Anéis quadráticos euclidianos e os não euclidianos

Felipe Baia Macedo

Universidade Federal do Pará

macedofelipe5@gmail.com

Resumo

A finalidade deste trabalho será apresentar alguns aspectos sobre os anéis quadráticos euclidianos complexos e classificá-los quando possuem um algoritmo da divisão, faremos uso da função norma para determinar os anéis quadráticos euclidianos. Além disso, vamos expor o caso de um anel quadrático não euclidiano que também não é um anel fatorial.

Introdução

O matemático alemão Johann Friedrich Gauss (1777-1855) introduziu os inteiros de Gauss, sendo $\alpha \in \mathbb{C}$, da forma α = { a + bi | a, b $\in \mathbb{Z}$ } e tomamos o anel Gaussiano $\mathbb{Z}[i]$ como um exemplo de anel quadrático euclidiano complexo que preserva a propriedade de ser um domínio fatorial e um domínio euclidiano com a norma $\mathcal{N}(a+bi) = a^2 + b^2$. Nosso objetivo será apresentar resultados dos anéis de inteiros quadráticos que são anéis euclidianos complexos e verificar que propriedades podemos obter quando eles são anéis não euclidianos.

Objetivos

1. Definir os anéis quadráticos euclidianos complexos.
2. Classificar os únicos anéis quadráticos euclidianos complexos que possuem um algoritmo da divisão.
3. Apresentar aspectos dos anéis quadráticos complexos euclidianos e os não euclidianos.

Resultados

Definição: Consideramos corpos quadráticos sendo subcorpos de $\mathbb{C}$ sobre $\mathbb{Q}$, de grau 2, ou seja, $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{C}$ e $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q} = 2]$, onde m $\in \mathbb{Z}$ é livre de quadrados.

Teorema: Seja $\alpha = \frac{a+b\sqrt{m}}{c}$ um inteiro de $\mathbb{Q}(\sqrt{m})$, com $c > 0$ e mdc(a,b,c) = 1, onde m $\in \mathbb{Z}$ é livre de quadrados, então

(i) se m $\equiv$ 1 (mod 4), os inteiros de $\mathbb{Q}(\sqrt{m})$ são os elementos de $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, e esses elementos serão escritos da seguinte forma,

$\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ = { $\frac{u}{2} + \frac{v}{2}\sqrt{m}$ | u,v $\in \mathbb{Z}$ } e u $\equiv$ v (mod 2), ou seja, u e v devem ter a mesma paridade.

(ii) se m $\equiv$ 2 ou 3 (mod 4), então c = 1 e os inteiros de $\mathbb{Q}(\sqrt{m})$ são os elementos de $\mathbb{Z}[\sqrt{m}]$.

Teorema: Seja o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ com m $\in \mathbb{Z}$ é livre de quadrados, temos que o anel de inteiros $\mathcal{O}_{\mathbb{K}}$.

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & se\ m \equiv 1 (mod\, 4) \\ \mathbb{Z}[\sqrt{m}] & se\ m \equiv 2\ ou\ 3 (mod\, 4) \end{cases}$$

Definição: Seja $\alpha \in \mathbb{C}$, temos que α é um inteiro algébrico se existe um polinômio mônico $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ tal que $f(\alpha) = 0$.

Proposição: Todo inteiro de $\mathbb{Q}(\sqrt{m})$ anula um polinômio mônico de grau 2 em $\mathbb{Z}[X]$.

Definição:(Algoritmo da divisão) Um domínio D é um anel euclidiano se existe uma aplicação da função norma

$$\mathcal{N} : D - \{0\} \to \mathbb{N}$$

que satisfaz as seguintes propriedades:

1) $\forall$ $\alpha, \beta \in$ D, $\beta \neq 0$, existem q, r $\in$ D tais que, $\alpha = \beta$q+ r, sendo r = 0 ou $\mathcal{N}(q) < \mathcal{N}(r)$

2) $\forall$ $\alpha, \beta \in$ D - $\{0\}$, $\mathcal{N}(\alpha) \leq \mathcal{N}(\alpha\beta)$

Teorema: Todo domínio euclidiano é principal e, portanto, fatorial.

A função norma é essencial para que anéis quadráticos sejam euclidianos, então, vamos definir para os elementos $m < 0$ do anel $\mathbb{Q}(\sqrt{m})$. Então

Definição: (Norma) Seja α = (a + b$\sqrt{m}$) e o seu conjugado representado como $\bar{\alpha}$ = (a - b$\sqrt{m}$) , com a, b $\in \mathbb{Z}$, tais que $\alpha, \bar{\alpha} \in \mathbb{Q}(\sqrt{m})$.

$$\mathcal{N}(\alpha) = \alpha\bar{\alpha} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Lema: A norma goza das seguintes propriedades:

1) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, $\forall$ $\alpha\beta \in \mathbb{Q}\sqrt{m}$.

2) Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, $\mathcal{N}(\alpha) \in \mathbb{Z}$.

3) Se $m < 0$, então $\mathcal{N}(a + bi) = a^2 + b^2$

Teorema: Se $m < 0$, existe um algoritmo da divisão em $\mathbb{Z}[\sqrt{m}]$, isto significa, $\mathbb{Z}[\sqrt{m}]$ é um anel euclidiano, quando m $\in$ { -1, -2, -3, -7, -11}.

Exemplo 1: Sejam m = -1, $\alpha = 7 - 6i$, $\beta = 2 + i$.

Temos, -1 $\equiv$ 3(mod 4) vamos encontrar q = x + y$\sqrt{m}$, r = s + t$\sqrt{m}$ $\in \mathbb{Z}[\sqrt{-1}]$ tais que α = qβ + r com $\mathcal{N}(r) < \mathcal{N}$(b).

Seja $\frac{\alpha}{\beta}$ = a + b$\sqrt{-1}$ = $\frac{8}{5} - \frac{19}{5}i$, temos a =$\frac{8}{5}$ e b = - $\frac{19}{5}$.

Tomamos x e y $\in \mathbb{Z}$ tais que | a - x | $\leq \frac{1}{2}$ e | b - y | $\leq \frac{1}{2}$.

Seja x = 2. Então

$$|a - x| = |\tfrac{8}{5} - 2| = | - \tfrac{2}{5}| = \tfrac{2}{5} \leq \tfrac{1}{2}.$$

Tomando y = - 4.

$$|b - y| = | - \tfrac{19}{5} + 4| = |\tfrac{1}{2}| = \tfrac{1}{2} \leq \tfrac{1}{2}.$$

Desse modo,

$$q = x + y\sqrt{m} = 2 - 4\sqrt{-1},$$
$$r = \alpha - q\beta = 7 - 6i - (2 - 4i)(2 + i) = -1$$

Portanto,

$$\mathcal{N}(r) = \mathcal{N}(-1) = 1 < 5 = \mathcal{N}(2 + i) = \mathcal{N}(\beta)$$

■

É suficiente para $\mathcal{O}_{\mathbb{K}}$ ser um domínio fatorial, porém não necessário, que ele seja euclidiano,

Exemplo 2: Sejam $m \in \{-19, -43, -67, -163\}$ então $\mathbb{Z}[\sqrt{m}]$ são anéis fatoriais que não são anéis euclidianos.

Exemplo 3: Sejam $\mathbb{Z}[\sqrt{-3}]$ e $\mathbb{Z}[\sqrt{-11}]$ são exemplos de anéis euclidianos complexos que não são anéis fatoriais.

Exemplo 4: Sejam $\mathbb{Z}[\sqrt{-5}]$ e $\mathbb{Z}[\sqrt{-13}]$ são exemplos de anéis não euclidianos que não são anéis fatoriais.

Referências

[1] ANDRADE, .J.F, *Tópicos especiais em álgebra*, SBM, 2013.

[2] ENDLER, .O, *Teoria dos números algébricos*, IMPA, 2014.

[3] GARCIA, .A e LEQUAIN, .Y, *Elementos de álgebra*, IMPA, 2022.

[4] GONÇALVES, .A. *Introdução à álgebra*, 5º edição. Rio de Janeiro, IMPA, 2011.

[5] FRÖHLICH. A e TAYLOR. M.J. *Algebraic number theory*, Cambridge University Press, 1993.

[6] NEUKIRCH. J. *Algebraic number theory*, Springer, 1992.

Agradecimentos

Grato à Deus, aos meus amigos e familiares, ao apoio da Facmat-UFPA, a PROEX-UFPA pelo suporte financeiro, ao 34º Colóquio Brasileiro de Matemática pela oportunidade, e em especial ao Prof. Dr Jean Carlos de Aguiar Lelis por sua atenção e incentivo.