Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Anéis de Inteiros Quadráticos

Bruna Neves Machado [1]
Unesp, Ilha Solteira-SP
Fabiana Aucco Egidio [2]
Unesp, Ilha Solteira-SP
Edson Donizete de Carvalho [3]
Departamento de Matemática-Unesp, Ilha Solteira-SP

1 Resumo

A importância do estudo de anéis de inteiros em sistemas de telecomunicação é de que suas propriedades algébricas permite gerá-los de forma simples e eficiente.

Consideraremos extensões quadráticas caracterizados da forma $\mathbb{K} = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$, onde m é um inteiro livre de quadrados $\mathbb{K} \subset \mathbb{C}$ é o menor corpo que contém $\mathbb{Q}$ e $\sqrt{m}$.

Dado $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$. Definimos $\overline{\alpha} = a - b\sqrt{m}$, o traço de α por $T(\alpha) = \alpha + \overline{\alpha} = 2a$ e a norma de α por $N(\alpha) = \alpha\overline{\alpha} = a^2 - mb^2$.

Temos que, α é raíz do polinômio com coeficeintes em $\mathbb{Q}$ dado por $p(x) = x^2 - T(\alpha)x + N(\alpha)$.

Dizemos que $\alpha \in \mathbb{Q}(\sqrt{m})$ é um **inteiro quadrático** se $T(\alpha)$ e $N(\alpha) \in \mathbb{Z}$. O conjuto de todos os inteiros quadráticos $O(m)$ formam um anel. São conhecidos por anéis de inteiros quadráticos $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z} \subset O(m)$ [1].

Teorema 1.1. *Sejam m um inteiro livre de quadrados e $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$.*

a) Se $m \equiv 1(mod\ 4)$, então $\alpha \in O(m)$ se, e somente se, $2a, 2b \in \mathbb{Z}$ e ambos tem a mesma paridade.

b) Se $m \equiv 2, 3(mod\ 4)$, então $O(m) = \mathbb{Z}[\sqrt{m}]$.

Demonstração:(a) Se $\alpha \in O(m)$, então $2a = T(\alpha) \in \mathbb{Z}$ e $4N(\alpha) = (2a)^2 - m(2b)^2 \in \mathbb{Z}$, logo $m(2b)^2 \in \mathbb{Z}$. Pela propriedade de m ser inteiro livre de quadrado, $2b \in \mathbb{Z}$.

Mostraremos que $2a$ e $2b$ tem a mesma paridade. Supomos que $2a$ seja par e $2b$ seja ímpar. Então, $2a = 2t$ e $2b = 2k + 1$, com $t, k \in \mathbb{Z}$. Assim, $(2a)^2 - m(2b)^2 = (2t)^2 - m(2k + 1)^2 = 4t^2 - m(4k^2 + 4k + 1) = 4t^2 - 4mk^2 + 4mk + m$.

Pelo fato de que, $m \nmid 4$, segue que $4 \nmid (2a)^2 - m(2b)^2$. O que é uma contradição. Se $(2a)$ ímpar e $(2b)$ for par, de forma análoga, obteremos uma contradição.

[1] bruna.neves28.bn@gmail.com
[2] fabiana.egidio30@hotmail.com
[3] edson.donizete@unesp.br

Logo, $2a, 2b \in \mathbb{Z}$ *tem a mesma paridade.*

(b) Suponhamos que $a \notin \mathbb{Z}$*, isto é que* $a = \frac{p}{q}$*,* $q \neq 1$ *e* $mdc(p, q) = 1$*. Assim,* $2a = \frac{2p}{q}$*. Para que* $2a \in \mathbb{Z}$ *devemos ter* $q = 2$*. Como* $mdc(p, q) = 1$*,* p *não pode ter* 2 *com um fator irredutível, isto é,* $p = p_1p_2...p_n$ *é tal que* $p_i \neq 2$*,* $\forall\, i \in \{1, ..., n\}$*. Portanto,* p *é ímpar. Assim, prova-se que* $2a$ *é da forma* $2k + 1$ *para algum* $k \in \mathbb{Z}$*.*

Como $2a$ *é ímpar, segue que* $2b$ *é ímpar (item(a)). Assim,* $(2a)^2 \equiv (2b)^2 \equiv 1(mod4)$*. Com efeito,* $(2a)^2 - 1 = (2k + 1) - 1 = 4(k^2 + k) + 1 - 1 = 4(k^2 - k)$*,* $(k^2 - k) \in \mathbb{Z}$*. Essa congruência nos leva a* $m \equiv 1(mod4)$ *então* $a, b \in \mathbb{Z}$*, isto é, se* $m \equiv 2(mod4)$ *ou* $m \equiv 3(mod4)$ *então* $a, b \in \mathbb{Z}$*. (Observe também que não podemos ter* $m \equiv 0(mod4)$*, pois* m *é livre de quadrados).Portanto,* $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ *e* $\mathbb{Z}[\sqrt{m}] = O(m)$*, desde que* $m \equiv 2$ *ou* $m \equiv 3(mod4)$*.*

Proposição 1.1. *Se* $m \equiv 1(mod\ 4)$*, então* $O(m) = \{a + b(\frac{1+\sqrt{m}}{2}) \setminus a, b \in \mathbb{Z}\}$*.*

Demonstração: Basta provarmos que $\alpha \in O(m)$ *se, e somente se, existem* $a, b \in \mathbb{Z}$ *tais que* $\alpha = a + b(\frac{1+\sqrt{m}}{2})$*. Seja* $\alpha = t + u\sqrt{m} \in O(m)$*, com* $2t, 2u \in \mathbb{Z}$ *e de mesma paridade, então* $t + u = \frac{2t+2u}{2} \in \mathbb{Z}$*. De fato,*

Caso $2t, 2u$ *sejam pares, teremos* $2t = 2k_1$ *e* $2u = 2k_2$*,* $k_1, k_2 \in \mathbb{Z}$*, assim* $\frac{2t+2u}{2} = \frac{2k_1+2k_2}{2} = \frac{2(k_1+k_2)}{2} = k_1 + k_2 \in \mathbb{Z}$*. Para o caso de* $2t, 2u$ *serem ímpares, é um caso análogo.*

Tomando $b = 2u$ *e* $a = t - u$*, obtemos:* $u = \frac{b}{2}$ *e* $t = a + u = a + \frac{b}{2}$*. Assim,* $\alpha = t + u\sqrt{m} = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{m} = a + b(\frac{1+\sqrt{m}}{2})$*. Reciprocamente, dado* $\alpha = a + b(\frac{1+\sqrt{m}}{2}) = a + b(\frac{1+\sqrt{m}}{2}) = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{m}$*, com* $a, b \in \mathbb{Z}$*. Temos que,* $2(a + \frac{b}{2}) = 2a + b \in \mathbb{Z}$ *e* $2(\frac{b}{2}) = b \in \mathbb{Z}$ *e mostra-se sem dificuldades que* $2a + b$ *e* b *tem a mesma paridade.*

Como exemplo, se $m = -1 \equiv 3(mod\, 4)$, temos $O(-1) = \mathbb{Z}[\sqrt{-1}]$ conhecido como anel de inteiros de Gauss e para $m = -3 \equiv 1(mod\, 4)$, temos $O(-3) = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ conhecido como anel de Eisenstein-Jacobi.

Agradecimentos

À FAPESP, pelo apoio financeiro no processo, nº 2018/21829-7.

Referências

[1] A. J. Engler, and P. Brumatti. *Inteiros Quadráticos e Grupos de Classe* . 23 Colóquio Brasileiro de Matemática, Publicações Matemáticas, IMPA, Rio de Janeiro, 2001.