ $(a, b \in \mathbb{R})$. Como α é um automorfismo de $\mathbb{C}$, para qualquer $1 \leqslant j \leqslant n$, existe um único $k \in \{1, 2, \ldots, n\}$ tal que $\alpha \circ \sigma_j = \sigma_k$. Além disso, $\alpha \circ \sigma_j = \sigma_j$ se, e somente se, σ_j é real. Seja r_1 o número de monomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$. Sendo assim, $n - r_1$ é o número de monomorfismos

complexos, que é, portanto, um número par. Logo, existe $r_2 \in \mathbb{Z}$ não-negativo tal que $r_1 + 2r_2 = n$. Neste caso, dizemos que (r_1, r_2) é a *assinatura* de $\mathbb{K}$. Vamos renumerar os monomorfismos da seguinte forma: para $1 \leqslant j \leqslant r_1$, sejam σ_j os monomorfismos reais; para $1 \leqslant j \leqslant r_2$, sejam σ_{r_1+j} os monomorfismos complexos não conjugados entre si (isto é, $\sigma_{r_1+j} \neq \alpha \circ \sigma_{r_1+k}$, com $1 \leqslant j, k \leqslant r_2$); para $1 \leqslant j \leqslant r_2$, sejam $\sigma_{r_1+r_2+j}$ os conjugados de σ_{r_1+j}, respectivamente (isto é, $\sigma_{r_1+r_2+j} = \alpha \circ \sigma_{r_1+j}$). Para qualquer $x \in \mathbb{K}$, definimos

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}. \tag{1.33}$$

Denotando por $\Im(x)$ a parte imaginária de um número complexo x e por $\Re(x)$ sua parte real, a aplicação σ pode ser definida de $\mathbb{K}$ em $\mathbb{R}^n$ pela expressão:

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \ldots \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))) \tag{1.34}$$

Esta aplicação é um monomorfismo de $\mathbb{K}$ em $\mathbb{R}^n$.

Definição 1.6.2. *A aplicação σ definida em (1.34) é chamada de* mergulho de Minkowski *ou* mergulho canônico.

Exemplo 1.6.1. *Seja $\mathbb{K} = \mathbb{Q}(i)$. Consideremos os monomorfismos de $\mathbb{Q}(i)$, que são definidos por $\sigma_1(a + bi) = a + bi$ e $\sigma_2(a + bi) = a - bi$, para todo $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 0$ e $r_2 = 1$ e, para qualquer $x = a + bi \in \mathbb{Q}(i)$, o mergulho de Minkowski associado a $\mathbb{Q}(i)$ é $\sigma(x) = (\Re(x), \Im(x)) = (a, b)$.*

Exemplo 1.6.2. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, então $r_1 = 2$ e $r_2 = 0$, em que os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\sqrt{3})$ são $\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ e $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$, com $a, b \in \mathbb{Q}$. Dessa forma, para qualquer $x = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, o mergulho de Minkowski é dado por $\sigma(x) = (a + b\sqrt{3}, a - b\sqrt{3})$.*

Seja M um $\mathbb{Z}$-módulo livre de posto n contido em um corpo de números $\mathbb{K}$ de grau n. Em particular, M pode ser o anel de inteiros de $\mathbb{K}$ ou algum ideal dele. Se σ é o mergulho de Minkowski associado a $\mathbb{K}$, então $\sigma(M)$ é um reticulado de posto completo em $\mathbb{R}^n$, chamado de *reticulado algébrico*. A demonstração deste fato compõe parte da proposição seguinte:

Proposição 1.6.2. *[Sam70] Sejam M um $\mathbb{Z}$-módulo livre de posto n contido em um corpo de números $\mathbb{K}$ de grau n e $\{x_1, x_2, \ldots, x_n\}$ uma $\mathbb{Z}$-base de M. Assim, $\sigma(M)$ é um reticulado de posto completo em $\mathbb{R}^n$ com base $\{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)\}$ e volume dado por*

$$vol(\sigma(M)) = 2^{-r_2} \left|\det \left[\sigma_i(x_j)\right]_{n\times n}\right|. \tag{1.35}$$

Demonstração. Primeiramente, notemos que $\sigma(M)$ é um reticulado gerado pelos vetores $\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)$, já que $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de M. Então, seja $G = (\sigma(x_j))_{1\leqslant j\leqslant n}$ a matriz geradora de $\sigma(M)$ escrita por vetores coluna. Dessa forma,

$vol(\sigma(M)) = D$, em que $D = |\det(G)|$. Agora, seja $H = (\sigma_i(x_j))_{1\leqslant i,j\leqslant n}$. Devemos mostrar que $D = 2^{-r_2}|\det(H)| \neq 0$. Vamos utilizar a propriedade de que, para qualquer número complexo z, tem-se $\Re(z) = (z+\overline{z})/2$ e $\Im(z) = (z-\overline{z})/(2i)$, em que $\overline{z}$ denota o conjugado complexo de z. Seja $L_R(i)$ a linha da matriz G composta pelo vetor

$$(\Re(\sigma_{r_1+i}(x_j)))_{1\leqslant j\leqslant n} = \left(\frac{\sigma_{r_1+i}(x_j) + \sigma_{r_1+r_2+i}(x_j)}{2}\right)_{1\leqslant j\leqslant n}. \tag{1.36}$$

Por sua vez, seja $L_I(i)$ a linha da matriz G composta pelo vetor

$$(\Im(\sigma_{r_1+i}(x_j)))_{1\leqslant j\leqslant n} = \left(\frac{\sigma_{r_1+i}(x_j) - \sigma_{r_1+r_2+i}(x_j)}{2i}\right)_{1\leqslant j\leqslant n}. \tag{1.37}$$

Utilizando propriedades de matrizes, realizamos os seguintes passos:
i) Retiremos o $1/2$ de cada uma das r_2 linhas $L_R(i)$ e o $1/(2i)$ de cada uma das r_2 linhas $L_I(i)$, obtendo novas linhas $L_R(i)'$ e $L_I(i)'$ e $D = (2.2i)^{-r_2}D'$, em que D' é o determinante da matriz obtida após a operação mencionada.
ii) Substituamos a nova linha $L_R(i)'$ da matriz com determinante D' pela soma com a sua nova linha $L_I(i)'$, obtendo uma nova linha $L_R(i)'' = (2.\sigma_{r_1+i}(x_j))_{1\leqslant j\leqslant n}$.
iii) Substituamos a linha $L_I(i)'$ da matriz com determinante D' pela subtração da linha $L_R(i)''$ por $2.L_I(i)$, obtendo uma nova linha $L_I(i)'' = (2.\sigma_{r_1+r_2+i}(x_j))_{1\leqslant j\leqslant n}$. Notemos que o determinante dessa última matriz é D'', que satisfaz $D' = (-1/2)^{r_2}D''$ (devido à última operação).
iv) Extraiamos 2 de cada uma das r_1 linhas $L_R(i)$ e de cada uma das r_1 linhas $L_I(i)$ da matriz com determinante D'', obtendo $D'' = 2^{2r_2}\det(G)$. Então

$$D = (2.2i)^{-r_2}D' = (2^2i)^{-r_2}(-1/2)^{r_2}D'' = (2^2i)^{-r_2}(-1/2)^{r_2}2^{2r_2}\det(G) = \frac{1}{(-2i)^{r_2}}\det(G). \tag{1.38}$$

Portanto,

$$D = (-2i)^{-r_2}\det_{1\leqslant i,j\leqslant n}\left[\sigma_i(x_j)\right]. \tag{1.39}$$

O fato de $\{x_i\}_{1\leqslant i\leqslant n}$ formar uma $\mathbb{Q}$-base para $\mathbb{K}$ acarreta $\det_{1\leqslant i,j\leqslant n}\left[\sigma_i(x_j)\right] \neq 0$. Portanto, $D \neq 0$. Logo, os vetores $\sigma(x_i)$ são linearmente independentes em $\mathbb{R}^n$. Por esse motivo, o $\mathbb{Z}$-módulo $\sigma(M)$ que eles geram é um reticulado em $\mathbb{R}^n$ e $\{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)\}$ é uma base do reticulado $\sigma(M)$. Ademais, $vol(\sigma(M)) = |D| = 2^{-r_2}\left|\det_{1\leqslant i,j\leqslant n}\left[\sigma_i(x_j)\right]\right|$, o que conclui a prova. □

Particularmente, se $M = I$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ (ou o próprio anel),

$$vol(\sigma(I)) = \frac{N(I)\sqrt{D(\mathbb{K})}}{2^{r_2}}. \tag{1.40}$$

A proposição a seguir, que pode ser encontrada, por exemplo, em [dA15, Seção 7.3], nos dá informações sobre o empacotamento esférico produzido por um reticulado algébrico:

Proposição 1.6.3. *Seja $\mathbb{K}$ um corpo de números de grau n.*
a) Para qualquer $x \in \mathbb{K}$, o quadrado da norma *(usual em $\mathbb{R}^n$) de $\sigma(x)$ é definido por*

$$\|x\|^2 = \|\sigma(x)\|^2 = \sigma_1(x)^2 + \ldots + \sigma_{r_1}(x)^2 + \sigma_{r_1+1}(x\overline{x}) + \ldots + \sigma_{r_1+r_2}(x\overline{x}). \tag{1.41}$$

b) Se $\mathbb{K}$ é um corpo de números totalmente real ou totalmente complexo e se M é um $\mathbb{Z}$-módulo livre de posto n em $\mathbb{K}$, o número $x \neq 0$ de norma mínima em M é o que minimiza a expressão $Tr_{\mathbb{K}}(x\overline{x})$.
c) Se $\mathbb{K}$ é totalmente real ou totalmente complexo, a densidade de centro do reticulado algébrico $\sigma(M)$, em que M é um $\mathbb{Z}$-módulo livre de posto n contido em $\mathcal{O}_{\mathbb{K}}$, é dada por

$$\delta = \frac{t_M^{n/2}}{2^n[\mathcal{O}_{\mathbb{K}} : M]\sqrt{D(\mathbb{K})}}, \tag{1.42}$$

onde $[\mathcal{O}_{\mathbb{K}} : M]$ denota o índice de M no anel de inteiros de $\mathbb{K}$ (lembremos que, se M é um ideal de $\mathbb{K}$, $[\mathcal{O}_{\mathbb{K}} : M] = N(M)$) e

$$t_M = \min\{Tr_{\mathbb{K}}(x\overline{x}) \ : \ x \in M, x \neq 0\}. \tag{1.43}$$

Demonstração. a) Consideremos $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $n = r_1 + 2r_2$ monomorfismos de $\mathbb{K}$ e denotemos por σ o mergulho de Minkowski. Calculando a norma, tem-se que

$$\|\sigma(x)\|^2 = \sigma_1(x)^2 + \ldots + \sigma_{r_1}(x)^2 + \Re(\sigma_{r_1+1}(x))^2 + \Im(\sigma_{r_1+1}(x))^2 + \ldots + \Im(\sigma_{r_1+r_2}(x))^2 \tag{1.44}$$

Como $\Re(\sigma_i(x))^2 + \Im(\sigma_i(x))^2 = \sigma_i(x)\overline{\sigma_i(x)} = \sigma_i(x\overline{x})$, $r_1 + 1 \leqslant i \leqslant r_1 + r_2$, segue que

$$\|\sigma(x)\|^2 = \sigma_1(x)^2 + \ldots + \sigma_{r_1}(x)^2 + \sigma_{r_1+1}(x\overline{x}) + \ldots + \sigma_{r_1+r_2}(x\overline{x}). \tag{1.45}$$

b) Por $\mathbb{K}$ ser totalmente real ou totalmente complexo, há apenas dois casos a considerar: $r_1 = 0$ ou $r_2 = 0$. Por um lado, se $r_1 = 0$, como $\sigma_{r_2+j}(x\overline{x}) = \overline{\sigma_j(x\overline{x})} = \sigma_j(x\overline{x})$, $1 \leqslant j \leqslant r_2$, então $\|\sigma(x)\|^2 = \sum_{j=1}^{r_2} \sigma_j(x\overline{x}) = \sum_{j=1}^{r_2} \sigma_{r_2+j}(x\overline{x})$ e, daí, $2\|\sigma(x)\|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x})$. Como os $\sigma_i(x\overline{x})$ são os conjugados de $x\overline{x}$, temos $\|\sigma(x)\|^2 = Tr_{\mathbb{K}}(x\overline{x})/2$. Por outro lado, se $r_2 = 0$, então $\|\sigma(x)\|^2 = \sum_{j=1}^{r_2} \sigma_j(x)^2$. Como $\sigma_i(x\overline{x}) = \sigma_i(x)\sigma_i(\overline{x}) = \sigma_i(x)\sigma_i(x) = \sigma_i(x)^2$, pois os monomorfismos têm imagem real, então $\|\sigma(x)\|^2 = \sum_{i=1}^{n} \sigma_i(x\overline{x}) = Tr_{\mathbb{K}}(x\overline{x})$. Isso significa que o vetor $x \neq 0$ de norma mínima é o que minimiza a expressão $Tr_{\mathbb{K}}(x\overline{x})$. Ademais, o raio de empacotamento de $\sigma(M)$ é $\rho = (1/2)\sqrt{(1/2)Tr_{\mathbb{K}}(x\overline{x})}$, se $r_1 = 0$, ou $\rho = (1/2)\sqrt{Tr_{\mathbb{K}}(x\overline{x})}$, se $r_2 = 0$.
c) Se M é um $\mathbb{Z}$-módulo de $\mathcal{O}_{\mathbb{K}}$ então $\sigma(M)$ é um reticulado algébrico em $\mathbb{R}^n$. Se $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ então, por definição, $D(\mathbb{K}) = [\det(\sigma_i(x_j))]^2$. Da Proposição 1.6.2 segue que $vol(\sigma(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}\sqrt{|D(\mathbb{K})|}$. Logo, como $\sigma(M)$ é um subgrupo de $\sigma(\mathcal{O}_{\mathbb{K}})$ de índice $[\mathcal{O}_{\mathbb{K}} : M]$, então $vol(\sigma(M)) = [\mathcal{O}_{\mathbb{K}} : M]2^{-r_2}\sqrt{|D(\mathbb{K})|}$. Pelo fato da densidade de centro de $\sigma(M)$ ser definida por $\delta = \rho^n/vol(\sigma(M))$, os valores de

ρ obtidos na parte (b) desta proposição mostram que, se $\mathbb{K}$ é totalmente real ($r_2 = 0$), então

$$\delta = \frac{(\sqrt{t_M}/2)^n}{[\mathcal{O}_\mathbb{K} : M]\sqrt{|D(K)|}} = \frac{t_M^{n/2}}{2^n\sqrt{|D(\mathbb{K})|}[\mathcal{O}_\mathbb{K} : M]}. \tag{1.46}$$

e que, se $\mathbb{K}$ é totalmente complexo ($r_1 = 0$), então

$$\delta = \frac{2^{n/2}\left(2^{-1}\sqrt{t_M/2}\right)^n}{[\mathcal{O}_\mathbb{K} : M]\sqrt{D(K)}} = \frac{t_M^{n/2}}{2^n\sqrt{|D(\mathbb{K})|}[\mathcal{O}_\mathbb{K} : M]}, \tag{1.47}$$

o que prova o resultado. □

Exemplo 1.6.3 (Reticulado de dimensão 2 com densidade de centro máxima)**.** *Consideremos o corpo ciclotômico $\mathbb{Q}(\sqrt{-3})$. A partir de seu anel de inteiros, $I = \mathbb{Z}\left[\frac{1-\sqrt{-3}}{2}\right]$, podemos construir o reticulado 2-dimensional $\sigma(I)$, onde σ é o mergulho de Minkowski associado a $\mathbb{Q}(\sqrt{-3})$. Sabe-se que $D(\mathbb{K}) = 3$ e $N(I) = 1$. Por fim, se $x = a + b\sqrt{-3}$ é um elemento não nulo qualquer de I, com $a, b \in \mathbb{Z}$, então $x\overline{x} = (a+b\sqrt{-3})(a-b\sqrt{-3}) = a^2+3b^2$ implica que*

$$Tr_\mathbb{K}(x\overline{x}) = Tr_\mathbb{K}(a^2 + 3b^2) = 2(a^2 + 3b^2), \tag{1.48}$$

donde segue que

$$t_I = \min\{2(a^2 + 3b^2) \ : \ a, b \in \mathbb{Z}\} = 2. \tag{1.49}$$

Portanto, a densidade de centro desse reticulado algébrico é $\delta = 2^{2/2}/(2^2.1.\sqrt{3}) = 1/(2\sqrt{3})$, que coincide com a densidade de centro do reticulado hexagonal, a máxima possível em dimensão 2. Na verdade, é possível observar que este reticulado é o próprio reticulado hexagonal.

Exemplo 1.6.4 (Reticulado de dimensão 4 com densidade de centro máxima)**.** *Consideremos o corpo ciclotômico $\mathbb{Q}(\zeta_8)$, de grau $\varphi(8) = 4$. Seu anel de inteiros é $\mathbb{Z}[\zeta_8]$ e tem base $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. Notemos que $Gal(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\sigma_i : \sigma_i(\zeta_8) = \zeta_8^i, \ i = 1, 3, 5, 7\}$ e que $D(\mathbb{Q}(\zeta_8)) = 256$. Seja $I = \langle 1 + \zeta_8 + \zeta_8^2 + \zeta_8^3\rangle$ um ideal principal de $\mathbb{Z}[\zeta_8]$, o qual tem norma $N(I) = N_\mathbb{K}(1 + \zeta_8 + \zeta_8^2 + \zeta_8^3) = 8$. Tomando $x = \alpha(1 + \zeta_8 + \zeta_8^2 + \zeta_8^3) \in I$, em que $\alpha = i + j\zeta_8 + k\zeta_8^2 + l\zeta_8^3 \in \mathbb{Z}[\zeta_8]$, com $i, j, k, l \in \mathbb{Z}$, vê-se que $Tr_\mathbb{K}(x\overline{x}) = 16(i^2 + ij + j^2 + jk + k^2 + kl + l^2 - il)$, cujo mínimo é igual 16. Assim, a densidade de centro desse reticulado algébrico é $\delta = 16^{4/2}/(2^4.8.\sqrt{256}) = 1/8$, que coincide com a do reticulado D_4, máxima possível em dimensão 4.*

1.7 Mergulho torcido

Nesta seção vamos tratar do mergulho torcido, uma generalização do mergulho de Minkowski (introduzido na Seção 1.6) que amplia a possibilidade de produção de reticulados a partir de $\mathbb{Z}$-módulos de posto máximo em anéis de inteiros de corpos de números [BFOV04]. Seja $\mathbb{K}$ um corpo de números de grau $n = r_1 + 2r_2$, em que r_1 é o número de monomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$ e $2r_2$ é o número de monomorfismos complexos. Sejam

$\sigma_1, \ldots, \sigma_{r_1}$ os monomorfismos reais e $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ os monomorfismos complexos, em que $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$, para todo $i = 1, 2, \ldots, r_2$. Consideremos ainda $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ o mergulho de Minkowski e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$.

Definição 1.7.1. *Um número $\alpha \in \mathbb{K}$ é dito* totalmente positivo *se $\sigma_i(\alpha) \in \mathbb{R}$ e $\sigma_i(\alpha) > 0$, para todo $i = 1, 2, \ldots, n$.*

Definição 1.7.2. *Seja $\alpha \in \mathbb{K}$ um número totalmente positivo. Definimos o* mergulho torcido *associado a $\mathbb{K}$ como sendo a transformação $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ dada por*

$$\sigma_\alpha(x) = \big(\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))\big) \tag{1.50}$$

em que $\alpha_i = \sigma_i(\alpha)$, $1 \leqslant i \leqslant r_1 + r_2$.

Observação 1.7.1. *Há outra possível forma de definir o mergulho torcido substituindo os termos $\sqrt{2\alpha_i}\sigma_i(x)$ da Definição 1.7.2 por $\sqrt{\alpha_i}\sigma_i(x)$. No entanto, em todo este trabalho adotaremos a Definição 1.7.2.*

Para um elemento totalmente positivo $\alpha \in \mathbb{K}$, podemos considerar a transformação linear $t_\alpha : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ definida por

$$t_\alpha(e_i) = \begin{cases} \sqrt{\alpha_i}e_i, & \text{se } 1 \leqslant i \leqslant r_1 \\ \sqrt{2\alpha_i}e_i, & \text{se } r_1 + 1 \leqslant i \leqslant 2r_2 \end{cases} \tag{1.51}$$

em que $\alpha_i = \sigma_i(\alpha)$ e $\{e_1, e_2, \ldots, e_n\}$ é a base canônica de $\mathbb{R}^n$. Dessa forma, o mergulho torcido $\sigma_\alpha(x)$ pode ser escrito da seguinte forma:

$$\sigma_\alpha(x) = t_\alpha \circ \sigma(x). \tag{1.52}$$

Se $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-base para um $\mathbb{Z}$-módulo livre M de posto n em $\mathcal{O}_\mathbb{K}$, denotando por A_α a matriz $n \times n$ cujas colunas são formadas pelos vetores $\sigma_\alpha(x_j)$ e por A a matriz $n \times n$ cujas colunas são formadas pelos vetores $\sigma(x_j)$, com $1 \leqslant j \leqslant n$, então

$$A_\alpha = A \cdot diag\left(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{r_1}}, \sqrt{2\alpha_{r_1+1}}, \sqrt{2\alpha_{r_1+1}}, \ldots, \sqrt{2\alpha_{r_1+r_2}}, \sqrt{2\alpha_{r_1+r_2}}\right) \tag{1.53}$$

em que $diag(u_1, \ldots, u_n)$ denota a matriz diagonal cujos elementos da diagonal principal são iguais a u_i na posição $i \times i$.[2] Assim, podemos garantir que $\sigma_\alpha(M)$ é um reticulado em $\mathbb{R}^n$ com base $\{\sigma_\alpha(x_1), \ldots, \sigma_\alpha(x_n)\}$. Tal conjunto é uma base porque $\det(\sigma(x_j)) \neq 0$. Portanto, temos demonstrado:

Proposição 1.7.1. *Se M é um $\mathbb{Z}$-módulo livre de posto n em $\mathcal{O}_\mathbb{K}$, então $\sigma_\alpha(M)$ é um reticulado de posto completo em $\mathbb{R}^n$, também chamado de* reticulado algébrico.

[2] Notemos que a matriz diagonal multiplicada à direita em (1.53) é a matriz associada à transformação linear t_α.

□

Como consequência dos resultados já vistos para o mergulho de Minkowski na Seção 1.6 prova-se que o volume do reticulado $\sigma_\alpha(M)$ é dado por

$$vol(\sigma_\alpha(M)) = |\det(A_\alpha)| = 2^{-r_2}|\det(A)|\left|\sqrt{2^{2r_2}\alpha_1\dots\alpha_{r_1}}\alpha_{r_1+1}\dots\alpha_{r_1+r_2}\right| \tag{1.54}$$

donde obtém-se a seguinte proposição:

Proposição 1.7.2 ([Fer08], Corolário 6.3.1)**.** *Se $\mathbb{K}$ é totalmente real ou totalmente complexo e $I \lhd \mathcal{O}_\mathbb{K}$, então:*

$$vol(\sigma_\alpha(I)) = N_\mathbb{K}(\alpha)^{1/2}|\det(A)| = N(I)\sqrt{N_\mathbb{K}(\alpha)D(\mathbb{K})} \tag{1.55}$$

Demonstração. O resultado segue de (2.17) e da igualdade $N(I)\sqrt{D(\mathbb{K})} = |\det(A)|$. □

Proposição 1.7.3 ([Fer08], Seção 6.3)**.** *Seja $\mathbb{K}$ um corpo de números de grau n.*
a) Para qualquer $x \in \mathbb{K}$,

$$|\sigma_\alpha(x)|^2 = c_\alpha Tr_\mathbb{K}(\alpha x\overline{x}) \tag{1.56}$$

em que $c_\alpha = 1$ se $\mathbb{K}$ é totalmente real ou $c_\alpha = 1/2$ se $\mathbb{K}$ é totalmente complexo.
b) Se $\mathbb{K}$ é um corpo de números totalmente real ou totalmente complexo e se M é um $\mathbb{Z}$-módulo livre de posto n em $\mathbb{K}$, então o número $x \neq 0$ de norma mínima em M é o que minimiza a expressão $Tr_\mathbb{K}(\alpha x\overline{x})$.
c) Se M é um $\mathbb{Z}$-módulo de $\mathcal{O}_\mathbb{K}$ livre de posto n, a densidade de centro do reticulado $\sigma_\alpha(M)$ é dada por

$$\delta = \frac{t_\alpha^{n/2}}{2^{kn}[\mathcal{O}_\mathbb{K} : M]\sqrt{|D(\mathbb{K})N(\alpha)|}} \tag{1.57}$$

em que

$$t_\alpha = \min\{Tr_\mathbb{K}(\alpha x\overline{x}) : x \in M, x \neq 0\} \tag{1.58}$$

e $k = 1$ se $\mathbb{K}$ é totalmente real ou $k = 3/2$ se $\mathbb{K}$ é totalmente complexo.

Demonstração. Os itens (a) e (b) são mostrados de maneira análoga ao que foi feito na Proposição 1.6.3. Para o item (c), como o raio de empacotamento é dado por $\rho = \sqrt{c_\alpha Tr_\mathbb{K}(\alpha x\overline{x})}/2$, em que x é o número de norma mínima que foi obtido no item (b), então

$$\delta = \frac{\rho^n}{vol(\sigma_\alpha(M))} = \frac{2^{-n}c_\alpha^{n/2}t_\alpha^{n/2}}{[\mathcal{O}_\mathbb{K} : M]\sqrt{|N(\alpha)D(\mathbb{K})|}} \tag{1.59}$$

donde segue o resultado, já que $c_\alpha = 1$ quando $\mathbb{K}$ é totalmente real e $c_\alpha = 1/2$ quando $\mathbb{K}$ é totalmente complexo. □

1.8 Diversidade e distância produto mínima de reticulados

Em canais de transmissão do tipo Rayleigh com desvanecimento, os parâmetros de diversidade e distância produto mínima que definiremos nesta seção tem grande importância, já que o problema de minimizar a probabilidade de ocorrência de erros na transmissão por esses canais está relacionado ao problema de encontrar reticulados com diversidade máxima e com maior distância produto mínima possível [BVRB96].

Definição 1.8.1. *a) A* diversidade *(ou distância de Hamming) entre dois vetores* $x = (x_1, x_2, \ldots, x_n)$ *e* $y = (y_1, y_2, \ldots, y_n)$ *em* $\mathbb{R}^n$ *é dada pelo número de coordenadas diferentes deles, isto é,*

$$div(x, y) = |\{i \ : \ x_i \neq y_i\}|. \tag{1.60}$$

b) Se $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$*, definimos a* diversidade de x *como sendo*

$$div(x) = div(x, 0) = |\{i \ : \ x_i \neq 0\}|. \tag{1.61}$$

c) Seja $S \subset \mathbb{R}^n$ *um subconjunto qualquer. A* diversidade mínima *(ou distância mínima de Hamming) de* S *é dada por*

$$div(S) = \min\{div(x, y) \ : \ x, y \in S, x \neq y\}. \tag{1.62}$$

Notemos na Definição 1.8.1 que, se S é um grupo abeliano aditivo em $\mathbb{R}^n$, então $0 \in S$, donde segue que $div(S) = \min\{div(x) : x \in S, x \neq 0\}$. Em particular, quando $S = \Lambda \subset \mathbb{R}^n$ é um reticulado,

$$div(\Lambda) = \min\{div(x) : x \in \Lambda, x \neq 0\}. \tag{1.63}$$

A fim de fazer aplicações a canais do tipo Rayleigh com desvanecimento, o objetivo é encontrar reticulados em $\mathbb{R}^n$ que têm diversidade máxima (igual a n). Isso significa encontrar reticulados cujos vetores não nulos não interceptam os eixos coordenados.

O exemplo a seguir mostra que o conceito de diversidade não é um invariante geométrico (na métrica euclidiana), visto que pode variar com rotações. No entanto, é possível mostrar que a diversidade é um invariante geométrico com a métrica da soma.

Exemplo 1.8.1. *Consideremos os reticulados* $\Lambda_1 = \mathbb{Z}_2$ *e* $\Lambda_2 = \langle(\cos\theta, -\text{sen}\theta), (\text{sen}\theta, \cos\theta)\rangle$ *em* $\mathbb{R}^2$*, sendo* θ *um ângulo entre* 0 *e* $\pi/2$ *(assim,* Λ_2 *é um* $\mathbb{Z}^2$*-rotacionado). Claramente, a diversidade mínima de* Λ_1 *é* 1*, já que* $div(1, 0) = 1$*. Por sua vez, se* $\text{tg}\theta \notin \mathbb{Q}$*, então* Λ_2 *tem diversidade mínima* 2*. De fato, seja* $(a\cos\theta - b\text{sen}\theta, a\text{sen}\theta + b\cos\theta)$ *qualquer elemento não nulo de* Λ_2*, com* $a, b \in \mathbb{Z}$*. Assim, a primeira coordenada é zero se, e somente se,*

$$a\cos\theta - b\text{sen}\theta = 0 \Longleftrightarrow \text{tg}\theta = \text{sen}\theta/\cos\theta = a/b \tag{1.64}$$

e a segunda coordenada é zero se, e somente se,

$$a\text{sen}\theta + b\cos\theta = 0 \Longleftrightarrow \text{tg}\theta = \text{sen}\theta/\cos\theta = -b/a. \tag{1.65}$$

Logo, se $\text{tg}\theta \notin \mathbb{Q}$*, então as duas coordenadas de qualquer elemento não nulo de* Λ_2 *são não nulas, o que comprova que a diversidade mínima de* Λ_2 *é* 2*.*

Definição 1.8.2 (Distância produto)**.** *Seja* $\Lambda \subset \mathbb{R}^n$ *um reticulado com diversidade* $l \leqslant n$*.*
a) Para qualquer $x = (x_1, x_2, \ldots, x_n) \in \Lambda$*, define-se a* l-distância produto *de* x *como sendo* $d_p^l(x) = \prod_{x_i \neq 0} |x_i|$*.*
b) A l-distância produto mínima *do reticulado* Λ *é definida como sendo*

$$d_{p,min}^l = \min\{d_p^l(x) \ : \ x \neq 0, x \in \Lambda\}. \tag{1.66}$$

Observação 1.8.1. *Se* $l = n$ *é a diversidade do reticulado* $\Lambda \subset \mathbb{R}^n$*, então na Definição 1.8.2 pode-se omitir a letra* l *tanto do título dos conceitos como das notações.*

Além de diversidade máxima, aplicações de reticulados a canais do tipo Rayleigh com desvanecimento pedem que a distância produto mínima seja a máxima possível. Como se pode perceber, não é tão fácil calcular a distância produto mínima de um reticulado. No entanto, reticulados algébricos aparecem como uma boa alternativa para contornar este problema devido ao que veremos na próxima proposição, considerando $\mathbb{K}$ um corpo de números de grau n, $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$, α um elemento totalmente positivo em $\mathbb{K}$ e σ_α o mergulho torcido (se $\alpha = 1$, assumimos que $\sigma_\alpha = \sigma$, o mergulho de Minkowski).

Proposição 1.8.1. *Se* $\mathbb{K}$ *é um corpo de números totalmente real e* $M \subset \mathbb{K}$ *é um* $\mathbb{Z}$*-módulo livre de posto* n*, então o reticulado algébrico* $\sigma_\alpha(M)$ *tem diversidade máxima (isto é,* $div(\sigma_\alpha(M)) = n$*).*

Demonstração. Seja $y = (y_1, y_2, \ldots, y_n) \neq 0$ um elemento de $\sigma_\alpha(M)$. Assim, existe $x \in M$ tal que $\sigma_\alpha(x) = y$, com $x \neq 0$. Como $\mathbb{K}$ é totalmente real, segue que todos os monomorfismos σ_i de $\mathbb{K}$, $1 \leqslant i \leqslant n$, são reais. Agora, $\sigma_i(x) = y_i$. Assim, se $y_i = 0$ então $\sigma_i(x) = 0$ e, da injetividade de σ_i, segue que $x = 0$, o que é um absurdo. Portanto, $y_i \neq 0$ para todo $i = 1, 2, \ldots, n$, donde concluímos que a diversidade de $\sigma_\alpha(M)$ é máxima. □

Conforme a Proposição 4.4.2 de [Jor12], se I é um ideal não zero de $\mathcal{O}_\mathbb{K}$, o reticulado $\sigma_\alpha(I)$ tem diversidade $r_1 + r_2$, em que (r_1, r_2) é a assinatura de $\mathbb{K}$, o que generaliza a Proposição 1.8.1. Em particular, se $\mathbb{K}$ é totalmente complexo, então sua diversidade é $n/2$. Note, portanto, que reticulados algébricos advindos de corpos de números totalmente reais são mais interessantes, visto que nesse caso a diversidade é máxima. Com relação à distância produto mínima, nesses casos, valem os seguintes resultados, cujas provas podem ser encontradas em [Jor12, Proposição 4.4.4]:

Proposição 1.8.2. *Se $\mathbb{K}$ é totalmente real e M é um $\mathbb{Z}$-módulo livre de posto n, então a distância produto mínima do reticulado $\sigma_\alpha(M)$ é dada por*

$$d_{p,min}(\sigma_\alpha(M)) = \sqrt{N_{\mathbb{K}}(\alpha)} \min_{0\neq y\in M} |N_{\mathbb{K}}(y)| \tag{1.67}$$

Corolário 1.8.1. *Se $\mathbb{K}$ é totalmente real e I é um ideal não zero de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima do reticulado $\sigma_\alpha(M)$ é dada por*

$$d_{p,min}(\sigma_\alpha(M)) = \sqrt{\frac{\det(\sigma_\alpha(I))}{|D(\mathbb{K})|}} \frac{\min_{0\neq y\in I} |N_{\mathbb{K}}(y)|}{N(I)}. \tag{1.68}$$

Se I é um ideal principal, do Corolário 1.8.1, segue que $N(I) = \min\limits_{0\neq y\in I} |N_{\mathbb{K}}(y)|$ e, portanto,

$$d_{p,min}(\sigma_\alpha(M)) = \sqrt{\frac{\det(\sigma_\alpha(I))}{|D(\mathbb{K})|}}. \tag{1.69}$$

Quando I não é um ideal principal, $N(I) < \min\limits_{0\neq y\in I} |N_{\mathbb{K}}(y)|$, o que aumenta a distância produto mínima.

CAPÍTULO 2

Construções algébricas de $\mathbb{Z}^n$ e D_n com diversidade máxima

Reticulados com diversidade máxima e grande distância produto mínima tem sido considerados para utilização em canais do tipo Rayleigh com desvanecimento [BVRB96]. O cálculo da distância produto mínima não é tão simples de ser feito em reticulados gerais, mas é facilitado em reticulados obtidos algebricamente, via ideais de anéis de inteiros de corpos de números através do mergulho torcido. Neste capítulo, apresentamos construções algébricas, via o mergulho torcido, de versões rotacionadas dos reticulados $\mathbb{Z}^n$ e D_n com diversidade máxima, para qualquer $n \in \mathbb{N}^*$, e calculamos sua distância produto mínima desde que determinadas hipóteses sejam satisfeitas. As construções de $\mathbb{Z}^n$ aqui apresentadas, para qualquer n, e de D_n, com n igual a uma potência de 2, já são conhecidas na literatura [BFN05, JC12, SO07]. Nossas contribuições consistem em apresentar a construção de D_n para qualquer n (não só potência de 2) e em aprofundar o cálculo da distância produto mínima em todas as construções de $\mathbb{Z}^n$ e D_n feitas aqui. Em particular, obteremos os reticulados D_3 e D_5 com diversidade máxima, os quais também podem ser recomendados para utilização em canais gaussianos, pois são os mais densos nas dimensões 3 e 5, respectivamente. Na Seção 2.1, apresentamos a construção algébrica de $\mathbb{Z}^n$ e D_n e analisamos suas distâncias produto mínimas para o caso n ímpar. Na Seção 2.2, são resgatados alguns resultados já conhecidos no caso em que n é uma potência de 2. Na Seção 2.3, apresentamos a construção algébrica geral de $\mathbb{Z}^n$ e D_n e suas distâncias produto mínimas quando n é par e não é uma potência de 2 através da colagem dos casos estudados nas duas seções anteriores. Por fim, na Seção 2.4, comparamos a distância produto mínima relativa entre $\mathbb{Z}^n$ e D_n e fazemos a análise de alguns casos particulares. Além dos itens mencionados acima, as referências principais deste capítulo incluem também [AAC, BFOV04, Ere88, ESK05, Jor12]. Resultados originais deste capítulo foram apresentados em [dA17] e estão disponíveis no trabalho conjunto [dAJ17].

2.1 Construções de $\mathbb{Z}^n$ e D_n, com n ímpar

Seja $n > 1$ um inteiro *ímpar*. Devido ao Teorema de Dirichlet [Ser73, Lema 3, Capítulo 3], existe um número primo p tal que $p \equiv 1 \ (mod\ n)$. Seja $\zeta_p = e^{\frac{2i\pi}{p}}$ a p-ésima raiz primitiva da unidade. A extensão ciclotômica $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ tem grupo de Galois cíclico gerado pelo automorfismo σ definido por $\sigma(\zeta_p) = \zeta_p^r$, em que r é um elemento primitivo do corpo $\mathbb{Z}_p$. Isso significa que r é um elemento tal que a sua menor potência j inteira estritamente positiva satisfazendo $r^j \equiv 1 \ (mod\ p)$ é $p-1$.

O subgrupo $H = \langle \sigma^n \rangle$ de $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ tem como corpo fixo um subcorpo de $\mathbb{Q}(\zeta_p)$ que denotamos por $\mathbb{K}$. Assim,

$$\mathbb{K} = \{y \in \mathbb{Q}(\zeta_p) \ : \ \sigma^n(y) = y\}. \tag{2.1}$$

Lema 2.1.1. *O corpo $\mathbb{K}$ tem grau n e é um corpo de números totalmente real.*

Demonstração. Seja i a ordem do grupo $H = \langle \sigma^n \rangle$. Assim, $ni = p-1$, pois $|\langle \sigma \rangle| = p-1$, já que $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle \sigma \rangle$. Logo,

$$\frac{|Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})|}{|H|} = \frac{p-1}{i} = n. \tag{2.2}$$

Como $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana, segue do Teorema da Correspondência de Galois [Sam70, Seção 6.1], que o valor obtido na Equação 2.2 deve coincidir com o grau da extensão de $\mathbb{K}$ sobre $\mathbb{Q}$. Portanto, o grau de $\mathbb{K}$ é n. Como n é ímpar e $p-1$ é par, segue que $i = 2\tilde{i}$, com $\tilde{i} \in \mathbb{Z}_{>0}$. Assim, se $y \in \mathbb{K}$, então $\sigma^n(y) = y$ e, daí, $\sigma^{\frac{p-1}{2}}(y) = \sigma^{n\tilde{i}}(y) = \sigma^n \circ \sigma^n \circ \ldots \circ \sigma^n(y) = y$. Logo, y é fixo por $\sigma^{\frac{p-1}{2}}$, o que significa que y pertence ao corpo maximal real $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Portanto, $\mathbb{K} \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subset \mathbb{R}$, o que prova que $\mathbb{K}$ é totalmente real. □

Consideremos em $\mathbb{Q}(\zeta_p)$ o elemento

$$\alpha = \prod_{j=0}^{m-1} \left(1 - \zeta_p^{r^j}\right) \tag{2.3}$$

em que $m = (p-1)/2$. Como p é primo e $r < p$, segue que $mdc(r-1, p) = 1$ e, consequentemente, existe um inteiro λ satisfazendo a congruência $\lambda(r-1) \equiv 1 \ (mod\ p)$. Consideremos também em $\mathbb{Q}(\zeta_p)$ o elemento

$$z = \zeta_p^{\lambda} \alpha (1 - \zeta_p). \tag{2.4}$$

Notemos que z é um inteiro algébrico. Por isso, o elemento

$$x = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z) \tag{2.5}$$

é um elemento que pertence a $\mathcal{O}_{\mathbb{K}}$.

Lema 2.1.2 ([BFOV04], Lemas 3 e 4)**.** *Valem as seguintes igualdades:*

a) $\sigma(\alpha) = -\zeta_p^{p-1}\alpha$

b) $\sigma(\zeta_p^{\lambda}\alpha) = -\zeta_p^{\lambda}\alpha$

c) $(\zeta_p^{\lambda}\alpha)^2 = (-1)^m p$

Lema 2.1.3 ([ESK05], Apêndice II)**.** $Tr_{\mathbb{K}}(x^2) = p^2$ *e* $Tr_{\mathbb{K}}(x\sigma^j(x)) = 0$*, se* $j \neq 0$.

Como consequência do Lema 2.1.3, segue o próximo resultado:

Proposição 2.1.1. *A matriz*

$$G = \frac{1}{p}\begin{pmatrix} x & \sigma(x) & \dots & \sigma^{n-2}(x) & \sigma^{n-1}(x) \\ \sigma(x) & \sigma^2(x) & \dots & \sigma^{n-1}(x) & x \\ \sigma^2(x) & \sigma^3(x) & \dots & x & \sigma(x) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma^{n-1}(x) & x & \dots & \sigma^{n-3}(x) & \sigma^{n-2}(x) \end{pmatrix}, \tag{2.6}$$

é ortogonal, ou seja, $GG^T = G^TG = I_n$.

A Proposição 2.1.1 nos permite afirmar que o reticulado algébrico $\sigma_{1/p^2}(I)$ é equivalente ao reticulado $\mathbb{Z}^n$, em que I é o $\mathbb{Z}$-módulo

$$I = \langle x, \sigma(x), \dots, \sigma^{n-1}(x)\rangle_{\mathbb{Z}}. \tag{2.7}$$

Como consequência, a proposição seguinte apresenta a construção do reticulado algébrico D_n através de um $\mathbb{Z}$-módulo contido em $\mathcal{O}_{\mathbb{K}}$.

Proposição 2.1.2. *Consideremos* $\beta = 1/p^2$ *e* M *o* $\mathbb{Z}$*-submódulo de* $\mathcal{O}_{\mathbb{K}}$ *gerado por*

$$\{x + \sigma(x), x - \sigma(x), \sigma(x) - \sigma^2(x), \dots, \sigma^{n-2}(x) - \sigma^{n-1}(x)\}. \tag{2.8}$$

O reticulado algébrico $\sigma_\beta(M)$ *é uma versão rotacionada de* D_n.

Demonstração. Uma matriz geradora de D_n é dada por

$$\begin{pmatrix} -1 & -1 & 0 & \dots & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -1 \end{pmatrix}. \tag{2.9}$$

Multiplicando a matriz de (2.9) pela matriz ortogonal G da Proposição 2.1.1, obtemos

$$\frac{1}{p}\begin{pmatrix} -x - \sigma(x) & -\sigma(x) - \sigma^2(x) & \dots & -\sigma^{n-1}(x) - x \\ x - \sigma(x) & \sigma(x) - \sigma^2(x) & \dots & \sigma^{n-1}(x) - x \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n-2}(x) - \sigma^{n-1}(x) & \sigma^{n-1}(x) - x & \dots & \sigma^{n-3}(x) - \sigma^{n-2}(x) \end{pmatrix}, \tag{2.10}$$

que é uma matriz geradora de $\sigma_\beta(M)$. Assim, $\sigma_\beta(M)$ é uma versão rotacionada de D_n. □

O reticulado obtido na Proposição 2.1.2 é um D_n-rotacionado, que é uma versão equivalente do reticulado D_n. Como reticulados equivalentes preservam a densidade de centro, o reticulado $\sigma_\beta(M)$ tem a maior densidade de centro conhecida, por exemplo, nas dimensões $n = 3$, $n = 5$ e $n = 37$ [Neb]. Em [Jor12] e [JC12] as autoras produzem reticulados D_n-rotacionados para $n = (p-1)/2$, em que p é um número primo ímpar. Anteriormente, obtivemos D_n para outros valores de n não considerados nessas referências, tais como $n = 7$.

Exemplo 2.1.1. *Neste exemplo, apresentamos versões rotacionadas com diversidade máxima de $\mathbb{Z}^7$ e de D_7. Seja $p = 29$, que é congruente a 1 módulo 7. Neste caso, $r = 2$ e $\lambda = 1$. Os valores de α, z e x são:*

$$\begin{aligned}\alpha = \zeta_{29}^{27} - \zeta_{29}^{26} - \zeta_{29}^{25} + \zeta_{29}^{24} + \zeta_{29}^{23} + \zeta_{29}^{22} + \zeta_{29}^{21} - \zeta_{29}^{20} + \zeta_{29}^{19} - \zeta_{29}^{18} - \zeta_{29}^{17} - \zeta_{29}^{16} + \zeta_{29}^{15} - \zeta_{29}^{14} \\ -\zeta_{29}^{13} + \zeta_{29}^{12} - \zeta_{29}^{11} - \zeta_{29}^{10} - \zeta_{29}^{9} + \zeta_{29}^{8} - \zeta_{29}^{7} + \zeta_{29}^{6} + \zeta_{29}^{5} + \zeta_{29}^{4} + \zeta_{29}^{3} - \zeta_{29}^{2} - \zeta_{29} + 1,\end{aligned} \tag{2.11}$$

$$\begin{aligned}z = -2\zeta_{29}^{27} - 4\zeta_{29}^{26} - 2\zeta_{29}^{25} - 2\zeta_{29}^{24} - 2\zeta_{29}^{23} - 4\zeta_{29}^{21} - 2\zeta_{29}^{19} - 2\zeta_{29}^{18} - 4\zeta_{29}^{17} - 2\zeta_{29}^{15} - 4\zeta_{29}^{14} - 2\zeta_{29}^{12} - \\ -2\zeta_{29}^{11} - 4\zeta_{29}^{10} - 4\zeta_{29}^{8} - 2\zeta_{29}^{7} - 2\zeta_{29}^{6} - 2\zeta_{29}^{5} - 2\zeta_{29}^{3} - 4\zeta_{29}^{2} - \zeta_{29} - 3,\end{aligned} \tag{2.12}$$

$$\begin{aligned}x = -3\zeta_{29}^{27} - \zeta_{29}^{26} - \zeta_{29}^{25} - 3\zeta_{29}^{24} - 3\zeta_{29}^{23} - \zeta_{29}^{22} - \zeta_{29}^{21} - \zeta_{29}^{20} - \zeta_{29}^{19} + 3\zeta_{29}^{18} + 3\zeta_{29}^{16} - 3\zeta_{29}^{15} - 3\zeta_{29}^{14} + \\ +3\zeta_{29}^{13} + 3\zeta_{29}^{11} - \zeta_{29}^{10} - \zeta_{29}^{9} - \zeta_{29}^{8} - \zeta_{29}^{7} - 3\zeta_{29}^{6} - 3\zeta_{29}^{5} - \zeta_{29}^{4} - \zeta_{29}^{3} - 3\zeta_{29}^{2} - 5.\end{aligned} \tag{2.13}$$

A matriz geradora de $\mathbb{Z}^7$ é dada por

$$\frac{1}{29}\begin{pmatrix} -19.747... & 4.729... & -13.016... & 2.244... & 2.387... & 7.991... & -13.588... \\ 4.729... & -13.016... & 2.244... & 2.387... & 7.991... & -13.588... & -19.747... \\ -13.016... & 2.244... & 2.387... & 7.991... & -13.588... & -19.747... & 4.729... \\ 2.244... & 2.387... & 7.991... & -13.588... & -19.747... & 4.729... & -13.016... \\ 2.387... & 7.991... & -13.588... & -19.747... & 4.729... & -13.016... & 2.244... \\ 7.991... & -13.588... & -19.747... & 4.729... & -13.016... & 2.244... & 2.387... \\ -13.588... & -19.747... & 4.729... & -13.016... & 2.244... & 2.387... & 7.991... \end{pmatrix} \tag{2.14}$$

enquanto a matriz geradora de D_7 é

$$\frac{1}{29}\begin{pmatrix} 15.017... & 8.286... & 10.772... & -4.631... & -10.378... & 5.597... & 33.335... \\ -24.477... & 17.746... & -15.260... & -0.143... & -5.603... & 21.579... & 6.158... \\ 17.746... & -15.260... & -0.143... & -5.603... & 21.579... & 6.158... & -24.477... \\ -15.260... & -0.143... & -5.603... & 21.579... & 6.158... & -24.477... & 17.746... \\ -0.143... & -5.603... & 21.579... & 6.158... & -24.477... & 17.746... & -15.260... \\ -5.603... & 21.579... & 6.158... & -24.477... & 17.746... & -15.260... & -0.143... \\ 21.579... & 6.158... & -24.477... & 17.746... & -15.260... & -0.143... & -5.603... \end{pmatrix}. \tag{2.15}$$

A grande vantagem das construções de $\mathbb{Z}^n$ e de D_n feitas anteriormente em relação às suas construções usuais é que as versões rotacionadas $\sigma_\beta(I)$ e $\sigma_\beta(M)$ têm diversidade máxima, já que o corpo $\mathbb{K}$ sobre o qual foram obtidas é totalmente real (Lema 2.1.1). Esse fato nos permite calcular a distância produto mínima dessas construções conforme a Proposição 1.8.2 da Seção 1.8. Sendo assim, os dois próximos resultados dão condições para o cálculo da distância produto mínima da versão de $\mathbb{Z}^n$ obtida anteriormente, com n ímpar.

Proposição 2.1.3. *O $\mathbb{Z}$-módulo I definido em (2.7) é um ideal em $\mathcal{O}_\mathbb{K}$.*

Demonstração. Consideremos o $\mathbb{Z}$-módulo $J = \langle z, \sigma(z), \ldots, \sigma^{p-2}(z)\rangle_\mathbb{Z}$ em $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. Vejamos que J é um ideal. Para isso, seja $j = \sum_{i=0}^{p-2} a_i\sigma^i(z)$ um elemento qualquer de J, em que $a_i \in \mathbb{Z}$, $0 \leqslant i \leqslant p-2$, e mostremos que $j\zeta_p \in J$. Devido ao item (b) do Lema 2.1.2,

$$j\zeta_p = \left(\sum_{i=0}^{p-2} a_i\sigma^i(z)\right)\zeta_p = \sum_{i=0}^{p-2}(-1)^i a_i\zeta_p^\lambda\alpha(1-\zeta_p^{r^i})\zeta_p. \tag{2.16}$$

Como $\{\zeta_p^{r^i}\}_{i=0}^{p-2} = \{\zeta_p^k\}_{k=1}^{p-1}$, podemos reenumerar a soma (2.16) denominando por b_k o termo $(-1)^i a_i$ tal que $\zeta_p^{r^i} = \zeta_p^k$, para todo $0 \leqslant i \leqslant p-2$:

$$j\zeta_p = \zeta_p^\lambda\alpha\sum_{k=1}^{p-1} b_k(1-\zeta_p^k)\zeta_p. \tag{2.17}$$

Sejam $c_1 = -\sum_{k=1}^{p-1} b_k$ e $c_i = b_{i-1}$, para $2 \leqslant i \leqslant p-1$. Assim,

$$\begin{aligned}\sum_{k=1}^{p-1} c_k(1-\zeta_p^k) &= -\sum_{k=1}^{p-1} b_k(1-\zeta_p) + \sum_{k=2}^{p-1} b_{k-1}(1-\zeta_p^k) = \\ &= b_{p-1}(\zeta_p - 1) + \sum_{k=1}^{p-2} b_k\left(\zeta_p - \zeta_p^{k+1}\right) = \\ = b_{p-1}(1-\zeta_p^{p-1})\zeta_p + \sum_{k=1}^{p-2} b_k\left(1-\zeta_p^k\right)\zeta_p &= \sum_{k=1}^{p-1} b_k\left(1-\zeta_p^k\right)\zeta_p.\end{aligned} \tag{2.18}$$

De (2.17), obtemos

$$j\zeta_p = \zeta_p^{\lambda}\alpha\sum_{i=1}^{p-1} c_i(1-\zeta_p^i) = \sum_{i=1}^{p-1} c_i\zeta_p^{\lambda}\alpha(1-\zeta_p^i). \tag{2.19}$$

Denominando por $(-1)^k d_k$ cada termo c_i tal que $\zeta_p^i = \zeta_p^{r^k}$, $1 \leqslant i \leqslant p-2$, segue que

$$j\zeta_p = \sum_{k=0}^{p-2}(-1)^k d_k\zeta_p^{\lambda}\alpha(1-\zeta_p^{r^k}) = \sum_{k=0}^{p-2} d_k\sigma^k(z). \tag{2.20}$$

Disso concluímos que $j\zeta_p \in J$ para todo $j \in J$. Por recorrência segue que $j\zeta_p^k \in J$ para $0 \leqslant k \leqslant p-2$. Como $\{\zeta_p^k\}_{k=0}^{p-2}$ é uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, podemos concluir que $j\mathcal{O}_{\mathbb{Q}(\zeta_p)} \subset J$, para todo $j \in J$. Logo, J é ideal em $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Por fim, o conjunto I coincide com o ideal $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(J)$, já que $x = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(z)$ e, para cada $\sigma^i(z)$ da $\mathbb{Z}$-base de J,

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(\sigma^i(z)) = \sigma^i(x) = \sigma^{qn+r}(x) = \sigma^r(x) \in I, \tag{2.21}$$

pois existem q e r tais que $i = qn + r$, $0 \leqslant r < n$, e $\sigma^n(x) = x$. Logo, I é um ideal de $\mathcal{O}_{\mathbb{K}}$. □

Proposição 2.1.4. *Se $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$, então I é um ideal principal de $\mathcal{O}_{\mathbb{K}}$ gerado por x.*

Demonstração. Como $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p] \cap \mathbb{K}$, segue que $u \in \mathcal{O}_{\mathbb{K}}$. Assim, $\sigma^i(u) \in \mathcal{O}_{\mathbb{K}}$ e

$$\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{n-1}(x)\} = \{x, ux, \sigma(u)ux, \ldots, \sigma^{n-2}(u)\sigma^{n-3}(u)\ldots\sigma(u)ux\} \subset x\mathcal{O}_{\mathbb{K}} \tag{2.22}$$

ou seja, $I \subset x\mathcal{O}_{\mathbb{K}}$. Como $x\mathcal{O}_{\mathbb{K}} \subset I$, segue que $I = x\mathcal{O}_{\mathbb{K}}$. □

Como consequência da Proposição 2.1.4 podemos calcular a distância produto mínima de $\sigma_\beta(I) \simeq \mathbb{Z}^n$, mas para isso precisamos do seguinte lema:

Lema 2.1.4. *[LNI02, Corolário 4.2] Se p é um primo ímpar e $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, então o discriminante de $\mathbb{K}$ é dado por $D(\mathbb{K}) = \pm p^{[\mathbb{K}:\mathbb{Q}]-1}$.*

Corolário 2.1.1. *Se $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$, então a distância produto mínima do reticulado $\sigma_\beta(I)$ (equivalente a $\mathbb{Z}^n$) é igual a $p^{\frac{1-n}{2}}$. Além disso, $|N_{\mathbb{K}}(x)| = p^{\frac{n+1}{2}}$.*

Demonstração. Devido à Proposição 2.1.4, I é um ideal principal em $\mathcal{O}_{\mathbb{K}}$ gerado por x. Segue de (1.69) que

$$d_{p,min}(\sigma_\beta(I)) = \sqrt{\frac{D}{|D(\mathbb{K})|}}, \tag{2.23}$$

onde D é o determinante do reticulado. Como o reticulado é $\mathbb{Z}^n$-rotacionado, então $D = 1$. Devido ao Lema 2.1.4, sabemos que $|D(\mathbb{K})| = p^{n-1}$. Portanto,

$$d_{p,min}(\sigma_\beta(I)) = \sqrt{\frac{1}{p^{n-1}}} = p^{\frac{1-n}{2}}. \tag{2.24}$$

Por outro lado, sabemos que a distância produto mínima é igual $\sqrt{N_{\mathbb{K}}(\beta)} \min_{0\neq y\in I} |N_{\mathbb{K}}(y)|$. Sendo $\beta = 1/p^2$ segue que $\sqrt{N_{\mathbb{K}}(\beta)} = (1/p)^n$. Além disso, como I é principal gerado por x, o valor de $\min_{0\neq y\in I} |N_{\mathbb{K}}(y)|$ deve ser atingido em x, ou seja,

$$|N_{\mathbb{K}}(x)| = \min_{0\neq y\in I} |N_{\mathbb{K}}(y)| = \frac{d_{p,min}(\sigma_\beta(I))}{\sqrt{N_{\mathbb{K}}(\beta)}} = p^{\frac{1-n}{2}} p^n = p^{\frac{n+1}{2}}, \tag{2.25}$$

como queríamos demonstrar. □

Observemos que na Proposição 2.1.4 e no Corolário 2.1.1 é necessário supor a hipótese de $\sigma(x)/x$ ser um elemento inteiro algébrico (ou seja, pertencer a $\mathbb{Z}[\zeta_p]$). A proposição a seguir garante que isso sempre vale quando o corpo $\mathbb{K}$ for o corpo maximal real $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ em $\mathbb{Q}(\zeta_p)$.

Proposição 2.1.5. *Se $(p-1)/n = 2$, então $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$.*

Demonstração. Devido ao Lema 2.1.2 e à definição de x, obtemos:

$$\begin{aligned} \frac{\sigma(x)}{x} &= \frac{-\zeta_p^\lambda \alpha \left(-(1-\zeta_p^{r^{n+1}}) + (1-\zeta_p^{r^{2n+1}})\right)}{\zeta_p^\lambda \alpha \left(-(1-\zeta_p^{r^n}) + (1-\zeta_p^{r^{2n}})\right)} = \\ = \frac{\zeta_p^r - \zeta_p^{r^{n+1}}}{\zeta_p^{r^n} - \zeta_p} &= -\frac{\zeta_p^r}{\zeta_p} \frac{\left(1-\zeta_p^{r^{n+1}-r}\right)}{\left(1-\zeta_p^{r^n-1}\right)} = -\zeta_p^{r-1} \frac{\left(1-\zeta_p^{r(r^n-1)}\right)}{\left(1-\zeta_p^{r^n-1}\right)}. \end{aligned} \tag{2.26}$$

Sabe-se que o termo expresso em (2.26) é uma unidade de $\mathcal{O}_{\mathbb{K}}$ [Was95, Lema 1.3]. Em particular, $\sigma(x)/x$ é um elemento de $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$, como queríamos demonstrar. □

A Proposição 2.1.5 nos garante que, quando $p = 2n+1$ é um número primo, existe $\mathbb{Z}^n$ com diversidade máxima e distância produto mínima igual a $p^{\frac{1-n}{2}}$. Isso ocorre, por exemplo, para $n = 3, 5, 9, 11, 15, 19, ...$ No entanto, os resultados desta seção nos permitem obter a distância produto mínima também em outros casos após verificarmos que $\sigma(x)/x$ é um inteiro algébrico, como no exemplo a seguir:

Exemplo 2.1.2. *Consideremos o $\mathbb{Z}^7$-rotacionado ($n = 7$) desenvolvido no Exemplo 2.1.1. Nesse caso utilizamos o número primo $p = 29$, que não satisfaz a igualdade $p = 2n+1$. Logo, para aplicar o Corolário 2.1.1 precisamos calcular o quociente $\sigma(x)/x$ e verificar se tal número é um inteiro algébrico. De fato,*

$$\frac{\sigma(x)}{x} = -\zeta_{29} - \zeta_{29}^{12} - \zeta_{29}^{17} - \zeta_{29}^{28} \tag{2.27}$$

pertence a $\mathbb{Z}[\zeta_{29}]$, pois é uma combinação inteira de potências de ζ_{29}. Portanto, o Corolário 2.1.1 garante que a distância produto mínima desse reticulado é

$$p^{\frac{1-n}{2}} = 29^{-3} \tag{2.28}$$

e que

$$|N_{\mathbb{K}}(x)| = p^{\frac{n+1}{2}} = 29^4. \tag{2.29}$$

Observação 2.1.1. *A hipótese $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$ não é sempre válida. Por exemplo, quando $n = 13$ e $p = 131$ (ou $p = 157$, ou $p = 313$), o quociente $\sigma(x)/x$ não é um inteiro algébrico. No entanto, se $p = 53$ ou $p = 79$, esse quociente pertence a $\mathbb{Z}[\zeta_p]$.*

Agora vamos analisar a distância produto mínima dos reticulados D_n-rotacionados construídos na Proposição 2.1.2 através do $\mathbb{Z}$-módulo

$$M = \{x + \sigma(x), x - \sigma(x), \sigma(x) - \sigma^2(x), \ldots, \sigma^{n-2}(x) - \sigma^{n-1}(x)\}. \tag{2.30}$$

Se M fosse um ideal principal, poderíamos concluir que a distância produto mínima de $\sigma_{1/p^2}(M)$ seria $2p^{\frac{1-n}{2}}$ [Jor12, Seção 4]. No entanto, veremos que em uma infinidade de situações e dadas algumas hipóteses esse valor é igual a $p^{\frac{1-n}{2}}$. Portanto, M não pode ser um ideal principal nesses casos.

Proposição 2.1.6. *Se $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$, então a distância produto mínima de $\sigma_{1/p^2}(M) \simeq D_n$ satisfaz $d_{p,min}(\sigma_{1/p^2}(M)) \geqslant p^{\frac{1-n}{2}}$.*

Demonstração. Esse resultado ocorre porque $\sigma_{1/p^2}(M)$ é um sub-reticulado de $\sigma_{1/p^2}(I)$, cuja distância produto mínima é $p^{\frac{1-n}{2}}$, segundo o Corolário 2.1.1. □

Proposição 2.1.7. *Se $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p]$ e se pelo menos um dos elementos $1 + u$ ou $1 - u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de $\sigma_{1/p^2}(M) \simeq D_n$ é igual a $p^{\frac{1-n}{2}}$.*

Demonstração. Se $1 + u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, então, do Corolário 2.1.1, segue que $x + \sigma(x) = x(1 + u)$ tem valor absoluto da norma dado por

$$|N_{\mathbb{K}}(x + \sigma(x))| = |N_{\mathbb{K}}(x)| = p^{\frac{n+1}{2}}. \tag{2.31}$$

O mesmo argumento vale no caso em que $1 - u$ é uma unidade. Por um lado, devido à Proposição 2.1.6, $d_{p,min}(\sigma_{1/p^2}(M)) \geqslant p^{\frac{1-n}{2}}$, donde segue que

$$\min_{0 \neq y \in M} |N_{\mathbb{K}}(y)| \geqslant N_{\mathbb{K}}(1/p^2)^{-2} p^{\frac{1-n}{2}} = p^{\frac{n+1}{2}}. \tag{2.32}$$

Por outro lado, um dos valores $y = x \pm \sigma(x)$ atinge esse mínimo. Disso, concluímos que $d_{p,min}(\sigma_{1/p^2}(M)) = p^{-n} p^{\frac{n+1}{2}} = p^{\frac{1-n}{2}}$. □

Observação 2.1.2. *Observemos que $1 \pm u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, vale a igualdade $|N_{\mathbb{K}}(x \pm \sigma(x))| = |N_{\mathbb{K}}(x)|$.*

Lembremos da Proposição 2.1.5 que $u \in \mathcal{O}_{\mathbb{K}}$ quando $(p - 1)/n = 2$. Portanto, nesses casos, para ver se a distância produto mínima é igual a $p^{\frac{1-n}{2}}$ deve-se apenas verificar se pelo menos um entre os elementos $1 + u$ ou $1 - u$ é uma unidade. Na próxima proposição vemos um caso em que $1 + u$ é sempre uma unidade em $\mathcal{O}_{\mathbb{K}}$:

Proposição 2.1.8. *Se $n = 3$ e $u \in \mathbb{Z}[\zeta_p]$, então $1+u$ é uma unidade em $\mathcal{O}_\mathbb{K}$. Consequentemente, a distância produto mínima do reticulado algébrico $\sigma_{1/p^2}(M) \simeq D_3$ construído via qualquer $p \equiv 1 \pmod 3$ é $1/p$.*

Demonstração. Seja $M = \langle x, \sigma(x), \sigma^2(x)\rangle_\mathbb{Z}$. O Lema 2.1.3 implica que

$$x\sigma(x) + \sigma(x)\sigma^2(x) + \sigma^2(x)x = 0. \tag{2.33}$$

Utilizando (2.33), temos:

$$\begin{aligned} N_\mathbb{K}(x+\sigma(x)) = (x+\sigma(x))(\sigma(x)+\sigma^2(x))(\sigma^2(x)+x) = \\ (x^2 + x\sigma(x) + \sigma(x)\sigma^2(x) + \sigma^2(x)x)(\sigma(x)+\sigma^2(x)) = \\ x^2(\sigma(x)+\sigma^2(x)) = x(x\sigma(x) + x\sigma^2(x)) = -x(\sigma(x)\sigma^2(x)) = -N_\mathbb{K}(x). \end{aligned} \tag{2.34}$$

Os resultados seguem da Observação 2.1.2 e da Proposição 2.1.7. □

Exemplo 2.1.3. *Consideremos o D_7-rotacionado ($n = 7$) desenvolvido no Exemplo 2.1.1, com primo $p = 29$. Já vimos no Exemplo 2.1.2 que $\sigma(x)/x$ é um inteiro algébrico. Além disso,*

$$1 - u = 1 + \zeta_{29} + \zeta_{29}^{12} + \zeta_{29}^{17} + \zeta_{29}^{28} \tag{2.35}$$

e seu inverso é

$$\begin{aligned} \frac{1}{1-u} = \zeta_{29}^{27} - 2\zeta_{29}^{26} - 2\zeta_{29}^{25} + \zeta_{29}^{24} - \zeta_{29}^{23} - 2\zeta_{29}^{22} - 2\zeta_{29}^{19} - \zeta_{29}^{18} - \zeta_{29}^{16} - \zeta_{29}^{15} - \zeta_{29}^{14} - \\ -\zeta_{29}^{13} - \zeta_{29}^{11} - 2\zeta_{29}^{10} - 2\zeta_{29}^{7} - \zeta_{29}^{6} + \zeta_{29}^{5} - 2\zeta_{29}^{4} - 2\zeta_{29}^{3} + \zeta_{29}^{2} - 3 \end{aligned} \tag{2.36}$$

do que podemos concluir que $1-u$ é uma unidade em $\mathbb{Z}[\zeta_p]$. Portanto, $1-u$ é uma unidade em $\mathcal{O}_\mathbb{K}$. Segue da Proposição 2.1.7 que a distância produto mínima de $\sigma_{1/29^2}(M) \simeq D_7$ é igual a 29^{-3}. Note, no entanto, que $1+u$ não é uma unidade em $\mathcal{O}_\mathbb{K}$, pois,

$$\begin{aligned} \frac{1}{1+u} = \frac{5}{17}\zeta_{29}^{27} + \frac{6}{17}\zeta_{29}^{26} + \frac{2}{17}\zeta_{29}^{25} + \frac{5}{17}\zeta_{29}^{24} + \frac{7}{17}\zeta_{29}^{23} + \frac{6}{17}\zeta_{29}^{22} + \frac{2}{17}\zeta_{29}^{21} + \frac{2}{17}\zeta_{29}^{20} + \frac{2}{17}\zeta_{29}^{19} \\ -\frac{1}{17}\zeta_{29}^{18} - \frac{1}{17}\zeta_{29}^{16} + \frac{7}{17}\zeta_{29}^{15} + \frac{7}{17}\zeta_{29}^{14} - \frac{1}{17}\zeta_{29}^{13} - \frac{1}{17}\zeta_{29}^{11} + \frac{2}{17}\zeta_{29}^{10} + \frac{2}{17}\zeta_{29}^{9} + \frac{2}{17}\zeta_{29}^{8} + \frac{6}{17}\zeta_{29}^{7} \\ \frac{7}{17}\zeta_{29}^{6} + \frac{5}{17}\zeta_{29}^{5} + \frac{2}{17}\zeta_{29}^{4} + \frac{6}{17}\zeta_{29}^{3} + \frac{5}{17}\zeta_{29}^{2} + \frac{7}{17} \end{aligned} \tag{2.37}$$

não é um inteiro algébrico.

Observação 2.1.3. *A hipótese de $1+u$ ou $1-u$ ser(em) unidade(s) nem sempre é válida. Como foi comentado na Observação 2.1.1, se $n = 13$ e $p = 53$ ou $p = 79$, então $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$. No entanto, nesses dois casos, nem $1+u$ nem $1-u$ são invertíveis em $\mathcal{O}_\mathbb{K}$.*

2.2 Construções de $\mathbb{Z}^n$ e D_n, com n potência de 2

Nesta seção, descreveremos as construções dos reticulados algébricos $\mathbb{Z}^n$ e D_n, com n igual a uma potência de 2, propostas em [SO07] e [JC12]. Para isso, sejam $m \geqslant 3$ um número inteiro, $n = 2^{m-2}$ e $\omega = e^{\frac{2\pi i}{2^m}}$ uma raiz 2^m-ésima primitiva da unidade. Denotando por θ o número $\omega + \omega^{-1}$, vemos que $\mathbb{L} = \mathbb{Q}(\theta)$ é o subcorpo maximal real do corpo ciclotômico $\mathbb{Q}(\omega)$, de modo que $[\mathbb{Q}(\omega) : \mathbb{L}] = 2$. Logo, o grau do corpo $\mathbb{L}$ é n. Além disso, $\mathcal{O}_\mathbb{L} = \mathbb{Z}[\theta]$ [Was95, Proposição 2.16]. A seguir, para cada $j \geqslant 0$, consideremos $\theta_j = \omega^j + \omega^{-j}$.

Proposição 2.2.1. *[SO07, Teorema 1] Consideremos os vetores $w_0 = 1$, $w_1 = 1 + \theta_1$, ..., $w_{n-1} = 1 + \theta_1 + \ldots + \theta_{n-1}$. O conjunto $H = \{w_0, w_1, \ldots, w_{n-1}\}$ é uma $\mathbb{Z}$-base para $\mathcal{O}_\mathbb{L}$. Além disso, sendo $\beta = 1/n - \theta/(2n)$, o reticulado $\sigma_\beta(\mathcal{O}_\mathbb{L})$ é uma versão rotacionada de $\mathbb{Z}^n$.*

Seja τ o gerador do grupo de Galois cíclico da extensão $\mathbb{L}$ sobre $\mathbb{Q}$, definido por $\tau(\omega) = \omega^r$, em que r é o elemento primitivo de $\mathbb{Z}^*_{2^{m-1}}$. A matriz geradora de $\sigma_\beta(\mathcal{O}_\mathbb{L})$ é, por definição,

$$G = \begin{pmatrix} w_0 & \tau(w_0) & \ldots & \tau^{n-1}(w_0) \\ w_1 & \tau(w_1) & \ldots & \tau^{n-1}(w_1) \\ \vdots & \vdots & \ddots & \vdots \\ w_{n-1} & \tau(w_{n-1}) & \ldots & \tau^{n-1}(w_{n-1}) \end{pmatrix} \begin{pmatrix} \sqrt{\beta} & 0 & \ldots & 0 \\ 0 & \sqrt{\tau(\beta)} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sqrt{\tau^{n-1}(\beta)} \end{pmatrix}. \tag{2.38}$$

Para calcular explicitamente a matriz, notemos que $\tau^j(w_0) = 1$ e que $\tau^j(w_i) = 1 + \theta_{r^j} + \theta_{2r^j} + \ldots + \theta_{ir^j}$, para $0 \leqslant i, j \leqslant n-1$. Consequentemente podemos construir o reticulado D_n, de forma análoga ao que foi feito em [JC12, Proposição 4.6]:

Proposição 2.2.2. *Consideremos o $\mathbb{Z}$-módulo*

$$L = \langle w_0 + w_1, w_0 - w_1, \ldots, w_{k-2} - w_{k-1} \rangle_\mathbb{Z} = \langle 2 + \theta_1, -\theta_1, -\theta_2, \ldots, -\theta_{k-1} \rangle_\mathbb{Z}. \tag{2.39}$$

O reticulado algébrico $\sigma_\beta(L)$ é uma versão rotacionada de D_n, sendo $n = 2^{m-2}$.

Demonstração. Basta multiplicar a matriz da Equação 2.9 pela matriz G de (2.38), tal como foi feito na demonstração da Proposição 2.1.2. O fato de G ser uma matriz de rotação garante que o reticulado é uma versão rotacionada de D_n. □

Outro conjunto de geradores para o $\mathbb{Z}$-módulo L da Proposição 2.2.2 é $\{2\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-1}\}$. Isso implica que o $\mathbb{Z}$-módulo L é o ideal principal $\theta_1\mathcal{O}_\mathbb{L}$ [JC12, Proposição 4.7].

Os reticulados $\mathbb{Z}^n$ e D_n, em que $n = 2^{m-2}$ e $m \geqslant 3$, têm diversidade máxima, já que são imagens, via o mergulho torcido, de ideais principais em anéis de inteiros de

corpos de números totalmente reais. Como esses ideais são principais e $D(\mathbb{L}) = 2^{(m-1)n-1}$ [Lop03, Teorema 3.2], a distância produto mínima de $\mathbb{Z}^n$ é

$$d_{p,min}(\sigma_\beta(\mathcal{O}_\mathbb{L})) = \sqrt{\frac{\det(\sigma_\beta(\mathcal{O}_\mathbb{L}))}{|D(\mathbb{L})|}} = \sqrt{\frac{1}{2^{(m-1)n-1}}} = 2^{\frac{1-(m-1)n}{2}} \tag{2.40}$$

e a distância produto mínima de D_n é

$$d_{p,min}(\sigma_\beta(\mathcal{O}_\mathbb{L})) = \sqrt{\frac{\det(\sigma_\beta(\mathcal{O}_\mathbb{L}))}{|D(\mathbb{L})|}} = \sqrt{\frac{4}{2^{(m-1)n-1}}} = 2^{\frac{3-(m-1)n}{2}}. \tag{2.41}$$

Exemplo 2.2.1. *Sejam $m = 3$, $n = 2$, $\theta = \zeta_8 + \zeta_8^{-1} = \sqrt{2}$, $\mathbb{L} = \mathbb{Q}(\sqrt{2})$ e $\beta = (2-\sqrt{2})/4$. O conjunto $H = \{w_0 = 1, w_1 = 1 + \sqrt{2}\}$ é uma $\mathbb{Z}$-base para o reticulado $\sigma_\beta(\mathbb{Z}[\sqrt{2}])$, equivalente a $\mathbb{Z}^2$. Por sua vez, $L = \langle 2, \sqrt{2}\rangle_\mathbb{Z}$ é o $\mathbb{Z}$-módulo cuja imagem por σ_β equivale ao reticulado D_2. Ambos os reticulados têm diversidade máxima. Nesta construção, a distância produto mínima de $\mathbb{Z}^2$ é $\sqrt{2}/4$ e a de D_2 é $\sqrt{2}/2$.*

Exemplo 2.2.2. *Sejam $m = 4$, $n = 4$, $\theta = \zeta_{16} + \zeta_{16}^{-1} = 2\cos(\pi/8)$, $\mathbb{L} = \mathbb{Q}(2\cos(\pi/8))$ e $\beta = (1-\cos(\pi/8))/4$. O conjunto $H = \{w_0 = 1, w_1 = 1+2\cos(\pi/8), w_2 = 1+2\cos(\pi/8) + \sqrt{2}, 1 + 2\cos(\pi/8) + \sqrt{2} + 2\cos(3\pi/8)\}$ é uma $\mathbb{Z}$-base para o reticulado $\sigma_\beta(\mathbb{Z}[2\cos(\pi/8)])$, equivalente a $\mathbb{Z}^4$. Por sua vez, $L = \langle 2, 2\cos(\pi/8), \sqrt{2}, 2\cos(3\pi/8)\rangle_\mathbb{Z}$ é o $\mathbb{Z}$-módulo cuja imagem via σ_β equivale ao reticulado D_4. Ambos os reticulados têm diversidade máxima. Nesta construção, a distância produto mínima de $\mathbb{Z}^4$ é $2^{-11/2}$ e a de D_4 é $2^{-9/2}$.*

2.3 Construções de $\mathbb{Z}^n$ e D_n, com $n > 1$ par

A seguir construiremos os reticulados $\mathbb{Z}^n$ e D_n, para qualquer número par $n > 1$ a partir da composição de corpos utilizados para obter as versões de $\mathbb{Z}^n$ e D_n com n ímpar e com n igual a uma potência de 2 nas Seções 2.1 e 2.2. Vamos fatorar o número inteiro $n > 1$ como $n = 2^{m-2}l$, em que $l > 1$ é um número ímpar e $m > 2$. Sejam $\mathbb{K}$ o corpo de grau l definido na Equação 2.1 da Seção 2.1 e $\mathbb{L} = \mathbb{Q}(\omega) = \mathbb{Q}(\zeta_{2^m} + \zeta_{2^m}^{-1})$ o corpo de grau 2^{m-2} definido na Seção 2.2.

Lema 2.3.1. *Considerando as notações do parágrafo anterior, valem as seguintes afirmações:*

a) $\mathbb{K} \cap \mathbb{L} = \mathbb{Q}$.

b) Se $\mathbb{KL}$ é o corpo composto de $\mathbb{K}$ e $\mathbb{L}$ (isto é, o menor corpo que contém $\mathbb{K}$ e $\mathbb{L}$ simultaneamente), então $Gal(\mathbb{KL}/\mathbb{Q}) \simeq Gal(\mathbb{K}/\mathbb{Q}) \times Gal(\mathbb{L}/\mathbb{Q})$.

c) O grau do corpo composto $\mathbb{KL}$ é n.

d) O discriminante de $\mathbb{KL}$ é $D(\mathbb{K})^{2^{m-2}} D(\mathbb{L})^l$.

e) O anel de inteiros de $\mathbb{KL}$ é $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Além disso, se $\{x_i\}_i$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e se $\{y_j\}_j$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{L}}$, então $\{x_i y_j\}_{i\times j}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{KL}}$.

f) $Tr_{\mathbb{KL}}(uv) = Tr_{\mathbb{K}}(u)Tr_{\mathbb{L}}(v)$, para todo $u \in \mathbb{K}$ e $v \in \mathbb{L}$.

Demonstração. Como $\mathbb{K}$ tem grau ímpar, $\mathbb{L}$ tem grau par e $\mathbb{K} \cap \mathbb{L}$ tem grau divisor simultâneo dos graus de $\mathbb{K}$ e de $\mathbb{L}$, e então o grau de $\mathbb{K} \cap \mathbb{L}$ é 1, donde segue o item (a). O item (b) é consequência do item (a) e pode ser provado a partir de [Rib01, Seção 2.7], já que as extensões $\mathbb{K}/\mathbb{Q}$ e $\mathbb{L}/\mathbb{Q}$ são galoisianas. Os itens (c), (d) e (e) são provados em [Rib01, W, capítulo 13]. Por fim, o item (f) é consequência do item (b). □

Devido ao item (c) do Lema 2.3.1, o corpo composto $\mathbb{KL}$ tem grau n e pode ser usado para construir $\mathbb{Z}^n$ e D_n. Consideremos o ideal I de (2.7), o anel $J = \mathcal{O}_{\mathbb{L}}$, o número primo p satisfazendo $p \equiv 1 \ (mod\ l)$, os números θ e w_i conforme foram definidos na Seção 2.2, $k = 2^{m-2}$ e σ e τ como nas Seções 2.1 e 2.2.

Proposição 2.3.1 ([BFOV04], Proposição 6)**.** *Sejam $\mathcal{I}$ o ideal produto $IJ \subset \mathcal{O}_{\mathbb{KL}}$ e $\beta = p^{-2}(1/k - \theta/2k)$. Assim, valem as seguintes afirmações:*

a) $\mathcal{I} = \langle w_0 x, w_0\sigma(x) \ldots, w_0\sigma^{l-1}(x), w_1 x, \ldots, w_1\sigma^{l-1}(x), \ldots, w_{k-1}x, \ldots, w_{k-1}\sigma^{l-1}(x)\rangle_{\mathbb{Z}}$.

b) $\sigma_\beta(\mathcal{I})$ é uma versão rotacionada de $\mathbb{Z}^n$.

c) A matriz geradora desse reticulado é o produto tensorial das matrizes G explicitadas na Proposição 2.1.1 e na Equação 2.38.

Demonstração. O item (a) ocorre porque o produto de ideais IJ é, por definição, o conjunto de todas as somas finitas de produtos de elementos de I por elementos de J. Denotemos por G_1 a matriz explicitada na Proposição 2.1.1 sem o termo escalar $1/p$, ou seja, $G_1 = (\sigma^i\sigma^j(x))_{0\leqslant i,j\leqslant l-1}$, por G_2 a matriz à esquerda no produto na Equação 2.38, por H_1 a matriz quadrada $l \times l$ com $1/p$ na diagonal e zero nas outras entradas e por H_2 a matriz diagonal à direita no produto na Equação 2.38. Assim, o item (b) do Lema 2.3.1 garante que a matriz geradora do reticulado $\sigma_\beta(\mathcal{I})$ é igual a

$$G_3 = (G_1 \otimes G_2)(H_1 \otimes H_2) = (G_1H_1) \otimes (G_2H_2) = (p^{-1}G_1) \otimes (G_2H_2) \tag{2.42}$$

em que $\otimes$ representa o produto tensorial entre duas matrizes e $H_1 \otimes H_2$ é a matriz quadrada de ordem $kl = n$ com diagonal $\sqrt{\sigma^i \circ \tau^j(\beta)}$. Agora, notemos que $p^{-1}G_1$ é a matriz geradora de $\sigma_{1/p^2}(I)$ da Proposição 2.1.1 e que G_2H_2 é a matriz G de (2.38), comprovando o item (c). Por fim, para provar que $\sigma_\beta(\mathcal{I})$ é uma versão rotacionada de $\mathbb{Z}^n$ basta provar que a matriz de Gram de $\sigma_\beta(\mathcal{I})$, dada por $G_3^T G_3$, é a matriz identidade. A matriz quadrada $G_3G_3^T$ tem ordem $lk = n$, onde cada entrada $(a+1)(c+1) \times (b+1)(d+1)$, $0 \leqslant a, b \leqslant l-1$

e $0 \leqslant c, d \leqslant k-1$, é dada por $Tr_{\mathbb{KL}}(\beta u_a w_c u_b w_d)$, em que $u_i = \sigma^i(c)$, $0 \leqslant i \leqslant l-1$. Devido ao item (f) do Lema 2.3.1 segue que

$$Tr_{\mathbb{KL}}(\beta u_a w_c u_b w_d) = Tr_{\mathbb{K}}(p^{-2} u_a u_b) Tr_{\mathbb{L}}\left((1/k - \theta/(2k)) w_c w_d\right), \tag{2.43}$$

Devido à Proposição 2.1.1 e à Proposição 2.2.1, o traço em (2.43) é igual a 1 quando $a = b$ e $c = d$, mas é zero nos outros casos. Isso significa que $G_3 G_3^T = G_3^T G_3 = I$, comprovando o item (b). □

Analogamente ao que fizemos nos casos tratados nas Seções 2.1 e 2.2, podemos extrair um reticulado D_n-rotacionado de $\mathbb{Z}^n$:

Proposição 2.3.2. *Consideremos o $\mathbb{Z}$-módulo $\mathcal{M}$ gerado por*

$$\{w_0(x + \sigma(x))\} \cup \{w_i \sigma^{l-1}(x) - w_{i+1} x, 0 \leqslant i \leqslant k-2\} \cup$$

$$\cup \left(\bigcup_{0 \leqslant j \leqslant k-1} \{w_j(\sigma^i(x) - \sigma^{i+1}(x)), 0 \leqslant i \leqslant l-2\} \right) \tag{2.44}$$

e $\beta = p^{-2}(1/k - \theta/(2k))$. O reticulado algébrico $\sigma_\beta(\mathcal{M})$ é uma versão rotacionada de D_n.

Demonstração. A matriz do reticulado obtido através do $\mathbb{Z}$-módulo $\mathcal{M}$ é o produto da matriz de (2.9) de ordem $n \times n$ pela matriz do item (c) da Proposição 2.3.1. Como esta última matriz é de rotação, então $\sigma_\beta(\mathcal{M})$ é uma versão rotacionada de D_n. □

Nas Proposições 2.3.1 e 2.3.2 construímos versões rotacionadas dos reticulados $\mathbb{Z}^n$ e D_n a partir de $\mathbb{Z}$-módulos do corpo composto $\mathbb{KL}$, que é um corpo totalmente real, já que $\mathbb{K}$ e $\mathbb{L}$ são totalmente reais. Isso implica que os reticulados $\sigma_\beta(\mathcal{I}) \simeq \mathbb{Z}^n$ e $\sigma_\beta(\mathcal{M}) \simeq D_n$ têm diversidade máxima. Por isso, a seguir calcularemos a distância produto mínimo de cada um desses reticulados a partir dos resultados conhecidos para os casos $k = 2^{m-2}$ ($m \geqslant 3$) e l ímpar. Na sequência, seja $\beta = p^{-2}(1/k - \theta/(2k))$, em que $p \equiv 1 \ (mod\ l)$.

Proposição 2.3.3. *Se $\sigma(x)/x \in \mathbb{Z}[\zeta_p]$, então o ideal $\mathcal{I} = I\mathcal{O}_{\mathbb{L}}$ é principal, gerado por x, e a distância produto mínima do reticulado $\sigma_\beta(\mathcal{I}) \simeq \mathbb{Z}^n$ é dada por $p^{\frac{k-n}{2}} 2^{\frac{l-n(m-1)}{2}}$. Além disso,*

$$|N_{\mathbb{KL}}(x)| = p^{\frac{n+k}{2}}. \tag{2.45}$$

Demonstração. A Proposição 2.1.4 garante que $I = x\mathcal{O}_{\mathbb{K}}$. Do item (e) do Lema 2.3.1 concluímos que $x\mathcal{O}_{\mathbb{KL}} = x\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} = I\mathcal{O}_{\mathbb{L}}$, ou seja, $\mathcal{I} = I\mathcal{O}_{\mathbb{L}}$ é principal gerado por x. O item (e) do Lema 2.3.1 implica que

$$d_{p,min}(\sigma_\beta(\mathcal{I})) = \sqrt{\frac{D}{|D(\mathbb{KL})|}} = \frac{1}{\sqrt{|D(\mathbb{K})|^k |D(\mathbb{L})|^l}} = p^{\frac{(1-l)k}{2}} 2^{\frac{l-l(m-1)k}{2}} = p^{\frac{k-n}{2}} 2^{\frac{l-n(m-1)}{2}}. \tag{2.46}$$

Finalmente, como $x \in \mathbb{K}$ e $|N_{\mathbb{K}}(x)| = p^{\frac{l+1}{2}}$ (Corolário 2.1.1), segue da propriedade transitiva da norma que

$$|N_{\mathbb{KL}}(x)| = |N_{\mathbb{K}}\left(N_{\mathbb{KL}/\mathbb{K}}(x)\right)| = |N_{\mathbb{K}}(x)|^k = p^{\frac{(l+1)k}{2}} = p^{\frac{n+k}{2}}, \tag{2.47}$$

o que prova o resultado. □

Corolário 2.3.1. *Se $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p]$, então a distância produto mínima de $\sigma_\beta(\mathcal{M}) \simeq D_n$ satisfaz*

$$d_{p,min}(\sigma_\beta(\mathcal{M})) \geqslant 2^{\frac{l-n(m-1)}{2}} p^{\frac{k-n}{2}}. \tag{2.48}$$

Demonstração. Esse fato ocorre porque $\sigma_\beta(\mathcal{M})$ é sub-reticulado de $\sigma_\beta(\mathcal{I})$, cuja distância produto mínima é igual a $2^{\frac{l-n(m-1)}{2}} p^{\frac{k-n}{2}}$ (Proposição 2.3.3). □

Corolário 2.3.2. *Se $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p]$ e se pelo menos um dos elementos $1+u$ ou $1-u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de $\sigma_\beta(\mathcal{M}) \simeq D_n$ é igual a*

$$2^{\frac{l-n(m-1)}{2}} p^{\frac{k-n}{2}}. \tag{2.49}$$

Demonstração. Faremos a prova supondo que $1 + u$ é unidade. O caso em que $1 - u$ é unidade é análogo. Sendo $1 + u$ uma unidade em $\mathcal{O}_{\mathbb{LK}}$, pois é em $\mathcal{O}_{\mathbb{K}}$, temos

$$N_{\mathbb{KL}}(x + \sigma(x))| = |N_{\mathbb{KL}}(x(1 + u))| = |N_{\mathbb{KL}}(x)|. \tag{2.50}$$

O primeiro elemento do conjunto de geradores de $\mathcal{M}$ enunciado na Proposição 2.3.2 é $w_0(x + \sigma(x)) = x + \sigma(x)$, pois $w_0 = 1$. Assim, de (2.45),

$$\min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{KL}}(y)| \leqslant |N_{\mathbb{KL}}(w_0(x + \sigma(x)))| = |N_{\mathbb{KL}}(x)| = p^{\frac{n+k}{2}}. \tag{2.51}$$

Por sua vez, $N_{\mathbb{KL}}(\beta) = p^{-2n}(2k)^{-n} N_{\mathbb{KL}}(2-\theta)$. Como $2-\theta = 2-\omega-\omega^{-1} = (1-\omega)(1-\omega^{-1})$, segue que

$$N_{\mathbb{Q}(\omega)}(2 - \theta) = N_{\mathbb{Q}(\omega)}\left((1 - \omega)(1 - \omega^{-1})\right) = \left(N_{\mathbb{Q}(\omega)}(1 - \omega)\right)^2 = 2^2 \tag{2.52}$$

e, usando a transitividade da norma,

$$N_{\mathbb{Q}(\omega)}(2 - \theta) = N_{\mathbb{L}}\left(N_{\mathbb{Q}(\omega)/\mathbb{L}}(2 - \theta)\right) = N_{\mathbb{L}}(2 - \theta)^2, \tag{2.53}$$

donde segue que $N_{\mathbb{L}}(2 - \theta) = 2$. Também pela transitividade da norma obtemos

$$N_{\mathbb{KL}}(2 - \theta) = N_{\mathbb{L}}\left(N_{\mathbb{KL}/\mathbb{L}}(2 - \theta)\right) = N_{\mathbb{L}}(2 - \theta)^l = 2^l. \tag{2.54}$$

Portanto,

$$d_{p,min}(\sigma_\beta(\mathcal{M})) = \sqrt{N_{\mathbb{KL}}(\beta)} \min_{0 \neq y \in \mathcal{M}} |N_{\mathbb{KL}}(y)| \leqslant p^{-n}(2k)^{-n/2} 2^{l/2} p^{\frac{n+k}{2}} = 2^{\frac{l-n(m-1)}{2}} p^{\frac{k-n}{2}}. \tag{2.55}$$

Finalmente, com a desigualdade demonstrada no Corolário 2.3.1 conclui-se a prova. □

Corolário 2.3.3. *Se $n = 3$, então o reticulado $\sigma_\beta(\mathcal{M})$ construído no Corolário 2.3.2 tem distância produto mínima igual a $2^{\frac{3-n(m-1)}{2}} p^{\frac{k-n}{2}}$.*

Demonstração. Segue da aplicação da Proposição 2.1.8 ao Corolário 2.3.2. □

Exemplo 2.3.1. *Para construir $\mathbb{Z}^{14}$ ($n = 2.7$, $k = 2$, $l = 7$) utilizamos o corpo $\mathbb{K}$ construído implicitamente no Exemplo 2.1.1 e o corpo $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. O ideal que gera uma versão rotacionada de $\mathbb{Z}^{14}$ é $\mathcal{I} = \langle x, \sigma(x), \ldots, \sigma^6(x), (1+\sqrt{2})x, (1+\sqrt{2})\sigma(x), \ldots, (1+\sqrt{2})\sigma^6(x)\rangle_{\mathbb{Z}}$, com $\beta = 29^{-2}(2-\sqrt{2})/4$. Sua diversidade é máxima e sua distância produto mínima é $2^{-21/2}29^{-6}$. Por sua vez, $\mathcal{M} = \langle x+\sigma(x), x-\sigma(x), \ldots, \sigma^5(x)-\sigma^6(x), \sigma^6(x) - (1+\sqrt{2})x, (1+\sqrt{2})(x-\sigma(x)), \ldots, (1+\sqrt{2})(\sigma^5(x)-\sigma^6(x))\rangle_{\mathbb{Z}}$ gera D_{14} com diversidade máxima e distância produto mínima dada por $2^{-21/2}29^{-6}$, já que a hipótese do Corolário 2.3.2 é válida neste exemplo.*

2.4 Análise dos resultados

Neste capítulo, trabalhamos em paralelo com versões rotacionadas dos reticulados $\mathbb{Z}^n$ e D_n. Comparando esses reticulados com relação ao empacotamento esférico, sabe-se que D_n tem maior densidade que $\mathbb{Z}^n$ quando $n > 2$, já que a densidade de centro de D_n é $2^{-(n+2)/2}$, enquanto a densidade de centro de $\mathbb{Z}^n$ é igual a 2^{-n}. Com relação à distância produto mínima dos reticulados construídos aqui, para que a comparação seja justa, é necessário que os reticulados $\mathbb{Z}^n$ e D_n tenham a mesma norma mínima. Como isso não ocorre, vamos compará-los usando a distância produto mínima relativa, definida a seguir:

Definição 2.4.1. *A distância produto mínima relativa (ou somente distância produto relativa) $d_{p,rel}(\Lambda)$ de um reticulado com diversidade máxima $\Lambda \subset \mathbb{R}^n$ com determinante D é definido como sendo $d_{p,rel}(\Lambda) = d_{p,min}(\Lambda)/\lambda^n$, em que λ é a distância mínima do reticulado Λ.*

A norma mínima de $\mathbb{Z}^n$ é 1. Logo, $d_{p,rel}(\mathbb{Z}^n)$ coincide com $d_{p,min}(\mathbb{Z}^n)$. Por sua vez, a norma mínima de D_n é $\sqrt{2}$, donde segue que $d_{p,rel}(D_n) = 2^{-n/2} d_{p,min}(D_n)$. Comparando as suas densidades de centro, obtemos:

$$\lim_{n\longrightarrow\infty} \frac{\sqrt[n]{\delta(\mathbb{Z}^n)}}{\sqrt[n]{\delta(D_n)}} = 0. \tag{2.56}$$

Em cada caso podemos comparar as distâncias produto relativas das construções $\mathbb{Z}^n$ e D_n feitas neste capítulo:

- Se $n > 1$ é um número ímpar, $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p]$ e pelo menos um dos elementos $1+u$ ou $1-u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, então segue do Corolário 2.1.1 e da Proposição 2.1.7 que as versões rotacionadas obtidas de $\mathbb{Z}^n$ e D_n satisfazem $\dfrac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2}$.

- Se $n > 1$ é uma potência de 2, então de (2.40) e (2.41) segue que as versões rotacionadas de $\mathbb{Z}^n$ e D_n descritas na Seção 2.2 satisfazem $\frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = 2^{\frac{1}{2}-\frac{1}{n}}$.
- Se $n = 2^{m-2}l$, com $m > 2$ e $l > 1$ ímpar, $u = \sigma(x)/x \in \mathbb{Z}[\zeta_p]$ e pelo menos um dos elementos $1+u$ ou $1-u$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$, então a Proposição 2.3.3 e o Corolário 2.3.2 implicam que as versões rotacionadas de $\mathbb{Z}^n$ e D_n obtidas nesse caso satisfazem $\frac{\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}}{\sqrt[n]{d_{p,rel}(D_n)}} = \sqrt{2}$.

Nas comparações feitas acima podemos notar que, à medida que n cresce, a razão entre as densidades de centro de $\mathbb{Z}^n$ e de D_n tende a zero, ao passo que a razão entre as distâncias produto relativas em todos os casos tende a $\sqrt{2}$. Isso significa que há uma vantagem em utilizar a versão rotacionada do reticulado D_n em comparação à versão rotacionada do reticulado $\mathbb{Z}^n$ (aqui construídas) em canais do tipo Rayleigh com desvanecimento e canais gaussianos, visto que a diferença entre as densidades de centro desses reticulados passa a ser significativa à medida que n cresce, enquanto a diferença entre suas distâncias produto relativas não.

Ao longo deste texto vimos que é possível calcular a distância produto mínima dos reticulados $\mathbb{Z}^n$ e D_n, n não potência de 2, quando algumas condições são válidas. Para $\mathbb{Z}^n$ precisamos verificar se $u = \sigma(x)/x$ é um inteiro algébrico, enquanto para D_n temos que ver se pelo menos um dos elementos $1+u$ ou $1-u$ é unidade em $\mathcal{O}_{\mathbb{K}}$. A Tabela 2 compara os resultados da raiz n-ésima da distância produto mínima relativa de $\mathbb{Z}^n$ com a de D_n para alguns valores de n que não são calculados em trabalhos anteriores. A mesma tabela também compara a densidade de centro desses reticulados em cada dimensão. Nela, as linhas referentes a $n = 7$ e $n = 28$ são as únicas que apresentam valores aproximados sobre a distância produto mínima relativa de D_n (e não apenas cotas inferiores), já que $1+u$ é unidade apenas nesses casos entre todos os presentes na tabela. Os casos $n = 19$ e $n = 31$ não estão presentes na tabela e também não aparecem em trabalhos anteriores. Isso ocorre porque não foi encontrado nenhum número primo $p < 400$, $p \equiv 1 \ (mod\ n)$, tal que $u = \sigma(x)/x$ é inteiro algébrico no anel de inteiros do corpo ciclotômico $\mathbb{Q}(\zeta_p)$. Portanto, permanece sendo um problema em aberto encontrar algum primo p nessas condições.

Em [JACS15] também são calculadas as raízes n-ésimas da distância produto relativa de $\mathbb{Z}^n$ e D_n para $n = 7$. Comparando o resultado desse artigo com os resultados deste capítulo, vemos que a distância produto relativa do reticulado $\mathbb{Z}^7$ construído no artigo mencionado ($\simeq 0.30...$) é melhor que a do aqui apresentado, mas a distância produto relativa de D_7 em [JACS15] é apenas limitada inferiormente por $\simeq 0.118$, enquanto aqui temos uma aproximação de 0.167 para esse valor.

Portanto, neste capítulo apresentamos a construção de versões rotacionadas dos reticulados $\mathbb{Z}^n$ e D_n com diversidade máxima, os quais podem ser usados tanto para canais do tipo Rayleigh com desvanecimento quanto para canais gaussianos. Observando

Tabela 2 – Comparação da distância produto relativa e da densidade de centro de $\mathbb{Z}^n$ e D_n em algumas dimensões

n	l	p	m	k	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)} \simeq$	$\sqrt[n]{d_{p,rel}(D_n)}$	$\delta(\mathbb{Z}^n) \simeq$	$\delta(D_n) \simeq$
7	-	29	-	-	0.2362	$\simeq 0.1670$	0.00781	0.04419
13	-	53	-	-	0.16	$\geqslant 0.1131$	0.000122	0.005524
17	-	103	-	-	0.1129	$\geqslant 0.0798$	0.000008	0.001381
25	-	101	-	-	0.1091	$\geqslant 0.0771$	3×10^{-8}	0.000086
27	-	109	-	-	0.1045	$\geqslant 0.0738$	7×10^{-9}	0.000043
28	7	29	4	4	0.0910	$\simeq 0.0643$	4×10^{-9}	0.000031
34	17	103	3	2	0.0671	$\geqslant 0.0474$	6×10^{-11}	0.000004
37	-	311	-	-	0.0622	$\geqslant 0.0439$	7×10^{-12}	0.000001
43	-	173	-	-	0.807	$\geqslant 0.057$	10^{-13}	10^{-7}
45	-	181	-	-	0.787	$\geqslant 0.0556$	3×10^{-14}	8×10^{-8}

a Tabela 2 nota-se que, na prática, em algumas situações, é mais vantajoso utilizar os reticulados D_n do que os reticulados $\mathbb{Z}^n$ quando se compara densidade de centro e distância produto mínima relativa.

CAPÍTULO 3

Forma traço associada a corpos de números cíclicos de grau primo ímpar

O cálculo da densidade de centro de um reticulado algébrico obtido através do mergulho de Minkowski sobre um corpo de números $\mathbb{K}$ depende da minimização da forma traço $Tr_{\mathbb{K}}(x\overline{x})$, com x pertencente ao $\mathbb{Z}$-módulo cuja imagem é esse reticulado (Proposição 1.6.3 do Capítulo 1). Em [OINL17, Oli15] é explicitada a expressão da forma traço $Tr_{\mathbb{K}}(x\overline{x})|_{\mathcal{O}_{\mathbb{K}}}$ quando $\mathbb{K}$ é um corpo de números cíclico de grau p, sendo p um número primo ímpar *não ramificado* sobre $\mathbb{K}$. Tal expressão depende apenas de invariantes do corpo de números $\mathbb{K}$ e dos coeficientes da combinação linear de x em relação à base normal do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Neste capítulo, contribuímos com a expressão da forma traço $Tr_{\mathbb{K}}(x\overline{x})|_{\mathcal{O}_{\mathbb{K}}}$ no caso em que $\mathbb{K}$ é um corpo de números cíclico de grau p primo ímpar *ramificado* sobre $\mathbb{K}$. Porém, nesta situação não existe base normal para o anel de inteiros de $\mathcal{O}_{\mathbb{K}}$ e, por isso, utilizamos uma base "quase normal" de $\mathcal{O}_{\mathbb{K}}$ obtida como consequência do Teorema de Leopoldt [Leo59, Let90, Cha15]. Na última seção, explicitamos a densidade de centro de alguns reticulados algébricos sobre corpos de números cíclicos de grau primo ímpar. As principais referências utilizadas neste capítulo consistem de [Was95, ILN06, NINL16, Flo96] e das já mencionadas acima. Alguns resultados deste capítulo foram apresentados inicialmente em [dA16] e [dA18] e submetidos para publicação conjunta em [dACAN18].

3.1 Corpos de números cíclicos de grau primo ímpar

Um corpo de números $\mathbb{K}$ é chamado *abeliano* se sua extensão sobre $\mathbb{Q}$ é abeliana, isto é, se a extensão $\mathbb{K}/\mathbb{Q}$ é galoisiana e o grupo de Galois $Gal(\mathbb{K}/\mathbb{Q})$ é abeliano. O Teorema de Kronecker-Weber [Was95] garante que um corpo de números é abeliano se, e somente se, está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$. Sendo assim, se $\mathbb{K}$ é um corpo de números abeliano, o menor número inteiro positivo n tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$ é chamado *condutor* de $\mathbb{K}$, denotado por $cond(\mathbb{K})$. Os subcorpos maximais reais $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ são

exemplos de corpos de números abelianos de condutor n. O resultado a seguir expressa a relação entre o discriminante de um corpo de números abeliano e seu condutor:

Proposição 3.1.1 ([ILN06]). *Se $\mathbb{K}$ é um corpo de números abeliano de condutor $n = \prod_{i=1}^{r} p_i^{e_i}$, em que os p_i's são primos distintos e $e_i \geqslant 1$, então*

$$|D(\mathbb{K})| = \frac{n^{[\mathbb{K}:\mathbb{Q}]}}{\prod_{i=1}^{r} p_i^{\beta_i}} \tag{3.1}$$

em que $\beta_i = \sum_{k=1}^{e_i} \left[\mathbb{K} \cap \mathbb{Q}(\zeta_{n/p_i^k}) : \mathbb{Q}\right]$.

A seguir apresentamos o Teorema de Leopoldt, que caracteriza o anel de inteiros de um corpo de números abeliano em função de seu condutor. Esse teorema foi provado pela primeira vez em 1959 por V.H. Leopoldt [Leo59] e aprimorado em 1990 por G. Lettl [Let90]. Em [dA15, Capítulo 6] esse resultado é demonstrado com um maior nível de detalhamento.

Teorema 3.1.1 (Teorema de Leopoldt). *Seja $\mathbb{K}$ um corpo de números abeliano de condutor n com grupo de Galois $G = Gal(\mathbb{K}/\mathbb{Q})$. Considere*

$$\mathcal{D}(n) = \{d \in \mathbb{Z}_{>0} : P_n \mid d,\ d \mid n \text{ e } d \not\equiv 2 \pmod 4\} \tag{3.2}$$

em que P_n denota o produto de todos os números primos ímpares distintos divisores de n. Para cada d no conjunto $\mathcal{D}(n)$, definamos $\mathbb{K}_d = \mathbb{K} \cap \mathbb{Q}(\zeta_d)$ e

$$\eta_d = Tr_{\mathbb{Q}(\zeta_d)/\mathbb{K}_d}(\zeta_d). \tag{3.3}$$

O anel de inteiros de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \bigoplus_{d \in \mathcal{D}(n)} \mathbb{Z}[G]\eta_d. \tag{3.4}$$

Se o anel de inteiros de um corpo de números $\mathbb{K}$ é da forma $\mathbb{Z}[G]\alpha$, em que $G = Gal(\mathbb{K}/\mathbb{Q})$ e $\alpha \in \mathcal{O}_{\mathbb{K}}$, dizemos que $\mathbb{K}$ possui uma base integral normal. Segue como consequência do Teorema de Leopoldt uma das implicações de um clássico resultado atribuído a D. Hilbert e A. Speiser que dá uma condição necessária e suficiente para que um corpo de números abeliano tenha base integral normal:

Teorema 3.1.2 (Teorema de Hilbert-Speiser). *Um corpo de números abeliano $\mathbb{K}$ tem base integral normal se, e somente se, o condutor de $\mathbb{K}$ é livre de quadrados. Neste caso, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[G]T$, em que $G = Gal(\mathbb{K}/\mathbb{Q})$ e $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$, com $n = cond(\mathbb{K})$.*

A recíproca do Teorema 3.1.2 segue como consequência do Teorema de Leopoldt. A outra parte da prova pode ser encontrada, por exemplo, em [dA15, Seção 4.2].

Um corpo de números $\mathbb{K}$ é dito *cíclico* quando sua extensão sobre os racionais é uma extensão cíclica, isto é, quando $\mathbb{K}$ é um corpo de números abeliano e o grupo de Galois $Gal(\mathbb{K}/\mathbb{Q})$ é cíclico. Todo corpo de números cíclico é abeliano, pois todo grupo cíclico é abeliano.

A seguir vamos explicitar algumas características de um corpo de números $\mathbb{K}$ cíclico de grau primo ímpar p. Primeiramente, como o corpo de números $\mathbb{K}$ é abeliano de grau ímpar, $\mathbb{K}$ é totalmente real. A Proposição 3.1.1 nos permite concluir que $|D(\mathbb{K})| = n^{p-1}$, em que n é o condutor de $\mathbb{K}$. A proposição seguinte nos diz que o condutor de $\mathbb{K}$ depende da ramificação de p em $\mathcal{O}_{\mathbb{K}}$:

Proposição 3.1.2 ([Oli15], Proposição 2.1.2)**.** *Seja $\mathbb{K}$ um corpo de números de grau primo ímpar e condutor n. Assim:*

(i) p se ramifica em $\mathbb{K}$ se, e somente se, $n = p^2p_1p_2\dots p_r$, com $r \geqslant 0$,

(ii) p não se ramifica em $\mathbb{K}$ se, e somente se, $n = p_1p_2\dots p_r$, com $r \geqslant 1$,

em que $p_i \equiv 1 \pmod p$ são primos distintos, $i \leqslant r$.[1]

De posse da Proposição 3.1.2 e dos teoremas de Leopoldt (Teorema 3.1.1) e de Hilbert-Speiser (Teorema 3.1.2) podemos obter bases integrais para corpos de números cíclicos de grau primo ímpar p dependendo da ramificação ou não de p.

Proposição 3.1.3. *Seja $\mathbb{K}$ um corpo de números cíclico de grau primo $p > 2$ com grupo de Galois $G = Gal(\mathbb{K}/\mathbb{Q}) = \langle\theta\rangle$ e condutor n. Se p é não ramificado em $\mathbb{K}$, então $\mathbb{K}$ admite base integral normal. Explicitamente, $\mathcal{O}_{\mathbb{K}}$ tem base $\{\theta(T), \theta^2(T), \dots, \theta^{p-1}(T), \theta^p(T) = T\}$, em que $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$.*

Demonstração. Pela Proposição 3.1.2, como p é não ramificado em $\mathbb{K}$, n é livre de quadrados. Logo, o resultado segue imediatamente do Teorema 3.1.2. □

Proposição 3.1.4 ([Cha15], Proposição 3.20)**.** *Seja $\mathbb{K}$ um corpo de números cíclico de grau primo $p > 2$ com grupo de Galois $G = Gal(\mathbb{K}/\mathbb{Q}) = \langle\theta\rangle$ e condutor n. Se p é ramificado em $\mathbb{K}$, então $\mathcal{O}_{\mathbb{K}}$ tem base $\{1, \theta(T), \dots, \theta^{p-1}(T)\}$, em que $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$.*[2]

Demonstração. Como p é ramificado, a Proposição 3.1.2 garante que $n = p^2p_1\dots p_r$, com $r \geqslant 0$. Consideremos as notações do Teorema 3.1.1. Notemos que $\mathcal{D}(n) = \{d_1 = pp_1\cdots p_r; d_2 = n\}$. Como o grau de $\mathbb{K}$ é primo, segue que $\mathbb{K}_{d_1} = \mathbb{K} \cap \mathbb{Q}(\zeta_{d_1})$ é $\mathbb{K}$ ou $\mathbb{Q}$. Se $\mathbb{K}_{d_1} = \mathbb{K}$, então teríamos uma contradição do fato de $\mathbb{K}$ ter condutor n. Logo, $\mathbb{K}_{d_1} = \mathbb{Q}$. Além disso, $\mathbb{K}_{d_2} = \mathbb{K}$. Assim, $\eta_{d_1} = Tr_{\mathbb{Q}(\zeta_{d_1})/\mathbb{Q}}(\zeta_{d_1}) = (-1)^{r+1}$ [Oli15, Proposição 1.3.1] e

[1] Esta proposição também é consequência do Teorema 1 de [SW03], o qual apresenta ainda uma relação entre o condutor e os coeficientes de um polinômio mônico irredutível $f(x)$ tal que $\mathbb{K} \simeq \mathbb{Q}[x]/\langle f(x)\rangle$.

[2] O Teorema 3.1.2 garante que não há base integral normal para $\mathbb{K}$ nas circunstância desta proposição.

$\eta_{d_2} = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n) = T$. O Teorema 3.1.1 garante que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[G]((-1)^{r+1}) \oplus \mathbb{Z}[G]T = \mathbb{Z} \oplus \mathbb{Z}[G]T$. Tomando $\mathcal{B} = \{1, \theta(T), \ldots, \theta^{p-1}(T)\}$, temos que $\mathcal{B} \cup \{\theta^p(T)\}$ gera $\mathcal{O}_\mathbb{K}$. Por n ser livre de quadrados e pela transitividade da norma, segue que $0 = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = Tr_{\mathbb{K}/\mathbb{Q}}(T) = \sum_{i=1}^{p-1} \theta^i(T) + \theta^p(T)$. Disso, segue que $\theta^p(T)$ pertence ao conjunto gerado por $\mathcal{B}$. Logo, $\mathcal{B}$ é um conjunto de geradores de $\mathcal{O}_\mathbb{K}$ contendo p elementos. Como $\mathcal{O}_\mathbb{K}$ é um $\mathbb{Z}$-módulo livre Noetheriano de posto p (e, portanto, é Hopfian), então $\mathcal{B}$ é $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$. □

3.2 Expressão da forma traço

Ao longo de toda esta seção, consideremos $\mathbb{K}$ um corpo de números cíclico de grau primo $p > 2$. A seguir explicitaremos a forma traço $Tr_\mathbb{K}(x\overline{x})|_{\mathcal{O}_\mathbb{K}}$. Notemos que, como $\mathbb{K}$ é totalmente real, segue que $x\overline{x} = x^2$, ou seja, neste contexto $Tr_\mathbb{K}(x\overline{x})|_{\mathcal{O}_\mathbb{K}} = Tr_\mathbb{K}(x^2)|_{\mathcal{O}_\mathbb{K}}$. Assim como fizemos para analisar o condutor e o anel de inteiros de $\mathbb{K}$ na Seção 3.1, precisamos considerar dois casos. No primeiro, assumimos que p é não ramificado e apenas apresentamos uma expressão já conhecida da forma traço [OINL17]. No segundo caso, consideramos p ramificado e, originalmente, calculamos a expressão da forma traço de modo detalhado.

3.2.1 Caso não ramificado

Suponha que p seja não ramificado em $\mathcal{O}_\mathbb{K}$. A Proposição 3.1.2 garante que o condutor de $\mathbb{K}$ é da forma $n = p_1 \ldots p_r$, com os p_i's primos distintos tais que $p_i \equiv 1 \ (mod\ p)$ e $r \geqslant 1$. Além disso, o anel de inteiros $\mathcal{O}_\mathbb{K}$ é gerado por $\{\theta(T), \theta^2(T), \ldots, \theta^p(T)\}$, em que $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$ e θ é o gerador do grupo de Galois $Gal(\mathbb{K}/\mathbb{Q})$ (Proposição 3.1.3).

No Teorema 1 de [OINL17] é provado que

$$Tr_{\mathbb{K}/\mathbb{Q}}(T\theta^k(T)) = \begin{cases} n - \dfrac{n-1}{p}, & se\ k = p \\ -\dfrac{n-1}{p}, & se\ 1 \leqslant k < p \end{cases} \tag{3.5}$$

e, consequentemente, no Corolário 1 do mesmo texto mostra-se que, para qualquer

$$x = \sum_{k=1}^{p} a_k \theta^k(T) \in \mathcal{O}_\mathbb{K}, \qquad a_k \in \mathbb{Z},\ 1 \leqslant k \leqslant p, \tag{3.6}$$

a expressão da forma traço associada a $\mathbb{K}$ é dada por

$$Tr_{\mathbb{K}/\mathbb{Q}}(x^2) = n\left(\sum_{k=1}^{p} a_k^2\right) - \frac{n-1}{p}\left(\sum_{k=1}^{p} a_k\right)^2. \tag{3.7}$$

3.2.2 Caso ramificado

Suponha que p é ramificado sobre $\mathbb{K}$. Isto significa que o condutor de $\mathbb{K}$ é $n = p^2 p_1 \dots p_r$, sendo os p_i's números primos tais que $p_i \equiv 1 \ (mod\ p)$ e $r \geqslant 0$ (Proposição 3.1.2). O estudo da forma traço $Tr_{\mathbb{K}/\mathbb{Q}}(x^2)$ no caso $r = 0$ foi tratado em [Fá12] e o caso $r \leqslant 1$ em [Cha15]. Abaixo generalizaremos esses resultados, descrevendo essa forma traço para qualquer $r \geqslant 0$.

Segue da Proposição 3.1.4 que o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ tem $\mathbb{Z}$-base $\{1, \theta(T), \dots, \theta^{p-1}(T)\}$, em que $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$ e θ é o gerador do grupo cíclico $Gal(\mathbb{K}/\mathbb{Q})$. Assim, todo elemento de $\mathcal{O}_{\mathbb{K}}$ pode ser escrito como

$$x = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(T), \qquad com\ a_i \in \mathbb{Z},\ 0 \leqslant i \leqslant p-1. \tag{3.8}$$

Daqui em diante nos dedicaremos a demonstrar o principal teorema deste capítulo:

Teorema 3.2.1. *Nas condições acima, para $x \in \mathcal{O}_{\mathbb{K}}$ explicitado em (3.8), temos:*

$$Tr_{\mathbb{K}}(x^2) = pa_0^2 + pp_1 \cdots p_r \left(-2 \sum_{1 \leqslant i < j \leqslant p-1} a_i a_j + (p-1) \sum_{i=1}^{p-1} a_i^2 \right). \tag{3.9}$$

Observação 3.2.1. *A expressão entre parênteses em (3.9) pode ser reescrita como a forma quadrática $Q_{p-1}(a_1, \cdots, a_{p-1}) = \sum_{i=1}^{p-1} a_i^2 + \sum_{1 \leqslant i < j \leqslant p-1} (a_i - a_j)^2$. Assim,*

$$Tr_{\mathbb{K}}(x^2) = p \left(a_0^2 + \frac{n}{p^2} Q_{p-1}(a_1, \cdots, a_{p-1}) \right). \tag{3.10}$$

Se $x = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(T) \in \mathcal{O}_{\mathbb{K}}$, $a_i \in \mathbb{Z}$, $0 \leqslant i \leqslant p-1$, então

$$\begin{aligned} Tr_{\mathbb{K}}(x^2) = pa_0^2 + 2a_0 \sum_{i=1}^{p-1} a_i Tr_{\mathbb{K}}\left(\theta^i(T)\right) \\ +2 \sum_{\substack{1 \leqslant i < \\ j \leqslant p-1}} a_i a_j Tr_{\mathbb{K}}\left(\theta^i(T)\theta^j(T)\right) + \sum_{i=1}^{p-1} a_i^2 Tr_{\mathbb{K}}\left(\theta^i(T)^2\right). \end{aligned} \tag{3.11}$$

Como $\theta^i(T)$ é conjugado de T na extensão $\mathbb{K}/\mathbb{Q}$, com $1 \leqslant i \leqslant p-1$, então $Tr_{\mathbb{K}}(\theta^i(T)) = Tr_{\mathbb{K}}(T) = Tr_{\mathbb{K}}\left(Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)\right) = Tr_{\mathbb{Q}(\zeta_n)}(\zeta_n) = 0$, já que n é livre de quadrados. Além disso, $Tr_{\mathbb{K}}\left(\theta^i(T)^2\right) = Tr_{\mathbb{K}}\left(T^2\right)$ e $Tr_{\mathbb{K}}\left(\theta^i(T)\theta^j(T)\right) = Tr_{\mathbb{K}}(T\theta^{j-i}(T))$. Daí segue que (3.11) pode ser reescrita como

$$Tr_{\mathbb{K}}(x^2) = pa_0^2 + 2 \sum_{1 \leqslant i < j \leqslant p-1} a_i a_j Tr_{\mathbb{K}}\left(T\theta^{j-i}(T)\right) + \sum_{i=1}^{p-1} a_i^2 Tr_{\mathbb{K}}\left(T^2\right). \tag{3.12}$$

Assim, para demonstrar o Teorema 3.2.1 basta calcular os valores $Tr_{\mathbb{K}}(T\theta^i(T))$ e $Tr_{\mathbb{K}}(T^2)$, com $1 \leqslant i \leqslant p-1$. Esses valores são obtidos calculando os traços de $T\theta^i(T)$ e T^2 na extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, pois $Tr_{\mathbb{K}}(y) = (p/\varphi(n))\, Tr_{\mathbb{Q}(\zeta_n)}(y)$ para todo $y \in \mathcal{O}_{\mathbb{K}}$.

Consideremos $\mathcal{H} = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$. Seja H o subgrupo de $\mathbb{Z}_n^*$ isomorfo a $Gal(\mathbb{Q}(\zeta_n)/\mathbb{K})$, contido em $\mathcal{H}$. Assim, $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n) = \sum_{\alpha \in H} \zeta_n^{\alpha}$. Consequentemente,

$$T^2 = \sum_{\alpha,\beta \in H} \zeta_n^{\alpha+\beta} \qquad e \qquad T\theta^i(T) = \sum_{\alpha,\beta \in H} \zeta_n^{\alpha+s^i\beta}, \tag{3.13}$$

onde $s \in \mathbb{Z}_n^*$ satisfaz $\theta(\zeta_n) = \zeta_n^s$. Como $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p^2}^* \times \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$, cada elemento $\alpha \in H$ pode ser escrito como $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_r)$, onde $\alpha_0 \in \mathbb{Z}_{p^2}^*$ e $\alpha_i \in \mathbb{Z}_{p_i}^*$, $1 \leqslant i \leqslant r$. Analogamente, $s = (s_0, s_1, \cdots, s_r)$. Assim, para $0 \leqslant i \leqslant p-1$,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T)) &= Tr_{\mathbb{Q}(\zeta_n)}\left(\sum_{\alpha,\beta \in H} \zeta_n^{\alpha+s^i\beta}\right) \\ = \sum_{\alpha,\beta \in H} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) & Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right) \cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right). \end{aligned} \tag{3.14}$$

A seguir apresentamos uma sequência de lemas dedicados a encontrar os valores de $Tr_{\mathbb{Q}(\zeta_n)}(T^2)$ e $Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T))$, para $1 \leqslant i \leqslant p-1$. De agora em diante, denotemos $q_j = p_j - 1$, para $1 \leqslant j \leqslant r$.

Lema 3.2.1. *Se $e \in \mathbb{Z}$ e $1 \leqslant i \leqslant r$, então*

$$Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^e\right) = \begin{cases} 0, & se\ mdc(e,p^2) = 1 \\ -p, & se\ mdc(e,p^2) = p \\ p(p-1), & se\ mdc(e,p^2) = p^2 \end{cases} \tag{3.15}$$

e

$$Tr_{\mathbb{Q}(\zeta_{p_i})}\left(\zeta_{p_i}^e\right) = \begin{cases} -1, & se\ mdc(e,p_i) = 1 \\ q_i, & se\ mdc(e,p_i) = p_i \end{cases}. \tag{3.16}$$

Demonstração. Como $\zeta_{p^2}^e$ é uma raiz p^2-ésima primitiva da unidade, se $mdc(e,p^2) = 1$, então $Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^e\right) = 0$. Se $mdc(e,p^2) = p^2$, então e é um múltiplo de p^2 e o traço desejado é igual ao grau da extensão $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$, isto é, $\varphi(p^2) = p(p-1)$. Se $mdc(e,p^2) = p$, então $e = pl$, onde l não é divisível por p. Neste caso, $Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^e\right) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(Tr_{\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}(\zeta_p)}\left(\zeta_p^l\right)\right) = Tr_{\mathbb{Q}(\zeta_p)}\left(p\zeta_p^l\right) = p(-1) = -p$. Pela mesma razão, $Tr_{\mathbb{Q}(\zeta_{p_i})}\left(\zeta_{p_i}^e\right) = -1$ se $mdc(e,p_i) = 1$. Finalmente, se $mdc(e,p_i) = p_i$, então e é um múltiplo de p_i e $Tr_{\mathbb{Q}(\zeta_{p_i})}\left(\zeta_{p_i}^e\right)$ é igual ao grau da extensão $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$, que é $\varphi(p_i) = q_i$. □

Lema 3.2.2. *Seja $A = \{i_j\}_{j=1}^k$ um subconjunto de $[r] = \{1, 2, \ldots, r\}$ e $\Pi_A : H \longrightarrow \mathbb{Z}_{p^2}^* \times \prod_{i \in A} \mathbb{Z}_{p_i}^*$ a projeção definida por $\Pi_A(\alpha_0, \alpha_1, \cdots, \alpha_r) = (\alpha_0, \alpha_{i_1}, \cdots, \alpha_{i_k})$. Para todo $y \in \mathbb{Z}_{p^2}^* \times \prod_{i \in A} \mathbb{Z}_{p_i}^*$, a cardinalidade do conjunto $\Pi_A^{-1}(y)$ é igual a $p^{-1} \prod_{i \in [r]\setminus A} q_i$.*

Demonstração. Primeiramente, notemos que Π_A é sobrejetora. De fato, seja $N = \Pi_A(H) \times \prod_{i\in[r]\setminus A} \mathbb{Z}_{p_i}^*$ um subgrupo de $\mathbb{Z}_n^*$. Notemos que $H \lhd N \lhd \mathbb{Z}_n^*$. Como o índice $[\mathbb{Z}_n^* : H]$ é um número primo ímpar, segue que $N = H$ ou $N = \mathbb{Z}_n^*$. Se $N = H$, então $\prod_{i\in[r]\setminus A} \mathbb{Z}_{p_i}^* \subset H$ e $\mathbb{K} \subset \mathbb{Q}\left(\zeta_{\prod_{i\in[r]\setminus A} p_i}\right)$, o que contradiz a minimalidade de n. Assim, $N = \mathbb{Z}_n^*$ e Π_A é sobrejetora. Isso significa que o núcleo de Π_A tem $|H|/(p(p-1)q_{i_1}\cdots q_{i_k}) = p^{-1}\prod_{i\in[r]\setminus A} q_i$ elementos, já que $|H| = (p-1)q_1\cdots q_r$. A prova fica completa observando que $|\Pi_A^{-1}(1)| = |\Pi_A^{-1}(y)|$ para todo $y \in \mathbb{Z}_{p^2}^* \times \prod_{i\in A} \mathbb{Z}_{p_i}^*$. □

Lema 3.2.3. *Seja $A = \{i_j\}_{j=1}^k$ um subconjunto de $[r]$ e $\pi_A : H \longrightarrow \mathbb{Z}_p^* \times \prod_{i\in A} \mathbb{Z}_{p_i}^*$ a aplicação $\pi_A(\alpha_0, \alpha_1, \cdots, \alpha_r) = (\mu(\alpha_0), \alpha_{i_1}, \cdots, \alpha_{i_k})$, onde $\mu : \mathbb{Z}_{p^2}^* \longrightarrow \mathbb{Z}_p^*$ é dada por $x \longmapsto x \ (mod\ p)$. Para todo $y \in \mathbb{Z}_p^* \times \prod_{i\in A} \mathbb{Z}_{p_i}^*$, a cardinalidade do conjunto $\pi_A^{-1}(y)$ é $\prod_{i\in[r]\setminus A} q_i$.*

Demonstração. Notemos que $\phi = \pi_{[r]}$ é sobrejetora . Consideremos ρ_A a projeção de $\mathbb{Z}_p^* \times \prod_{i\in[r]} \mathbb{Z}_{p_i}^*$ em $\mathbb{Z}_p^* \times \prod_{i\in A} \mathbb{Z}_{p_i}^*$. Assim, $\pi_A = \rho_A \circ \phi$ é sobrejetora, já que ρ_A e ϕ são sobrejetoras. Disso segue o resultado. □

Lema 3.2.4. *Se m é um número inteiro positivo, então $\sum_{0\leqslant i\leqslant m} (-1)^i \binom{m}{i} = 0$.*

Demonstração. Segue diretamente da identidade binomial $(1-1)^m = 0$. □

Lema 3.2.5. *Se $L = 1 + \sum_{1\leqslant i\leqslant r} q_i^{-1} + \sum_{1\leqslant i<j\leqslant r} q_i^{-1}q_j^{-1} + \cdots + q_1^{-1}\cdots q_r^{-1}$, então $L = \dfrac{n(p-1)}{\varphi(n)p}$.*

Demonstração. Notemos que $q_1\cdots q_r L = q_1\cdots q_r + \sum_{1\leqslant i\leqslant r} q_1\cdots q_r/q_i + \sum_{1\leqslant i<j\leqslant r} q_1\cdots q_r/(q_iq_j) + \cdots + 1$. A última expressão é igual ao produto de polinômios $(1+q_1)\cdots(1+q_r)$. Assim, $q_1\cdots q_r L = p_1\cdots p_r$, o que implica $\varphi(n)L/(p(p-1)) = n/p^2$. □

Lema 3.2.6. $Tr_{\mathbb{Q}(\zeta_n)}(T^2) = |H|n(p-1)/p$.

Demonstração. Fixe $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_r) \in H$. Para cada $A \subset [r]$, denotemos por H_A o conjunto dos elementos $\beta = (\beta_0, \beta_1, \cdots, \beta_r) \in H$ tais que $\beta_0 \equiv -\alpha_0 \ (mod\ p^2)$ e $\beta_i \not\equiv -\alpha_i \ (mod\ p_i)$ para $i \in A$. Definamos H'_A como sendo o conjunto dos elementos $\beta = (\beta_0, \beta_1, \cdots, \beta_r) \in H$ tais que $\beta_0 \not\equiv -\alpha_0 \ (mod\ p^2)$, $\beta_0 \equiv -\alpha_0 \ (mod\ p)$ e $\beta_i \not\equiv -\alpha_i \ (mod\ p_i)$ para $i \in A$. Seja $\tilde{H}$ o conjunto dos elementos $\beta = (\beta_0, \beta_1, \cdots, \beta_r) \in H$ tais que $\beta_0 \not\equiv -\alpha_0 \ (mod\ p^2)$ e $\beta_0 \not\equiv -\alpha_0 \ (mod\ p)$. Assim,

$$H = \tilde{H} \cup \dot{\bigcup}_{A\subset[r]} H_A \cup \dot{\bigcup}_{A\subset[r]} H'_A. \tag{3.17}$$

Como $Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+\beta_0}\right)=0$ para $\beta\in\tilde{H}$ (Lema 3.2.1), de (3.14) segue que

$$\begin{aligned}Tr_{\mathbb{Q}(\zeta_n)}(T^2)=\sum_{\alpha\in H}\sum_{A\subset[r]}\sum_{\beta\in H_A}\sum_{\beta\in H'_A}Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+\beta_0}\right)Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+\beta_1}\right)\cdots\\ \cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+\beta_r}\right).\end{aligned}\tag{3.18}$$

Consideremos $N_A=|H_A|$. Se $A=\varnothing$, então $N_A=1$, pois existe um único $\beta=-\alpha\in H_A$, já que a conjugação complexa pertence a H (de fato, $\mathbb{K}$ é totalmente real). Se $A=\{i\}$, para algum $i\in[r]$, o Lema 3.2.2 garante que $N_A=|\Pi^{-1}_{[r]\setminus A}(y)|-N_\varnothing=q_i/p-1$, onde $y=(-\alpha_0,\cdots,-\alpha_{i-1},-\alpha_{i+1},\cdots,-\alpha_r)$. Se $A\subset[r]$ tem somente dois elementos $i<j$, $N_A=|\Pi^{-1}_{[r]\setminus A}(y)|-\sum\limits_{\substack{B\subset A\\|B|=1}}N_B+N_\varnothing=q_iq_j/p-q_i/p-q_j/p+1$, em que $y=(-\alpha_0,\cdots,-\alpha_{i-1},-\alpha_{i+1},\cdots,-\alpha_{j-1},-\alpha_{j+1},\cdots,-\alpha_r)$. Por indução, para cada $A=\{i_1<\cdots<i_k\}\subset[r]$, segue que

$$N_A=(-1)^k+\sum_{t=1}^{k}\sum_{\substack{B\subset A\\|B|=t}}\frac{(-1)^{k-t}}{p}\prod_{i\in B}q_i.\tag{3.19}$$

Do Lema 3.2.1, segue que

$$\begin{aligned}S_1&=\sum_{A\subset[r]}\sum_{\beta\in H_A}Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+\beta_0}\right)Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+\beta_1}\right)\cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+\beta_r}\right)\\&=\sum_{A\subset[r]}N_Ap(p-1)(-1)^{|A|}\prod_{i\notin A}q_i\\&=\sum_{A\subset[r]}\frac{\varphi(n)(-1)^{|A|}}{\prod_{i\in A}q_i}\left((-1)^{|A|}+\sum_{t=1}^{|A|}\sum_{\substack{B\subset A\\|B|=t}}\frac{(-1)^{|A|-t}}{p}\prod_{i\in B}q_i\right)\\&=\varphi(n)\sum_{A\subset[r]}\left(\frac{1}{\prod_{i\in A}q_i}+\sum_{t=1}^{|A|}\sum_{\substack{B\subset A\\|B|=t}}\frac{(-1)^t}{p}\prod_{i\in A\setminus B}\frac{1}{q_i}\right)=\varphi(n)\left(L+\frac{1}{p}S'_1\right),\end{aligned}\tag{3.20}$$

onde $L=\dfrac{n(p-1)}{\varphi(n)p}$ é definido no Lema 3.2.5 e

$$S'_1=\sum_{A\subset[r]}\sum_{t=1}^{|A|}\sum_{\substack{B\subset A\\|B|=t}}(-1)^t\prod_{i\in A\setminus B}\frac{1}{q_i}.\tag{3.21}$$

O termo S'_1 pode ser reescrito, por argumentos de contagem[3] e pelo Lema 3.2.4, como

$$\begin{aligned}S'_1&=\sum_{t=0}^{r-1}\sum_{C\subset[r]}\sum_{j=1}^{r-t}(-1)^j\binom{r-t}{r-t-j}\prod_{i\in C}\frac{1}{q_i}\\&=-\sum_{t=0}^{r-1}\sum_{C\subset[r]}\prod_{i\in C}\frac{1}{q_i}=-\left(L-\frac{1}{q_1\cdots q_r}\right)=\frac{(p-1)(p^2-n)}{\varphi(n)p}.\end{aligned}\tag{3.22}$$

[3] Basta contar o número de subconjuntos de $[r]$ que contém propriamente um subconjunto C fixo com t elementos.

Daí,

$$S_1 = \frac{(p-1)\left(n(p-1)+p^2\right)}{p^2}. \tag{3.23}$$

Agora, consideremos $N'_A = |H'_A|$. Para $A = \varnothing$ no Lema 3.2.3, a aplicação $\phi = \pi_{[r]\setminus A}$ é um isomorfismo entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$. Se há $\beta \in H$ tal que $\beta_0 \equiv -\alpha_0 \ (mod\ p)$ e $\beta_i \equiv -\alpha_i \ (mod\ p_i)$, $1 \leqslant i \leqslant r$, então $\phi(\beta) = \phi(-\alpha)$ e, portanto, $\beta = -\alpha$. Disso segue que $\beta_0 \equiv -\alpha_0 \ (mod\ p^2)$. Assim, $N'_\varnothing = 0$. Se $A = \{i\}$, para algum $i \in [r]$, o Lema 3.2.3 garante que $|\pi_A^{-1}(y)| = q_i$, onde $y = (-\alpha_0, \cdots, -\alpha_{i-1}, -\alpha_{i+1}, \cdots, -\alpha_r)$. Logo, $N'_A = |\pi_A^{-1}(y)| - |\Pi_A^{-1}(y)| = (p-1)q_i/p$. Para $A = \{i < j\} \subset [r]$ segue que $N'_A = |\pi_A^{-1}(y)| - |\Pi_A^{-1}(y)| - N'_{\{i\}} - N'_{\{j\}} = (p-1)(q_iq_j - q_i - q_j)/p$, onde $y = (-\alpha_0, \cdots, -\alpha_{i-1}, -\alpha_{i+1}, \cdots, -\alpha_{j-1}, -\alpha_{j+1}, \cdots, -\alpha_r)$. Por indução, para cada $A = \{i_1 < \cdots < i_k\} \subset [r]$ prova-se que

$$N'_A = \frac{p-1}{p} \sum_{t=1}^{k} \sum_{\substack{B\subset A \\ |B|=t}} (-1)^{k-t} \prod_{i\in B} q_i. \tag{3.24}$$

Do Lema 3.2.1, segue que

$$\begin{aligned} S_2 &= \sum_{A\subset[r]} \sum_{\beta\in H'_A} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+\beta_1}\right) \cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+\beta_r}\right) \\ &= \sum_{A\subset[r]} N'_A(-p)(-1)^{|A|} \prod_{i\notin A} q_i \\ &= -\sum_{A\subset[r]} p(-1)^{|A|} \left(\frac{p-1}{p} \sum_{t=1}^{|A|} \sum_{\substack{B\subset A \\ |B|=t}} (-1)^{|A|-t} \prod_{i\in B} q_i \right) \prod_{i\notin A} q_i \\ &= -\sum_{A\subset[r]} \sum_{t=1}^{|A|} \sum_{\substack{B\subset A \\ |B|=t}} (-1)^t \frac{\varphi(n)}{p} \prod_{i\in A\setminus B} \frac{1}{q_i} = -\frac{\varphi(n)}{p} S'_1 = -\frac{(p-1)(p^2-n)}{p^2}. \end{aligned} \tag{3.25}$$

Por fim, como S_1 e S_2 não dependem de $\alpha \in H$, (3.18) acarreta

$$Tr_{\mathbb{Q}(\zeta_n)}(T^2) = \sum_{\alpha\in H} (S_1 + S_2) = |H| \frac{(p-1)n}{p}, \tag{3.26}$$

o que prova o lema. □

Lema 3.2.7. *Se $i \in \{1, \cdots, p-1\}$, então $Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T)) = -|H|n/p$.*

Demonstração. Fixemos um índice i. Seja $s \in \mathbb{Z}_n^* \simeq \mathbb{Z}_{p^2}^* \times \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ satisfazendo $\theta(\zeta_n) = \zeta_n^s$, com $s = (s_0, s_1, \cdots, s_r)$. Consideremos $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_r) \in H$. Para cada $A \subset [r]$, consideremos H_A o conjunto dos elementos $\beta = (\beta_0, \beta_1, \cdots, \beta_r) \in H$ tais que $\alpha_0 \equiv -s^i\beta_0 \ (mod\ p^2)$ e $\alpha_k \not\equiv -s^i\beta_k \ (mod\ p_k)$ para $k \in A$. Analogamente, definamos H'_A o conjunto dos elementos $\beta = (\beta_0, \beta_1, \cdots, \beta_r) \in H$ satisfazendo $\alpha_0 \not\equiv -s^i\beta_0 \ (mod\ p^2)$,

$\alpha_0 \equiv -s^i\beta_0 \ (mod\ p)$ e $\alpha_k \not\equiv -s^i\beta_k \ (mod\ p_k)$ para $k \in A$. Como $Tr_{\mathbb{Q}(\zeta_{p^2})}(\zeta_{p^2}^{\alpha_0+s^i\beta_0}) = 0$ se $\alpha_0 \not\equiv -s^i\beta_0 \ (mod\ p^2)$ e $\alpha_0 \not\equiv -s^i\beta_0 \ (mod\ p)$, a Equação 3.14 acarreta

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T)) = \sum_{\alpha\in H}\sum_{A\subset[r]}\sum_{\beta\in H_A}\sum_{\beta\in H'_A} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right)\cdots \\ \cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right). \end{aligned} \tag{3.27}$$

Definamos $N_A = |H_A|$ e $N'_A = |H'_A|$. Se existe $\beta \in H_\varnothing$, então $\alpha \in (-s^iH) \cap H$, o que não é possível já que $\mathbb{Z}_n^* \simeq \dot{\bigcup}_{0\leqslant j\leqslant p-1} s^jH$. Logo, $N_\varnothing = 0$. Por sua vez, existe um único $\beta \in H'_\varnothing$. De fato, considerando a notação do Lema 3.2.3 e denotando por $\phi = \pi_{[r]}$ o isomorfismo entre H e $\mathbb{Z}_p^* \times \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$, existe um único $\beta \in H$ tal que

$$\phi(\beta) = \left(-\alpha_0 s^{-i} \ (mod\ p), -\alpha_1 s^{-i} \ (mod\ p_1), \cdots, -\alpha_r s^{-i} \ (mod\ p_r)\right) \neq -\alpha s^{-i}. \tag{3.28}$$

Assim, $N'_\varnothing = 1$. Procedendo analogamente à demonstração do Lema 3.2.6 podemos mostrar que, para cada $A = \{i_1 < \cdots < i_k\} \subset [r]$,

$$N_A = \frac{1}{p}\sum_{\varnothing\neq B\subset A}(-1)^{k-|B|}\prod_{j\in B} q_j \tag{3.29}$$

e

$$N'_A = (-1)^k + \frac{p-1}{p}\sum_{\varnothing\neq B\subset A}(-1)^{k-|B|}\prod_{j\in B} q_j. \tag{3.30}$$

Utilizando o Lema 3.2.1 e aplicando uma técnica similar à que foi utilizada para demonstrar o Lema 3.2.6, mostra-se que

$$\begin{aligned} S_1 &= \sum_{A\subset[r]}\sum_{\beta\in H_A} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right)\cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right) \\ &= \sum_{\varnothing\neq A\subset[r]} N_A(-1)^{|A|}p(p-1)\prod_{j\in[r]\setminus A} q_j = (p-1)\left(1-\frac{n}{p^2}\right) \end{aligned} \tag{3.31}$$

e

$$\begin{aligned} S_2 &= \sum_{A\subset[r]}\sum_{\beta\in H'_A} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right)\cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right) \\ &= \sum_{\varnothing\neq A\subset[r]} N'_A(-1)^{|A|}(-p)\prod_{j\in[r]\setminus A} q_j = \frac{\varphi(n)}{p-1} - \frac{n}{p^2} + 1 - p. \end{aligned} \tag{3.32}$$

Além disso,

$$S_3 = \sum_{\beta\in H_\varnothing} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right)\cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right) = 0 \tag{3.33}$$

e

$$\begin{aligned} S_4 = \sum_{\beta\in H'_\varnothing} Tr_{\mathbb{Q}(\zeta_{p^2})}\left(\zeta_{p^2}^{\alpha_0+s_0^i\beta_0}\right) Tr_{\mathbb{Q}(\zeta_{p_1})}\left(\zeta_{p_1}^{\alpha_1+s_1^i\beta_1}\right)\cdots Tr_{\mathbb{Q}(\zeta_{p_r})}\left(\zeta_{p_r}^{\alpha_r+s_r^i\beta_r}\right) \\ = (-p)q_1\cdots q_r = -\frac{\varphi(n)}{p-1}. \end{aligned} \tag{3.34}$$

Portanto, pela Equação 3.27, segue que

$$Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T)) = |H|\,(S_1 + S_2 + S_3 + S_4) = |H|\left(\frac{-n}{p}\right), \tag{3.35}$$

o que prova o lema. □

Finalmente estamos em condições de demonstrar o Teorema 3.2.1:

Demonstração do Teorema 3.2.1. Como $|H| = \varphi(n)/p$, segue do Lema 3.2.6 que

$$Tr_{\mathbb{K}}(T^2) = \frac{p}{\varphi(n)} Tr_{\mathbb{Q}(\zeta_n)}(T^2) = |H|^{-1}|H|\frac{n(p-1)}{p} = \frac{n(p-1)}{p} \tag{3.36}$$

e, para $1 \leqslant i \leqslant p-1$, o Lema 3.2.7 garante que

$$Tr_{\mathbb{K}}(T\theta^i(T)) = \frac{p}{\varphi(n)} Tr_{\mathbb{Q}(\zeta_n)}(T\theta^i(T)) = -|H|^{-1}|H|\frac{n}{p} = -\frac{n}{p}. \tag{3.37}$$

A demonstração fica completa substituindo esses valores na Equação 3.12. □

3.3 Reticulados algébricos via corpos de números de grau primo ímpar

Sejam M um $\mathbb{Z}$-módulo contido no anel de inteiros de um corpo de números cíclico $\mathbb{K}$ de grau primo $p > 2$ e condutor n e σ o mergulho de Minkowski associado a $\mathbb{K}$. Sabemos, pela Proposição 1.6.3 do Capítulo 1, que $\sigma(M)$ é um reticulado de posto completo em $\mathbb{R}^p$ com densidade de centro

$$\delta(\sigma(M)) = \frac{t_M^{p/2}}{2^p[\mathcal{O}_{\mathbb{K}} : M]\sqrt{|D(\mathbb{K})|}} = \frac{t_M^{p/2}}{2^p[\mathcal{O}_{\mathbb{K}} : M]n^{p-1}}, \tag{3.38}$$

em que

$$t_M = \min_{0 \neq x \in M} Tr_{\mathbb{K}}(x^2). \tag{3.39}$$

Se $M = \mathcal{O}_{\mathbb{K}}$, então $[\mathcal{O}_{\mathbb{K}} : M] = 1$ e $t_M = [\mathbb{K} : \mathbb{Q}] = p$, pois $1 \in \mathcal{O}_{\mathbb{K}}$. Logo,

$$\delta(\sigma(\mathcal{O}_{\mathbb{K}})) = \frac{p^{p/2}}{2^p n^{\frac{p-1}{2}}}. \tag{3.40}$$

Pela Proposição 3.1.2, o condutor de $\mathbb{K}$ deve ser $n = p_1 \dots p_r$, com $r \geqslant 1$, (quando p é não ramificado) ou $n = p^2 p_1 \dots p_r$, com $r \geqslant 0$, (quando p é ramificado), com $p_i \equiv 1 \ (mod\ p)$, $1 \leqslant i \leqslant r$. Um número primo se ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, divide o discriminante de $\mathbb{K}$ [Sam70, Teorema 1]. Como neste caso $|D(\mathbb{K})| = n^{p-1}$, os números primos que aparecem na fatoração de n se ramificam em $\mathcal{O}_{\mathbb{K}}$ (e são os únicos nessa condição). Além disso, como $\mathbb{K}$ é uma extensão galoisiana, segue da Igualdade Fundamental (Capítulo 1) que existe um único ideal primo $\mathfrak{P}_i \lhd \mathcal{O}_{\mathbb{K}}$ acima de cada p_i, $1 \leqslant i \leqslant r$. A seguir vamos analisar, no caso ramificado e no caso não ramificado, as densidades de centro dos reticulados algébricos obtidos via o mergulho de Minkowski aplicado a $\mathfrak{P}_i$ e a $\mathbb{Z}$-módulos generalizados desses ideais.

3.3.1 Caso não ramificado

Se p é não ramificado, segundo [Cha15, Proposição 3.9], o ideal $\mathfrak{P}_i$ acima de cada p_i na fatoração de n $(1 \leqslant i \leqslant r)$ pode ser descrito como

$$\mathfrak{P}_i = \left\{ \sum_{k=1}^{p} a_k \theta^k(T) \ : \ \sum_{k=1}^{p} a_k \equiv 0 \ (mod\ p_i) \right\}, \tag{3.41}$$

sendo θ e T como na Proposição 3.1.3. De forma mais geral, em [OINL17, Oli15] foi definido, para cada número inteiro $m > 0$, o $\mathbb{Z}$-módulo

$$M_m = \left\{ \sum_{k=1}^{p} a_k \theta^k(T) \ : \ \sum_{k=1}^{p} a_k \equiv 0 \ (mod\ m) \right\}. \tag{3.42}$$

Observemos que os ideais primos $\mathfrak{P}_i$ pertencem à família dos $\mathbb{Z}$-módulos M_m (basta tomar $m = p_i$). A proposição abaixo dá algumas propriedades de M_m:

Proposição 3.3.1 ([NINL16])**.** *Sejam $\mathbb{K}$ um corpo de números de grau primo ímpar p não ramificado com grupo de Galois $Gal(\mathbb{K}/\mathbb{Q}) = \langle\theta\rangle$ e M_m o $\mathbb{Z}$-módulo definido em (3.42), para $m > 0$. Assim, são válidas as seguintes afirmações:*

a) M_m tem posto p.

b) $[\mathcal{O}_{\mathbb{K}} : M_m] = m$.

c) Consideremos a aplicação $F(x) = (x^2 + nr(p-r))/p$, sendo $x = pl + r$ qualquer número inteiro, com $l, r \in \mathbb{Z}$ e $0 \leqslant r < p$. Assim,

$$\lambda = \min_{0 \neq x \in M_m} ||\sigma(x)||^2 = \min\{2n, F(m), F(2m), \ldots, F(pm)\}. \tag{3.43}$$

Se $\lambda = 2n$, então λ é obtido pelos elementos $x = \theta^i(T - \theta(T))$, com $0 \leqslant i \leqslant p-1$. Se λ é igual a $F(jm)$, para algum $1 \leqslant j \leqslant p$, então λ é atingido pelos elementos $x = \sum_{i=0}^{p-1} a_i \theta^i(T)$ onde exatamente r_j coeficientes a_i são iguais a $l_j + 1$ e os outros $p - r_i$ coeficientes a_i são iguais a l_j, sendo $jm = l_j p + r_j$, com $l_j, r_j \in \mathbb{Z}$ e $0 \leqslant r_j < p$.

Demonstração. Os itens (b) e (c) são provados no Lema 4 e no Teorema 3 de [NINL16]. Para ver que o item (a) é válido, basta provar que o conjunto

$$B = \left\{T - \theta(T), T - \theta^2(T), \ldots, T - \theta^{p-1}(T), mT\right\} \tag{3.44}$$

é uma $\mathbb{Z}$-base de M_m. De fato, $\langle B\rangle_{\mathbb{Z}} \subset M_m$, pois a soma dos coeficientes de $T - \theta^i(T)$, $1 \leqslant i \leqslant p-1$, é $1 - 1 \equiv 0 \ (mod\ m)$ e a soma dos coeficientes de mT é $m \equiv 0 \ (mod\ m)$. Por outro lado, $M_m \subset \langle B\rangle_{\mathbb{Z}}$, já que

$$\begin{gathered} x \in M_m \Longrightarrow x = \sum_{k=1}^{p} a_k \theta^k(T), \ com \ \sum_{k=1}^{p} a_k = mt, \ t \in \mathbb{Z} \\ \Longrightarrow x = \left(\sum_{k=1}^{p} a_k\right) T - \sum_{k=1}^{p} a_k \left(T - \theta^k(T)\right) = tmT - \sum_{k=1}^{p-1} a_k \left(T - \theta^k(T)\right) \in \langle B\rangle_{\mathbb{Z}}. \end{gathered} \tag{3.45}$$

Portanto, $M_m = \langle B \rangle_{\mathbb{Z}}$. Por fim, B é um conjunto linearmente independente, já que

$$\sum_{k=1}^{p-1} a_k \left(T - \theta^k(T)\right) + a_p m T = 0 \Longrightarrow T\left(a_p m + \sum_{k=1}^{p-1} a_k\right) - \sum_{k=1}^{p-1} a_k \theta^k(T) = 0 \tag{3.46}$$

e, como $\{\theta(T), \ldots, \theta^p(T) = T\}$ é linearmente independente, então $a_k = 0$, para $k = 1, \ldots, p-1$, e $a_p m = 0$, donde segue que $a_p = 0$ (pois $m \neq 0$). Portanto, B é uma $\mathbb{Z}$-base de M_m. □

Corolário 3.3.1. *Sob as hipóteses e notações da Proposição 3.3.1, a densidade de centro do reticulado $\sigma(M_m) \subset \mathbb{R}^p$ é*

$$\delta(\sigma(M_m)) = \frac{\lambda_m^{p/2}}{2^p m n^{\frac{p-1}{2}}}. \tag{3.47}$$

Demonstração. Decorre de forma direta da Equação 3.38 e da Proposição 3.3.1. □

Exemplo 3.3.1. *Consideremos $\mathbb{K}$ um corpo de números de grau 3 e condutor $n = 1729 = 7 \times 13 \times 19$. Observemos que $p_1 = 7 \equiv 1 \ (mod\ 3)$, $p_2 = 13 \equiv 1 \ (mod\ 3)$ e $p_3 = 19 \equiv 1 \ (mod\ 3)$. Assim, $\delta(\sigma(\mathcal{O}_{\mathbb{K}})) \simeq 0,000376$ (Equação 3.40). Pondo $m = p_1$, $m = p_2$ e $m = p_3$ no Corolário 3.3.1, obtém-se $\lambda_{p_1} = F(3p_1) = 147$, $\lambda_{p_2} = F(3p_2) = 507$ e $\lambda_{p_3} = F(3p_3) = 1083$, donde segue que $\delta(\sigma(\mathfrak{P}_1)) \simeq 0,0184$, $\delta(\sigma(\mathfrak{P}_2)) \simeq 0,06349$ e $\delta(\sigma(\mathfrak{P}_3)) \simeq 0,135613$. Notemos que $\delta(\sigma(\mathfrak{P}_3))$ corresponde a aproximadamente 76% da maior densidade de centro possível em terceira dimensão, que é $\simeq 0,17678$.*

Em [NINL16, Seção 4.4] são analisadas as densidades de centro obtidas via alguns $\mathbb{Z}$-módulos M_m nos casos $p = 3, 5, 7$. Para $m \equiv 0 \ (mod\ p)$ notou-se que é possível atingir no máximo 81% da maior densidade de centro em dimensão 3, 63% da maior densidade de centro em dimensão 5 e 38% da maior densidade de centro em dimensão 7. Por sua vez, utilizando $m = 379 \equiv 1 (mod\ 3)$ no caso $p = 3$ com $n = 35911$, atingiu-se uma densidade de centro correspondente a 99,999% da maior possível em dimensão 3. Resultado análogo foi obtido no caso $p = 5$ com $n = 92111$ e $m = 607$ e no caso $p = 7$ com $n = 511057$ e $m = 1011$. Isso mostra que a família de $\mathbb{Z}$-módulos M_m pode ser utilizada para obter reticulados algébricos com boa densidade de centro pelo menos nessas três dimensões primas ímpares.

3.3.2 Caso ramificado

Se p é ramificado e $r \geqslant 1$, segue de [Cha15, Seção 3.4.3] que o ideal $\mathfrak{P}_i$ acima de cada p_i na fatoração de $n = p^2 p_1 \ldots p_r$ $(1 \leqslant i \leqslant r)$ pode ser descrito como

$$\mathfrak{P}_i = \left\{ a_0 + \sum_{k=1}^{p-1} a_k \theta^k(T) \ : \ a_0 \equiv 0 \ (mod\ p_i) \right\}. \tag{3.48}$$

sendo θ e T assim como na Proposição 3.1.4. A próxima proposição expressa a densidade de centro do reticulado algébrico $\sigma(\mathfrak{P}_i)$. Para demonstrá-la, necessitamos do seguinte lema:

Lema 3.3.1 ([Flo96], p. 64)**.** *Consideremos a forma quadrática*

$$Q_m(a_1, \cdots, a_m) = \sum_{i=1}^{m} a_i^2 + \sum_{1 \leqslant i < j \leqslant m} (a_i - a_j)^2, \tag{3.49}$$

com $a_i \in \mathbb{Z}$, $m \geqslant 1$. O mínimo não nulo da forma quadrática $Q_m(a_1, \cdots, a_m)$ é igual a m, o qual é atingido pelos vetores $\pm(1, 1, \ldots, 1) \in \mathbb{Z}^m$ e $\pm e_i \in \mathbb{Z}^m$, em que e_i é o i-ésimo elemento da base canônica de $\mathbb{Z}^m$.

Proposição 3.3.2. *Sob as hipóteses anteriores (com p ramificado), a densidade de centro do reticulado de posto completo $\sigma(\mathfrak{P}_i) \subset \mathbb{R}^p$ é*

$$\delta(\sigma(\mathfrak{P}_i)) = \frac{\lambda_i^{p/2}}{2^p p_i n^{\frac{p-1}{2}}} \tag{3.50}$$

onde

$$\lambda_i = \min\left\{pp_i^2,\ n(p-1)/p\right\}. \tag{3.51}$$

Demonstração. Seja $x = a_0 + \sum_{i=1}^{p-1} a_i \theta^i(T)$ um elemento de $\mathfrak{P}_i$, isto é, $a_0 \equiv 0\ (mod\ p_i)$. Se $a_0 = 0$, a Equação 3.10 acarreta

$$\min_{x \in \mathfrak{P}_i} Tr_{\mathbb{K}}(x^2) = pp_1 \cdots p_r \min_{(a_1, \cdots, a_{p-1}) \in \mathbb{Z}^{p-1}} Q_{p-1}(a_1, \cdots, a_{p-1}) = p(p-1)p_1 \cdots p_r, \tag{3.52}$$

já que $\theta(T) \in \mathfrak{P}_i$ e $\min_{(a_1, \cdots, a_{p-1}) \in \mathbb{Z}^{p-1}} Q_{p-1}(a_1, \cdots, a_{p-1}) = p - 1$ (Lema 3.3.1). Se $a_0 \neq 0$ então o menor valor que a_0 pode assumir é p_i, já que $a_0 \equiv 0\ (mod\ p_i)$. Neste caso, a forma quadrática $Q_{p-1}(a_1, \ldots, a_{p-1})$ assume seu menor valor quando é nula. Logo,

$$\min_{x \in \mathfrak{P}_i} Tr_{\mathbb{K}}(x^2) = pp_i^2. \tag{3.53}$$

Portanto, $t_{\mathfrak{P}_i} = \min\left\{pp_i^2,\ n(p-1)/p\right\} =: \lambda_i$. Para completar a demonstração, observemos que $[\mathcal{O}_{\mathbb{K}} : \mathfrak{P}_i] = N(\mathfrak{P}_i) = p_i$. □

Exemplo 3.3.2. *Seja $\mathbb{K}$ um corpo de números de grau $p = 3$ e condutor $n = 819 = 3^2 \times 7 \times 13$. Notemos que $p_1 = 7$ e $p_2 = 13$ são congruentes a 1 módulo 3. Devido à Equação 3.40, a densidade de centro de $\sigma(\mathcal{O}_{\mathbb{K}})$ é igual a aproximadamente $0,000793$. Sendo $\mathfrak{P}_i$ os ideais primos acima de p_i em $\mathcal{O}_{\mathbb{K}}$, $i = 1, 2$, a Proposição 3.3.2 nos diz que a densidade de centro de $\sigma(\mathfrak{P}_1)$ é aproximadamente igual a $0,03886$, já que $\lambda_1 = 3 \times 7^2 = 147$, enquanto a densidade de centro de $\sigma(\mathfrak{P}_2)$ é igual a aproximadamente $0,13403$, pois $\lambda_2 = 3 \times 13^2 = 507$. Assim, a densidade de centro de $\sigma(\mathfrak{P}_2)$ é a maior dentre todas as calculadas acima e corresponde a cerca de 75% da maior densidade de centro possível em terceira dimensão, que é de $0,17678$.*

CAPÍTULO 4

Reticulados algébricos bem arredondados

Reticulados bem arredondados são aqueles cujos vetores de norma mínima geram o espaço euclidiano de dimensão igual ao posto do reticulado. Tais reticulados têm sido considerados para aplicações em teoria de códigos, especialmente para canais MIMO e SISO sem fio [GBK+16, GTKH16], e estão relacionados a outros problemas envolvendo reticulados, como a conjectura de Minkowski [McM05, Mar03]. Recentemente têm surgido alguns trabalhos relacionando os reticulados bem arredondados aos reticulados ideais [FP12, FHL+13]. Em [FP12], por exemplo, é mostrado que existem infinitos corpos de números quadráticos reais e imaginários contendo um ideal do seu anel de inteiros cujo reticulado obtido via o mergulho de Minkowski é bem arredondado em $\mathbb{R}^2$. É provado também que, em qualquer dimensão $n \geqslant 2$, um reticulado algébrico obtido via anel de inteiros de um corpo de números é bem arredondado se, e somente se, esse corpo é ciclotômico (na verdade, é necessário fazer uma ressalva de que esse resultado é válido quando o corpo é totalmente real ou totalmente complexo). Seguindo esta linha, neste capítulo iremos utilizar os $\mathbb{Z}$-módulos M_m definidos no Capítulo 3 para provar a existência de infinitos reticulados algébricos não equivalentes em $\mathbb{R}^p$, para todo $p > 2$ primo. Além disso, mostraremos que para cada corpo de números cíclico de grau primo ímpar existe um reticulado algébrico bem arredondado obtido como imagem de um $\mathbb{Z}$-módulo contido no seu anel de inteiros através do mergulho de Minkowski. Na Seção 4.1, definimos o conjunto dos vetores mínimos e os mínimos sucessivos de um reticulado e estudamos a relação deles com determinados parâmetros desse reticulado. Na Seção 4.2, introduzimos e exemplificamos o conceito de reticulado bem arredondados. Na Seção 4.3, analisamos situações em que um reticulado algébrico obtido do anel de inteiros de um corpo de números via o mergulho de Minkowski é bem arredondado. Por fim, a Seção 4.4, reúne as principais contribuições originais que foram mencionadas acima. As principais referências bibliográficas deste capítulo incluem as já mencionadas acima e também [Mic02, Mar03, OINL17, NINL16]. Os principais resultados deste capítulo foram apresentados no Congresso Internacional de Matemáticos 2018 [dAC18b] e aceitos para publicação no periódico Archiv der Mathematik [dAC18a].

4.1 Mínimos sucessivos de um reticulado

Sejam $n \geqslant 2$ inteiro e Λ um reticulado de posto completo em $\mathbb{R}^n$. Como definido em (1.9), a norma mínima $N_{\min}(\Lambda)$ desse reticulado é o mínimo entre as normas euclidianas de todos os seus vetores não nulos.

Definição 4.1.1. *O* conjunto dos vetores mínimos $S(\Lambda)$ *de um reticulado de posto completo $\Lambda \subset \mathbb{R}^n$ é o que contém todos os vetores $x \in \Lambda \backslash \{0\}$ com norma igual à norma mínima do reticulado, isto é,*

$$S(\Lambda) = \{x \in \Lambda \ : \ \|x\| = N_{min}(\Lambda)\}. \tag{4.1}$$

O número de elementos de $S(\Lambda)$ é chamado de número de contato[1] *de Λ.*

A norma mínima $N_{min}(\Lambda)$ de um reticulado $\Lambda \subset \mathbb{R}^n$ também costuma ser denotada por $\lambda_1(\Lambda)$ e ser chamada de primeiro mínimo sucessivo de Λ, já que pode ser generalizada pela seguinte definição:

Definição 4.1.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo. Para cada $k \leqslant n$, chama-se de k-ésimo* mínimo sucessivo *de Λ ao valor $\lambda_k(\Lambda)$ correspondente ao menor raio r tal que a bola centrada na origem de $\mathbb{R}^n$ com raio r contém k vetores linearmente independentes pertencentes a Λ.*

Observação 4.1.1. *O mínimo sucessivo $\lambda_k(\Lambda)$ pode ser denotado apenas por λ_k quando não houver possibilidade de confusão.*

A Definição 4.1.2 equivale a dizer que o mínimo sucessivo $\lambda_k(\Lambda)$ é o menor valor real $r > 0$ tal que o reticulado Λ possui k vetores linearmente independentes com norma euclidiana menor ou igual a r. Como consequência, vale a seguinte cadeia de desigualdades:

$$\lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_n. \tag{4.2}$$

Definição 4.1.3. *O* invariante de Hermite *de um reticulado $\Lambda \subset \mathbb{R}^n$ é definido por*

$$\gamma(\Lambda) = \frac{N_{min}(\Lambda)^2}{\det(\Lambda)^{1/n}}. \tag{4.3}$$

A constante de Hermite *de dimensão n é igual a*

$$\gamma_n = \sup_{\Lambda \subset \mathbb{R}^n} \gamma(\Lambda) \tag{4.4}$$

e um reticulado Λ tal que $\gamma(\Lambda) = \gamma_n$ é chamado de reticulado crítico *em dimensão n.*

Observação 4.1.2. *A densidade de centro (1.12) de $\Lambda \subset \mathbb{R}^n$ é igual a $\delta(\Lambda) = 2^{-n}\gamma(\Lambda)^{n/2}$.*

[1] *Kissing number*, em inglês.

Por exemplo, em $\mathbb{R}^2$, o reticulado hexagonal é crítico e tem invariante de Hermite $\lambda_2 = 2/\sqrt{3}$. Nesta dimensão atinge-se a seguinte desigualdade, que vale para qualquer outra dimensão:

$$\gamma(\Lambda) \leqslant \left(\frac{4}{3}\right)^{\frac{n-1}{2}}. \tag{4.5}$$

A demonstração desta desigualdade pode ser obtida pelo Corolário 2.2.2 de [Mar03].

A proposição abaixo mostra a relação entre os mínimos sucessivos e a constante de Hermite:

Proposição 4.1.1 ([Mar03], Teorema 2.6.8)**.** *Sendo $\Lambda \subset \mathbb{R}^n$ um reticulado, para qualquer $r \leqslant n$ vale a desigualdade*

$$\lambda_1\lambda_2 \ldots \lambda_r \leqslant \gamma_n^r \det(\Lambda)^{r/n}. \tag{4.6}$$

Por fim, observamos uma interessante relação entre o raio de cobertura μ de um reticulado e seu último mínimo sucessivo:

Proposição 4.1.2 ([Mic], Seção 5)**.** *Se Λ é um reticulado n-dimensional, então*

$$\frac{\lambda_n(\Lambda)}{2} \leqslant \mu(\Lambda) \leqslant \frac{\sqrt{n}\lambda_n(\Lambda)}{2}. \tag{4.7}$$

4.2 Reticulados bem arredondados

Nesta seção, estudamos os reticulados que têm todos os mínimos sucessivos iguais, os quais são chamados de reticulados bem arredondados, conforme a definição a seguir:

Definição 4.2.1. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo.*
(a) O reticulado Λ é dito bem arredondado[2] *se $S(\Lambda)$ gera $\mathbb{R}^n$, ou seja, se $S(\Lambda)$ tem n vetores linearmente independentes.*
(b) O reticulado Λ é chamado fortemente bem arredondado *se $S(\Lambda)$ gera Λ.*

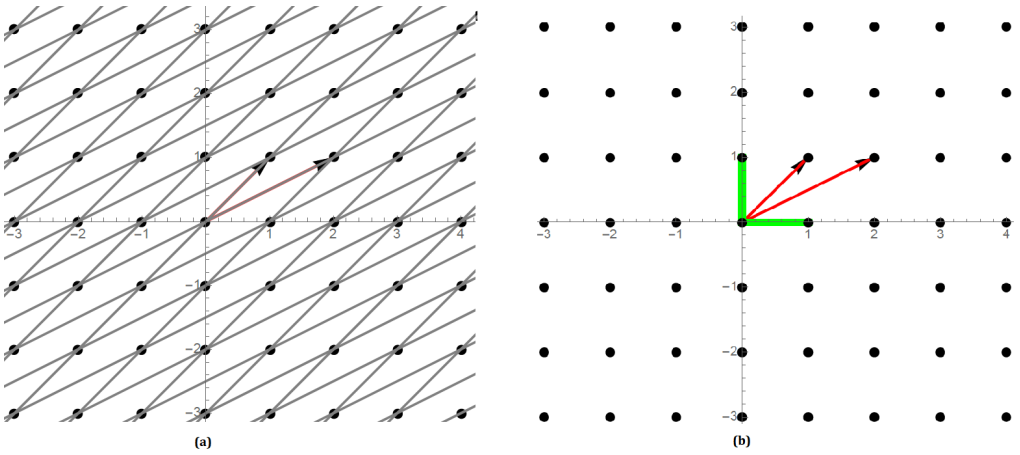
A Definição 4.2.1, item (a), equivalentemente diz que um reticulado bem arredondado é aquele cujos mínimos sucessivos são todos iguais: $\lambda_1 = \lambda_2 = \ldots = \lambda_n$.

Observação 4.2.1. *Se $\Lambda \subset \mathbb{R}^n$ é um reticulado bem arredondado, então $\langle S(\Lambda)\rangle_{\mathbb{Z}}$ é um sub-reticulado de Λ que é fortemente bem arredondado. Portanto, todo reticulado bem arredondado possui um sub-reticulado fortemente bem arredondado.*

Reticulados bem arredondados que são sub-reticulados de versões rotacionadas de $\mathbb{Z}^n$ podem ser úteis para otimizar a relação sinal-ruído (SNR) em códigos Rayleigh SISO/MIMO com desvanecimento [GTKH16, GBK+16]. Esses reticulados também têm associação com outros problemas de reticulados (empacotamento e cobertura de esferas, por exemplo) [Mar03] e com a conjectura de Minkowski [McM05].

[2] *Well-rounded (WR) lattice*, em inglês.

Figura 4 – Reticulado ortogonal gerado pelos vetores $(1,1)$ e $(2,1)$.



Exemplo 4.2.1. *Na Figura 4 (a) vemos a representação do reticulado* Λ *gerado pelos vetores* $u = (1,1)$ *e* $v = (2,1)$ *em* $\mathbb{R}^2$*. Notemos que* u *e* v *não são vetores de mesma norma euclidiana, o que pode nos levar à falsa conclusão de que* Λ *não é bem arredondado. Porém,* Λ *tem outra base dada pelos vetores* $a = (1,0)$ *e* $b = (0,1)$*. Isso significa que* $\Lambda = \mathbb{Z}^2$*, que é bem arredondado porque* a *e* b *são vetores de norma igual à norma mínima do reticulado (*$N_{min}(\Lambda) = 1$*). Na Figura 4 (b) vemos a representação de* Λ *com a indicação dos vetores* u*,* v*,* a *e* b*.*

Em dimensão dois, temos o resultado a seguir:

Proposição 4.2.1 ([FP12])**.** *Seja* $\Lambda \subset \mathbb{R}^2$ *um reticulado de posto completo.*
(a) Λ *tem* 2*,* 4 *ou* 6 *vetores mínimos;*
(b) Λ *é bem arredondado se, e somente se, o número de vetores mínimos for* 4 *ou* 6*;*
(c) Λ *é equivalente ao reticulado hexagonal se, e somente se, tem exatamente* 6 *vetores mínimos.*

Demonstração. Se v é um vetor de norma mínima de Λ, então $-v$ também é. Isto significa que $|S(\Lambda)|$ é par, já que $0 \notin S(\Lambda)$. Sejam u e v dois vetores linearmente independentes em $S(\Lambda)$ (assim, $v \neq \pm u$). Consideremos θ o ângulo entre u e v. Se $\theta < \pi/3$, então a Lei dos Cossenos implica

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2\|u\|\|v\| \cos\theta < \|u\|^2 = \|v\|^2 \tag{4.8}$$

já que u e v têm mesma norma. Porém, de (4.8) concluímos que $u = v$, o que não é admitido. Portanto, $\theta \geqslant \pi/3$. Além disso, como todos os vetores de $S(\Lambda)$ pertencem à mesma circunferência de raio $N_{min}(\Lambda)$, segue que o número de elementos de $S(\Lambda)$ é no máximo igual a $2\pi/(\pi/3) = 6$. Portanto, $|S(\Lambda)|$ é igual a 2 (quando só tem dois elementos linearmente dependentes), 4 ou 6, já que essa quantidade é par. Isso prova os itens (a) e (b). Para provar o item (c), basta notar que Λ é equivalente ao reticulado hexagonal se, e somente se, dois vetores de norma mínima linearmente independentes em Λ tem ângulo exatamente igual a $\pi/3$ ou $2\pi/3$, ou seja, quando $|S(\Lambda)| = 2\pi/(\pi/3) = 6$. □

Figura 5 – Reticulado gerado pelos vetores $(1,0)$ e $(\cos(5\pi/12), \text{sen}(5\pi/12))$

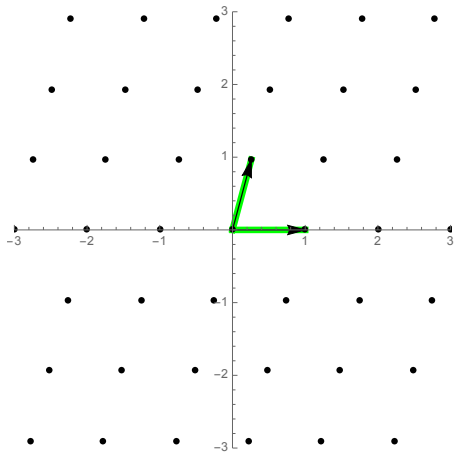
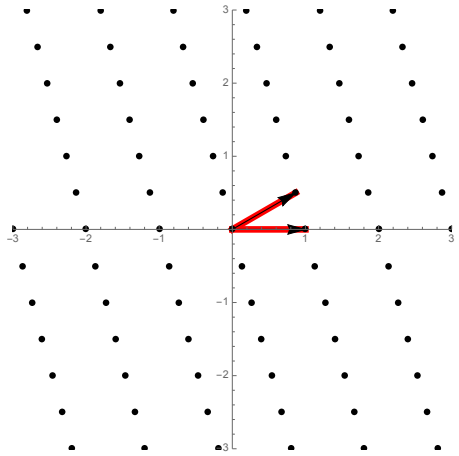


Figura 6 – Reticulado gerado pelos vetores $(1,0)$ e $(\cos(\pi/6), \text{sen}(\pi/6))$



Exemplo 4.2.2. *Para cada $\theta \in (0, \pi/2]$, consideremos o reticulado $\Lambda(\theta) \subset \mathbb{R}^2$ gerado por $u = (1,0)$ e $v = (\cos\theta, \text{sen}\theta)$. Seguindo a ideia da demonstração da Proposição 4.2.1 é possível ver que $\Lambda(\theta)$ é bem arredondado quando $\pi/3 \leqslant \theta \leqslant \pi/2$, pois tem entre 4 e 6 vetores de norma mínima, e não é bem arredondado quando $0 < \theta < \pi/3$, pois tem apenas 2 vetores de norma mínima. A Figura 4 ilustra o reticulado $\Lambda(\theta)$ com $\theta = 5\pi/12 > \pi/3$, o qual é, portanto, bem arredondado. Por sua vez, o reticulado $\Lambda(\theta)$ representado na Figura 4.2.2 não é bem arredondado, já que $\theta = \pi/6 < \pi/3$.*

Como complemento à Proposição 4.2.1, o artigo [FP12] prova que há infinitos reticulados não equivalentes em $\mathbb{R}^2$, todos com quatro vetores mínimos.

4.3 Reticulados bem arredondados obtidos via o mergulho de Minkowski

No artigo [FP12] são provados alguns resultados associando reticulados bem arredondados e reticulados algébricos obtidos via ideais de anéis de inteiros de corpos de

números através do mergulho de Minkowski (reticulados ideais). Em $\mathbb{R}^2$, por exemplo, é provado que existem infinitos corpos de números reais e imaginários cujos anéis de inteiros possuem algum ideal I tal que a imagem de I pelo mergulho de Minkowski é um reticulado bem arredondado em $\mathbb{R}^2$. Explicitamente, denotando por σ o mergulho de Minkowski e sendo d um número inteiro livre de quadrados, [FP12] apresenta os seguintes resultados:

- O reticulado $\sigma\left(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}\right)$ é bem arredondado se, e somente se, $d = -1$ ou $d = -3$ (Lema 2.2);
- Existem infinitos $d > 1$ livres de quadrado, $d \equiv -1 \ (mod\ 4)$, para os quais existe $I \lhd \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ tal que $\sigma(I)$ é bem arredondado (Lema 2.5);
- Existem infinitos $d > 1$ livres de quadrado, $d \equiv 1 \ (mod\ 4)$, para os quais existe $I \lhd \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ tal que $\sigma(I)$ é bem arredondado (Lema 2.6).

Em $\mathbb{R}^n$, para $n > 2$, não há muitos estudos sobre reticulados ideais bem arredondados. Um dos poucos trabalhos nesta linha é [FP12], no qual os autores afirmam que a imagem do anel de inteiros de um corpo de números pelo mergulho de Minkowski é um reticulado bem arredondado se, e somente se, esse corpo é ciclotômico (Teorema 1.2 de [FP12]). No entanto, a demonstração dessa afirmação está comprometida devido a um erro ocorrido na prova de um dos lemas desse trabalho. Considerando apenas corpos de números totalmente reais ou totalmente complexos, porém, esse resultado é válido:

Teorema 4.3.1. *Seja $\mathbb{K}$ um corpo de números totalmente real ou totalmente complexo com mergulho de Minkowski σ. O reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.*

Para provar o Teorema 4.3.1 precisamos de alguns lemas que estão enunciados e justificados a seguir. O primeiro lema é bem conhecido e, por isso, omitiremos sua demonstração:

Lema 4.3.1 (Desigualdade das médias aritmética e geométrica)**.** *Se $a_1, \ldots, a_k$ são números reais não negativos, então*

$$\left(\prod_{i=1}^{k} a_i\right)^{1/k} \leqslant \frac{1}{k}\sum_{i=1}^{k} a_i. \tag{4.9}$$

A igualdade ocorre se, e somente se, $a_1 = \ldots = a_k$.

Lema 4.3.2. *Sejam $\mathbb{K}$ um corpo de números de grau n e σ o mergulho de Minkowski associado. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então*

$$N_{min}(\sigma(I))^2 \geqslant \frac{n}{2} N(I)^{\frac{2}{n}} \tag{4.10}$$

Demonstração. Denotemos por $\sigma_1, \ldots, \sigma_{r_1}$ os monomorfismos reais de $\mathbb{K}$, por σ_{r_1+1}, ..., $\sigma_{r_1+r_2}$ os r_2 monomorfismos complexos de $\mathbb{K}$ não conjugados entre si e por $\sigma_{i+r_1+r_2}$, $1 \leqslant i \leqslant r_2$, os monomorfismos complexos conjugados a σ_{i+r_1}, respectivamente. Se $x \in \mathcal{O}_{\mathbb{K}}$, então

$$|N_{\mathbb{K}}(x)|^{\frac{1}{r_1+r_2}} = \left(\prod_{i=1}^{r_1} |\sigma_i(x)|^2 \prod_{i=1}^{r_2} |\sigma_{i+r_1}(x)\sigma_{i+r_1+r_2}(x)|^2\right)^{\frac{1}{2(r_1+r_2)}}$$

$$= \left(\prod_{i=1}^{r_1} |\sigma_i(x)|^2 \prod_{i=1}^{r_2} \left(\Re(\sigma_{i+r_1}(x))^2 + \Im(\sigma_{i+r_1}(x))^2\right)^2\right)^{\frac{1}{2(r_1+r_2)}}. \tag{4.11}$$

Do Lema 4.3.1 e da igualdade $n = r_1 + 2r_2$ segue que

$$|N_{\mathbb{K}}(x)|^{\frac{1}{r_1+r_2}} \leqslant \left(\frac{1}{n}\left(\sum_{i=1}^{r_1} \sigma_i(x)^2 + 2\sum_{i=1}^{r_2} \left(\Re(\sigma_{i+r_1}(x))^2 + \Im(\sigma_{i+r_1}(x))^2\right)\right)\right)^{\frac{n}{r_1+n}}$$

$$\leqslant \left(\frac{2}{n}\|\sigma(x)\|^2\right)^{\frac{n}{r_1+n}} \tag{4.12}$$

e, como $(r_1 + n)/(n(r_1 + r_2)) = 2/n$, então

$$\|\sigma(x)\|^2 \geqslant \frac{n}{2} |N_{\mathbb{K}}(x)|^{\frac{2}{n}}. \tag{4.13}$$

Como a Equação 4.13 é válida para todo inteiro algébrico x, em particular vale para os elementos de I. Assim,

$$N_{min}(\sigma(I))^2 = \min_{0 \neq x \in I} \|\sigma(x)\|^2 \geqslant \min_{0 \neq x \in I} \frac{n}{2} |N_{\mathbb{K}}(x)|^{\frac{2}{n}} \geqslant \frac{n}{2} N(I)^{\frac{2}{n}} \tag{4.14}$$

em que a última desigualdade segue do fato que $|N_{\mathbb{K}}(x)| \geqslant N(I)$ para todo $x \in I \backslash \{0\}$ [Sam70, Seção 3.5]. □

Lema 4.3.3. *Sejam $\mathbb{K}$ um corpo de números* totalmente real *de grau $n = r_1$ e σ o mergulho de Minkowski. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então*

$$N_{min}(\sigma(I))^2 \geqslant n N(I)^{\frac{1}{n}}. \tag{4.15}$$

Demonstração. Denotando por $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ (todos reais, já que $n = r_1$), segue do Lema 4.3.1 que, para todo $x \in \mathcal{O}_{\mathbb{K}}$,

$$|N_{\mathbb{K}}(x)|^{\frac{1}{n}} = \left(\prod_{i=1}^{n} |\sigma_i(x)|\right)^{\frac{1}{n}} = \left(\prod_{i=1}^{n} \sigma_i(x)^2\right)^{\frac{1}{2n}} \leqslant \left(\frac{1}{n}\sum_{i=1}^{n} \sigma_i(x)^2\right)^{\frac{1}{2}} = \left(\frac{1}{n}\|\sigma(x)\|^2\right)^{\frac{1}{2}}. \tag{4.16}$$

Daí obtemos, como na demonstração do Lema 4.3.2, que

$$N_{min}(\sigma(I))^2 = \min_{0 \neq x \in I} \|\sigma(x)\|^2 \geqslant \min_{0 \neq x \in I} n|N_{\mathbb{K}}(x)|^{\frac{2}{n}} = nN(I)^{\frac{2}{n}} \geqslant nN(I)^{\frac{1}{n}} \tag{4.17}$$

em que a última desigualdade vem da combinação dos fatos $N(I) \geqslant 1$ e $2/n > 1/n$. □

Lema 4.3.4. *Sejam $\mathbb{K}$ um corpo de números totalmente real ou totalmente complexo de grau n e σ o mergulho de Minkowski. Dado $x \in \mathcal{O}_{\mathbb{K}}$, se $\sigma(x) \in S(\sigma(\mathcal{O}_{\mathbb{K}}))$, então x é uma raiz da unidade.*

Demonstração. Suponha que $\mathbb{K}$ é totalmente complexo, ou seja, $n = 2r_2$. Como $N(\mathcal{O}_{\mathbb{K}}) = 1$, o Lema 4.3.2 garante que $N_{min}(\sigma(\mathcal{O}_{\mathbb{K}}))^2 = n/2 = r_2$, já que $\|\sigma(1)\|^2 = r_2$. Tal qual na demonstração desse lema, como $|N_{\mathbb{K}}(x)| \geqslant 1$ ($x \in \mathcal{O}_{\mathbb{K}}$), segue que, se $\sigma(x) \in S(\sigma(\mathcal{O}_{\mathbb{K}}))$, então

$$1 \leqslant |N_{\mathbb{K}}(x)|^{\frac{1}{r_2}} = \left(\prod_{i=1}^{r_2} \left(\Re(\sigma_i(x))^2 + \Im(\sigma_i(x))^2 \right) \right)^{\frac{1}{r_2}}$$

$$\leqslant \frac{1}{r_2} \sum_{i=1}^{r_2} \left(\Re(\sigma_i(x))^2 + \Im(\sigma_i(x))^2 \right) = \frac{\|\sigma(x)\|^2}{r_2} = 1. \tag{4.18}$$

O Lema 4.3.1 também garante que

$$\Re(\sigma_1(x))^2 + \Im(\sigma_1(x))^2 = \ldots = \Re(\sigma_{r_2}(x))^2 + \Im(\sigma_{r_2}(x))^2 = 1. \tag{4.19}$$

Logo, todos os conjugados de x tem valor absoluto igual a 1. Portanto, segue do Teorema de Kronecker [PL04, Teorema 4.5.4] que x é uma raiz da unidade. Por sua vez, suponha que $\mathbb{K}$ é totalmente real, isto é, $n = r_1$. Analogamente ao que foi feito no caso imaginário, o Lema 4.3.3 e sua demonstração garantem que $N_{min}(\sigma(\mathcal{O}_{\mathbb{K}}))^2 = r_1$ e, para cada x tal que $\sigma(x) \in S(\sigma(\mathcal{O}_{\mathbb{K}}))$,

$$1 \leqslant |N_{\mathbb{K}}(x)|^{\frac{1}{r_1}} \leqslant \left(\prod_{i=1}^{r_2} (\sigma_i(x))^2 \right)^{\frac{1}{r_1}} \leqslant \frac{1}{r_1} \sum_{i=1}^{r_1} (\sigma_i(x))^2 = \frac{\|\sigma(x)\|^2}{r_1} = 1, \tag{4.20}$$

pois $\|\sigma(1)\|^2 = r_1$. Novamente do Lema 4.3.1 segue que

$$\sigma_1(x) = \ldots = \sigma_{r_1}(x) = 1. \tag{4.21}$$

O Teorema de Kronecker garante que x é raiz da unidade. □

De posse dos Lemas 4.3.1, 4.3.2, 4.3.3 e 4.3.4 já é possível provar o Teorema 4.3.1:

Demonstração do Teorema 4.3.1. Suponha inicialmente que $\mathbb{K}$ seja totalmente real. Se $\mathbb{K} = \mathbb{Q} = \mathbb{Q}(\zeta_1)$, então $\sigma(\mathcal{O}_{\mathbb{K}}) = \sigma(\mathbb{Z}) = \mathbb{Z}$ é bem arredondado. Se $\mathbb{K} \neq \mathbb{Q}$, então $\mathbb{K}$ não é ciclotômico e as únicas raízes da unidade de $\mathbb{K}$ são 1 e -1 (caso contrário, haveria um corpo ciclotômico não trivial contido em $\mathbb{K}$, o que o impediria de ser real). O Lema 4.3.4 implica então que $S(\sigma(\mathcal{O}_{\mathbb{K}})) \subset \{\sigma(\pm 1)\}$ e, como $\sigma(1) = -\sigma(-1)$, não há r_1 vetores linearmente independentes em $S(\sigma(\mathcal{O}_{\mathbb{K}}))$. Portanto, se $\mathbb{K}$ é totalmente real, então $\sigma(\mathcal{O}_{\mathbb{K}})$ é bem arredondado se, e somente se, $\mathbb{K} = \mathbb{Q}$, que é o único dos corpos totalmente reais que é ciclotômico. Por sua vez, suponha que $\mathbb{K}$ seja totalmente complexo, isto é, $n = 2r_2$.

Como provado no Lema 4.3.4, os únicos elementos $x \in \mathcal{O}_\mathbb{K}$ tais que $\sigma(x) \in S(\sigma(\mathcal{O}_\mathbb{K}))$ são as raízes da unidade ζ. Além disso, se ζ é uma raiz da unidade de $\mathbb{K}$, então

$$\|\sigma(\zeta)\|^2 = \sum_{i=1}^{r_2} \left(\Re(\sigma_i(\zeta))^2 + \Im(\sigma_i(\zeta))^2\right) = \sum_{i=1}^{r_2} 1 = r_2, \tag{4.22}$$

pois $\sigma_i(\zeta)$ pertence à bola unitária em $\mathbb{R}^2$. Do Lema 4.3.2, segue que $N_{min}(\sigma(\mathcal{O}_\mathbb{K}))^2 = r_2$ e que $S(\sigma(\mathcal{O}_\mathbb{K})) = \{\sigma(x) \ : \ x \in C\}$, em que C é o subgrupo finito de $\mathbb{K}^*$ formado pelas raízes da unidades de $\mathbb{K}$. O grupo C é cíclico, gerado por (digamos) $\zeta_k = \exp(2\pi i/k)$, para algum $k \in \mathbb{Z}$. Disso segue que $C \subset \mathbb{Z}[\zeta_k] \subset \mathcal{O}_\mathbb{K}$, ou seja, todas as raízes da unidade de $\mathbb{K}$ são combinações lineares inteiras dos números 1, ζ_k, ζ_k^2, ..., $\zeta_k^{\varphi(k)-1}$, os quais são raízes da unidade linearmente independentes entre si. Portanto, o subgrupo C tem exatamente $\varphi(k)$ raízes da unidades linearmente independentes, implicando que $S(\sigma(\mathcal{O}_\mathbb{K}))$ tem $\varphi(k) \leqslant n$ vetores linearmente independentes. Dessa forma, $\sigma(\mathcal{O}_\mathbb{K})$ é bem arredondado se, e somente se, $\varphi(k) = n$, o que só pode ocorrer quando $\mathbb{K} = \mathbb{Q}(\zeta_k)$, que é um corpo ciclotômico. □

Como consequência do Teorema 4.3.1 podemos ver que o Corolário 1.3 de [FP12] continua válido, o qual garante que a imagem de qualquer ideal fracionário de um corpo ciclotômico pelo mergulho de Minkowski é um reticulado bem arredondado. Outra consequência do Teorema 4.3.1 é a seguinte:

Corolário 4.3.1. *Se $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana e σ denota o mergulho de Minkowski associado a $\mathbb{K}$, então o reticulado $\sigma(\mathcal{O}_\mathbb{K})$ é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico.*

Demonstração. Como $\mathbb{K}/\mathbb{Q}$ é uma extensão galoisiana, então a Proposição 1.6.1 da Seção 1.6 garante que $\mathbb{K}$ é totalmente real ou totalmente complexo. Portanto, o resultado segue do Teorema 4.3.1. □

O Teorema 4.3.1 fecha a questão para corpos totalmente reais ou totalmente complexos sobre quais reticulados algébricos obtidos como imagens de anéis de inteiros pelo mergulho de Minkowski são bem arredondados. Porém, deixa algumas questões abertas, tais como as seguintes:

(i) O Teorema 4.3.1 é válido quando $\mathbb{K}$ é um corpo de números misto (isto é, com $r_1 \neq 0$ e $r_2 \neq 0$)?

(ii) Dado $\mathbb{K}$ um corpo de números de grau n, existe algum $\mathbb{Z}$-módulo $M \subset \mathcal{O}_\mathbb{K}$ (ou ideal) tal que $\sigma(M)$ é um reticulado bem arredondado em $\mathbb{R}^n$?

(iii) Em $\mathbb{R}^n$ existe algum reticulado algébrico $\sigma(M)$ bem arredondado, sendo M um $\mathbb{Z}$-módulo (ou ideal) de algum anel de inteiros? Se existir, a quantidade desses reticulados (não equivalentes) é infinita?

(iv) Como fica o Teorema 4.3.1 se σ for substituído por algum mergulho torcido σ_α?

Na seção seguinte mostraremos que a resposta para a questão (ii) é positiva sobre $\mathbb{Z}$-módulos quando $\mathbb{K}$ é um corpo de números de grau primo $p > 2$. Também veremos que a resposta para a questão (iii) é positiva em $\mathbb{R}^p$, sendo $p > 2$ um número primo, e que, nesse caso, existem infinitos reticulados algébricos bem arredondados, não equivalentes entre si, obtidos via $\mathbb{Z}$-módulos. As questões (ii) e (iii) para n geral e as questões (i) e (iv) permanecem abertas.

4.4 Reticulados algébricos bem arredondados em dimensões primas ímpares

Nosso principal objetivo, nesta seção, é mostrar que em todo corpo de números cíclico de grau primo ímpar não ramificado existe um $\mathbb{Z}$-módulo contido no seu anel de inteiros cuja imagem pelo mergulho de Minkowski é um reticulado bem arredondado. Para isso, utilizaremos conceitos, definições e resultados apresentados no Capítulo 3 deste trabalho. Mostraremos também que existem infinitos reticulados algébricos bem arredondados não equivalentes entre si em $\mathbb{R}^p$, sendo $p > 2$ um número primo qualquer. Os resultados desta seção foram aceitos para publicação na revista Archiv der Mathematik [dAC18a].

Seja $\mathbb{K}$ um corpo de números cíclico de grau primo $p > 2$ tal que $p\mathcal{O}_\mathbb{K}$ é um ideal não ramificado. Conforme vimos no Capítulo 3, o condutor de $\mathbb{K}$ é da forma $n = p_1 p_2 \dots p_r$, com $p_i \equiv 1 \ (mod\ p)$ primos distintos, $1 \leqslant i \leqslant r$ (Proposição 3.1.2). Assim, $\mathbb{K} \subset \mathbb{Q}(\zeta_n)$. Sejam θ o gerador do grupo de Galois $G = Gal(\mathbb{K}/\mathbb{Q})$ e $T = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$. Segundo a Proposição 3.1.3, o anel de inteiros de $\mathbb{K}$ é dado por

$$\mathcal{O}_\mathbb{K} = \mathbb{Z}[G]T = \langle T, \theta(T), \theta^2(T), \dots, \theta^{p-1}(T)\rangle_\mathbb{Z}. \tag{4.23}$$

Para cada inteiro $m > 0$, consideremos o $\mathbb{Z}$-módulo M_m definido em (3.42):

$$M_m = \left\{ \sum_{k=0}^{p-1} a_k \theta^k(T) \ : \ \sum_{k=0}^{p-1} a_k \equiv 0 \ (mod\ m) \right\}. \tag{4.24}$$

Sabemos que M_m tem posto p, índice m sobre $\mathcal{O}_\mathbb{K}$ e mínimo dado na Proposição 3.3.1. Consideremos também $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^p$ o mergulho de Minkowski associado a $\mathbb{K}$.

Lema 4.4.1. *Sejam $a \in \mathbb{C}$ fixado e $n \geqslant 1$ inteiro. O determinante da matriz $n \times n$*

$$A_n(a) = \begin{pmatrix} a+1 & a & \dots & a \\ a & a+1 & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a+1 \end{pmatrix} \tag{4.25}$$

é igual a $na + 1$.

Demonstração. Consideremos a matriz $m \times m$ dada por

$$B_m(a) = \begin{pmatrix} \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a{+}1} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a} & \mathrm{a{+}1} & \dots & \mathrm{a} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a{+}1} \end{pmatrix}. \tag{4.26}$$

Vamos mostrar que $\det(B_m(a)) = a$, para todo $m \geqslant 1$. Se $m = 1$, então $B_1(a) = (a)$ tem determinante igual a a. Assumamos, por hipótese de indução, que $\det(B_k(a)) = a$ para $k \geqslant 1$. Utilizando propriedades de determinantes, segue que:

$$\begin{aligned} \det(B_{k+1}(a)) &= \begin{vmatrix} \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a} & \mathrm{a{+}1} & \dots & \mathrm{a} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a{+}1} \end{vmatrix} + \begin{vmatrix} \mathrm{a} & 0 & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & 1 & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & 0 & \mathrm{a{+}1} & \dots & \mathrm{a} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{a} & 0 & \mathrm{a} & \dots & \mathrm{a{+}1} \end{vmatrix} \\ &= 0 + \det(B_k(a)) = a. \end{aligned} \tag{4.27}$$

No cálculo de (4.27), a primeira parcela da soma é igual a zero porque há duas colunas iguais, enquanto a segunda parcela resultou em $\det(B_k(a))$ aplicando o método de Laplace à segunda coluna. Portanto, $\det(B_m(a)) = a$, para todo $m \geqslant 1$. Por sua vez, $A_1(a) = (a{+}1)$ tem determinante igual a $a + 1$. Suponhamos, por hipótese de indução, que $\det(A_k(a)) = ka + 1$, para $k \geqslant 1$. Utilizando propriedades de determinantes, segue que:

$$\begin{aligned} \det(A_{k+1}(a)) &= \begin{vmatrix} \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a{+}1} & \mathrm{a} & \dots & \mathrm{a} \\ \mathrm{a} & \mathrm{a} & \mathrm{a{+}1} & \dots & \mathrm{a} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{a} & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a{+}1} \end{vmatrix} + \begin{vmatrix} 1 & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a} \\ 0 & \mathrm{a{+}1} & \mathrm{a} & \dots & \mathrm{a} \\ 0 & \mathrm{a} & \mathrm{a{+}1} & \dots & \mathrm{a} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \mathrm{a} & \mathrm{a} & \dots & \mathrm{a{+}1} \end{vmatrix} \\ &= \det(B_{k+1}(a)) + \det(A_k(a)) = a + ka + 1 = (k+1)a + 1. \end{aligned} \tag{4.28}$$

No cálculo de (4.28), a segunda parcela foi obtida pelo método de Laplace aplicado à primeira coluna e pela hipótese de indução. Logo, $\det(A_n(a)) = na + 1$, como queríamos demonstrar. □

Lema 4.4.2. *Seja $m > 0$ inteiro tal que $m \equiv 1 \ (mod\ p)$. O conjunto*

$$\mathcal{B} = \{\theta^i \left((l+1)T + l\theta(T) + l\theta^2(T) + \ldots + l\theta^{p-1}(T)\right) \ : \ 0 \leqslant i < p\} \tag{4.29}$$

é uma $\mathbb{Z}$-base de M_m, em que $l = (m-1)/p$.

Demonstração. Consideremos a aplicação $f : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}^p$ definida por

$$f\left(a_1T + a_2\theta(T) + \ldots + a_{p-1}\theta^{p-1}(T)\right) = (a_1, a_2, \ldots, a_p). \tag{4.30}$$

A aplicação f é um isomorfismo entre os grupos abelianos aditivos $\mathcal{O}_{\mathbb{K}}$ e $\mathbb{Z}^p$. Assim, para provar que $\mathcal{B}$ é uma $\mathbb{Z}$-base de M_m é suficiente provar que o conjunto

$$f(\mathcal{B}) = \{(l+1, l, \ldots, l), (l, l+1, \ldots, l), \ldots, (l, l, \ldots, l+1)\} \tag{4.31}$$

é uma $\mathbb{Z}$-base de $f(M_m)$. Mostremos este último fato. O conjunto $f(\mathcal{B})$ é linearmente independente, pois, pelo Lema 4.4.1, $\det(A_p(l)) = pl + 1 = m > 0$. Vamos mostrar que $f(\mathcal{B})$ gera o conjunto $f(M_m)$. Por um lado, a soma das coordenadas de cada vetor em $f(\mathcal{B})$ é $l + 1 + (p-1)l = pl + 1 = m \equiv 0 \ (mod\ m)$. Logo, $f(\mathcal{B}) \subset f(M_m)$, ou seja, $\langle f(\mathcal{B})\rangle_{\mathbb{Z}} \subset f(M_m)$, já que $f(M_m)$ é um $\mathbb{Z}$-módulo em $\mathbb{Z}^p$. Por outro lado, seja $x \in f(M_m)$. Desta forma, $x = (a_0, a_1, \ldots, a_{p-1})$, com $\sum_{i=0}^{p-1} a_i \equiv 0 \ (mod\ m)$. A última congruência implica que existe $k \in \mathbb{Z}$ tal que $\sum_{i=0}^{p-1} a_i = mk$. Defina, para cada $j \in \{0, 1, \ldots, p-1\}$, o número inteiro $b_j = a_j - lk$. Assim,

$$\sum_{j=0}^{p-1} b_j = \sum_{j=0}^{p-1} (a_j - lk) = mk - plk = (m - pl)k = k. \tag{4.32}$$

Disso segue que, para cada $j \in \{0, 1, \ldots, p-1\}$,

$$a_j = b_j + lk = b_j + l\sum_{j=0}^{p-1} b_j = b_0 l + b_1 l + \ldots + b_j(l+1) + \ldots + b_{p-1} l. \tag{4.33}$$

Portanto,

$$x = (a_0, a_1, \ldots, a_{p-1}) = b_0(l+1, l, \ldots, l) + b_1(l, l+1, \ldots, l) + \ldots + b_{p-1}(l, l, \ldots, l+1) \tag{4.34}$$

é uma combinação linear sobre $\mathbb{Z}$ dos elementos de $f(\mathcal{B})$. Portanto, $f(M_m) \subset \langle f(\mathcal{B})\rangle_{\mathbb{Z}}$. Concluímos, então, que $f(M_m)$ é gerado por $f(\mathcal{B})$, donde segue o lema. □

A seguir enunciamos o principal teorema desta seção:

Teorema 4.4.1. *Se $m > 0$ é inteiro satisfazendo $m \equiv 1 \ (mod\ p)$ e*

$$\sqrt{\frac{n}{p+1}} \leqslant m \leqslant \sqrt{n(p+1)}, \tag{4.35}$$

então $\sigma(M_m)$ é um reticulado fortemente bem arredondado em $\mathbb{R}^p$.

Demonstração. Como $m \equiv 1 \ (mod\ p)$, segue que existe um inteiro l positivo tal que $m = pl + 1$. Como na Proposição 3.3.1, definimos a aplicação $F(m) = (m^2 + n(p-1))/p$. Por hipótese, $m \leqslant \sqrt{n(p+1)}$. Disso obtemos:

$$m^2 \leqslant n(p+1) \Longrightarrow m^2 + np - n \leqslant 2pn \Longrightarrow \frac{m^2 + n(p-1)}{p} \leqslant 2n \Longrightarrow F(m) \leqslant 2n. \tag{4.36}$$

Para cada $i \in \{1, 2, \ldots, p\}$ sejam $\tilde{l}$ e $\tilde{r}$, respectivamente, o quociente e o resto da divisão de im por p, isto é, $im = p\tilde{l} + \tilde{r}$, com $0 \leqslant \tilde{r} < p$. Se $i = p$, então $\tilde{r} = 0$. Neste caso, $F(pm) = pm^2$. Como, por hipótese, $\sqrt{\dfrac{n}{p+1}} \leqslant m$, segue que $n \leqslant (1+p)m^2$ e, multiplicando essa expressão por $(1-p) < 0$, temos $n(1-p) \geqslant m^2(1-p^2)$. Daí,

$$m^2 + n(p-1) \leqslant p^2m^2 \Longrightarrow F(m) = \frac{m^2 + n(p-1)}{p} \leqslant pm^2 = F(pm). \tag{4.37}$$

Se $1 \leqslant i < p$ é um número inteiro, então $\tilde{r} = i$, pois $im = i(pl+1) = p(il)+i$, com i menor do que p. Assim, $F(im) = (i^2m^2 + ni(p-i))/p$. Como, por hipótese, $n/(p+1) \leqslant m^2$, segue que

$$m^2 \geqslant \frac{n(1+p) - np}{p+1} = n - \frac{np}{p+1} > n - \frac{np}{i+1} \tag{4.38}$$

em que a última desigualdade ocorre porque $i < p$. Daí, como $1 - i \leqslant 0$,

$$m^2(i+1) > n(i+1-p) \Longrightarrow m^2(1-i^2) < n(1-i)(i+1-p) = n(ip - i^2 - p + 1) \tag{4.39}$$

donde segue que $m^2 + n(p-1) < i^2m^2 + ni(p-i)$, ou seja, $F(p) < F(ip)$, para todo $1 \leqslant i < p$. Disso e de (4.36) e (4.37) segue que $F(m) \leqslant 2n$ e $F(m) \leqslant F(im)$, para todo $i \in \{1, 2, \ldots, p\}$. Assim, pela Proposição 3.3.1, segue que

$$\min_{0 \neq x \in M_m} \|\sigma(x)\|^2 = \min\{2n, F(m), F(2m), \ldots, F(pm)\} = F(m), \tag{4.40}$$

ou seja, $N_{min}(\sigma(M_m))^2 = F(m)$. Esse mínimo é atingido pelos elementos $x = \displaystyle\sum_{i=0}^{p-1} a_i\theta^i(T)$ onde exatamente um a_i é igual a $l+1$ e os outros a_i são iguais a l. Isso significa que $N_{min}(\sigma(M_m))$ é atingido pelos elementos do conjunto $\mathcal{B}$ do Lema 4.4.2. Como $\mathcal{B}$ é uma $\mathbb{Z}$-base de M_m, então $\sigma(\mathcal{B})$ é uma base para o reticulado $\sigma(M_m)$ na qual todos os elementos têm norma igual a norma mínima do reticulado. Logo, $\sigma(M_m)$ é um reticulado fortemente bem arredondado. □

Uma importante consequência do Teorema 4.4.1 é o objetivo traçado no início desta seção:

Corolário 4.4.1. *Seja $\mathbb{K}$ um corpo de números cíclico de grau $p > 2$ com condutor $n = p_1p_2\ldots p_r$, em que cada p_i é um número primo distinto tal que $p_i \equiv 1 \pmod p$. Então existem $m > 0$ e um $\mathbb{Z}$-módulo $M_m \subset \mathcal{O}_\mathbb{K}$, definido em (4.24), tal que $\sigma(M_m)$ é um reticulado fortemente bem arredondado em $\mathbb{R}^p$.*

Demonstração. Consideremos a aplicação F definida na Proposição 3.3.1. Como $m \equiv 1 \pmod p$, segue que $F(m) = (m^2 + n(p-1))/p$, em que $m = pl + 1$ para algum número inteiro l. Devido à hipótese de que $m \leqslant \sqrt{n(p+1)}$, tem-se que $F(m) \leqslant 2n$. Para cada $i \in \{1, 2, \ldots, p\}$ sejam $\tilde{l}$ e $\tilde{r}$ números inteiros satisfazendo $im = p\tilde{l} + \tilde{r}$, com $0 \leqslant \tilde{r} < p$. Se $i = p$, então $\tilde{r} = 0$ e $F(pm) = pm^2$. Como $\sqrt{\dfrac{n}{p+1}} \leqslant m$, segue que $n \leqslant (1+p)m^2$ e, após

multiplicar essa expressão por $(1-p) < 0$, obtemos $n(1-p) \geqslant m^2(1-p^2)$. Disso segue que $F(m) \leqslant pm^2 = F(pm)$. Por fim, se $1 < i < p$, então $\tilde{r} = i$, já que $im = i(pl+1) = p(il)+i$. Logo, $F(im) = (i^2m^2 + ni(p-i))/p$. Como $i < p$ e $\sqrt{n/(p+1)} \leqslant m$ (por hipótese), segue que

$$m^2 \geqslant \frac{n(1+p)-np}{p+1} = n - \frac{np}{p+1} > n - \frac{np}{i+1} \Longrightarrow m^2(i+1) > n(i+1-p). \quad (4.41)$$

Multiplicando essa expressão por $1-i$, obtemos $m^2 + n(p-1) < i^2m^2 + ni(p-i)$, isto é, $F(m) < F(im)$, para cada $1 < i < p$. Em resumo, temos $F(m) \leqslant 2n$ e $F(m) \leqslant F(im)$ para todo $1 < i < p$. Devido à Proposição 3.3.1, isso significa que

$$N_{min}(\sigma(M_m))^2 = \min_{0 \neq x \in M_m} \|\sigma(x)\|^2 = \min\{2n, F(m), F(2m), \ldots, F(pm)\} = F(m) \quad (4.42)$$

Este mínimo é atingido pelos elementos $\sum_{i=0}^{p-1} a_i\theta^i(t)$ onde exatamente um a_i é igual a $l+1$ e os outros a_i são iguais a l. Isso implica que o valor de $N_{min}(\sigma(M_m))$ é atingido pelos elementos do conjunto $\mathcal{B}$ definido no Lema 4.4.2. Como $\mathcal{B}$ é uma $\mathbb{Z}$-base de M_m, $\sigma(\mathcal{B})$ é uma base do reticulado $\sigma(M_m)$, na qual todos os vetores têm norma igual à norma mínima do reticulado. Portanto, $\sigma(M_m)$ é um reticulado fortemente bem arredondado. □

Observação 4.4.1. *Consideremos a transformação linear $\tau : \mathbb{R}^p \longrightarrow \mathbb{R}^p$ definida por $\tau(x_1, x_2, \ldots, x_p) = (x_2, x_3 \ldots, x_p, x_1)$, com $x_i \in \mathbb{R}$, $1 \leqslant i \leqslant n$. Como, para todo $x \in \mathbb{K}$, $\sigma(x) = (x, \theta(x), \ldots, \theta^{p-1}(x))$ e $\tau^i(\sigma(x)) = \sigma(\theta^i(x))$, $1 \leqslant i \leqslant p-1$, segue que $\sigma(M_m)$ tem uma base cíclica $\sigma(\mathcal{B})$, isto é, $\sigma(\mathcal{B})$ é da forma $\{v, \tau(v), \tau^2(v), \ldots, \tau^{p-1}(v)\}$, para algum $v \in \mathbb{R}^p$.*

A seguir, considerando a construção acima, vamos demonstrar que existem infinitos reticulados algébricos bem arredondados não equivalentes entre si no espaço euclidiano p-dimensional para qualquer número primo $p > 2$. Para isso, utilizaremos o fato de que dois reticulados equivalentes possuem mesma densidade de centro (Proposição 1.3.1).

Para cada corpo de números $\mathbb{K}$ de grau primo $p > 2$ e condutor $n = p_1p_2 \ldots p_r$, com $p_i \equiv 1 \ (mod\ p)$, e $m > 0$ inteiro, consideremos o $\mathbb{Z}$-módulo M_m. Segue da Proposição 3.3.1 que a densidade de centro do reticulado $\Lambda = \sigma(M_m)$ é dada por

$$\delta = \frac{|\Lambda|^{p/2}}{2^p[\mathcal{O}_{\mathbb{K}} : M]\sqrt{|D(\mathbb{K})|}} = \frac{(m^2 + n(p-1))^{p/2}}{2^p p^{p/2} m n^{\frac{p-1}{2}}}. \quad (4.43)$$

Corolário 4.4.2. *Existem infinitos reticulados algébricos bem arredondados não equivalentes entre si em $\mathbb{R}^p$, para qualquer número primo $p > 2$.*

Demonstração. Sejam p_1 e p_2 dois números primos ímpares distintos satisfazendo $p_i \equiv 1 \ (mod\ p)$, $i = 1, 2$. Sem perda de generalidade podemos supor que $p_2 > p_1$. Como

$Gal(\mathbb{Q}(\zeta_{p_i})/\mathbb{Z})$ é cíclico, existem corpos de números $\mathbb{K}_i$ de grau p e condutor p_i, para cada $i = 1, 2$. Pelo fato de $\mathbb{K}_1$ e $\mathbb{K}_2$ terem condutores distintos, segue que são corpos distintos. Segue do Corolário 4.4.1 que para $i = 1, 2$ existe um inteiro positivo $m_i \in \left[\sqrt{\frac{p_i}{p+1}}, \sqrt{p_i(p+1)}\right]$ tal que $\Lambda_i = \sigma(M_{m_i})$ é um reticulado algébrico bem arredondado. Vamos mostrar que Λ_1 e Λ_2 são reticulados não equivalentes provando que as densidades de centro δ_1 e δ_2 de Λ_1 e Λ_2, respectivamente, são diferentes. De (4.43) segue que

$$\delta_i = \frac{(m_i^2 + p_i(p-1))^{p/2}}{2^p p^{p/2} m_i p_i^{\frac{p-1}{2}}}. \tag{4.44}$$

Se $\delta_1 = \delta_2$, então $\delta_1^2 = \delta_2^2$ e

$$m_2^2 p_2^{p-1} \left(m_1^2 + p_1(p-1)\right)^p = m_1^2 p_1^{p-1} \left(m_2^2 + p_2(p-1)\right)^p. \tag{4.45}$$

Nesta última expressão vemos que p_2 divide $m_1^2 p_1^{p-1} \left(m_2^2 + p_2(p-1)\right)^p$. Como p_2 é um número primo diferente de p_1, então p_2 divide m_1 ou m_2. No entanto, como $m_1 \leqslant \sqrt{p_1(p+1)}$ e $p_1 > p+1$, já que $p_1 \equiv 1 \ (mod\ p)$, então $m_1 < p_2$. Logo, m_1 não é múltiplo de p_2, donde segue que p_2 divide m_2. Por sua vez, $m_2 < p_2$, ou seja, p_2 não divide m_2, o que é uma contradição. Portanto, $\delta_1 \neq \delta_2$ e Λ_1 e Λ_2 não são equivalentes. Isso significa que para qualquer par de números primos ímpares distintos p_1 e p_2 tais que $p_1 \equiv 1 \ (mod\ p)$ e $p_2 \equiv 1 \ (mod\ p)$ existem dois reticulados algébricos bem arredondados não equivalentes entre si. Finalmente, a conclusão deste corolário segue do Teorema de Dirichlet [Was95, Corolário 2.11], que garante a existência de infinitos números primos q tais que $q \equiv 1 \ (mod\ p)$. □

Como vimos no Capítulo 3, construções algébricas envolvendo os reticulados M_m em corpos de números de grau primo ímpar têm sido usados na busca por reticulados densos. O exemplo seguinte apresenta a construção de um reticulado algébrico bem arredondado obtido como foi proposto nesta seção e com alta densidade de centro em $\mathbb{R}^3$:

Exemplo 4.4.1. *Seja $\mathbb{K}$ um corpo de números de grau $p = 3$ e condutor $n = p_1.p_2.p_3$, onde $p_1 = 7$, $p_2 = 13$ e $p_3 = 19$. Assim, $n = 1729$. Para aplicar o Teorema 4.4.1, consideremos $m = 82$. Temos que $82 \equiv 1 \ (mod\ 3)$ e $82 \in \left[\sqrt{\frac{n}{p+1}}, \sqrt{n(p+1)}\right] \supset [20.8, 83.16]$. Seja M_{82} o conjunto dos elementos $\sum_{i=0}^{2} a_i \theta^i(t)$ tais que $a_0 + a_1 + a_2 \equiv 0 \ (mod\ 82)$, onde θ é o gerador do grupo de Galois $Gal(\mathbb{K}/\mathbb{Q})$ e $t = Tr_{\mathbb{Q}(\zeta_n)/\mathbb{K}}(\zeta_n)$. Então, $\sigma(M_{82})$ é um reticulado bem arredondado em $\mathbb{R}^3$ cuja densidade de centro é dada por $\delta \simeq 0,1743$. Lembrando que a máxima densidade de centro em $\mathbb{R}^3$ é aproximadamente igual a $0,1768$ e é atingida pelo reticulado D_3, temos que o reticulado $\sigma(M_{82})$ tem uma taxa de empacotamento muito boa nessa dimensão.*

O próximo exemplo é mais construtivo:

Exemplo 4.4.2. *Sejam $p = 5$ e $n = 11$. Observemos que p e n são números primos ímpares tais que $n \equiv 1 \ (mod\ p)$. Sendo $\zeta_{11} = e^{\frac{2\pi i}{11}}$ a 11-ésima raiz primitiva da unidade, $G = Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) = \langle\phi\rangle \simeq (\mathbb{Z}/11\mathbb{Z})^*$, onde $\phi(\zeta_{11}) = \zeta_{11}^2$, já que 2 é o elemento primitivo de $(\mathbb{Z}/11\mathbb{Z})^*$. Consideremos $\theta = \phi^5$ dado por $\theta(\zeta_{11}) = \phi^5(\zeta_{11}) = \zeta_{11}^{2^5} = \zeta_{11}^{10} = \zeta_{11}^{-1}$. Seja $\mathbb{K}$ o corpo fixo do grupo $H = \langle\theta\rangle = \{\theta, \theta^2\}$, cujo grau é $10/2 = 5 = p$. Notemos que*

$$t = Tr_{\mathbb{Q}(\zeta_{11})/\mathbb{K}}(\zeta_{11}) = \theta(\zeta_{11}) + \theta^2(\zeta_{11}) = \zeta_{11} + \zeta_{11}^{-1}. \tag{4.46}$$

Assim, $\mathbb{K} = \mathbb{Q}(t) = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ é o subcorpo maximal real de $\mathbb{Q}(\zeta_{11})$. O Teorema da Correspondência de Galois [Sam70, Teorema 2, Seção 6.1] implica que $Gal(\mathbb{K}/\mathbb{Q}) \simeq G/H = \langle\phi^2\rangle$. Como $\mathbb{K}$ é totalmente real, o mergulho de Minkowski de $\mathbb{K}$ é definido por

$$\sigma(x) = (x, \phi^2(x), \phi^4(x), \phi^6(x), \phi^8(x)). \tag{4.47}$$

Para construir o reticulado precisamos de um número inteiro $m \in \left[\sqrt{11/6}, \sqrt{66}\right]$ tal que $m \equiv 1 \ (mod\ 5)$. Tomamos $m = 6$, o maior valor satisfazendo essas condições. Seja M_6 o conjunto

$$M_6 = \left\{ \sum_{i=0}^{4} a_i \phi^{2i}(x) \ : \ \sum_{i=0}^{4} a_i \equiv 0 \ (mod\ 6) \right\}. \tag{4.48}$$

Assim, devido ao Teorema 4.4.1, segue que $\Lambda = \sigma(M_6)$ é um reticulado algébrico bem arredondado em $\mathbb{R}^5$ com base $\{v, \tau(v), \tau^2(v), \tau^3(v), \tau^4(v)\}$, onde τ é a transformação linear definida na Observação 4.4.1 e

$$v = (\zeta_{11} + \zeta_{11}^{-1} - 1, \zeta_{11}^2 + \zeta_{11}^{-2} - 1, \zeta_{11}^4 + \zeta_{11}^{-4} - 1, \zeta_{11}^8 + \zeta_{11}^{-8} - 1, \zeta_{11}^5 + \zeta_{11}^{-5} - 1). \tag{4.49}$$

O reticulado produzido tem norma mínima ao quadrado igual a $F(6) = 16$. A densidade de centro de Λ é dada por

$$\delta = \frac{16^{5/2}}{2^5 \times 5^{5/2} \times 8 \times 11^2} \simeq 0,0441. \tag{4.50}$$

A maior densidade de centro possível em dimensão 5 é aproximadamente igual a $0,08839$, atingida pelo reticulado D_5.

A construção do exemplo acima pode ser generalizada para outras dimensões escolhendo um condutor primo ímpar n satisfazendo $n \equiv 1 \ (mod\ p)$ tão grande quanto se queira.

CAPÍTULO 5

Criptografia via reticulados algébricos

A iminência do advento dos computadores quânticos mantém na comunidade científica a preocupação de que os atuais protocolos criptográficos não sobreviverão. De fato, no final da década de 1990, Peter Shor apresentou algoritmos que tornam viável resolver em computadores quânticos problemas matemáticos que fundamentam a segurança dos atuais sistemas criptográficos [Sho97], tais como o RSA. Desde então buscam-se novos modelos que não possam ser quebrados por algoritmos quânticos. Uma das propostas mais importantes para a chamada criptografia pós-quântica fundamenta-se em problemas envolvendo reticulados, tais como o problema do vetor mais curto e o problema do vetor mais próximo. Neste capítulo, vamos apresentar um resumo sobre a criptografia baseada em reticulados e o estado atual de pesquisa, com a intenção de que um leitor sem conhecimento de teoria da computação seja capaz de compreender este tema de modo introdutório. Um dos problemas centrais sobre os quais nos debruçamos é o Anel-LWE (RLWE), que é baseado em reticulados algébricos via o mergulho de Minkowski. Uma contribuição original que fazemos neste capítulo consiste na proposta do problema Anel-LWE torcido (α-RLWE), o qual baseia-se em reticulados algébricos obtidos via o mergulho torcido σ_α, e na demonstração de segurança da versão de busca deste problema (Teorema 5.4.1). Na Seção 5.1, apresentamos os conceitos básicos e um curto histórico sobre criptografia. Na Seção 5.2, introduzimos a criptografia baseada em reticulados a partir dos sistemas NTRU e GGH e enunciamos alguns problemas de reticulados sobre os quais essa teoria se sustenta. Na Seção 5.3, apresentamos os principais problemas computacionais relacionados a esta linha de estudo. Na Seção 5.4, propomos o problema Anel-LWE torcido e demonstramos sua segurança. Por fim, na Seção 5.5, mostramos algumas fragilidades da criptografia baseada em reticulados, as quais nos dizem quais parâmetros devem ser evitados na prática. As referências bibliográficas que fundamentam este capítulo incluem [MvOV01, DH76, RSA78, Sho97, Ajt96, Pei16, PRSD17, Mic02, NIS17, GGH97, HPS98, Reg05, BCLvV16, LPR10, CLS17, BV11, LS15, EHL14, ELOS15]. Como resultado dos assuntos mencionados aqui foi desenvolvido o trabalho conjunto preliminar [OdAD+18a] e apresentado o trabalho [OdAD+18b].

5.1 Alguns conceitos preliminares sobre Criptografia

Ao longo dos séculos os seres humanos se viram necessitados de tornar segura a transmissão de informação entre eles, mesmo quando ela ainda era realizada por meio físico e não digital. A *segurança da informação* é buscada através de alguns objetivos, tais como a confidencialidade, a integridade dos dados, a autenticação, a assinatura, a validação, o controle de acesso, a certificação, a confirmação do recebimento, a prevenção de alteração de dados, entre outros. Com o advento dos computadores, das mídias digitais e da internet, a necessidade de manter segura a transmissão de informações se tornou ainda mais latente, ao mesmo tempo em que os mecanismos de transmissão ficaram mais complexos. É importante notar ainda que a segurança da informação depende tanto de protocolos e algoritmos matemáticos como de procedimentos técnicos e físicos [MvOV01].

Diante deste contexto envolvendo a segurança da informação podemos definir *criptografia* como sendo o estudo de técnicas matemáticas que objetivam a confidencialidade, a integridade, a autenticação e a não repudiação dos dados. Dessa forma, um dos objetivos da criptografia é estudar e buscar por protocolos que garantam a comunicação sigilosa entre um emissor e um destinatário. Há relatos do uso da criptografia pelos egípcios há mais de quatro mil anos atrás, mas ela ganhou notória importância com o papel decisivo que ocupou durante a Segunda Guerra Mundial (1939-1945), pois a máquina de criptografia Enigma foi uma poderosa arma alemã nos combates. Desde o início da era digital a criptografia é imprescindível, pois visa garantir a segurança na transmissão de dados não só para fins diplomáticos e militares, mas também para fins comerciais, bancários, entre outros.

A confidencialidade (ou segredo) é a qualidade de garantir que apenas aqueles que são autorizados tenham acesso à mensagem. A integridade dos dados é a qualidade de não ter o conteúdo da mensagem alterado por parte não autorizada. A autenticação garante ao destinatário ter a certeza de quem é o emissor da mensagem. A não repudiação previne que algum participante alegue que não participou da transição.

A criptografia estuda e constrói *sistemas criptográficos* (ou criptossistemas), que são conjuntos de algoritmos que buscam garantir a segurança da informação. Um sistema criptográfico contém um algoritmo de geração de chaves, um de encriptação e um de decriptação. Uma *chave* é utilizada para encriptar um *texto simples* (*plaintext*, em inglês) em um *texto em claro* (*cyphertext*, em inglês) e para decriptar o texto em claro no texto simples. Os esquemas de encriptação dependem de um *alfabeto* $\mathcal{A}$ (ex.: corpo binário $\mathbb{F}_2 = \{0, 1\}$), de um *espaço de mensagens* $\mathcal{M}$, que é formado por sequências de símbolos do alfabeto (ex.: $\mathbb{F}_2^n$), e de um *espaço de textos em claro* $\mathcal{C}$, que também é formado por sequências de símbolos do alfabeto, podendo ou não ser igual a $\mathcal{M}$. Um *espaço de chaves* $\mathcal{K}$ é um conjunto de elementos que determinam bijeções entre $\mathcal{M}$ e $\mathcal{C}$. Se $e \in \mathcal{K}$, uma bijeção $E_e : \mathcal{M} \longrightarrow \mathcal{C}$ é chamada *função de encriptação*. Por sua vez, se $d \in \mathcal{K}$, uma

bijeção $D_d : \mathcal{C} \longrightarrow \mathcal{M}$ é chamada de *função de decriptação*. O processo que obtém $E_e(m)$, com $m \in \mathcal{M}$, é chamado de *encriptação* da mensagem m. Por sua vez, se $c \in \mathcal{C}$, o processo que calcula $D_d(c)$ é chamado de *decriptação* do texto em claro c. No conjunto $\mathcal{K}$ deve ser garantido que para cada $e \in \mathcal{K}$ exista (um único) $d \in \mathcal{K}$ tal que $D_d(E_e(m)) = m$, para todo $m \in \mathcal{M}$. Os conjuntos $\mathcal{E} = \{E_e : e \in \mathcal{K}\}$ e $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ formam o chamado *esquema de encriptação* (ou *cifra*). O par (e, d) é denominado *par de chaves*.

Um sistema criptográfico depende unicamente da escolha de $\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$, $\mathcal{E}$ e $\mathcal{D}$, os quais são de conhecimento público. No entanto, o par de chaves (e, d) deve ser guardado em segredo. Um esquema de encriptação é considerado *frágil* quando um terceiro agente diferente do emissor e do destinatário de uma mensagem consegue descobrir o texto simples a partir do correspondente texto em claro em tempo hábil sem, *a priori*, conhecer o par de chaves. Um esquema de encriptação é de *chave simétrica* quando, para todo par de chaves (e, d), é "fácil" descobrir d desde que e seja conhecido e vice-versa. Por outro lado, um esquema de encriptação é de *chave pública* (ou *chave assimétrica*) quando, para todo par de chaves (e, d), é impraticável descobrir d quando e é conhecido e vice-versa. Esse conceito foi introduzido em 1976 por Diffie e Hellman [DH76]. Por exemplo, suponha que Alice e Bob queiram se comunicar. No esquema de chave pública Bob seleciona um par de chaves (e, d), mantém consigo a chave d, em segredo, e envia para Alice a chave e. Por não ser sigilosa, a chave e é chamada de chave pública. Quando Alice quiser enviar uma mensagem $m \in \mathcal{M}$ para Bob, ela enviará o texto em claro $c = E_e(m)$. Como somente Bob tem conhecimento de d, só ele poderá redescobrir m fazendo $m = D_d(c)$.

O primeiro esquema de encriptação de chave pública estabelecido na prática veio com Rivest, Shamir e Adleman em 1978, o RSA [RSA78]. O método RSA sobrevive até hoje e sua segurança está assentada no problema da fatoração de números inteiros. Abaixo descrevemos os algoritmos que compõe esse esquema:

- Geração de chaves: escolhem-se aleatoriamente dois números primos p e q suficientemente grandes e com grande diferença entre si; calculam-se o *módulo* $n = pq$, que é tornado público, e a função totiente de Euler $\varphi(n) = (p-1)(q-1)$; define-se a chave pública como sendo um elemento $e \in \{1, 2, \ldots, \varphi(n)\}$ tal que $mdc(e, \varphi(n)) = 1$; calcula-se a chave privada d tal que $de \equiv 1 \ (mod\ \varphi(n))$. Assim, o par de chaves é $((n, e), d)$.

- Codificação: sendo $m \in \mathcal{M}$ uma mensagem, computa-se o texto em claro c de modo que $c \equiv m^e \ (mod\ n)$.

- Decodificação: Tomando o texto em claro c, o detentor da chave privada d descobre m fazendo $m \equiv c^d \ (mod\ n)$.

Para quebrar o método RSA é necessário descobrir d a partir de e e de n. Porém, isso só é factível computacionalmente quando se conhecem os primos p e q, os quais não são

conhecidos por terceiros que queiram quebrar o sistema. Além disso, obter p e q a partir de n significa fatorar n, o que é um problema impossível de ser resolvido em tempo hábil por computadores clássicos quando p e q são suficientemente grandes e distintos entre si. Isso torna o RSA seguro.

Outro esquema de chave pública criado após o RSA foi desenvolvido por El-Gamal em 1985 [Elg85]. A segurança deste esquema, denominado El-Gamal, depende da impossibilidade de computar logaritmos discretos, em determinadas condições, por computadores clássicos em tempo hábil.

Apesar dos esquemas RSA e El-Gamal serem ainda inquebráveis para vários parâmetros, isso não deve resistir ao advento dos computadores quânticos. De fato, Peter Shor apresentou em 1996 um algoritmo quântico que resolve o problema da fatoração de números inteiros e do logaritmo discreto em tempo hábil [Sho97]. Isso deu margem a novas linhas de pesquisa que busquem outros esquemas criptográficos que não possam ser quebrados por computadores quânticos. As propostas que se enquadram nesta categoria formam a chamada *criptografia pós-quântica*. Alguns problemas computacionais difíceis para os quais ainda não se conhece solução viável por meio quântico e que têm sido usados em criptografia envolvem equações quadráticas multivariadas, funções Hash, isogenias super-singulares, códigos corretores de erros e reticulados [Ort18]. No restante deste capítulo vamos focar na criptografia pós-quântica baseada em reticulados.

5.2 Criptografia baseada em reticulados

A *criptografia baseada em reticulados* se iniciou em 1996 quando Ajtai mostrou que problemas computacionais envolvendo reticulados conjecturadamente difíceis podiam ser utilizados para fins criptográficos [Ajt96]. Desde então surgiram várias propostas de sistemas criptográficos cuja segurança depende da impossibilidade de resolver determinados problemas sobre reticulados, tais como o NTRU, o GGH, o SIS, o RSIS, o LWE e o RLWE. As vantagens de utilizar criptografia baseada em reticulados englobam: a conjecturada segurança contra ataques quânticos, já que não são conhecidos algoritmos quânticos eficientes que resolvam os principais problemas sobre reticulados; o paralelismo, a eficiência e a simplicidade dos algoritmos, principalmente quando os reticulados são construídos por via algébrica; e a versatilidade das construções, pois a criptografia baseada em reticulados vai além de apenas garantir confidencialidade, mas pode também, por exemplo, ser usada para a antes utópica encriptação homomórfica total (*fully homomorphic encryption*, em inglês), que permite a usuários não confiáveis fazerem adições e multiplicações nos dados encriptados sem aprender nada com eles [Pei16].

Evidenciando a importância da criptografia baseada em reticulados no contexto da criptografia pós-quântica, a agência norte-americana NIST[1] fez em 2017 uma

[1] National Institute Standards and Technology

chamada por esquemas criptográficos pós-quânticos a serem padronizados, dos quais aproximadamente 34% dos 82 trabalhos submetidos eram relacionados a reticulados [NIS17]. Em [Ort18, Tabela 1] estão resumidas as submissões baseadas em reticulados. Além disso, o Google anunciou em 2016 experimentos com criptografia pós-quântica [Goo16], para os quais escolheu o algoritmo *New Hope* proposto por Alkim, Ducas, Pöppelmann e Schwabe em 2015 [ADPS15], o qual se enquadra na criptografia baseada em reticulados.

Os dois primeiros sistemas criptográficos com chave pública baseados em reticulados propostos foram o GGH e o NTRU. Em 1997, Goldreich, Goldwasser e Halevi propuseram o esquema GGH [GGH97], que tem sua segurança conjecturada, mas não ainda demonstrada. No esquema de encriptação do GGH a chave pública é uma base *ruim* de um reticulado (isto é, formada por vetores longos e altamente não ortogonais) e a chave privada é uma base *boa* desse mesmo reticulado (isto é, formada por vetores curtos e altamente ortogonais). Por sua vez, em 1998, Hoffstein, Pipher e Silverman apresentaram um esquema de encriptação de chave pública chamado NTRU [HPS98], o qual é construído sobre quocientes de anéis de polinômios $R = \mathbb{Z}[x]/\langle f(x)\rangle$, mas pode ser considerado baseado em reticulados. O sistema criptográfico NTRU é prático e eficiente, mas não se sabe com certeza se ele é seguro. Sua chave privada é um polinômio $s \in R$ e sua chave pública é um polinômio da forma $2hs^{-1}$ com coeficientes tomados módulo um número inteiro q ímpar suficientemente grande. Mais detalhes sobre o GGH e o NTRU podem ser encontrados em [Pei16].

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado de posto completo com base $\mathcal{B}$ e mínimos sucessivos $\lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_n$. Consideremos ainda um número real $\gamma = \gamma(n) \geqslant 1$ que cresce em função da dimensão n, o qual é chamado de *fator de aproximação*. Com essa notação, elencamos abaixo alguns problemas computacionais sobre reticulados que têm sido usados em criptografia:

- **Problema do vetor mais curto (SVP)**[2]**:** encontrar $c \in \Lambda$ tal que $\|c\| = \lambda_1(\Lambda)$.
- **Problema do vetor mais curto aproximado ($\mathbf{SVP}_\gamma$)**[3]**:** encontrar $c \in \Lambda$, não nulo, tal que $\|c\| \leqslant \gamma \cdot \lambda_1(\Lambda)$.
- **Problema de decisão do vetor mais curto aproximado ($\mathbf{GapSVP}_\gamma$)**[4]**:** sabendo que $\lambda_1(\Lambda) \leqslant 1$ ou $\lambda_1(\Lambda) > \gamma$, determinar qual dessas alternativas ocorre.
- **Problema dos vetores indepedentes mais curtos aproximados ($\mathbf{SIVP}_\gamma$)**[5]**:** encontrar um conjunto $S = \{s_i\}_i^n \subset \Lambda$ com n elementos linearmente independentes tais que $\|s_i\| \leqslant \gamma \cdot \lambda_n(\Lambda)$, com $1 \leqslant i \leqslant n$.

[2] Do inglês, *shortest vector problem.*
[3] Do inglês, *approximate shortest vector problem.*
[4] Do inglês, *decisional approximate shortest vector problem.*
[5] Do inglês, *approximate shortest independent vector problem.*

- **Problema do vetor mais próximo (CVP)**[6]**:** dado $t \in \mathbb{R}^n$ qualquer (chamado *vetor alvo*), encontrar $c \in \Lambda$ que minimiza a distância $\|c - t\|$.
- **Problema de decodificação da distância limitada (BDD$_\gamma$)**[7]**:** dado um vetor alvo $t \in \mathbb{R}^n$ tal que $dist(t, \Lambda) < d = \lambda_1(\Lambda)/(2\gamma)$, encontrar o único vetor $v \in \Lambda$ tal que $\|t - v\| < d$.

Os problemas enunciados acima são conjecturadamente intratáveis, a não ser para fatores de aproximação muito grandes [Pei16, Subseção 2.2.2]. Observemos que os problemas CVP e BDD$_\gamma$ são parecidos, tendo sua diferença principal caracterizada pelo vetor alvo t, que no CVP pode ser tomado de forma arbitrária, ao passo que no BDD$_\gamma$ ele é tomado "próximo" aos pontos do reticulado.

5.3 Fundamentos dos sistemas criptográficos baseados em reticulados

A seguir vamos apresentar os principais problemas computacionais que têm servido como fundamento para o desenvolvimento de sistemas criptográficos, os quais têm sua segurança baseada nos problemas computacionais sobre reticulados que foram enunciados anteriormente.

Solução Inteira Curta (SIS)[8]**.** Consideremos β um número real e n e q números inteiros positivos. Dados m vetores aleatórios $a_i \in \mathbb{Z}_q^n$ distribuídos uniformemente, o problema SIS consiste em encontrar um vetor não trivial $z = (z_1, \ldots, z_m) \in \mathbb{Z}^m$ com norma euclidiana no máximo igual a β tal que $\sum_{i=1}^{m} a_i z_i = 0 \in \mathbb{Z}_q^n$.

O problema SIS foi proposto em [Ajt96] e não tem sido utilizado para encriptação com chave pública, mas tem encontrado outras aplicações em criptografia, como assinatura digital, funções hash, esquemas de identificação, entre outras. Sua segurança está baseada na dificuldade de solucionar os problemas GapSVP$_\gamma$ e do SIVP$_\gamma$ para reticulados n-dimensionais arbitrários.

Aprendendo Com Erros (LWE)[9]**.** Sejam n e q inteiros positivos e χ uma distribuição de erros sobre $\mathbb{Z}$ (por exemplo, χ pode ser uma distribuição gaussiana discreta). Para cada vetor $s \in \mathbb{Z}_q^n$, chamado *segredo*, a *distribuição LWE* $A_{s,\chi}$ sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ é dada por amostras da forma $(a, b = \langle s, a \rangle + e \ (mod\ q))$, em que $a \in \mathbb{Z}_q^n$ é tomado pela distribuição uniforme e e é aleatório em χ. Suponha que s seja escolhido pela distribuição uniforme em $\mathbb{Z}_q^n$. Assim, o *problema de busca LWE* consiste em descobrir s a partir de m amostragens independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ escolhidas pela distribuição $A_{s,\chi}$. Por sua vez, o *problema*

[6] Do inglês, *closest vector problem*.
[7] Do inglês, *bounded distance decoding problem*.
[8] Do inglês, *Short Integer Solution*.
[9] Do inglês, *Learning With Errors*.

de decisão LWE consiste em distinguir se m amostras independentes $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ foram obtidas pela distribuição LWE $A_{s,\chi}$ (s fixado) ou pela distribuição uniforme.

O problema LWE foi introduzido em [Reg05]. Ao contrário do SIS, o LWE pode ser usado para encriptação com chave pública. Os problemas de busca e de decisão LWE são considerados seguros porque solucioná-los é, no mínimo, tão difícil quanto resolver GapSVP_γ e SIVP_γ para reticulados n-dimensionais arbitrários. Um exemplo de sistema criptográfico baseado em LWE é o Frodo [BCD+16], que foi submetido como proposta à agência NIST [NIS17].

Movidos pelas ideias do NTRU, alguns cientistas definiram versões do SIS e do LWE que adicionam estruturas algébricas a esses problemas, tornando-os mais eficientes, as quais conhecemos por RSIS e RLWE.

Anel-SIS (RSIS). Consideremos o anel $R = \mathbb{Z}[x]/\langle f(x)\rangle$, em que $f(x) = x^n - 1$ se n é primo ou $f(x) = x^n + 1$ se n é uma potência de 2. Seja q um número inteiro positivo, chamado *módulo*, m outro número inteiro positivo e $\beta > 0$ um número real. Seja $R_q = R/qR$. Dados m elementos $a_i \in R_q$ tomados pela distribuição uniforme, o problema RSIS consiste em encontrar um vetor não nulo $z = (z_1, \ldots, z_m) \in R^m$ de norma euclidiana menor ou igual a β tal que $\sum_{i=1}^{m} a_i z_i = 0 \in R_q$.

O problema RSIS foi definido da forma enunciada acima em [Mic02]. Sua vantagem em relação ao SIS é a eficiência. A dificuldade de resolvê-lo está associada à dificuldade de resolver o SVP_γ. Em trabalhos posteriores o RSIS foi definido de forma análoga ao estabelecido acima, mas trocando o anel $R = \mathbb{Z}[x]/\langle f(x)\rangle$ pelo anel de inteiros de um corpo de números qualquer, e foi provado ser pelo menos tão difícil de resolver quanto o problema SVP_γ para reticulados ideais arbitrários.

A seguir precisaremos do conceito de ideal dual. Se J é um ideal fracionário contido em $\mathbb{K}$, denomina-se por *ideal dual* de J o conjunto $J^\vee = \{x \in \mathbb{K} : Tr_{\mathbb{K}}(xJ) \subset \mathbb{Z}\}$. Em particular, o ideal $\mathcal{O}_\mathbb{K}^\vee$ é chamado de *ideal codiferente*. É interessante notar que a norma desse ideal é o inverso do discriminante $D(\mathbb{K})$ (Seção 1.5).

Anel-LWE (RLWE). Sejam $\mathbb{K}$ um corpo de números, $R = \mathcal{O}_\mathbb{K}$ seu anel de inteiros, $\mathbb{K}_\mathbb{R} = \mathbb{K} \otimes_\mathbb{Q} \mathbb{R}$, $\mathbb{T} = \mathbb{K}_\mathbb{R}/qR^\vee$, ψ uma distribuição sobre $\mathbb{K}_\mathbb{R}$, $q \geqslant 2$ um número inteiro, chamado *módulo*, e $R_q = R/qR$. Para $s \in R_q^\vee$, chamado *segredo*, define-se a *distribuição RLWE* $A_{s,\psi}$ como sendo aquela que produz amostras da forma $(a, b = as + e \ mod \ qR^\vee) \in R_q \times \mathbb{T}$, em que a é distribuído uniformemente em R_q e o *erro* e é aleatoriamente selecionado por ψ. Sejam s tomado pela distribuição uniforme sobre $R_q^\vee$ e ψ escolhido aleatoriamente em uma família de distribuições sobre $\mathbb{K}_\mathbb{R}$. O *problema de busca RLWE* consiste em encontrar s dado um conjunto com muitas amostras independentes geradas por $A_{s,\psi}$. Por sua vez, o *problema de decisão RLWE* consiste em distinguir entre amostras independentes geradas por $A_{s,\psi}$ e o mesmo número de amostras independentes geradas pela distribuição uniforme em $R_q \times \mathbb{T}$.

O RLWE, introduzido em [LPR10], enquadra-se na categoria de problemas utilizados em criptografia baseada em reticulados porque o mergulho de Minkowski permite dar uma interpretação geométrica a estruturas algébricas relacionadas a $\mathbb{K}$. Sua principal vantagem em relação ao LWE é a eficiência. A dificuldade de resolver os problemas RLWE está associada com a dificuldade de resolver por meio quântico os problemas SVP_γ e BDD_γ [LPR10, PRSD17].

A versão definida anteriormente pode ser chamada também de *RLWE dual*, já que o segredo s é tomado em $R_q^\vee$. Há ainda a versão *RLWE não dual*, em que se toma $s \in R_q$. Os problemas de *busca RLWE não dual* e de *decisão RLWE não dual* são definidos de forma análoga aos problemas de busca e decisão RLWE (dual). Apesar da diferença, as versões dual e não dual do RLWE podem ser reduzidas uma à outra por meio de uma mudança na distribuição de erro. Porém, essa mudança pode causar uma distorção na distribuição de erro (em particular, uma distribuição gaussiana esférica pode se transformar numa gaussiana elíptica) [CLS17].

Uma distribuição ψ comumente utilizada nos problemas RLWE é a distribuição gaussiana discreta. Considerando $r > 0$ um número real, Γ um reticulado de posto completo em $\mathbb{R}^n$ e $\rho_r(x) = \exp\left(-\|x\|^2/r^2\right)$ (chamada *função gaussiana*), para todo $x \in \Gamma$, define-se a *distribuição gaussiana discreta de comprimento* r por

$$D_{\Gamma,r}(x) = \frac{\rho_r(x)}{\sum_{y\in\Gamma}\rho_r(y)}. \tag{5.1}$$

Neste caso, utiliza-se $\psi = D_{\sigma(R^\vee),r}$ para o RLWE dual e $\psi = D_{\sigma(R),r}$ para o RLWE não dual, em que σ denota o mergulho de Minkowski associado a $\mathbb{K}$.

Observação 5.3.1. *As definições dos problemas RLWE dual e não dual feitas acima levaram em consideração distribuições ψ contínuas sobre $\mathbb{K}_\mathbb{R}$. No entanto, como implícito no parágrafo anterior, é comum utilizar distribuições discretas, tais como $D_{\Gamma,r}$. Notemos que sempre é possível transformar uma amostra $(a, b) \in R_q \times \mathbb{T}$ em uma amostra $(a, \lfloor b \rceil) \in R_q \times R_q^\vee$ (ou $R_q \times R_q$), com $\lfloor . \rceil$ denotando a função de arredondamento.*

Há uma versão simplificada (e distinta) dos problemas RLWE que utiliza anéis de polinômios ao invés de anéis de inteiros de corpos de números, a qual é conhecida como PLWE (ou *poly-LWE*):

Polinomial-LWE (PLWE). Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio mônico e irredutível de grau n, q um número primo tal que $f(x)$ se fatora completamente módulo q, $P = \mathbb{Z}[x]/\langle f(x)\rangle$, $P_q = P/qP = \mathbb{Z}_q[x]/\langle f(x)\rangle$ e $\sigma > 0$ um número real. Consideremos ψ uma distribuição definida sobre P. Seja $s(x) \in P_q$, chamado *segredo*. A *distribuição PLWE* $A_{s,\psi}$ consiste de amostras da forma $(a(x), b(x) = a(x)s(x) + e(x)) \in P_q \times P_q$, em que $a(x)$ é escolhido uniformemente em P_q e $e(x)$ é aleatoriamente selecionado por ψ em P_q. O *problema de busca PLWE* consiste em descobrir $s(x)$ a partir de várias amostras independentes tomadas em $A_{s,\psi}$. Por sua vez, o *problema de decisão PLWE* consiste em

distinguir amostras independentes $(a(x), b(x) = a(x)s(x) + e(x)) \in P_q \times P_q$ geradas por $A_{s,\psi}$ daquelas geradas pela distribuição uniforme.

Apesar de ser uma versão simplificada do RLWE, o PLWE foi inicialmente definido de forma explícita em [BV11]. O problema PLWE não é mais difícil de ser resolvido do que o problema RLWE. A diferença essencial do PLWE para o RLWE consiste no mergulho geométrico utilizado para a obtenção do erro e. Enquanto no RLWE usa-se o mergulho de Minkowski, no PLWE usa-se o chamado mergulho por coeficientes, que associa os coeficientes de um polinômio de grau $n-1$ a n-uplas no espaço n-dimensional da seguinte forma:

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \longmapsto (a_0, a_1, \ldots, a_{n-1}). \tag{5.2}$$

Tem sido proposta ainda a utilização de uma versão híbrida dos problemas LWE e RLWE conhecida como módulo-LWE (MLWE), cuja redução de segurança para problemas SIVP_γ sobre uma classe particular de reticulados foi apresentada em [LS15].

5.4 RLWE através do mergulho torcido

Nesta seção, vamos introduzir uma variação dos problemas RLWE e PLWE que, ao invés de utilizar o mergulho de Minkowski ou o mergulho por coeficientes, utiliza o mergulho torcido. Provaremos que o novo problema proposto nesta seção é ao menos tão seguro quanto o problema RLWE. Ao longo de toda esta seção, consideremos $\mathbb{K}$ um corpo de números e α um elemento totalmente positivo em $\mathcal{O}_\mathbb{K}$. Denotemos por σ_α o mergulho torcido associado a $\mathbb{K}$ e ao elemento totalmente positivo α, introduzido na Definição 1.7.2 do Capítulo 1, e por σ o mergulho de Minkowski.

Na definição das distribuições RLWE dual e não dual, o erro e é obtido aleatoriamente por uma distribuição ψ sobre $\mathbb{K}_\mathbb{R}$. Como $\sigma(\mathbb{K}_\mathbb{R}) = \mathbb{R}^n$ (estendendo σ por linearidade a $\mathbb{K}_\mathbb{R}$), podemos considerar o erro e como sendo a imagem inversa de um elemento aleatoriamente selecionado em $\mathbb{R}^n$ segundo alguma distribuição ψ (como, por exemplo, a distribuição gaussiana discreta) pelo mergulho de Minkowski, isto é,

$$e = \sigma^{-1}(\tilde{e}), \qquad com \;\; \tilde{e} \xleftarrow{\psi} \mathbb{R}^n. \tag{5.3}$$

Como $\sigma_\alpha(\mathbb{K}_\mathbb{R}) = \mathbb{R}^n$, segue que podemos trocar σ por σ_α, obtendo

$$e = \sigma_\alpha^{-1}(\tilde{e}), \qquad com \;\; \tilde{e} \xleftarrow{\psi_\alpha} \mathbb{R}^n. \tag{5.4}$$

Observação 5.4.1. *Se $\mathbb{K}$ é um corpo de números totalmente real de grau n, a função gaussiana ρ_r é definida pela expressão* $\exp\left(Tr_\mathbb{K}(x^2)/r^2\right)$ *quando o mergulho utilizado é o de Minkowski. Quando o mergulho é o torcido, $\rho_r(x) = \exp\left(Tr_\mathbb{K}(x^2)/\tilde{r}^2\right)$, em que $\tilde{r} = \dfrac{r^2}{\sum_{i=1}^n \sigma_i(\alpha)^2}$.*

Denotemos por ψ_α a distribuição associada ao mergulho torcido σ_α, conforme explícito em (5.4). Assim, definimos a *distribuição α-RLWE* como sendo aquela que produz amostras da forma $(a, b = as+e \ mod \ R_q^\vee) \in R_q \times \mathbb{T}$, em que a é tomado uniformemente em R_q e o erro e é aleatoriamente selecionado por ψ_α. Analogamente ao RLWE, o *problema de busca α-RLWE* consiste em encontrar o segredo s a partir de várias amostras independentes geradas pela distribuição α-RLWE com parâmetros α, s e ψ_α fixados. Por sua vez, o *problema de decisão α-RLWE* busca distinguir entre amostras independentes geradas pela distribuição α-RLWE daquelas que são geradas pela distribuição uniforme sobre $R_q \times \mathbb{T}$.

A seguir vamos provar que o problema de busca α-RLWE é no mínimo tão seguro quanto o problema de busca RLWE. No contexto da teoria de complexidade computacional, um problema A é *redutível* ao problema B quando um algoritmo capaz de resolver o problema B possui uma sub-rotina que é capaz de resolver o problema A. Isso é denotado por $A \leqslant B$. Portanto, dizer que $A \leqslant B$ significa que o problema B é no mínimo tão difícil de ser resolvido quanto o problema A. O resultado abaixo é fruto de um trabalho conjunto e está disponível em [OdAD+18a]:

Teorema 5.4.1. *Seja α um elemento totalmente positivo em $\mathbb{K}$. O problema de busca RLWE é redutível ao problema de busca α-RLWE.*

Demonstração. Vamos mostrar que, se existe um algoritmo que resolve o problema de busca α-RLWE em tempo polinomial, ele também resolve o problema de busca RLWE. Sejam um segredo $s \in R_q^\vee$, uma distribuição de erros ψ e um conjunto de amostras independentes geradas pela distribuição RLWE $A_{s,\psi}$ dado por

$$(a_i, b_i = a_i s + e_i \mod qR^\vee), \qquad i \in I, \tag{5.5}$$

onde $e_i = \sigma^{-1}(\tilde{e}_i)$, $\tilde{e}_i \leftarrow \psi$ e I é um conjunto finito de índices. Tomando o menor inteiro positivo representante de a_i e b_i em R/qR, podemos reescrever as amostras em (5.5) como

$$(a_i, b_i = a_i s + \sigma^{-1}(\tilde{e}_i)), \qquad i \in I. \tag{5.6}$$

Aplicando o mergulho de Minkowski σ ao conjunto de amostras em (5.6), obtemos

$$(\sigma(a_i), \sigma(a_i)\sigma(s) + \tilde{e}_i), \qquad i \in I. \tag{5.7}$$

Aplicando a transformação linear t_α, definida em (1.51), obtemos

$$((t_\alpha \circ \sigma)(a_i), (t_\alpha \circ \sigma)(a_i)\sigma(s) + t_\alpha(\tilde{e}_i)), \qquad i \in I. \tag{5.8}$$

De (1.52) segue que essas amostras podem ser escritas como

$$(\sigma_\alpha(a_i), \sigma_\alpha(a_i)\sigma(s) + t_\alpha(\tilde{e}_i)), \qquad i \in I, \tag{5.9}$$

e, aplicando σ_α^{-1},

$$\left(a_i,\ a_i(\sigma_\alpha^{-1}\circ\sigma)(s)+\sigma_\alpha^{-1}(t_\alpha(\tilde{e_i}))\right), \qquad i\in I. \tag{5.10}$$

Supondo que existe um algoritmo que resolve o problema α-RLWE, este pode ser utilizado para encontrar $\tilde{s}=(\sigma_\alpha^{-1}\circ\sigma)(s)$ a partir das amostras em (5.10), já que o erro acima foi gerado como imagem inversa por σ_α^{-1}. Assim, podemos obter s aplicando σ_α e σ^{-1} sucessivamente a $\tilde{s}$, isto é,

$$s=(\sigma^{-1}\circ\sigma_\alpha)(\tilde{s}). \tag{5.11}$$

Portanto, tendo um algoritmo que resolve α-RLWE é possível descobrir o segredo s associado às amostras em (5.5). Isso soluciona o problema de busca RLWE. □

Em [OdAD+18a] é demonstrado também que o problema de decisão RLWE é redutível ao problema de decisão α-RLWE e é dada uma aplicação do conceito de α-RLWE utilizando reticulados $\mathbb{Z}^n$.

5.5 Fragilidades do RLWE

Apesar de existirem teoremas que garantem a dificuldade de resolver os problemas LWE, RLWE, PLWE, SIS e RSIS, há certas instâncias, ou seja, escolhas de parâmetros, que podem produzir esquemas criptográficos inseguros e rápidos de serem quebrados. Os problemas RLWE e PLWE foram propostos como uma alternativa ao problema LWE com a justificativa de serem mais eficientes. No entanto, as estruturas algébricas que dão essa eficiência podem também deixá-los mais suscetíveis a ataques. Nesta seção, trazemos um compacto resumo sobre os ataques que têm sido feitos contra o RLWE recentemente, visando perspectivas futuras em nosso trabalho conjunto sobre este tópico.

Lembremos que o problema RLWE (dual ou não dual) depende de um corpo de números $\mathbb{K}$ de grau n, de uma distribuição de erros ψ e de um módulo q. Não se há muito estudo sobre quais parâmetros devem ser recomendados para fins práticos. Geralmente se utiliza o módulo q como sendo um número primo que se decompõe totalmente em $\mathbb{K}$ e a distribuição ψ como sendo a gaussiana discreta. Em [LP11] se recomenda a utilização de um módulo q que seja suficiente grande em relação a n de modo que a distribuição gaussiana discreta se aproxime da distribuição gaussiana contínua com mesmo desvio padrão. É comum ainda utilizar-se $\mathbb{K}$ como sendo um corpo ciclotômico da forma $\mathbb{Q}(\zeta_{2^k})$ ou $\mathbb{Q}(\zeta_p)$ (p primo). No entanto, em [BCLvV16] é sugerido, no contexto do NTRU, a substituição desses corpos por outros que não sejam galoisianos, pois o autor pondera que os ciclotômicos são mais sujeitos a ataques. Como alternativa, em [BCLvV16] é proposta a utilização de corpos de números $\mathbb{K}\simeq\mathbb{Q}[x]/\langle x^p-x-1\rangle$, com p primo, que não são galoisianos e têm o maior grupo de Galois possível, o grupo de permutações S_p.

Alguns artigos já têm mencionado algumas instâncias ligadas à escolha de parâmetros do RLWE que são frágeis, ou seja, quebráveis em tempo curto. Em [EHL14] é mostrado que as instâncias do problema RLWE com parâmetros satisfazendo os seis itens a seguir são quebráveis, considerando $\mathbb{K} = \mathbb{Q}(\beta)$ um corpo de números de grau n, $f(x)$ o polinômio minimal de β e q um número inteiro positivo:

1. O ideal $q\mathcal{O}_{\mathbb{K}}$ se decompõe completamente e q não divide $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\beta]]$.
2. A extensão de corpos $\mathbb{K}/\mathbb{Q}$ é galoisiana.
3. O corpo de números $\mathbb{K}$ é *monogênico*, isto é, existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$, e $f'(\alpha) \mod q$ pequeno.
4. A transformação entre o mergulho de Minkowski de $\mathbb{K}$ e a representação da base de potências de $\mathbb{K}$ é representada por uma matriz ortogonal.
5. $f(1) \equiv 0 \mod q$
6. O módulo q é suficientemente grande em relação a n.

Os itens 1 e 2 garantem que o problema de busca RLWE pode ser reduzido para o problema de decisão, os itens 3 e 4 transformam o RLWE em um problema PLWE e os itens 5 e 6 atacam o PLWE. Assim, é possível quebrar uma instância do problema RLWE nas condições acima ao transferi-la para uma instância do problema PLWE atacável. A redução do problema RLWE para o PLWE deve-se principalmente à ocorrência do item 3, que garante que o anel de inteiros do corpo de números $\mathbb{K}$ pode ser visto como $\mathbb{Z}[x]/\langle g(x)\rangle$, em que $g(x)$ é o polinômio minimal de α. Em [ELOS15] é proposto um ataque ao RLWE nas mesmas condições acima, mas suprimindo o item 4, o qual funciona com alta probabilidade. Além disso, corpos de números da forma $\mathbb{Q}[x]/\langle x^n + q - 1\rangle$ (q primo satisfazendo $f(1) \equiv 0 \mod q$) são apresentados em [ELOS15] como uma família de corpos de números que produzem instâncias do RLWE provavelmente fracas. Em [ELOS15] também é mostrado que os corpos ciclotômicos são imunes ao ataque proposto.

Em [CLS17] é proposto outro ataque ao problema RLWE, o qual depende da existência de um homomorfismo $\rho : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{F}$, em que $\mathbb{K}$ é um corpo de números e $\mathbb{F}$ é um corpo finito pequeno. Se ρ existe, então o problema de decisão RLWE pode ser resolvido em quatro passos com complexidade $O(nq^2)$ [CLS17, Seção 2.8]. Em especial, o ataque ocorre se o módulo q é um número primo com grau residual igual a 2 abaixo de um ideal primo $\mathfrak{Q}$ no corpo de números $\mathbb{K}$ e a aplicação $\rho : \mathcal{O}_{\mathbb{K}}/(q) \longrightarrow \mathcal{O}_{\mathbb{K}}/\mathfrak{Q}$ satisfaz a condição de que a probabilidade de $\rho(e)$ pertencer ao subcorpo $\mathbb{F}_q$ de $\mathbb{F}_{q^2}$ é computacionalmente distinguível de $1/q$, em que $e \in \mathcal{O}_{\mathbb{K}}/(q)$ é amostrado pela distribuição RLWE discreta. Na Tabela 1 de [CLS17] são apresentados exemplos de instâncias RLWE que sofrem esse ataque em tempo curto. Por exemplo, se $n = 144$ e $q = 953$, o problema é quebrado em menos de 115 minutos. Também em [CLS17] é apresentada uma família infinita de instâncias RLWE

que são vulneráveis a ataques. Essas instâncias consideram $\mathbb{K}/\mathbb{Q}$ uma extensão galoisiana, $p > 2$ um número primo, $d > 1$ um número inteiro livre de quadrados coprimo com p satisfazendo $d \equiv 2, 3 \ (mod\ 4)$ e $q > 2$ um número primo tal que $q \equiv 1 \ (mod\ p)$ e inerte em $\mathbb{Q}(\sqrt{d})$. Porém, é provado que corpos ciclotômicos da forma $\mathbb{Q}(\zeta_{2^k})$ com um módulo q não ramificado são seguros contra esses ataques, apesar do problema RLWE não dual ser equivalente ao PLWE para esses corpos [CLS17, Lema 1].

CAPÍTULO 6

Reticulado logarítmico

As unidades do anel de inteiros de um corpo de números formam um subgrupo multiplicativo desse anel. Segundo o Teorema das Unidades de Dirichlet, esse subgrupo possui um conjunto de geradores. Utilizando os $\mathbb{Q}$-monomorfismos do corpo e a função logarítmica, é possível definir o mergulho logarítmico e obter o reticulado logarítmico, que é a imagem do subgrupo das unidades do anel de inteiros por esse mergulho. Tal reticulado não tem posto completo no espaço euclidiano de dimensão igual ao grau do corpo, mas está contido num determinado subespaço. Os reticulados logarítmicos têm sido estudados visando aplicações tanto em códigos quanto em criptografia. Em [CLB16, CLB18] é possível ver a dependência da capacidade de canais de desvanecimento em bloco com o raio de cobertura do reticulado logarítmico. Em [CDPR16] é mostrado que o reticulado logarítmico é eficientemente decodificável quando o corpo é ciclotômico de ordem igual a uma potência de primo, o que pode ser utilizado para atacar problemas em criptografia baseados no Problema do Ideal Principal. Também em [CDPR16] é dado um limitante superior para o raio de cobertura na norma infinito do reticulado logarítmico associado a corpos ciclotômicos de ordem igual a uma potência de primo, com alta probabilidade. Generalizando esse trabalho, daremos uma cota superior determinada para o reticulado logarítmico de qualquer corpo ciclotômico. O cálculo desse limitante é o assunto central da Seção 6.3, onde também apresentamos a realização do reticulado hexagonal como reticulado logarítmico associado ao corpo ciclotômico $\mathbb{Q}(\zeta_7)$. Antes, na Seção 6.1, definimos os conceitos de unidade, mergulho logarítmico, regulador e reticulado logarítmico e enunciamos o Teorema das Unidades de Dirichlet. Na Seção 6.2, enunciamos resultados sobre unidades associadas a corpos ciclotômicos. As principais referências bibliográficas utilizadas aqui são os artigos mencionados acima e também [ST02, Was95].

6.1 O Teorema das Unidades de Dirichlet e o reticulado logarítmico

Se R é um anel comutativo com elemento neutro multiplicativo 1, diz-se que um elemento $u \in R$ é uma *unidade* (ou um *elemento invertível*) em R se existe $u' \in R$, chamado *inverso* de u, tal que $uu' = 1$. É um simples fato algébrico que um ideal I de R possui uma unidade se, e somente se, $I = R$. O conjunto de todas as unidades em R, denotado por R^*, constitui um grupo multiplicativo chamado *grupo das unidades de* R. Considerando $R = \mathcal{O}_\mathbb{K}$ o anel de inteiros de um corpo de números $\mathbb{K}$ de grau n, o grupo das unidades desse anel é formado por todos os elementos $u \in \mathcal{O}_\mathbb{K}$ tais que $|N_\mathbb{K}(u)| = 1$ [Sam70, Seção 4.4, Proposição 1].

Exemplo 6.1.1. *[ST02, Proposição 4.2] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, em que d é negativo e livre de quadrados. Assim, o grupo das unidades do anel de inteiros de $\mathbb{K}$ é:*

- $\mathcal{O}_\mathbb{K}^* = \{\pm 1, \pm i\}$, *se* $d = -1$, *em que* $i = \sqrt{-1}$.
- $\mathcal{O}_\mathbb{K}^* = \{\pm 1, \pm\omega, \pm\omega^2\}$, *se* $d = -3$, *em que* $\omega = e^{2\pi i/3}$.
- $\mathcal{O}_\mathbb{K}^* = \{\pm 1\}$, *se* $d < 0$, $d \neq -1$ *e* $d \neq -3$.

Daqui em diante nesta seção, seja $\mathbb{K}$ um corpo de números com assinatura (r_1, r_2) e anel de inteiros $\mathcal{O}_\mathbb{K}$. Denotemos por $\sigma_1, \ldots, \sigma_{r_1}$ os monomorfismos reais e por $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ os monomorfismos complexos não conjugados entre si associados a $\mathbb{K}$.

Definição 6.1.1. *A função* $Log : \mathbb{K}^* \longrightarrow \mathbb{R}^{r_1+r_2}$ *definida por*

$$Log(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, \log|\sigma_{r_1+1}(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|), \tag{6.1}$$

para todo $x \in \mathbb{K}^*$, *é chamada* mergulho logarítmico *de* $\mathbb{K}$, *em que* log *denota a função logarítmica com base* 10 *em* $\mathbb{R}$.[1]

O mergulho logarítmico é um homomorfismo entre os grupos $(\mathbb{K}^*, .)$ e $(\mathbb{R}^{r_1+r_2}, +)$, pois vale a propriedade

$$Log(xy) = Log(x) + Log(y), \qquad \forall x, y \in \mathcal{O}_\mathbb{K}^*. \tag{6.2}$$

A restrição do homomorfismo Log ao grupo das unidades do anel de inteiros de $\mathbb{K}$,

$$Log : \mathcal{O}_\mathbb{K}^* \longrightarrow \mathbb{R}^{r_1+r_2}, \tag{6.3}$$

tem núcleo W igual ao conjunto das raízes da unidade pertencentes a $\mathcal{O}_\mathbb{K}^*$. Assim, W constitui um grupo cíclico multiplicativo finito de ordem par [ST02, Lema B.1]. Além disso, a imagem $Log(\mathcal{O}_\mathbb{K}^*)$ é um reticulado em $\mathbb{R}^{r_1+r_2}$.

[1] Se y é um número complexo, a notação $|y|$ se refere à norma complexa de y, isto é, $|y| = \sqrt{\Re(y)^2 + \Im(y)^2}$.

Definição 6.1.2. *O reticulado* $Log(\mathcal{O}_{\mathbb{K}}^*) \subset \mathbb{R}^{r_1+r_2}$ *é chamado de* reticulado logarítmico *associado a* $\mathbb{K}$.

O próximo resultado é o teorema que dá nome a esta seção e que caracteriza o grupo das unidades do anel de inteiros de um corpo de números em função de algumas "unidades básicas", determinando, consequentemente, o posto do seu reticulado logarítmico. A demonstração deste teorema pode ser encontrada em [Sam70, Seção 4.4, Teorema 1] e [ST02, Teorema B.6].

Teorema 6.1.1 (Teorema das Unidades de Dirichlet)**.** *Seja* $\mathbb{K}$ *um corpo de números com assinatura* (r_1, r_2)*. Denotemos por* W *o grupo das raízes da unidade contidas em* $\mathbb{K}$ *e consideremos* $r = r_1 + r_2 - 1$*. Assim, o grupo aditivo* $Log(\mathcal{O}_{\mathbb{K}}^*)$ *é isomorfo a* $\mathbb{Z}^r$*, ou seja, o grupo das unidades de* $\mathbb{K}$ *é isomorfo a* $W \times \mathbb{Z}^r$*.*

Uma consequência imediata do Teorema 6.1.1 indica que em cada corpo de números $\mathbb{K}$ com assinatura (r_1, r_2) existem $r = r_1 + r_2 - 1$ unidades u_i, $1 \leqslant i \leqslant r$, tais que toda unidade $u \in \mathcal{O}_{\mathbb{K}}^*$ pode ser escrita de modo único como

$$u = w u_1^{e_1} u_2^{e_2} \dots u_r^{e_r}, \qquad w \in W, e_i \in \mathbb{Z} \ (1 \leqslant i \leqslant r). \tag{6.4}$$

As unidades u_i, $1 \leqslant i \leqslant r$, são chamadas de *unidades fundamentais* de $\mathbb{K}$.

Definição 6.1.3. *Se* $u_1, \dots, u_r$ *constitui um sistema de unidades fundamentais de* $\mathbb{K}$*, o valor absoluto do determinante da matriz* $(\log(\sigma_i(u_j)))_{r\times r}$ *é chamado de* regulador *de* $\mathbb{K}$*.*

O Teorema 6.1.1 também garante que o reticulado logarítmico $\Lambda = Log(\mathcal{O}_{\mathbb{K}}^*)$ tem posto $r = r_1 + r_2 - 1$ em $\mathbb{R}^{r_1+r_2}$. Além disso, é possível ver que Λ está contido no subespaço de $\mathbb{R}^{r_1+r_2}$ que é ortogonal ao vetor unitário $(1, 1, \dots, 1)$, e Λ é de posto completo nesse subespaço. O Exemplo 6.1.4 pode servir como dica para a demonstração desse fato.

Exemplo 6.1.2. *Seja* $\mathbb{K}$ *um corpo quadrático imaginário, ou seja, com assinatura* $(0, 1)$*. Segundo o Teorema 6.1.1, o grupo das unidades de* $\mathbb{K}$ *é isomorfo ao conjunto das raízes da unidade de* $\mathbb{K}$*, já que* $r = r_1 + r_2 - 1 = 0$*. Isso justifica o fato de que, no Exemplo 6.1.1, as unidades constituem um conjunto finito em cada um dos casos considerados.*

Exemplo 6.1.3. *Consideremos o corpo quadrático real* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$*, o qual tem assinatura* $(2, 0)$ *e anel de inteiros* $\mathbb{Z}[\sqrt{3}]$*, uma vez que* $3 \not\equiv 1 \pmod 4$*. O grupo das unidades de* $\mathbb{K}$ *é isomorfo a* $\mathbb{Z}_2 \times \mathbb{Z}$*, já que* $r = r_1 + r_2 - 1 = 1$ *e* $W = \{\pm 1\}$*, pois* $\mathbb{K}$ *é totalmente real e a imagem das raízes da unidade pelo mergulho de Minkowski está contida no círculo unitário. É possível provar que* $2 + \sqrt{3}$ *é uma unidade fundamental de* $\mathbb{K}$ *[Sam70, Seção 4.6]. Assim,* $a + b\sqrt{3} \in \mathcal{O}_{\mathbb{K}}^*$ *se, e somente se,* $a + b\sqrt{3} = \pm(2 + \sqrt{3})^e$*,* $e \in \mathbb{Z}$*, ou ainda*

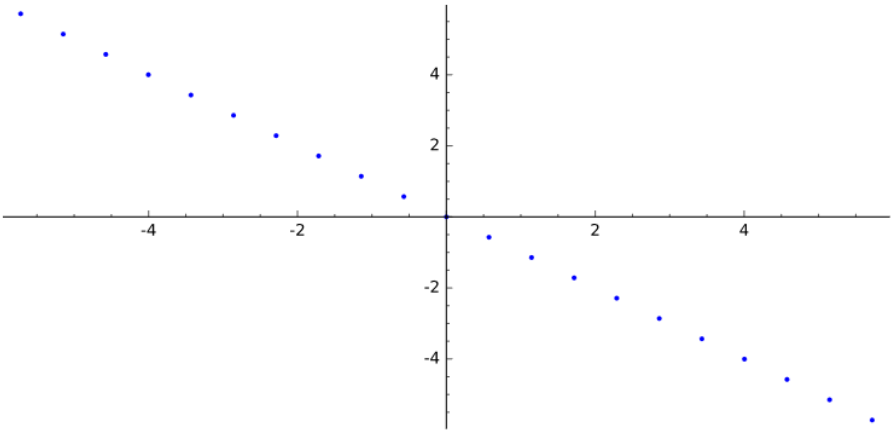
$$\pm 1 = N_{\mathbb{K}}(a + b\sqrt{3}) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2. \tag{6.5}$$

O mergulho logarítmico $Log : \mathcal{O}_{\mathbb{K}}^* \longrightarrow \mathbb{R}^2$ *pode ser definido da seguinte forma:*

$$\begin{aligned} Log(\pm(2+\sqrt{3})^e) &= \left(\log|\sigma_1(\pm(2+\sqrt{3})^e)|, \log|\sigma_2(\pm(2-\sqrt{3})^e)|\right) = \\ &= \left(e\log(2+\sqrt{3}), e\log(2-\sqrt{3})\right), \ e \in \mathbb{Z}. \end{aligned} \tag{6.6}$$

O reticulado $Log(\mathcal{O}_{\mathbb{K}}^*)$ *de dimensão* $r = 1$ *em* $\mathbb{R}^2$ *está representado na Figura 7. O regulador de* $\mathbb{K}$ *é dado por* $|\det(\log(\sigma_1(2+\sqrt{3})))_{1\times 1}| = \log(2+\sqrt{3})$.

Figura 7 – Reticulado logarítmico associado a $\mathbb{K} = \mathbb{Q}(\sqrt{3})$



Exemplo 6.1.4. *Em geral, se* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d > 1$, *é um corpo quadrático real, então* $\mathcal{O}_{\mathbb{K}}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}$ *e a imagem do reticulado logarítmico* $Log(\mathcal{O}_{\mathbb{K}}^*)$ *é isomorfa a* $\mathbb{Z}$ *em* $\mathbb{R}^2$. *Especificamente,* $Log(\mathcal{O}_{\mathbb{K}}^*)$ *está contido no subespaço de* $\mathbb{R}^2$ *que é ortogonal ao vetor unitário* $(1,1)$. *De fato, se* u_1 *é uma unidade fundamental de* $\mathbb{K}$ *então, para qualquer* $e \in \mathbb{Z}$,

$$Log(\pm u^e) = e \cdot (\log(|\sigma_1(u)|), \log|\sigma_2(u)|), \tag{6.7}$$

e o vetor à direita satisfaz

$$\langle(\log(|\sigma_1(u)|), \log|\sigma_2(u)|); (1,1)\rangle = \log|\sigma_1(u)\sigma_2(u)| = \log|N_{\mathbb{K}}(u)| = \log 1 = 0. \tag{6.8}$$

Como exemplo, as unidades fundamentais de $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ *e* $\mathbb{Q}(\sqrt{7})$ *são, respectivamente,* $1+\sqrt{2}$, $(1+\sqrt{5})/2$ *e* $8+3\sqrt{7}$. *Um algoritmo para obter as unidades fundamentais de* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d > 1$, *é apresentado em [Sam70, Seção 4.6].*

6.2 Unidades em corpos ciclotômicos

Em geral, não é fácil explicitar o grupo das unidades de um corpo de números. Nesta seção vamos apresentar sintetizadamente alguns resultados clássicos que envolvem unidades em corpos ciclotômicos $\mathbb{Q}(\zeta_n)$. Uma discussão mais completa sobre o assunto pode ser encontrada em [Was95], especialmente nos capítulos 1, 4 e 8.

Primeiramente, consideremos o corpo ciclotômico $\mathbb{Q}(\zeta_p)$, com p primo. Um subconjunto das unidades desse corpo é formado pelos números $(\zeta_p^r - 1)/(\zeta_p^s - 1)$, sendo r e

s números inteiros tais que $mdc(p, rs) = 1$ [Was95, Lema 1.3]. Há uma interessante relação entre as unidades desse corpo e as unidades do seu subcorpo maximal real: se u é uma unidade em $\mathbb{Z}[\zeta_p]$, o anel de inteiros de $\mathbb{Q}[\zeta_p]$, então existe uma unidade $u_1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ tal que $u = \zeta_p^r u_1$, para algum $r \in \mathbb{Z}$ [Was95, Proposição 1.5].

Em geral, podemos considerar o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_n)$ para qualquer número inteiro positivo n. Neste caso, se W denota o grupo das raízes da unidade de $\mathbb{K}$ e se $\mathbb{K}^+$ denota o subcorpo maximal real $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então o índice $[\mathcal{O}_{\mathbb{K}}^* : W\mathcal{O}_{\mathbb{K}^+}^*]$ é igual a 1, se n é potência de um número primo, ou igual a 2, se n é divisível por pelo menos dois números primos distintos [Was95, Corolário 4.13]. Tal qual acima, este último fato nos mostra que conhecer as unidades reais de um corpo ciclotômico é quase suficiente para conhecer todas as outras.

A seguir vamos definir o *subgrupo das unidades ciclotômicas* de $\mathbb{K} = \mathbb{Q}(\zeta_n)$, que não deve ser confundido com $\mathcal{O}_{\mathbb{K}}^*$. Consideremos o subgrupo multiplicativo de $\mathbb{K}^*$ dado por

$$V_n = \langle \pm\zeta_n, 1 - \zeta_n^e \ : \ 1 < e < n \rangle. \tag{6.9}$$

Definição 6.2.1. *O grupo $C_n = V_n \cap \mathcal{O}_{\mathbb{K}}^*$ é chamado de* subgrupo das unidades ciclotômicas *de $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Observação 6.2.1. *Em geral, podemos definir o subgrupo das unidades ciclotômicas de qualquer corpo de números abeliano $\mathbb{L}$ como sendo $C_{\mathbb{L}} = \mathcal{O}_{\mathbb{L}}^* \cap C_n$, sendo n o condutor de $\mathbb{L}$. Particularmente essa definição vale para o subcorpo maximal real $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

Se $n = p^m$ para algum número primo p e $m \geqslant 1$, então o subgrupo das unidades ciclotômicas $C_{\mathbb{L}}$ de $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ tem índice finito em $\mathcal{O}_{\mathbb{L}}^*$ [Was95, Teorema 8.2], o que significa que o reticulado $Log(C_{\mathbb{L}})$ é um sub-reticulado do reticulado logarítmico $Log(\mathcal{O}_{\mathbb{L}}^*)$ de mesmo posto. O resultado a seguir nos dá um conjunto de geradores do subgrupo das unidades ciclotômicas de $\mathbb{L}$ e de $\mathbb{Q}(\zeta_n)$:

Proposição 6.2.1 ([Was95], Lema 8.1)**.** *Sejam $n = p^m$, com p primo e $m \geqslant 1$, $\mathbb{K} = \mathbb{Q}(\zeta_n)$ e $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. O subgrupo das unidades ciclotômicas $C_{\mathbb{L}}$ é gerado por -1 e pelas unidades*

$$\xi_a = \zeta_n^{(1-a)/2} \frac{1 - \zeta_n^a}{1 - \zeta_n}, \qquad 1 < a < n/2, \ mdc(a, p) = 1. \tag{6.10}$$

Por sua vez, as unidades ciclotômicas de $\mathbb{K}$ são geradas por ζ_n e por $C_{\mathbb{L}}$.

Se n não é uma potência de primo, é preciso tomar mais cuidado, já que nesse caso nem toda unidade ciclotômica é produto de raízes da unidade por números da forma $(1 - \zeta_n^r)/(1 - \zeta_n)$, conforme comentado na observação após o Lema 8.1 de [Was95]. A proposição a seguir trata desse caso geral e nos apresenta um outro subgrupo contido no subgrupo das unidades ciclotômicas que tem índice finito:

Proposição 6.2.2 ([Was95], Teorema 8.3)**.** *Sejam $n = p_1^{e_1} \dots p_s^{e_s}$, com p_i primos distintos e $e_i \geqslant 1$ $(1 \leqslant i \leqslant s)$[2], $\mathbb{K} = \mathbb{Q}(\zeta_n)$ e $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Para cada conjunto I pertencente a $\Gamma = \{I \subsetneq \{1, \dots, s\}\}$, seja $n_I = \prod_{i \in I} p_i^{e_i}$. Se a é um número inteiro tal que $1 < a < n/2$ e $mdc(a, n) = 1$, então os números*

$$\xi_a = \prod_{i \in I} \zeta_n^{\frac{n_I(1-a)}{2}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right) \tag{6.11}$$

formam um conjunto de unidades multiplicativamente independentes de $\mathbb{L}$. Além disso, o subgrupo

$$C = \langle -1, \xi_a \ : \ 1 < a < n/2, \ mdc(a, n) = 1 \rangle, \tag{6.12}$$

tem índice não nulo em $\mathcal{O}_{\mathbb{L}}^*$.

Observação 6.2.2. *O fato mencionado na Proposição 6.2.2 de que o índice de C em $\mathcal{O}_{\mathbb{L}}^*$ é não nulo indica que $Log(C)$ é um sub-reticulado de $Log(\mathcal{O}_{\mathbb{L}}^*)$ de mesmo posto.*

6.3 Raio de cobertura do reticulado logarítmico em corpos ciclotômicos

Nesta seção, apresentamos um limitante superior para o raio de cobertura do reticulado logarítmico obtido via corpos ciclotômicos $\mathbb{Q}(\zeta_n)$, para qualquer $n \in \mathbb{Z}$. Em [CDPR16, Corolário 6.4] é mostrado que, com *alta probabilidade*, o raio de cobertura na *norma infinito* do reticulado logarítmico associado ao corpo $\mathbb{Q}(\zeta_n)$ é da ordem de $\sqrt{n \log(n)}$, em que n é uma *potência de primo*. Aqui, nosso objetivo é demonstrar o teorema a seguir:

Teorema 6.3.1. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_n)$, com n um inteiro qualquer[3]. O raio de cobertura $\mu(Log(\mathcal{O}_{\mathbb{K}}^*))$ associado ao corpo $\mathbb{K}$ satisfaz*

$$\mu(Log(\mathcal{O}_{\mathbb{K}}^*)) \leqslant K(2^s - 1)n \tag{6.13}$$

em que K é uma constante positiva independente de n e s é o número de primos distintos presentes na fatoração de n.

Em comparação com [CDPR16, Corolário 6.4] vemos que o Teorema 6.3.1, além de valer para qualquer n (não só potência de primo, ou seja, não só para $s = 1$), também retira a condição de alta probabilidade (é empírico). Se $n = p^e$, para algum número primo p e um número inteiro $e \geqslant 1$, o raio de cobertura na norma infinito apresentada no artigo mencionado é da ordem de $\sqrt{nlog(n)}$. Como $\|(x_1, \dots, x_m)\| \leqslant \sqrt{m}\|(x_1, \dots, x_m)\|_\infty$, segue que esse raio de cobertura na norma euclidiana é da ordem de $\sqrt{\varphi(n) n \log(n)}$, enquanto

[2] Notemos que é possível considerar $n \not\equiv 2 \ (mod\ 4)$, uma vez que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

[3] Podemos supor $n \not\equiv 2 \ (mod\ 4)$ por motivo semelhante ao já comentado na Seção 6.2.

o limitante do Teorema 6.3.1 é da ordem de n. Notemos que, à medida que p cresce, o limitante n é melhor do que o limitante $\sqrt{\varphi(n)n\log(n)}$. De fato,

$$\varphi(n)\log(n) = (p-1)p^{e-1}e\log(p) > p^e = n \iff \left(e - \frac{e}{p}\right)\log(p) > 1 \tag{6.14}$$

e a última desigualdade ocorre quando $p \longrightarrow \infty$ (com $e = 1$ a desigualdade passa a valer a partir de $p = 13$). Nesse caso, (6.14) garante que $\varphi(n)\log(n) > n$, donde segue que $\sqrt{\varphi(n)n\log(n)} > n$. Portanto, o limitante provado no Teorema 6.3.1 é melhor do que o obtido em [CDPR16] à medida que p cresce.

Para provar o Teorema 6.3.1 precisamos de alguns lemas que enunciamos e demonstramos a seguir. No resto desta seção, seja $\mathbb{K} = \mathbb{Q}(\zeta_n)$, em que $n = p_1^{e_1}\dots p_s^{e_s}$ ($n \not\equiv 2 \pmod 4$), com p_i primos distintos e $e_i \geqslant 1$ ($1 \leqslant i \leqslant s$). Consideremos ainda $\Gamma = \{I \subsetneq \{1,\dots,s\}\}$.

Lema 6.3.1. *Para qualquer número inteiro $m \geqslant 1$,*

$$\sum_{k=1}^{\lfloor m/2\rfloor} \log^2\left(2\text{sen}\left(\frac{\pi k}{m}\right)\right) \leqslant K_1 m, \tag{6.15}$$

onde K_1 é uma constante positiva independente de m.

Demonstração. [4] Consideremos a função $f : [0,1/2] \longrightarrow \mathbb{R}$ dada por $f(x) = \log^2(2\text{sen}(\pi x))$. Se $x \in [1/6,1/2]$, como sen é uma função crescente nesse intervalo, então

$$1 = 2\text{sen}(\pi/6) \leqslant 2\text{sen}(\pi x) \leqslant 2\text{sen}(\pi/2) = 2, \tag{6.16}$$

donde segue que

$$x \in [1/6,1/2] \Longrightarrow 0 \leqslant f(x) \leqslant \log^2(2) < \log(2). \tag{6.17}$$

Por sua vez, se $x \in [0,1/6]$, então $2x \leqslant \text{sen}(\pi x)$ (basta observar o gráfico dessas duas funções para verificar a desigualdade) e, como log é uma função crescente, segue que

$$x \in [0,1/6] \Longrightarrow \log(2x) < \log(\text{sen}(\pi x)) < 0 \Longrightarrow f(x) < \log^2(2x). \tag{6.18}$$

Abrindo o somatório de (6.15) em duas parcelas

$$\sum_{k=1}^{\lfloor m/2\rfloor} \log^2\left(2\text{sen}\left(\frac{\pi k}{m}\right)\right) = \sum_{k=1}^{\lfloor m/6\rfloor} f(k/m) + \sum_{k=\lfloor m/6\rfloor+1}^{\lfloor m/2\rfloor} f(k/m) \tag{6.19}$$

concluímos, de (6.17), que a segunda parcela é limitada superiormente por $\log(2)$ e, de (6.18), que a primeira parcela satisfaz

$$\sum_{i=1}^{\lfloor m/6\rfloor} f(k/m) \leqslant \sum_{i=1}^{\lfloor m/6\rfloor} \log^2(4k/m) \leqslant m\int_0^{1/6} \log^2(4x)dx. \tag{6.20}$$

[4] A demonstração deste lema está contida na demonstração do Lema 6.7 de [CDPR16].

Fazendo $\tilde{K} = \int_0^{1/6} \log^2(4x)dx$, vemos que

$$\tilde{K} = \int_0^{1/6} \log^2(4x)dx = \frac{1}{4}\int_0^{2/3} \log^2(x)dx = \frac{1}{6}\left(\log^2\left(\frac{2}{3}\right) - 2\log\left(\frac{2}{3}\right) + 2\right) \tag{6.21}$$

é uma constante positiva independente de m. Tomando $K_1 = \tilde{K} + \log(2)$, obtemos de (6.19) que

$$\sum_{k=1}^{\lfloor m/2 \rfloor} \log^2\left(2\text{sen}\left(\frac{\pi k}{m}\right)\right) \leqslant \tilde{K}m + \log(2) \leqslant m(\tilde{K} + \log(2)) = K_1 m \tag{6.22}$$

como queríamos demonstrar. □

Lema 6.3.2. *Seja a um número inteiro tal que $1 \leqslant a < n/2$ e $mdc(a,n) = 1$. Se $I \in \Gamma$, então*

$$\left\| Log\left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\| \leqslant K_2\sqrt{n} \tag{6.23}$$

em que K_2 é uma constante independente de n.

Demonstração. Sejam $\sigma_1, \ldots, \sigma_{\varphi(n)/2}$ os monomorfismos de $\mathbb{K}$ tais que $\sigma_i \neq \overline{\sigma_j}$, para $1 \leqslant i < j \leqslant \varphi(n)/2$. A definição do mergulho logarítmico Log em $\mathbb{K}$ indica que

$$\left\| Log\left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\|^2 = \sum_{k=1}^{\varphi(n)/2} \log^2\left|\sigma_k\left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{-an_I}{2}}\right)\right| = \sum_{k\in G} \log^2\left|\zeta_n^{\frac{-akn_I}{2}} - \zeta_n^{\frac{-akn_I}{2}}\right|, \tag{6.24}$$

onde $G = \{k \in \mathbb{Z} : 1 \leqslant k < n/2, gcd(k,n) = 1\} = \mathbb{Z}_n^*/\{\pm 1\} \simeq Gal(\mathbb{L}/\mathbb{Q})$, sendo $\mathbb{L} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ o subcorpo maximal real de $\mathbb{K}$. Como

$$\zeta_n^{-\frac{akn_I}{2}} - \zeta_n^{\frac{akn_I}{2}} = -2i\text{sen}\left(\frac{\pi akn_I}{n}\right) \tag{6.25}$$

e, definindo $m_I = n/n_I$, de (6.24), segue que

$$\left\| Log\left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\|^2 = \sum_{k\in G} \log^2\left|2\text{sen}\left(\frac{\pi ak}{m_I}\right)\right| = \sum_{k\in G} \log^2\left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \tag{6.26}$$

já que $\{ka : k \in G\} = \{k : k \in G\}$. Como $m_I > 1$, segue que $G \subset \left\{k \in \mathbb{Z} : 1 \leqslant k \leqslant \left\lfloor \frac{n}{2} \right\rfloor\right\}$ e $\left\lfloor \frac{n}{2} \right\rfloor \leqslant \frac{n}{2} \leqslant 2m_I\left\lceil \frac{n_I}{4} \right\rceil$. Logo, devido à igualdade $\text{sen}\left(\frac{\pi k}{m_I}\right) = \text{sen}\left(\frac{\pi(k+2m_I)}{m_I}\right)$, temos

$$\left\| Log\left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\|^2 \leqslant \sum_{\substack{k=1 \\ gcd(k,n)=1}}^{\lfloor n/2 \rfloor} \log^2\left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant \left\lceil \frac{n_I}{4} \right\rceil \sum_{k=1}^{2m_I} \log^2\left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right|. \tag{6.27}$$

O Lema 6.3.1 garante que existe uma constante positiva K_1 independente de m_I tal que

$$\sum_{k=1}^{\lfloor m_I/2 \rfloor} \log^2\left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant K_1 m_I. \tag{6.28}$$

Consequentemente, como $\text{sen}(x) = \text{sen}(\pi - x)$, segue que

$$\sum_{k=\lfloor m_I/2\rfloor+1}^{m_I-1} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| = \sum_{k=\lfloor m_I/2\rfloor+1}^{m_I-1} \log^2 \left|2\text{sen}\left(\frac{\pi(m_I-k)}{m_I}\right)\right|$$

$$\leqslant \sum_{k=1}^{\lfloor m_I/2\rfloor} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant K_1 m_I \tag{6.29}$$

(na penúltima desigualdade foi utilizada uma mudança de variável). Analogamente, como $\text{sen}(x) = -\text{sen}(x - \pi)$, segue que

$$\sum_{k=m_I+1}^{\lfloor 3m_I/2\rfloor} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| = \sum_{k=m_I+1}^{\lfloor 3m_I/2\rfloor} \log^2 \left|2\text{sen}\left(\frac{\pi(k-m_I)}{m_I}\right)\right| \leqslant \sum_{k=1}^{\lfloor m_I/2\rfloor} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant K_1 m_I. \tag{6.30}$$

Da mesma forma, uma vez que $\text{sen}(x) = -\text{sen}(2\pi - x)$, segue que

$$\sum_{k=\lfloor 3m_I/2\rfloor+1}^{2m_I-1} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| = \sum_{k=\lfloor 3m_I/2\rfloor+1}^{2m_I-1} \log^2 \left|2\text{sen}\left(\frac{\pi(2m_I-k)}{m_I}\right)\right|$$

$$\leqslant \sum_{k=1}^{\lfloor m_I/2\rfloor} \log^2 \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant K_1 m_I. \tag{6.31}$$

Substituindo (6.28), (6.29), (6.30) e (6.31) em (6.27), obtemos

$$\left\|Log\left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\|^2 \leqslant \left\lceil \frac{n_I}{4} \right\rceil \sum_{k=1}^{2m_I} \left|2\text{sen}\left(\frac{\pi k}{m_I}\right)\right| \leqslant \left\lceil \frac{n_I}{4} \right\rceil 4K_1 m_I \leqslant 5K_1 n = K_2 n \tag{6.32}$$

em que $K_2 = 5K_1$ é uma constante positiva independente n. □

A seguir, consideremos o subgrupo $C \subset \mathcal{O}_{\mathbb{L}}^*$ definido na Proposição 6.2.2 e o grupo de Galois $G = \{k \in \mathbb{Z} \ : \ 1 \leqslant k < n/2, \ mdc(k,n) = 1\} = \mathbb{Z}_n^*/\{\pm 1\} \simeq Gal(\mathbb{L}/\mathbb{Q})$. No próximo lema vamos calcular a ordem da norma euclidiana do mergulho logarítmico aplicado aos elementos geradores de C:

Lema 6.3.3. *Para cada $a \in G\backslash\{1\}$, vale*

$$\|Log(\xi_a)\| = K_3(2^s - 1)\sqrt{n} \tag{6.33}$$

em que ξ_a é o elemento definido na Proposição 6.2.2 e K_3 é uma constante positiva independente de n.

Demonstração. Primeiro notemos que

$$\xi_a = \prod_{i\in I} \zeta_n^{\frac{n_I(1-a)}{2}} \left(\frac{1-\zeta_n^{an_I}}{1-\zeta_n^{n_I}}\right) = \prod_{i\in I} \left(\frac{\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}}}\right). \tag{6.34}$$

Disso, obtemos

$$\|Log(\xi_a)\| \leqslant \sum_{I\in\Gamma} \left\| Log\left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right)\right\| + \sum_{I\in\Gamma} \left\| Log\left(\zeta_n^{-\frac{n_I}{2}} - \zeta_n^{\frac{n_I}{2}}\right)\right\|. \tag{6.35}$$

Segue do Lema 6.3.2 que

$$\|Log(\xi_a)\| \leqslant 2|\Gamma|K_2\sqrt{n} = K_3(2^s-1)\sqrt{n}, \tag{6.36}$$

onde $K_3 = 2K_2$ é uma constante positiva independente de n. □

Enfim, o Teorema 6.3.1 pode ser demonstrado:

Prova do Teorema 6.3.1. Consideremos o sub-reticulado $Log(C) \subset Log(\mathcal{O}_{\mathbb{K}}^*)$, onde C é o subgrupo definido na Proposição 6.2.2. Notemos que $\{Log(b_a) : a \in G\backslash\{1\}\}$ é uma base de $Log(C)$. Assim, denotando por $\lambda_i(L)$ o i-ésimo mínimo sucessivo de um reticulado L, o Lema 6.3.3 garante que existe uma constante positiva K_3 independente de n tal que

$$\lambda_r(Log(C)) \leqslant ||Log(b_a)|| \leqslant K_3(2^s-1)\sqrt{n}, \tag{6.37}$$

para algum $a \in G\backslash\{1\}$, já que $\{Log(\xi_a) : a \in G\backslash\{1\}\}$ tem $r = \varphi(n)/2 - 1$ vetores linearmente independentes e $\lambda_r(Log(C))$ é o menor ρ tal que $Log(C)$ tem r vetores linearmente independentes de norma no máximo igual a ρ. Devido à Proposição 4.1.2, $\mu(Log(C)) \leqslant \dfrac{\sqrt{n}}{2}\lambda_n(Log(C))$, donde segue que

$$\mu(Log(C)) \leqslant \frac{\sqrt{n}}{2}K_3(2^s-1)\sqrt{n} = Kn(2^s-1) \tag{6.38}$$

em que $K = K_3/2 > 0$. Portanto, como $Log(C)$ é um sub-reticulado de $Log(\mathcal{O}_{\mathbb{K}}^*)$, segue que

$$\mu(Log(\mathcal{O}_{\mathbb{K}}^*))Log(C)) \leqslant K(2^s-1)n, \tag{6.39}$$

concluindo a prova. □

Observação 6.3.1. *Pelas demonstrações feitas nesta seção é possível concluir que a constante K do Teorema 6.3.1 é igual a*

$$K = 5\left(\log(2) + \frac{1}{6}\left(\log^2(2/3) - 2\log(2/3) + 2\right)\right) \simeq 3.49. \tag{6.40}$$

Exemplo 6.3.1. *Consideremos o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_7)$, de grau 6, e o corpo maximal real $\mathbb{L} = \mathbb{Q}(\zeta_7+\zeta_7^{-1})$, de grau $6/2 = 3$. A partir dos resultados da Seção 6.2 concluímos que o reticulado logarítmico $Log(\mathcal{O}_{\mathbb{L}}^*)$ tem posto 2 em $\mathbb{R}^3$. Sua base é a imagem do mergulho logarítmico Log aplicado aos elementos $\xi_2 = \zeta_7^{-1/2}\left(\dfrac{1-\zeta_7^2}{1-\zeta_7}\right)$ e $\xi_3 = \zeta_7^{-1}\left(\dfrac{1-\zeta_7^3}{1-\zeta_7}\right)$. Assim, a matriz geradora do reticulado $Log(\mathcal{O}_{\mathbb{L}}^*)$ é dada por*

$$M = \begin{bmatrix} \log|2\cos(\pi/7)| & \log|2\cos(3\pi/7)| & \log|2\cos(2\pi/7)| \\ \log|1+2\cos(2\pi/7)| & \log|1+2\cos(6\pi/7)| & \log|1+2\cos(4\pi/7)| \end{bmatrix}, \tag{6.41}$$

donde segue que a matriz de Gram de $Log(\mathcal{O}_{\mathbb{L}}^*)$ *é igual a*

$$G = c \begin{bmatrix} 1 & -1/2 \\ -1/2 & 1 \end{bmatrix}, \tag{6.42}$$

em que $c = 1,0509....$ *Portanto,* $Log(\mathcal{O}_{\mathbb{L}}^*)$ *é equivalente ao reticulado hexagonal.*

No Exemplo 6.3.1 obtemos a realização do reticulado hexagonal como um reticulado logarítmico a partir das unidades do anel de inteiros do corpo ciclotômico $\mathbb{Q}(\zeta_7)$. O reticulado hexagonal é conhecido por ser a solução do problema da cobertura esférica em dimensão 2. O problema da cobertura esférica foi descrito na Seção 1.2 e consiste em minimizar o raio de cobertura $\mu(\Lambda)$ de um reticulado n-dimensional Λ com determinante igual a 1. Em dimensões $n = 3, 4, 5$ sabe-se que a melhor cobertura obtida *via reticulados* é realizada pelo reticulado A_n^*. O reticulado A_n^* também é o que produz a melhor solução conhecida até o momento para o problema da cobertura esférica nas dimensões de 6 a 21 (porém, não é provado que não há outros reticulados com cobertura melhor nessas dimensões). Em dimensão 24, o reticulado de Leech é a melhor solução conhecida até o momento. Uma discussão mais detalhada sobre esse assunto pode ser encontrada em [CS98].

Considerações finais e perspectivas futuras

Neste trabalho, apresentamos construções e propriedades de reticulados obtidas por diferentes meios algébricos para diversas aplicações. Em suma, os capítulos deste trabalho perpassaram a construção de versões rotacionadas dos reticulados D_n e $\mathbb{Z}^n$ com diversidade máxima (para todo n) e o estudo de suas distâncias produto mínimas, o cálculo da forma traço $Tr_{\mathbb{K}}(x^2)|_{\mathcal{O}_{\mathbb{K}}}$ para corpos de números cíclicos $\mathbb{K}$ de grau primo ímpar ramificado, um estudo sobre reticulados algébricos bem arredondados, uma análise sobre os avanços recentes em criptografia baseada em reticulados e o cálculo de um limitante superior para o raio de cobertura do reticulado logarítmico $Log(\mathcal{O}^*_{\mathbb{Q}(\zeta_n)})$. A seguir relembramos os tópicos delineados em cada capítulo e colocamos algumas perspectivas futuras relacionadas a cada tópico.

No Capítulo 1, somente definimos os principais conceitos e propriedades envolvendo reticulados e teoria algébrica dos números. No Capítulo 2, resgatamos e construímos versões de D_n e $\mathbb{Z}^n$ com diversidade máxima, para todo n. No caso n ímpar, vimos que o $\mathbb{Z}$-módulo utilizado para obter $\mathbb{Z}^n$ é um ideal. Calculamos a distância produto mínima desses reticulados quando a razão $u = \sigma(x)/x$ é um inteiro algébrico e um dos elementos $1 \pm u$ é uma unidade. Além disso, provamos resultados que consideram situações em que essas hipóteses são válidas. Para trabalhos posteriores temos interesse em pesquisar outras condições e casos em que u é um inteiro algébrico e $1 \pm u$ é uma unidade.

No Capítulo 3, explicitamos a forma traço $Tr_{\mathbb{K}}(x^2)|_{\mathcal{O}_{\mathbb{K}}}$ no caso em que $\mathbb{K}$ é um corpo de números cíclico de grau primo ímpar p cujo ideal $p\mathcal{O}_{\mathbb{K}}$ é ramificado, completando um estudo iniciado em trabalhos anteriores. Estudamos ainda a densidade de centro de alguns reticulados algébricos obtidos através desses corpos. Para o futuro pensamos em buscar novos $\mathbb{Z}$-módulos e ideais nesses corpos, e também em corpos cujo grau é não ramificado, cujas imagens pelo mergulho de Minkowski sejam reticulados densos. Além disso, pretendemos estudar corpos de números abelianos s de grau p^2 ímpar.

No Capítulo 4, definimos reticulados bem arredondados e vimos alguns resultados recentes relacionados a esse tópico. Tratamos do teorema de [FP12] cujo resultado garante que o reticulado algébrico obtido do anel de inteiros de um corpo de números $\mathbb{K}$ via o mergulho de Minkowski é bem arredondado se, e somente se, $\mathbb{K}$ é um corpo ciclotômico. Ressalvamos que esse resultado é verdadeiro quando $\mathbb{K}$ é totalmente real ou

totalmente complexo mas pode não ser verdadeiro em outros casos. Um dos problemas em aberto consiste em provar esse resultado para qualquer $\mathbb{K}$ ou exibir um contra-exemplo que comprove sua invalidez. Provamos que para qualquer corpo de números cíclico $\mathbb{K}$ de grau primo ímpar existe um número inteiro $m > 0$ tal que o reticulado algébrico obtido através do $\mathbb{Z}$-módulo M_m (definido em 3.42) pelo mergulho de Minkowski é bem arredondado. Também demonstramos que existem infinitos reticulados algébricos bem arredondados não equivalentes entre si em $\mathbb{R}^p$, para qualquer primo $p > 2$. Uma perspectiva de sequência sobre esse tópico consiste em estudar reticulados algébricos obtidos através do mergulho torcido e pesquisar famílias de ideais e $\mathbb{Z}$-módulos que produzam reticulados algébricos bem arredondados em diversas dimensões.

No Capítulo 5, definimos conceitos básicos em criptografia, fizemos um histórico apresentando a criptografia pós-quântica, enunciamos problemas computacionais que fundamentam a criptografia baseada em reticulados, conhecemos os problemas GGH, NTRU, SIS, LWE, RSIS, RLWE e PLWE e propusemos uma adaptação do RLWE para produzir um novo problema chamado α-RLWE ao trocar o mergulho de Minkowski pelo mergulho torcido. Mostramos que o α-RLWE é no mínimo tão difícil de ser resolvido quanto o problema RLWE. Por fim, analisamos resultados recentes sobre as fragilidades e instâncias fracas do RLWE. Para trabalhos futuros queremos esclarecer quais as vantagens do α-RLWE sobre o RLWE tradicional e pretendemos colaborar no estudo sobre os parâmetros que fragilizam problemas de criptografia baseados em reticulados.

Por fim, no Capítulo 6, enunciamos o Teorema das Unidades de Dirichlet, introduzimos o reticulado logarítmico, demos um limitante superior para o raio de cobertura do reticulado logarítmico $Log(\mathcal{O}^*_{\mathbb{Q}(\zeta_n)})$, para qualquer inteiro $n > 0$, e vimos uma forma de construir o reticulado hexagonal como reticulado logarítmico através do corpo $\mathbb{Q}(\zeta_7)$. Para trabalhos futuros temos a intenção de generalizar esses resultados para corpos de números abelianos quaisquer e estudar outras propriedades dos reticulados logarítmicos, tais como a densidade de centro e a realização de outros reticulados notáveis.

Além das perspectivas futuras mencionadas nos parágrafos acima, temos ainda a intenção de aprofundar os estudos sobre monogênese de anéis de inteiros de corpos de números, conceito que foi introduzido na Seção 1.5 e que está ligado às fragilidades do problema criptográfico RLWE.

Referências

[AAC] A. A. Andrade, C. Alves, and T. B. Carlos. Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$. International Journal of Applied Mathematics, v.19, n.3, p.1-13. 2010.

[ADPS15] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092, 2015. `https://eprint.iacr.org/2015/1092`.

[Ajt96] M. Ajtai. Generating Hard Instances of Lattice Problems (Extended Abstract). STOC '96, pages 99–108, New York, NY, USA, 1996. Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. ACM.

[BCD+16] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. CCS '16, pages 1006–1018, New York, NY, USA, 2016. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM.

[BCLvV16] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. NTRU Prime: reducing attack surface at low cost. Cryptology ePrint Archive, Report 2016/461, 2016. `http://eprint.iacr.org/2016/461`.

[BFN05] E. Bayer-Fluckiger and G. Nebe. On the euclidian minimum of some real number fields. 2005. Journal de theorie des nombres de Bordeaux, v.17, n.2, p. 437-454.

[BFOV04] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. New algebraic constructions of rotated zn-lattice constellations for the rayleigh fading channel. *IEEE Transactions on Information Theory*, 50(4):702–714, 2004.

[BV11] Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. pages 505–524, Berlin, Heidelberg, 2011. Advances in Cryptology – CRYPTO 2011. Springer Berlin Heidelberg.

[BVRB96] J. Boutros, E. Viterbo, C. Rastello, and J. Belfiore. Good lattice constellations for both rayleigh fading and gaussian channel. 1996. IEEE Transactions on Information Theory, v.42, n.2, p.502-517.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. pages 559–585, New York, NY, USA, 2016. Proceedings of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT 2016 - Volume 9666. Springer-Verlag New York, Inc.

[Cha15] A. C. M. M. Chagas. Uma contribuição a teoria dos números e reticulados. 2015. 2015. 78 f. Tese (Doutorado) - Universidade Estadual Paulista Julio de Mesquita Filho, Instituto de Biociências, Letras e Ciências Exatas.

[CLB16] A. Campello, C. Ling, and J. Belfiore. Algebraic lattice codes achieve the capacity of the compound block-fading channel. pages 910–914, 2016. 2016 IEEE International Symposium on Information Theory (ISIT).

[CLB18] A. Campello, C. Ling, and J-C. Belfiore. Universal lattice codes for mimo channels. pages 1–1, 2018. IEEE Transactions on Information Theory.

[CLS17] H. Chen, K. E. Lauter, and K. E. Stange. Security considerations for galois non-dual RLWE families. *CoRR*, abs/1710.03316, 2017.

[COC+17] S. I. R. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo. *Lattices Applied to Coding for Reliable and Secure Communications*. Springer, Cham, 2017.

[Cos16] S. I. R. Costa. Tópicos em geometria. 2016. Notas de aula.

[CS98] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and group*. Springer-Verlag, Nova Iorque, 3ª ed., 1998.

[dA15] R. R. de Araujo. Anéis de inteiros de corpos de números e aplicações. Dissertação de mestrado, Universidade Estadual Paulista Julio de Mesquita Filho, Instituto de Biociências, Letras e Ciências Exatas, 2015.

[dA16] R. R. de Araujo. Leopoldt's theorem: a new tool to construct algebraic lattices. XXIV Escola de Álgebra, Diamantina, 2016.

[dA17] R. R. de Araujo. Reticulados dn-rotacionados via corpos de números totalmente reais. Minissimpósio Códigos e reticulados algébricos do XXXVII Congresso Nacional de Matemática Aplicada e Computacional - CNMAC, 2017.

[dA18] R. R. de Araujo. Reticulados algébricos em corpos de números abelianos de grau primo. Minissimpósio Construções de Códigos Reticulados Algébricos do XXXVIII Congresso Nacional de Matemática Aplicada e Computacional - CNMAC, 2018.

[dAC18a] R. R. de Araujo and S. I. R. Costa. Well-rounded algebraic lattices in odd prime dimension. *Archiv der Mathematik*, 2018.

[dAC18b] R. R. de Araujo and S. I. R. Costa. Well-rounded lattices from $\mathbb{Z}$-modules of cyclotomic fields via the minkowski embedding. International Congress of Mathematicians - ICM, Rio de Janeiro, 2018.

[dACAN18] R. R. de Araujo, A. C. M. M. Chagas, A. A. Andrade, and T. P. N. Neto. Trace form associated to cyclic number fields of ramified odd prime degree. 2018. Submetido para Publicação.

[dAJ17] R. R. de Araujo and G. C. Jorge. Construction of full diversity d_n-lattices for all n. 2017. Submetido para Publicação. Disponível no arXiv: `https://arxiv.org/abs/1709.05536`.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DI03] H. H. Domingues and G. Iezzi. *Álgebra Moderna: Edição reformulada.* Atual, 2003.

[EHL14] K. Eisenträger, S. Hallgren, and K. Lauter. *Weak Instances of PLWE*, pages 183–194. Cham, 2014. Selected Areas in Cryptography – SAC 2014: 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers. Springer International Publishing.

[Elg85] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[ELOS15] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. *Provably Weak Instances of Ring-LWE*, pages 63–92. Berlin, Heidelberg, 2015. Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, Springer Berlin Heidelberg.

[End05] O. Endler. *Teoria dos corpos.* Publicações matemáticas. IMPA, 2005.

[End14] O. Endler. *Teoria dos números algébricos.* IMPA, 2ª edição, 2014.

[Ere88] B. Erez. The galois structure of the trace form in extensions of odd prime degree. 1988. Journal of Algebra, v. 118, p. 438-446.

[ESK05] P. Elia, B. A. Sethuraman, and P. V. Kumar. Perfect space-time codes with minimum and non-minimum delay for any number of antennas. 2005. IEEE Transactions on Information Theory.

[Fá12] E. R. Fávaro. Corpos cujo condutor é potência de primo: caracterização e reticulados ideais associados. 2012. 2012. 109 f. Tese (Doutorado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas.

[Fer08] A. J. Ferrari. *Reticulados algébricos via corpos abelianos*. 2008. Dissertação (mestrado). Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas.

[FHL+13] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices ii. *International Journal of Number Theory*, 09(01):139–154, 2013.

[Flo96] A. L. Flores. Representação geométrica de ideais de corpos de números. 1996. 1996. 86 f. Dissertação (Mestrado) - Universidade de Campinas, Instituto de Matemática, Estatística e Ciência da Computação.

[FP12] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *International Journal of Number Theory*, 08(01):189–206, 2012.

[GBK+16] O. Gnilke, A. Barreal, A. Karrila, H. Tran, D. Karpuk, and C. Hollanti. Well-rounded lattices for coset coding in mimo wiretap channels. pages 289–294, 2016. 26th International Telecommunication Networks and Applications Conference, ITNAC 2016.

[GGH97] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. pages 112–131, Berlin, Heidelberg, 1997. Advances in Cryptology — CRYPTO '97. Springer Berlin Heidelberg.

[Goo16] Google. Experimenting with Post-Quantum Cryptography, 2016. `https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html`.

[GTKH16] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti. Well-rounded lattices for reliability and security in rayleigh fading siso channels. pages 359–363, 2016. 2016 IEEE Information Theory Workshop (ITW).

[HK71] K. M. Hoffman and R. A. Kunze. *Linear Algebra*. Prentice-Hall Mathematics Series. N.J., Prentice-Hall, 1971.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. 1998.

[Hun74] T. W. Hungerford. *Álgebra*. Graduate texts in mathematics. Holt, Rinehart and Winston, 1974.

[ILN06] J. C. Interlando, J. O. D. Lopes, and T. P. N. Neto. The discriminant of abelian number fields. *Journal of Algebra and Its Applications*, 05(01):35–41, 2006.

[JACS15] G. C. Jorge, A. A. Andrade, S. I. R. Costa, and J. E. Strapasson. Algebraic constructions of densest lattices. *Journal of Algebra*, 429:218 – 235, 2015.

[JC12] G. C. Jorge and S. I. R. Costa. Rotated d_n-lattices. 2012. Journal of Number Theory, v. 132, n. 11, p. 2397-2406.

[Jor12] G. C. Jorge. *Reticulados q-ários e algébricos*. 2012. Tese (Doutorado). Imecc, Unicamp. Campinas.

[Lan05] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

[LASC12] C. C. Lavor, M. M. S. Alves, R. M. Siqueira, and S. I. R. Costa. *Uma Introdução à Teoria de Códigos*. Notas em Matemática Aplicada, v. 21, Sociedade Brasileira de Matemática Aplicada e Computacional, São Carlos, 2012.

[Leo59] V. H. Leopoldt. Ûber die hauptordnung der ganzen elemente eines abelschen zahlkorpers. 1959. J. Reine Angew. Math., 201, pp. 119-149.

[Let90] G. Lettl. The ring of integers of an abelian number field. 1990. J. Reine Angew. Math., 404, pp. 162-170.

[LNI02] J. O. D. Lopes, T. P. N. Neto, and J. C. Interlando. On computing discriminant of subfields of $\mathbb{Q}(\zeta_{p^r})$. 2002. Journal of Number Theory, v.96, n.2, p.319-325.

[Lop03] J. O. D. Lopes. Discriminants of subfields of $\mathbb{Q}(\zeta_{2^r})$. 2003. Journal of Algebra And Its Applications, v.2, p. 463-469.

[LP11] R. Lindner and C. Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. pages 319–339, Berlin, Heidelberg, 2011. Topics in Cryptology – CT-RSA 2011. Springer Berlin Heidelberg.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. *On Ideal Lattices and Learning with Errors over Rings*, pages 1–23. Berlin, Heidelberg, 2010. Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings. Springer Berlin Heidelberg.

[LS15] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

[Mar95] D. A. Marcus. *Number Fields*. Universitext. Springer New York, 1995.

[Mar03] J. Martinet. *Perfect Lattices in Euclidean Spaces*. 2003. Springer-Verlag Berlin Heidelberg.

[McM05] C. T. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *Journal of the American Mathematical Society*, 18(3):711–734, 2005.

[Mic] D. Micciancio. Minkowski's theorem. `https://cseweb.ucsd.edu/classes/sp14/cse206A-a/lec2.pdf`. Acessado em: 03-09-2018.

[Mic02] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. pages 356–365, Vancouver, Canada, 2002. Proceedings of the 43rd Annual Symposium on Foundations of Computer Science - FOCS 2002. Full version in Computational Complexity 16:365-411.

[Mil72] F. C. P. Milies. *Anéis e modulos*. Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo. 1972.

[MvOV01] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. 2001. CRC Press.

[Neb] G. Nebe. Index to catalogue of lattices. Disponível em ¡http://www.math.rwth-aachen.de/ Gabriele.Nebe/LATTICES¿. Acesso em nov/2016.

[NINL16] J. V. L. Nunes, J. C. Interlando, T. P. N. Neto, and J. O. D. Lopes. New p-dimensional lattices from cyclic extensions. 2016. Journal of Algebra and Its Applications, pp. 175-186.

[NIS17] National Institute of Standards and Technology - NIST. Post-Quantum Crypto Standardization, 2017.

[NRS02] G. Nebe, E. M. Rains, and N. J. A. Sloane. *A simple construction for the barnes-wall lattices*. Codes, Graphs, and Systems: A Celebraton of the Life and Career of G. David Forney, Jr. on the Occasion of his Sixtieth Birthday, ed. R. E. Blahut and R. Koetter, Kluwer, 2002.

[OdAD+18a] J. N. Ortiz, R. R. de Araujo, R. Dahab, D. F. Aranha, and S. I. R. Costa. In praise of twisted canonical embedding. Cryptology ePrint Archive, Report 2018/356, 2018. `https://eprint.iacr.org/2018/356`.

[OdAD+18b] J. N. Ortiz, R. R. de Araujo, R. Dahab, D. F. Aranha, and S. I. R. Costa. On lattices for cryptography. Latin American Week on Coding and Information - LAWCI, 2018.

[OINL17] E. L. Oliveira, J. C. Interlando, T. P. N. Neto, and J. O. D. Lopes. The integral trace form of cyclic extensions of odd prime degree. 2017. Rocky Mountain J. Math. 47, no. 4, pp. 1075-1088.

[Oli15] E. L. Oliveira. Torres de extensões abelianas de grau primo ímpar não ramificado. 2015. 2015. 62 f. Tese (Doutorado) - Universidade Estadual Paulista Julio de Mesquita Filho, Instituto de Biociências, Letras e Ciências Exatas.

[Ort18] J. N. Ortiz. Non-cyclotomic number fields for lattice-based cryptography. 2018.

[Pei16] C. Peikert. A Decade of Lattice Cryptography. *Found. Trends Theor. Comput. Sci.*, 10(4):283–424, 2016. Now Publishers Inc.

[PL04] V.V. Prasolov and D. Leites. *Polynomials*. Number v. 13 in Algorithms and Computation in Mathematics. 2004. Springer.

[PRSD17] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. STOC 2017, pages 461–473, New York, NY, USA, 2017. Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing. ACM.

[Reg05] O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. STOC '05, pages 84–93, New York, NY, USA, 2005. Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing. ACM.

[Rib01] P. Ribenboim. *Classical Theory of Algebraic Numbers*. Universitext. Springer New York, 2001.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. ACM.

[Sam70] P. Samuel. *Algebraic theory of numbers*. Hermann, 1970.

[Ser73] J. Serre. A course in arithmetic. 1973. Springer-Verlag New York, vol. 7.

[Sho97] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[SO07] B. A. Sethuraman and F. Oggier. Constructions of orthonormal lattices and quaternion division algebra for totally real number fields. 2007.

[ST02] I. Stewart and D. O. Tall. *Algebraic number theory and Fermat's last theorem /.* AK Peters„ Natick, Mass. :, 3rd ed. edition, 2002.

[SW03] B. K. Spearman and K. S. Williams. The discriminant of a cyclic field of odd prime degree. *Rocky Mountain J. Math.*, 33(3):1101–1122, 2003. Rocky Mountain Mathematics Consortium.

[Was95] L. Washington. *Introduction to Cyclotomic Fields*. 1995. Springer-Verlag New York, 2 ed.

APÊNDICE A - Índice