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

Uma Nota Sobre Base Integral de um Corpo Cúbico

Maria C. L. Taddone[1], Antonio A. de Andrade[2]
Unesp, São José do Rio Preto, SP

Sejam $\mathbb{K}$ um corpo de números de grau $n > 1$ e $\alpha \in \mathbb{K}$. O elemento α é chamado um número algébrico se é raiz de um polinômio não nulo com coeficientes em $\mathbb{Q}$, e 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. Uma base de $\mathcal{O}_{\mathbb{K}}$ é chamada de uma base integral de $\mathbb{K}$. O problema de encontrar a estrutura do anel $\mathcal{O}_{\mathbb{K}}$ é equivalente ao de encontrar uma base integral de um corpo de números, sendo um tópico muito interessante e possui vários aplicações na teoria de códigos e reticulados, como pode ser visto em [4]

A valorização p-ádica de um inteiro n é definida por $v_p(n) = k$, onde p^k divide n e p^{k+1} não divide n. Dado um polinômio mônico irredutível $h(x) = x^3 - ax + b$, com $a, b \in \mathbb{Z}$, θ uma raiz de h e $\mathbb{K} = \mathbb{Q}(\theta)$. Se tivermos, para cada primo $p \in \mathbb{Z}$, que $v_p(a) \geq 2$ e $v_p(b) \geq 3$, então $\dfrac{\theta}{p} \in \mathcal{O}_{\mathbb{K}}$, portanto, podemos considerar $v_p(a) < 2$ ou $v_p(b) < 3$. ([1] p. 21)

Teorema 1. *([1] p. 63) Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo cúbico, com θ uma raiz do polinômio irredutível $h(x) = x^3 - ax + b \in \mathbb{Z}[x]$, $v_p(a) < 2$ ou $v_p(b) < 3$, com $p \in \mathbb{Z}$ um número primo. Considere os inteiros R_2, S_2, T_2, R_3, S_3, T_3, R_p, S_p e T_p, com $p > 3$, como nos Corolários 2.2.1, 2.3.1 e 2.4.1 de [1], respectivamente. Sejam $R, S \in \mathbb{Z}$ tais que para todo número primo p, implica que*

$$R \equiv R_p \pmod{p^{T_p}} \text{ e } S \equiv S_p \pmod{p^{T_p}}$$

e seja $T = \prod_{p \text{ primo}} p^{T_p}$. Uma base integral para o corpo $\mathbb{K}$ é dada por

1. $\left\{1, \dfrac{b+\theta}{3}, \dfrac{R + S\theta + \theta^2}{T}\right\}$, *se* $v_3(b) = 0$, $a \equiv 3 \pmod 9$ *e* $b^2 \equiv a + 1 \pmod{27}$;
2. $\left\{1, \theta, \dfrac{R + S\theta + \theta^2}{T}\right\}$, *caso contrário.*

Com base nestes fatos, neste trabalho, apresentamos um método para encontrar a base integral de um corpo cúbico, ou seja, um método para encontrar a base integral de um corpo de números de grau 3, $\mathbb{K} = \mathbb{Q}(\alpha)$, com α raiz de um polinômio $f(x) = x^3 + b_1x^2 + c_1x + d_1 \in \mathbb{Z}[x]$.

Seja $f(x)$ um polinômio irredutível de grau 3 dado por $f(x) = x^3 + a_1x^2 + b_1x + c_1 \in \mathbb{Z}[x]$. Fazendo a mudança de variável de x para $x - \dfrac{a_1}{3}$ no polinômio $f(x)$ ([3] p. 75), obtemos o

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

polinômio reduzido: $g_1(x) = x^3 + \dfrac{-a_1^2 + 3b_1}{3}x + \dfrac{2a_1^3 - 9a_1b_1 + 27c_1}{27}$. Tal polinômio pode ser visto como $g_1(x) = \frac{1}{27}g(x)$, onde $g(x) = 27x^3 + 9(3b_1 - a_1^2)x + 2a_1^3 - 9a_1b_1 + 27c_1$.

Consideramos neste trabalho $\mathbb{K} = \mathbb{Q}(\gamma)$, com γ uma raiz de um polinômio irredutível

$$g(x) = 27x^3 + ax + b \in \mathbb{Z}[x]. \tag{1}$$

Note que $\gamma \notin \mathcal{O}_{\mathbb{K}}$, ou seja, γ não é um inteiro algébrico.

Teorema 2. *([2] p. 85) Se γ é um número algébrico, então γ pode escrito da forma $\gamma = \dfrac{\theta}{d}$, com θ um inteiro algébrico e $d \in \mathbb{Z}$ não nulo.*

Neste caso, d é o mínimo múltiplo comum dos denominadores dos coeficientes do polinômio do qual γ é raiz e $\theta = d\gamma$

Teorema 3. *([2] p. 109) Se $\mathbb{K}$ é um corpo de números, então existe um inteiro algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$.*

Considerando γ uma raiz do polinômio (1), obtemos $\theta = 27 \cdot \gamma$ como sendo uma raiz do polinômio irredutível

$$h(x) = x^3 + 27 \cdot a \cdot x + 27^2 b \in \mathbb{Z}[x]. \tag{2}$$

Com base nos resultados anteriores, apresentamos um método para obter uma base integral para um corpo de números da forma $\mathbb{K} = \mathbb{Q}(\gamma)$, com γ uma raiz do polinômio irredutível $g(x) = 27 \cdot x^3 + a \cdot x + b$, com $a, b \in \mathbb{Z}$.

Exemplo 0.1. *Sejam o polinômio irredutível $g(x) = 27x^3 + 2x + 3$ e γ raiz de $g(x)$. Considerando $\mathbb{K} = \mathbb{Q}(\gamma)$, segue que $\gamma \notin \mathcal{O}_{\mathbb{K}}$. Como $\theta = 27\gamma \in \mathcal{O}_{\mathbb{K}}$ é uma raiz de $h(x) = x^3 + 54 \cdot x + 2187$ e $\mathbb{K} = \mathbb{Q}(\theta)$, segue que uma base integral é dada por $\left\{1, \frac{\theta}{3}, \frac{\theta^2}{27}\right\}$.*

Exemplo 0.2. *Sejam o polinômio irredutível $g(x) = 27x^3 + 3x + 1$ e γ raiz de $g(x)$. Considerando $\mathbb{K} = \mathbb{Q}(\gamma)$, segue que $\gamma \notin \mathcal{O}_{\mathbb{K}}$. Como $\theta = 27\gamma \in \mathcal{O}_{\mathbb{K}}$ é uma raiz de $h(x) = x^3 + 81 \cdot x + 729$ e $\mathbb{K} = \mathbb{Q}(\theta)$, segue que uma base integral é dada por $\left\{1, \frac{\theta}{9}, \frac{\theta^2}{81}\right\}$.*

Desse modo, através de uma translação da variável obtemos uma base integral dos corpos de números da forma $\mathbb{K} = \mathbb{Q}(\alpha)$, com α raiz de um polinômio irredutível $f(x) = x^3 + a_1x^2 + b_1x + c_1$, $a_1, b_1, c_1 \in \mathbb{Z}$ a partir da base integral do corpo $\mathbb{Q}(\gamma)$, com γ uma raiz do polinômio reduzido $g(x) = 27x^3 + ax + b$, com $a, b \in \mathbb{Z}$, fazendo uso dos casos elencados por Saban Alaca [1].

Além disso, também é possível estender para o corpo $\mathbb{K} = \mathbb{Q}(\alpha)$, com α uma raiz do polinômio irredutível $f_1(x) = a_1x^3 + b_1x^2 + c_1x + d_1 \in \mathbb{Z}[x]$, ou seja, obtemos uma base integral para os corpos gerados por esses polinômios irredutíveis.

Referências

[1] S. Alaca. "p-Integral Bases of Algebraic Number Fields". Tese de doutorado. Carleton University, 1994.

[2] S. Alaca e K. S. Williams. **Intruductory Algebraic Number Theory**. 1ª ed. New York: Cambridge University Press, 2004.

[3] A. A. Andrade. **Uma Introdução à Teoria dos Números Algébricos**. 1ª ed. São José do Rio Preto: Amazon.com, 2021.

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