Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 12, n. 1, 2026.

Trabalho apresentado no XLIV CNMAC, Fundação Getulio Vargas - Rio de Janeiro - RJ, 2025.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Um Estudo sobre Reticulados Algébricos Cíclicos

Maria F. Z. Bonini[1], Antonio A. Andrade[2]
Ibilce - UNESP, São José do Rio Preto, SP
Robson R. Araujo[3]
IFSP, Catanduva, SP

Sejam $\mathbb{K}$ um corpo de números de grau $n > 1$ e $\alpha \in \mathbb{K}$. O elemento α é chamado um inteiro algébrico se é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$. Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$, ou seja, o conjunto

$$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \text{ tal que } \alpha \text{ é raiz de um polinômio mônico } f(x) \in \mathbb{Z}[x]\}.$$

O anel $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n e uma base de $\mathcal{O}_{\mathbb{K}}$ é chamada de uma base integral de $\mathbb{K}$. [1] Um reticulado $L \subset \mathbb{R}^n$ de dimensão k é definido como $L = B\mathbb{Z}^k$, onde $1 \leq k \leq n$ e B é uma matriz $n \times k$ de posto k. Um reticulado L possui posto completo se $k = n$.

Os reticulados são estruturas geométricas amplamente utilizadas em aplicações de problemas como empacotamento esférico, códigos e criptografia pós-quântica. Uma maneira de obter reticulados é utilizando ferramentas da Teoria Algébrica dos Números e os calculando a partir de corpos de números; estes reticulados são chamados *reticulados algébricos*. Há várias propriedades que podem ser exploradas na Teoria dos Reticulados, como por exemplo os *reticulados cíclicos*, que recentemente apareceram em trabalhos de criptografia [3] [4]. Essa aplicação na criptografia baseada em reticulados motiva o estudo mais aprofundado deles, como o que foi feito em [2].

Considere $\mathbb{R}_+$ o conjunto dos números reais positivos e $O_n(\mathbb{R})$ o grupo das matrizes reais ortogonais $n \times n$. Dois reticulados em $\mathbb{R}^n$, L_1 e L_2, são ditos *similares*, se existe $\alpha \in \mathbb{R}_+$ e $U \in O_n(\mathbb{R})$ tais que $L_2 = \alpha U L_1$. Denotamos dois reticulados similares por $L_1 \sim L_2$.

Nosso principal objetivo, neste trabalho, são os reticulados cíclicos, que são definidos da seguinte forma: Um reticulado $L \subset \mathbb{R}^n$, não necessariamente de dimensão completa, é chamado de *cíclico* em $\mathbb{R}^n$ se é fechado sob a operação linear rotação shift $\rho : \mathbb{R}^n \to \mathbb{R}^n$, dada por

$$\rho(c_1, c_2, \ldots, c_n) = (c_n, c_1, \ldots, c_{n-1}), \tag{1}$$

isto é, se $\rho(L) = L$. A propriedade de ser cíclico não é preservada sob a relação de similaridade. Um contraexemplo é o reticulado inteiro $\mathbb{Z}^2$ que é cíclico e similar ao reticulado $\begin{bmatrix} 1 & -a \\ a & 1 \end{bmatrix} \mathbb{Z}^2$, que por sua vez não é cíclico para nenhum $a \notin \mathbb{Q}$.

A conexão entre similaridade e reticulados cíclicos é dada pelo fato de que um reticulado do posto completo $L \subset \mathbb{R}^n$ é similar a um reticulado cíclico se, e somente se, L tem uma isometria com o polinômio minimal $x^n - 1$. Esse resultado é fácil verificação, uma vez que o operador ρ é uma isometria cujo minimal é $x^n - 1$, isto é, $\rho^n = I$ e nenhum polinômio de grau menor que n anula ρ.

Uma classe importante de reticulados são obtidos via o anel de inteiros de um corpo de números, por isso é interessante verificar sob quais hipóteses esses reticulados são cíclicos.

[1] maria.bonin@unesp.br
[2] antonio.andrade@unesp.br
[3] robson.ricardo@ifsp.edu.br

Seja $\mathbb{K}$ um corpo de números de grau $n = r_1 + 2r_2$ com os monomorfismos

$$\sigma_1, \ldots, \sigma_n : \mathbb{K} \hookrightarrow \mathbb{C},$$

onde r_1 são totalmente reais e $2r_2$ são totalmente complexos. O traço de um elemento $\alpha \in \mathbb{K}$ é definido por $Tr_{\mathbb{K}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$. O conjunto $K_{\mathbb{R}} = \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$ pode ser visto como subespaço de $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \subseteq \mathbb{C}^n$, dado por (a menos da permutação das coordenadas)

$$\{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \overline{y}_j \, \forall \, 1 \leq j \leq r_2\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subseteq \mathbb{C}^n.$$

O conjunto $K_{\mathbb{R}}$ é um espaço euclidiano com respeito a forma bilinear induzida pelo traço $\langle \alpha, \beta \rangle$ no corpo de números $\mathbb{K}$ dada por $\langle \alpha, \beta \rangle := \mathrm{Tr}_{\mathbb{K}}(\alpha\overline{\beta}) \in \mathbb{R}$, para quaisquer $\alpha, \beta \in \mathbb{K}$, onde $\mathrm{Tr}_{\mathbb{K}}$ é o traço definido no corpo de números $\mathbb{K}$.

Seja a aplicação $\varphi_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}_{\mathbb{R}}$ definida por $\varphi_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_n(x))$. O anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é um reticulado de posto completo em $K_{\mathbb{R}}$ sob essa aplicação. Denotamos $\Lambda_{\mathbb{K}}$ para a imagem $\varphi_{\mathbb{K}}(\mathcal{O}_K)$. Equivalentemente, podemos descrever $\Lambda_{\mathbb{K}}$ como um $\mathbb{Z}$-módulo livre $\mathcal{O}_{\mathbb{K}}$ com a forma bilinear $\langle \cdot, \cdot \rangle$. Seja $\mathrm{Aut}(\Lambda_K)$ o grupo de automorfismos do reticulado $\Lambda_{\mathbb{K}}$, isto é, o grupo de isometrias dessa forma bilinear induzida pelo traço. Em [2] é determinado quando o anel de inteiros de um corpo de números galoisiano é cíclico:

Teorema: Suponha que $\mathbb{K}/\mathbb{Q}$ seja uma extensão de Galois com grupo de Galois G. Assim, Λ_K é cíclico se, e somente se, $\mathbb{K}/\mathbb{Q}$ for uma extensão cíclica com $G = \langle \sigma \rangle$, onde o automorfismo $\sigma : \mathbb{K} \to K$ satisfaz $\rho(\varphi_K(\alpha)) = \varphi_K(\sigma(\alpha))$ para todo $\alpha \in \mathcal{O}_K$.

A analise que está sendo feita é quando os submódulos (ou ideais) de $\mathcal{O}_K$ são cíclicos. A princípio, este estudo tem sido feito quando consideramos homomorfismo canônico dado por:

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x)), \ldots, \sigma_{r_1+r_2}(x)) \, . \tag{2}$$

A aplicação σ é um monomorfismo de K em $\mathbb{R}^n$, onde cada σ_i é um monomorfismo de K em $\mathbb{R}$.

Com base nesses resultados, provamos o seguinte fato. Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d > 0$, então $\mathcal{O}_K$ tem base integral $\{1, \sqrt{d}\}$. Seja o submódulo $\mathcal{M} \subset \mathcal{O}_k$ dado por $\mathcal{M} = \langle u + v\sqrt{d}, x + y\sqrt{d} \rangle$. O reticulado $\sigma(\mathcal{M})$ é cíclico quando $u = x$, $v = -y$. Neste caso, é suficiente considerar $u \neq 0$ e $v \neq 0$. Analogamente, para o caso $d < 0$, isto é, quando $\mathbb{K} = \mathbb{Q}(i\sqrt{d}), d > 0$. Neste caso, não existe reticulado algébrico cíclico, exceto quando $d = 1$. Além disso, apresentamos uma generalização para outros módulos contidos no anel de inteiros de corpos de números cíclicos, ou seja, quando o grupo de Galois é cíclico.

Agradecimentos

Agradecemos a Fapesp, Processo 2022/02303-0 pelo apoio financeiro.

Referências

[1] A. A. Andrade. **Uma Introdução a Teoria dos Inteiros Algébricos - Volume 4**. 1. ed. São José do Rio Preto: Série Álgebra, 2021.

[2] L. Fukshansky; D. Kogan. "Cyclic and well-rounded lattices". Em: **Mosc. J. Comb. Number Theory 11** (2022), pp. 79–96. DOI: https://doi.org/10.2140/moscow.2022.11.79.

[3] D. D. Micciancio. "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions". Em: **Comput. Complexity** 16(4) (2007), pp. 365–411.

[4] C. Peikert; A. Rosen. "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices." Em: **Theory of cryptography, Lecture Notes in Comput.** Ed. por Sci. Vol. 3876. Springer, Berlin, 2006, pp. 145–166.