Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Corpos Puros de Grau 6 e Aplicações em Reticulados

Linara S. Facini[1], Prof. Dr. Antonio A. Andrade[2]
UNESP/IBILCE, São José do Rio Preto, SP

Resumo. Um grande desafio da Teoria Algébrica dos Números é encontrar as bases integrais dos corpos puros. Neste trabalho, apresentamos algo diferente do que as literaturas atuais propõem, que são as bases integrais dos corpos puros não monogênicos de grau 6 e seus respectivos discriminantes. Os dados obtidos permitem a construção de reticulados via corpos puros de grau 6.

Palavras-chave. Corpo Puro, Não Monogênico, Anel de Inteiros Algébricos, Discriminante, Reticulados

1 Introdução

O presente trabalho tem por objetivo apresentar o anel de inteiros algébricos de corpos puros de grau 6, o discriminante associado e aplicações em construções de reticulados via estes corpos de números. Um problema atual contido na Teoria da Informação é o empacotamento esférico, que consiste em dispor esferas de mesmo raio no espaço euclidiano n-dimensional de tal modo que no máximo duas esferas se tangenciem e que ocupem a maior fração deste espaço, ou seja, que esta distribuição tenha alta densidade. Estamos interessados no conjunto de pontos centrais das esferas que sejam reticulado. Em 1948, com a publicação do artigo *A Mathematical Theory of Communication* do matemático Claude E. Shannon, ficou estabelecido que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes, e assim, é possível associar o estudo dos códigos aos reticulados de modo que, ao transmitir uma mensagem (código) emitimos um vetor, se esse vetor for enviado diretamente ao centro da esfera a mensagem foi entregue com sucesso, caso o vetor atinja o interior da esfera no processo a mensagem foi entregue com erro, ou seja, aconteceu o chamado "ruído" mas é possível corrigi-lá. Agora, se o vetor atingir os espaços entre as esferas a mensagem por sua vez acaba se perdendo e é menos provável de haver uma correção [1], [2] e [3]. Com base nesses fatos, neste trabalho apresentamos novos resultados que surgiram com a inspiração da referência [4].

2 Resultados Básicos da Teoria Algébrica dos Números

Essa seção tem como objetivo embasar e fundamentar alguns resultados básicos envolvendo a Teoria Algébrica dos Números. Assim, admitimos o conhecimento prévio da Álgebra Clássica e da Álgebra Moderna que envolvam as estruturas de grupos, anéis, corpos e módulos, [5] e [6]. No mais, serão usados os conhecimentos da Álgebra Linear Clássica, como os espaços vetoriais, que podem ser reforçados pela leitura em [7].

Definição 2.1. Seja $\mathbb{K} \subseteq \mathbb{C}$ um corpo.

[1]linara.facini@unesp.br
[2]antonio.andrade@unesp.br

1. Se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, então $\mathbb{K}$ é chamado de **corpo de números algébricos**, ou simplesmente, **corpo de números**.

2. Se $\mathbb{K}$ é um corpo de números, os elementos de $\mathbb{K}$ que são inteiros sobre $\mathbb{Z}$ são chamados de **inteiros algébricos** de $\mathbb{K}$. O conjunto desses elementos é chamado **anel dos inteiros algébricos** de $\mathbb{K}$, ou simplesmente, de **anel dos inteiros** de $\mathbb{K}$, o qual denotamos por $\mathcal{O}_{\mathbb{K}}$.

3. Uma base do anel de inteiros algébricos de $\mathbb{K}$ é chamada de **base integral**.

4. Quando a base integral de $\mathbb{K}$ é base de potências de um elemento, chamamos $\mathbb{K}$ de **corpo monogênico**.

Para $\mathbb{K}$ um corpo de números de grau n, existem exatamente n $\mathbb{Q}$-monomorfismos distintos. Fazendo uso dessa estrutura, é possível estender a noção de traço e de polinômio característico da Álgebra Linear para o traço e o polinômio característico de um elemento $\alpha \in \mathbb{K}$ usando os $\mathbb{Q}$-monomorfismos.

Proposição 2.1. [1] Sejam $\mathbb{K}$ um corpo de números com $[\mathbb{K} : \mathbb{Q}] = n$ e $\sigma_1, \ldots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Se $\alpha \in \mathbb{K}$, então

1. O **traço** de α sobre $\mathbb{K}$ é dado por

$$\mathcal{T}r(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{1}$$

2. O **polinômio característico** de α sobre $\mathbb{K}$ é dado por

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)). \tag{2}$$

Proposição 2.2. [1] Seja $\mathbb{K}$ um corpo de números. Assim, $\alpha \in \mathbb{K}$ é um inteiro algébrico se, e somente se, seu polinômio característico tem coeficientes inteiros.

A seguir, definimos o conceito de discriminante que será essencial nas aplicações.

Definição 2.2. Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o seu anel dos inteiros algébricos. O **discriminante** de $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{O}_{\mathbb{K}}^n$, é definido por:

$$\mathcal{D}_{B|A}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\mathcal{T}r_{B|A}(\alpha_i \alpha_j)) \in \mathbb{Z}, \tag{3}$$

onde $i, j = 1, 2, \ldots, n$.

3 Resultados Preliminares de Corpos Puros

Nesta seção, apresentamos alguns resultados de corpos da forma $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[n]{d}$, $n > 2$, $d \in \mathbb{Z}$, $d \neq 1$ e livre de quadrados. Os resultados aqui apresentados são novos, de nossa autoria, e estão disponíveis em [8].

Definição 3.1. O corpo $\mathbb{K}$ é chamado de **corpo puro** de grau n.

DOI: 10.5540/03.2025.011.01.0373

O elemento $\theta = \sqrt[n]{d}$ é um inteiro algébrico, uma vez que $p(x) = x^n - d$ é o seu polinômio minimal sobre $\mathbb{Z}$. Pela Teoria de Corpos, segue que $[\mathbb{Q}(\sqrt[n]{d}) : \mathbb{Q}] = \partial(p) = n$ e de fato $\mathbb{K} = \mathbb{Q}(\sqrt[n]{d})$ é um corpo de números cujo elemento primitivo é o próprio $\sqrt[n]{d}$. Salvo menção contrária, $\theta = \sqrt[n]{d}$ é o elemento primitivo, com $d \in \mathbb{Z}$ livre de quadrados e o corpo de números em questão é o $\mathbb{K} = Q(\theta)$.

Sejam $\theta, \theta\xi_n, \ldots, \theta\xi_n^{n-1}$ as raízes do polinômio $p(x)$, onde ξ_n^k são as raízes primitivas da unidade, para $k = 0, 1, 2, \ldots, n-1$. Assim,

$$\xi_n^k = e^{\frac{2\pi i}{n}k} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right). \tag{4}$$

Podemos considerar σ_k os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\theta)$ em $\mathbb{C}$ que fixam os elementos de $\mathbb{Q}$ e tal que $\sigma_k(\theta) = \theta\xi_n^{k-1}$, com $k = 1, 2 \ldots, n$. Pela Teoria de Corpos, segue que o conjunto $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, e assim, para qualquer $\alpha \in \mathbb{K}$, segue que $\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$, tendo $a_i \in \mathbb{Q}$, com $i = 0, 1, 2, \ldots, n-1$.

A seguir, apresentamos novos resultados, de nossa autoria, envolvendo os corpos puros de grau n.

Proposição 3.1. [8] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo puro de grau n. Se $\mathcal{O}_\mathbb{K}$ é o seu anel dos inteiros algébricos, então $\theta\mathcal{O}_\mathbb{K} \cap \mathbb{Z} = d\mathbb{Z}$.

Proposição 3.2. [8] Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo puro de grau n e $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos. Se $x \in \theta\mathcal{O}_\mathbb{K}$, então $\mathcal{T}r(x) \in d\mathbb{Z}$.

Proposição 3.3. [8] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo puro de grau n, então

$$\mathcal{T}r(\theta^k) = \begin{cases} 0, \text{ se } k = 1, 2, \ldots, n-1, \\ nd^s, \text{ se } k = ns, \text{ com } s \in \mathbb{N}, \\ 0, \text{ se } k > n \text{ e } k \not\equiv 0(mod\ n). \end{cases} \tag{5}$$

Proposição 3.4. [8] Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo puro de grau n e $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \in \mathbb{K}$, com $a_0, a_1, a_2 \ldots, a_{n-1} \in \mathbb{Q}$. Se α é um inteiro algébrico, então

$$na_0, na_1, na_2 \ldots, na_{n-1} \in \mathbb{Z}. \tag{6}$$

Proposição 3.5. [8] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo puro de grau n e $p(x) = x^n - d \in \mathbb{Z}[x]$ o polinômio minimal de θ, com d não nulo, então

$$\mathcal{D}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = (-1)^{\frac{n^2+n+2}{2}}[n^n d^{n-1}]. \tag{7}$$

4 Anel dos Inteiros Algébricos de Corpos Puros de Grau 6

Nessa seção, apresentamos o anel dos inteiros algébricos de corpos puros de grau 6 e o discriminante desses corpos. Para isso, seja $\mathbb{K} = \mathbb{Q}(\sqrt[6]{d})$, onde $d \in \mathbb{Z}$, $d \neq 1$ e livre de quadrados. Assim, apresentamos novos resultados na determinação do anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K} = \mathbb{Q}(\theta)$. O Teorema 4.1, tem como o objetivo determinar para todas as congruências módulo 36 uma base integral para $\mathcal{O}_\mathbb{K}$, e é uma das nossas contribuições.

DOI: 10.5540/03.2025.011.01.0373

Proposição 4.1. [8] Se $\alpha = a_0+a_1\theta+a_2\theta^2+a_3\theta^3+a_4\theta^4+a_5\theta^5 \in \mathbb{K}$, com $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}$, então o polinômio característico de α é dado por

$$\begin{aligned}
f_\alpha(x) = {} & x^6 - x^5[6a_0] + x^4[3(5a_0^2 - (a_3^2 + 2a_2a_4 + 2a_1a_5)d)] - x^3[2(10a_0^3 + (a_2^3 + \\
& + 6a_1a_2a_3 - 6a_0a_3^2 + 3a_1^2a_4 - 12a_0a_2a_4 - 12a_0a_1a_5)d + (a_4^3 + 6a_3a_4a_5 + \\
& + 3a_2a_5^2)d^2)] + x^2[3(5a_0^4 + (-3a_1^2a_2^2 + 2a_0a_2^3 - 2a_1^3a_3 + 12a_0a_1a_2a_3 - \\
& - 6a_0^2a_3^2 + 6a_0a_1^2a_4 - 12a_0^2a_2a_4 - 12a_0^2a_1a_5)d + (a_3^4 + 3a_2^2a_4^2 - 6a_1a_3a_4^2 + \\
& + 2a_0a_4^3 - 6a_2^2a_3a_5 + 12a_0a_3a_4a_5 + 3a_1^2a_5^2 + 6a_0a_2a_5^2)d^2 + (-3a_4^2a_5^2 - \\
& - 2a_3a_5^3)d^3)] - x[6(a_0^5 + (a_1^4a_2 - 3a_0a_1^2a_2^2 + a_0^2a_2^3 - 2a_0a_1^3a_3 + 6a_0^2a_1a_2a_3 - \\
& - 2a_0^3a_3^2 + 3a_0^2a_1^2a_4 - 4a_0^3a_2a_4 - 4a_0^3a_1a_5)d + (a_2^3a_3^2 - 2a_1a_2a_3^3 + a_0a_3^4 - \\
& - a_2^4a_4 + 3a_1^2a_3^2a_4 + 3a_0a_2^2a_4^2 - 6a_0a_1a_3a_4^2 + a_0^2a_4^3 + 2a_1a_2^3a_5 - 6a_0a_2^2a_3a_5 - \\
& - 2a_1^3a_4a_5 + 6a_0^2a_3a_4a_5 + 3a_0a_1^2a_5^2 + 3a_0^2a_2a_5^2)d^2 + (a_3^2a_4^3 - a_2a_4^4 - 2a_3^3a_4a_5 + \\
& + 2a_1a_4^3a_5 + 3a_2a_3^2a_5^2 - 3a_0a_4^2a_5^2 - 2a_1a_2a_5^3 - 2a_0a_3a_5^3)d^3 + (a_4a_5^4)d^4)] + \\
& + [a_0^6 + (-a_1^6 + 6a_0a_1^4a_2 - 9a_0^2a_1^2a_2^2 + 2a_0^3a_2^3 - 6a_0^2a_1^3a_3 + 12a_0^3a_1a_2a_3 - \\
& - 3a_0^4a_3^2 + 6a_0^3a_1^2a_4 - 6a_0^4a_2a_4 - 6a_0^4a_1a_5)d + (a_2^6 - 6a_1a_2^4a_3 + 9a_1^2a_2^2a_3^2 + \\
& + 6a_0a_2^3a_3^2 - 2a_1^3a_3^3 - 12a_0a_1a_2a_3^3 + 3a_0^2a_3^4 + 6a_1^2a_2^3a_4 - 6a_0a_2^4a_4 - \\
& - 12a_1^3a_2a_3a_4 + 18a_0a_1^2a_3^2a_4 + 3a_1^4a_4^2 + 9a_0^2a_2^2a_4^2 - 18a_0^2a_1a_3a_4^2 + 2a_0^3a_4^3 - \\
& - 6a_1^3a_2^2a_5 + 12a_0a_1a_2^3a_5 + 6a_1^4a_3a_5 - 18a_0^2a_2^2a_3a_5 - 12a_0a_1^3a_4a_5 + \\
& + 12a_0^3a_3a_4a_5 + 9a_0^2a_1^2a_5^2 + 6a_0^3a_2a_5^2)d^2 + (-a_3^6 + 6a_2a_3^4a_4 - 9a_2^2a_3^2a_4^2 - \\
& - 6a_1a_3^3a_4^2 + 2a_2^3a_4^3 + 12a_1a_2a_3a_4^3 + 6a_0a_3^2a_4^3 - 3a_1^2a_4^4 - 6a_0a_2a_4^4 - 6a_2^2a_3^3a_5 + \\
& + 6a_1a_3^4a_5 + 12a_2^3a_3a_4a_5 - 12a_0a_3^3a_4a_5 - 18a_1a_2^2a_4^2a_5 + 12a_0a_1a_4^3a_5 - \\
& - 3a_2^4a_5^2 - 9a_1^2a_3^2a_5^2 + 18a_0a_2a_3^2a_5^2 + 18a_1^2a_2a_4a_5^2 - 9a_0^2a_4^2a_5^2 - 2a_1^3a_5^3 - \\
& - 12a_0a_1a_2a_5^3 - 6a_0^2a_3a_5^3)d^3 + (a_4^6 - 6a_3a_4^4a_5 + 9a_3^2a_4^2a_5^2 + 6a_2a_4^3a_5^2 - 2a_3^3a_5^3 - \\
& - 12a_2a_3a_4a_5^3 - 6a_1a_4^2a_5^3 + 3a_2^2a_5^4 + 6a_1a_3a_5^4 + 6a_0a_4a_5^4)d^4 + (-a_5^6)d^5].
\end{aligned} \tag{8}$$

Demonstração. Segue direto da Proposição 2.1. □

O próximo teorema determina para cada congruência módulo 36 uma bases integral de $\mathcal{O}_\mathbb{K}$. Este resultado é de nossa autoria e explora bases integrais além dos casos monogênicos, [9].

Teorema 4.1. [8] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O anel dos inteiros algébricos $\mathcal{O}_\mathbb{K}$ de $\mathbb{K}$ é dado por

$$\begin{cases}
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\theta^4+\mathbb{Z}\theta^5 = \mathbb{Z}[\theta], \text{ se } d \not\equiv \pm1, \pm17, \pm10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+4\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{3+4\theta+3\theta^2+\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 1 (mod\ 36) \\
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+2\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+2\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -10, -1 (mod\ 36) \\
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{4+3\theta+2\theta^2+\theta^4}{6}\right)+\mathbb{Z}\left(\frac{4\theta+3\theta^2+2\theta^3+\theta^5}{6}\right), \text{ se } d \equiv 17 (mod\ 36) \\
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\theta^3+\mathbb{Z}\left(\frac{1+\theta^2+\theta^4}{3}\right)+\mathbb{Z}\left(\frac{\theta+\theta^3+\theta^5}{3}\right), \text{ se } d \equiv -17, 10 (mod\ 36) \\
\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2+\mathbb{Z}\left(\frac{1+\theta^3}{2}\right)+\mathbb{Z}\left(\frac{\theta+\theta^4}{2}\right)+\mathbb{Z}\left(\frac{\theta^2+\theta^5}{2}\right), \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36).
\end{cases}$$

Demonstração. A ideia da demonstração é usar a Proposição 2.2. Basta analisarmos que $\alpha \in \mathcal{O}_\mathbb{K}$ se, e somente se, $\frac{r_0}{6}+\frac{r_1}{6}\theta+\frac{r_2}{6}\theta^2+\frac{r_3}{6}\theta^3+\frac{r_4}{6}\theta^4+\frac{r_5}{6}\theta^5 \in \mathcal{O}_\mathbb{K}$, com $r_0, r_1, r_2, r_3, r_4, r_5 \in \{0, 1, 2, 3, 4, 5\}$.

Assegurados pela Proposição 4.1 e pela Proposição 2.2, encontramos os possíveis valores dos r_i's relacionados as bases integrais enunciadas e depois pela biunivocidade da Proposição 2.2 analisamos quais as possíveis congruências de d módulo 36 que tornam α um inteiro algébrico. □

Exemplo 4.1. Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[6]{7}$. Como $d = 7$ e $7 \equiv 7(mod\ 36)$, pelo Teorema 4.1, segue que o anel dos inteiros algébricos desse caso é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$.

Corolário 4.1. [8] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}$ livre de quadrados. O discriminante do anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por

$$\mathcal{D}(\mathbb{K}) = \begin{cases} 46656d^5, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13(mod\ 36) \\ 9d^5, \text{ se } d \equiv 1, 17(mod\ 36) \\ 576d^5, \text{ se } d \equiv -17, -10, -1, 10(mod\ 36) \\ 729d^5, \text{ se } d \equiv -15, -11, -7, -3, 5, 13(mod\ 36). \end{cases}$$

Demonstração. Segue direto da Definição 2.2. □

Exemplo 4.2. Seja $\mathbb{K} = Q(\theta)$, com $\theta = \sqrt[6]{7}$. Como $d = 7$ e $7 \equiv 7(mod\ 36)$, pela Proposição 4.1, segue que o discriminante é dado por $\mathcal{D}(\mathbb{K}) = 784147392$.

5 Reticulados

Nesta seção, apresentamos o conceito de reticulados no $\mathbb{R}^n$ e alguns de seus parâmetros como matriz de Gram, volume, raio de empacotamento e densidade de centro [1]. Um estudo mais aprofundado sobre densidade de centro ótima encontra-se na referência [10].

Definição 5.1. Sejam $v_1, v_2, \ldots, v_m$ vetores de $\mathbb{R}^n$ linearmente independentes sobre $\mathbb{R}$, com $m \leq n$. O conjunto dos elementos da forma

$$\Lambda_B = \left\{ x = \sum_{i=1}^{m} a_i v_i \mid a_i \in \mathbb{Z} \right\}, \tag{9}$$

é chamado de **reticulado** com base $B = \{v_1, v_2, \ldots, v_m\}$. Se $m = n$, o reticulado Λ_B é chamado um **reticulado completo**.

Definição 5.2. Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $B = \{v_1, v_2, \ldots, v_n\}$ uma base de Λ. Para $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, com $i = 1, 2, \ldots, n$ consideramos a matriz M dada por $M = [v_{ij}]_{n \times n}$.

1. A matriz M é chamada de **matriz geradora** do reticulado Λ.
2. O **volume do reticulado** Λ é definido por $\mathcal{V}ol(\Lambda) = \mathcal{V}ol(\mathcal{P}) = |\det(M)|$.

Definição 5.3. Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e ρ o raio de empacotamento Λ. O parâmetro

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)}, \tag{10}$$

é chamado de **densidade de centro** de Λ. Quando a densidade de centro é a maior possível chamamos-a de **densidade de centro ótima**.

Agora, seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo puro de grau n. Consideramos r_1 o número que representa a quantidade de índices k tal que $\sigma_k(\mathbb{K}) \subset \mathbb{K}$, ou seja, são reais. Sendo assim, $n - r_1$ é um número par. Portanto, existe um número natural r_2 tal que $r_1 + 2r_2 = n$.

Definição 5.4. A aplicação $\sigma_{\mathbb{K}}$ é chamada **homomorfismo de Minkowski** ou **homomorfismo canônico** de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ como $\mathbb{R}^n$, e este homomorfismo pode ser visto como

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \ldots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))), \quad (11)$$

onde $\Re(x)$ representa a parte real de x e $\Im(x)$ representa a parte imaginária de x.

Proposição 5.1. [1] Seja $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$, então

1. $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é um reticulado algébrico.
2. O volume de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é $\mathcal{V}ol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{\sqrt{|\mathcal{D}(\mathbb{K})|}}{2^{r_2}}$.
3. A densidade de centro de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})))^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}}$.

Para construir $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ um reticulado algébrico e obter sua densidade de centro é preciso os seguintes passos.

1. Conhecer a estrutura de $\mathcal{O}_{\mathbb{K}}$ (anel dos inteiros algébricos de $\mathbb{K}$);
2. Conhecer a estrutura de $\mathcal{D}(\mathbb{K})$ (discriminante da base integral);
3. Calcular $||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||^2$ (norma mínima dos elementos de $\mathcal{O}_{\mathbb{K}}$);
4. Obter $\rho = \dfrac{||\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})||}{2}$ (raio de empacotamento do reticulado);
5. Calcular $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{2^{r_2}\rho^n}{\sqrt{|\mathcal{D}(\mathbb{K})|}}$ (densidade de centro do reticulado).

6 Aplicações em Corpos Puros de Grau 6

Essa seção tem por objetivo aplicar os conceitos desenvolvidos neste trabalho, como anel de inteiros algébricos e discriminante dos corpos puros de grau 6, para encontrar reticulados algébricos de densidade ótima nesta dimensão.

Observação 6.1. A densidade de centro ótima para a dimensão 6 é $\delta = \dfrac{1}{8\sqrt{3}} \approx 0,07217$.

Aplicando o passo a passo a construção do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, no próximo resultado, apresentamos a densidade de centro.

Teorema 6.1. [8] Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números, onde $\theta = \sqrt[6]{d}$ com $d \in \mathbb{Z}_+$ livre de quadrados. A densidade de centro do reticulado algébrico $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de $\mathbb{K}$ é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \dfrac{1}{54\sqrt{d^5}}, \text{ se } d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36) \\ \dfrac{4}{3\sqrt{d^5}}, \text{ se } d \equiv 1, 17 (mod\ 36), \\ \dfrac{1}{6\sqrt{d^5}}, \text{ se } d \equiv -17, -10, -1, 10 (mod\ 36), \\ \dfrac{4}{27\sqrt{d^5}}, \text{ se } d \equiv -15, -11, -7, -3, 5, 13 (mod\ 36). \end{cases}$$

DOI: 10.5540/03.2025.011.01.0373

Demonstração. Como ideia da demonstração, suponhamos que d é um inteiro positivo e livre de quadrados. Logo $\theta = \sqrt[6]{d} \in \mathbb{K}$ e os $\mathbb{Q}$-monomorfismos aplicados em θ são $\sigma_k(\theta) = \theta\xi_6^{k-1}$, com $1 \leq k \leq 6$. Assim, $\mathbb{K}$ é um corpo misto de grau $n = 6$, onde $r_1 = 2$ e $r_2 = 2$. Do Teorema 4.1, calculamos a norma mínima através do homomorfismo de Minkowski e obtemos o discriminante pelo Corolário 4.1. Da Proposição 5.1, ao substituir estes valores, segue a densidade de centro. □

Exemplo 6.1. Seja $\mathbb{K} = \mathbb{Q}(\sqrt[6]{2})$. Como $d = 2$ e $d \not\equiv \pm 1, \pm 17, \pm 10, -15, -11, -7, -3, 5, 13 (mod\ 36)$, segue que $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \dfrac{1}{54\sqrt{d^5}} = \dfrac{1}{54\sqrt{2^5}} \approx 0,00327$.

7 Considerações Finais

Os corpos puros de acordo com seus graus emitem uma estrutura e um elemento primitivo que causam uma complexidade para encontrar o anel de inteiros algébricos e seu discriminante, exigindo um grande auxílio computacional. Neste trabalho, focamos nos corpos puros de grau 6 para encontrar seu anel de inteiros algébricos de acordo com as características do polinômio minimal, e consequentemente, usando os $\mathbb{Q}$-monomorfismos. Via o homomorfismo de Minkowski, apresentamos exemplos de reticulados algébricos via a imagem do monomorfismo $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$. Assim, coube uma minuciosa exploração de exemplos para obter reticulados de densidade ótima, mas, somente via $\mathcal{O}_{\mathbb{K}}$, não se permitiu ter exemplos bons e por este motivo desperta-se a curiosidade para estudar os reticulados algébricos sobre os $\mathbb{Z}$-módulos contidos no corpo $\mathbb{K}$. As perspectivas futuras englobam a padronização dos graus e generalização dos casos em conjuntos com o estudo dos reticulados sobre os $\mathbb{Z}$-módulos contidos no corpo $\mathbb{K}$. Com isso, imagina-se que objetivamente podemos conseguir reticulados com densidade de centro ótima.

Referências

[1] A. A. de Andrade, **Uma introdução a teoria algébrica dos números**, 1ª ed. São José do Rio Preto - SP: Amazon.com, 2021.

[2] R. R. de Araujo, "Anéis de inteiros de corpos de números e aplicações," Dissertação de mestrado, Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2015.

[3] M. Viana, **Viana explica a descoberta da teoria da informação**, Acesso em: 27 de agosto de 2021, 2020. endereço: `https://impa.br/noticias/marcelo-viana-explica-a-descoberta-da-teoria-da-informacao/`.

[4] V. C. da Silva Rodrigues, "Reticulados de Posto 4 em Corpos de Números," Dissertação de mestrado, Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2001.

[5] H. H. Domingues e G. Iezzi, **Álgebra Moderna**, 5ª ed. São Paulo: Saraiva, 2018.

[6] P. Samuel, **Algebraic Theory of Numbers**. Paris: Hermann, 1970.

[7] F. C. Ulhoa e M. L. Lourenço, **Um Curso de Álgebra Linear**. São Paulo: EDUSP, 2005.

[8] L. S. Facini, "Uma introdução aos corpos não abelianos de grau menor ou igual a 6," Dissertação de mestrado, Universidade Estadual Paulista "Júlio de Mesquita Filho"-IBILCE, 2021.

[9] S. M. H. S. Ahmad T. Nakahara, **Powe integral bases for certain pure sextic fields**. Pakistan: World Scientific, 2014.

[10] J. H. Conway e N. J. A. Sloane, **Sphere Packings, Lattices and Groups**. New York: Springer-Verlag, 1999.

