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

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

# O Teorema das Unidades de Dirichlet e o Reticulado Logarítmico

Maria Clara Lopes Taddone[1], Antonio Aparecido de Andrade[2]
DMAT/UNESP, São José do Rio Preto, SP

Seja $\mathbb{K}$ um corpo de números, ou seja, uma extensão finita de grau $n$ de $\mathbb{Q}$, e seja

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

o seu anel de inteiros algébricos. O conjunto das unidades (elementos inversíveis) de $\mathcal{O}_{\mathbb{K}}$, denotado por $\mathcal{O}_{\mathbb{K}}^*$, forma um subgrupo multiplicativo. Além disso, os elementos deste subgrupo são da forma $u \in \mathcal{O}_{\mathbb{K}}$ tais que $|N_{\mathbb{K}}(u)| = 1$, onde $N_{\mathbb{K}}(u)$ denota a norma do elemento $u$.

Como $\mathbb{K}$ é um corpo de números de grau $n$, segue que existem $n$ $\mathbb{Q}$-monomorfismos distintos $\sigma_j : \mathbb{K} \longrightarrow \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente $n$ raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, o monomorfismo $\sigma_j$ é chamado real, e caso contrário, o monomorfismo $\sigma_j$ é chamado imaginário. Quando todos os monomorfismos são reais, o corpo $\mathbb{K}$ é chamado um corpo totalmente real e quando são todos imaginários o corpo $\mathbb{K}$ é chamado um corpo totalmente imaginário. Se $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \ldots, n$, segue que $\alpha \circ \sigma_j = \sigma_k$, com $1 \leq k \leq n$, e que $\sigma_k = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando $r_1$ para denotar o número de índices tal que $\sigma_j(K) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$, são os monomorfismos imaginários. Assim, $n - r_1$ é um número par, e podemos escrever $r_1 + 2r_2 = n$.

Seja $\mathbb{K}^*$ o conjunto dos elementos inversíveis de $\mathbb{K}$. A função $Log : \mathbb{K}^* \longrightarrow \mathbb{R}^{r_1+r_2}$ definida por

$$Log(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1}(x)|, \log|\sigma_{r_1+1}(x)|, \ldots, \log|\sigma_{r_1+r_2}(x)|), \tag{1}$$

para todo $x \in \mathbb{K}^*$, é chamada de mergulho logarítmico de $\mathbb{K}$, em que log denota a função logarítmica com base 10 em $\mathbb{R}$ e se $y$ é um número complexo, a notação $|y|$ se refere à norma complexa de $y$, isto é, $|y| = \sqrt{\Re(y)^2 + \Im(y)^2}$ [3].

O mergulho logarítmico é um homomorfismo entre os grupos $(\mathbb{K}^*, .)$ e $(\mathbb{R}^{r_1+r_2}, +)$, uma vez que vale a propriedade

$$Log(xy) = Log(x) + Log(y), \qquad \text{para todo } \; x, y \in \mathcal{O}_{\mathbb{K}}^*. \tag{2}$$

A restrição do homomorfismo $Log$ ao grupo das unidades do anel de inteiros de $\mathbb{K}$,

$$Log : \mathcal{O}_{\mathbb{K}}^* \longrightarrow \mathbb{R}^{r_1+r_2}, \tag{3}$$

tem núcleo $W$ igual ao conjunto das raízes da unidade pertencentes a $\mathcal{O}_{\mathbb{K}}^*$. Prova-se que $W$ constitui um grupo cíclico multiplicativo finito de ordem par [4]. Além disso, a imagem $Log(\mathcal{O}_{\mathbb{K}}^*)$ é um reticulado em $\mathbb{R}^{r_1+r_2}$.

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

O reticulado $Log(\mathcal{O}_{\mathbb{K}}^*) \subset \mathbb{R}^{r_1+r_2}$ é chamado de reticulado logarítmico associado ao corpo de números $\mathbb{K}$. Quando $\mathbb{K}$ for um corpo ciclotômico de ordem igual a uma potência de um primo, o reticulado logarítmico é eficientemente decodificável [2], tal fato pode ser utilizado em problemas baseados no Problema do Ideal Primo [1].

Como um exemplo, seja o corpo quadrático real $\mathbb{K} = \mathbb{Q}(\sqrt{3})$. Neste caso, $r_1 = 2$, $r_2 = 0$ e o anel de inteiros é dado por $\mathbb{Z}[\sqrt{3}]$, uma vez que $3 \not\equiv 1 \ (mod\ 4)$. O grupo das unidades de $\mathbb{K}$ é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}$, uma vez 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. O elemento $2+\sqrt{3}$ é uma unidade fundamental de $\mathbb{K}$. 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 seja,

$$\pm 1 = N_{\mathbb{K}}(a + b\sqrt{3}) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2. \tag{4}$$

O mergulho logarítmico $Log : \mathcal{O}_{\mathbb{K}}^* \longrightarrow \mathbb{R}^2$ é definido por

$$\begin{aligned} Log(\pm(2+\sqrt{3})^e) &= \Big(\log|\sigma_1(\pm(2+\sqrt{3})^e)|, \log|\sigma_2(\pm(2-\sqrt{3})^e)|\Big) = \\ &= \Big(e\log(2+\sqrt{3}), e\log(2-\sqrt{3})\Big), \ e \in \mathbb{Z}. \end{aligned} \tag{5}$$

O reticulado $Log(\mathcal{O}_{\mathbb{K}}^*)$ tem dimensão $r = 1$ em $\mathbb{R}^2$.

Assim, neste trabalho, apresentamos o Teorema das Unidades de Dirichlet e fazendo uso dos $\mathbb{Q}$-monomorfismos de um corpo de números de grau $n$ e da função logarítmica apresentamos construções de reticulados logarítmicos, que é a imagem do subgrupo das unidades do anel de inteiros por esse mergulho.

Os reticulados obtidos por esse método de construção não tem posto completo no espaço euclidiano de dimensão igual ao grau do corpo de números. Os reticulados logarítmicos têm sido ultimamente estudados visando aplicações tanto em códigos quanto em criptografia.

## Agradecimentos

Agradeço ao meu orientador Prof. Dr. Antonio Aparecido de Andrade por todo apoio, as minhas amigas Maria Fernanda Zordan Bonini e Linara Stéfani Fachini por serem minhas companheiras de estudos e à CAPES pelo apoio financeiro.

## Referências

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

[2] R. Cramer et al. "Recovering short generators of principal ideals in cyclotomic rings". Em: **Proceedings of the 35th Annual International Conference on Advances in Cryptology** (2016), pp. 559–585.

[3] P. Ribenboim. **Classical Theory of Algebraic Numbers**. 1a. ed. New York: Springer-Verlag, 2001. ISBN: 978-1-4419-2870-2.

[4] I. Stewart e D. O. Tall. **Algebraic number theory and Fermat's last theorem**. 3a. ed. Natick, MA: AK Peters, 2002. ISBN: 1-56881-119-5.