Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Reticulados via corpos de números de grau 3

Maria Fernanda Zordan Bonini[1], Antonio Aparecido de Andrade[2]
DMAT/UNESP, São José do Rio Preto, SP

Na teoria dos códigos corretores de erros e criptografia, temos uma estrutura matemática chamada de reticulados, que são subgrupos discretos de pontos do $\mathbb{R}^n$, e surgiram a partir de um problema geométrico de como cobrir da melhor maneira possível o espaço $\mathbb{R}^n$ com esferas idênticas de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem o maior espaço possível [5].

O problema de cobrir o espaço da melhor maneira possível é chamado de empacotamento esférico no espaço euclidiano n-dimensional. Dentre os empacotamentos esféricos, aqueles cujo conjunto de centros das esferas constituem um subgrupo discreto do $\mathbb{R}^n$, despertaram grande interesse e passaram a se chamar empacotamentos reticulados [3].

Uma das aplicações desse problema é na Teoria da Informação, onde foi observado que encontrar códigos corretores de erro eficientes está vinculado ao problema de encontrar empacotamentos esféricos densos, isto é, ao dispor as esferas no espaço, as esferas devem ocupar a maior fração desse espaço (neste caso, esta distribuição terá alta densidade), e em um dado espaço é equivalente a encontrar códigos corretores de erro eficientes. Mas as aplicações da solução do problema do empacotamento de esferas, também abrange áreas de otimização, física, química, biologia, medicina, entre outras.

Uma maneira de obtermos empacotamentos esféricos densos é através da Teoria Algébrica dos Números, fazendo uso da imersão de um corpo de números $\mathbb{K}$ (uma extensão finita dos racionais $\mathbb{Q}$) no espaço $\mathbb{R}^n$, de modo que a imagem de $\mathbb{Z}$-módulos no anel dos inteiros

$$\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \alpha \text{ é raiz de um polinômio mônico com coeficientes em } \mathbb{Z}\}$$

correspondam a reticulados no espaço $\mathbb{R}^n$ [2].

Assim, neste trabalho, consideramos $\mathbb{K}$ um corpo de números de grau n. Desse modo, existem n $\mathbb{Q}$-monomorfismos distintos σ_i: $\mathbb{K} \to \mathbb{C}$ [1], para $i = 1, 2, \ldots, n$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. 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 $\mathbb{C}$. Se um monomorfismo σ_i satisfazer $\sigma_i(\mathbb{L}) \subset \mathbb{R}$, ele é chamado real. Caso contrário, é chamado complexo. Caso σ_i for real para todo $i = 1, 2, \ldots, n$, dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão totalmente real. Analogamente, se σ_i é complexo para todo $i = 1, 2, \ldots, n$, dizemos que $\mathbb{L}/\mathbb{K}$ é uma extensão totalmente complexa.

Dessa forma, sejam $\sigma_1, \sigma_2, \ldots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ 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 $1 \leq j \leq n$, segue que 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 $\mathbb{K}$. Renumerarando esses monomorfismos da seguinte forma: para $1 \leq j \leq r_1$, considere σ_j

[1] maria.bonini@unesp.br
[2] antonio.andrade@unesp.br

os monomorfismos reais; para $1 \leq j \leq r_2$, considere 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 $1 \leq j, k \leq r_2$); para $1 \leq j \leq r_2$, sejam $\sigma_{r_1+r_2+j}$ os conjugados de σ_{r_1+j}, respectivamente (isto é, $\sigma_{r_1+r_2+j} = \alpha \circ \sigma_{r_1+j}$).

Assim, para qualquer $x \in \mathbb{K}$, definimos

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}. \tag{1}$$

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:

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

A aplicação σ é um monomorfismo de $\mathbb{K}$ em $\mathbb{R}^n$, chamada de homomorfismo de Minkowski ou homomorfismo canônico.

Dessa forma, no presente trabalho, apresentaremos construções de reticulados via o homomorfismo canônico através de corpos de números providos de uma extensão cúbica, ou seja, $[\mathbb{K} : \mathbb{Q}] = 3$ [4], onde $\mathbb{K} = \mathbb{Q}(\theta)$, com θ é raiz de um polinômio minimal $p(x) = x^3 + ax + b \in \mathbb{Z}[x]$.

Agradecimentos

Agradeço primeiramente ao meu orientador, que me dá todo apoio na pesquisa, e as minhas companheiras de estudo, Maria Clara Lopes Taddone e Linara Stéfani Fachini. Também à CAPES pelo financiamento.

Referências

[1] S. Alaca e K. S. Williams. **Introductory Algebraic Number Theory**. 1a. ed. New York: Cambridge University Press, 2004. ISBN: 978-0-511-16494-1.

[2] R. R. de Araujo. "Anéis de inteiros de corpos de números e aplicações". Dissertação de mestrado. UNESP, 2015.

[3] R. R. de Araujo. "Reticulados algébricos e aplicações a códigos e criptografia". Tese de doutorado. UNICAMP, 2018.

[4] L. S. Fachini. "Uma introdução aos corpos não abelianos de grau menor ou igual a 6". Dissertação de mestrado. UNESP, 2021.

[5] P. Samuel. **Algebraic Theory of Numbers**. Paris: HERMANN, 1970. ISBN: 9780486466668.