

Oliviana do Nascimento

Vinicius Loti

Orientador: Danilo S. da Silveira

Os Inteiros Gaussianos

Anéis

Seja A um conjunto com pelo menos dois elementos munido de duas operações chamadas de adição (+) e multiplicação ($\bullet$). A tripla $(A, +, \bullet)$ é chamado de *anel* se as seguintes propriedades forem satisfeitas:

A1) $(a + b) + c = a + (b + c)$, $\forall a, b, c \in A$. (*Associatividade da adição*)

A2) $a + b = b + a$, $\forall a, b \in A$. (*Comutatividade da adição*)

A3) $\exists 0 \in A$ tal que $0 + a = a$, $\forall a \in A$. (*Existência do elemento neutro da adição.*)

A4) Para todo $a \in A$, $\exists -a \in A$ tal que $a + (-a) = a - a = 0$. (*Existência do simétrico de todo elemento de A.*)

M1) $(a \bullet b) \bullet c = a \bullet (b \bullet c)$, $\forall a, b, c \in A$. (*Associatividade da multiplicação.*)

M2) $\exists 1 \in A$ tal que $1 \bullet a = a$, $\forall a \in A$. (*Existência da unidade.*)

AM) $a \bullet (b + c) = a \bullet b + a \bullet c$, $\forall a, b, c \in A$. (*Distributividade da multiplicação em relação a soma.*)

Obs.: A partir de agora, vamos denotar a multiplicação de dois elementos $a \bullet b$ por ab .

Exemplos: O conjunto $\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \text{ e } i^2 = -1 \}$ é um exemplo de anel. As operações neste conjunto são definidas por $(a + bi) + (c + di) = (a + c) + (b + d)i$ e $(a + bi)(c + di) = (ac - bd) + (ad + cb)i$. O elemento neutro aditivo é $(0 + 0i) = 0$ e o elemento neutro multiplicativo é $(1 + 0i)$. O inverso aditivo de um elemento $(a + bi)$ é $(-a + (-bi))$, pois $(a + bi) + (-a + (-bi)) = (a - a) + (b - b)i = 0 + 0i = 0$.

Subanéis

Um subconjunto não vazio B de um anel $(A, +, \bullet)$ é dito *subanel de A* se B é um anel com as operações de A .

Proposição: Sejam A um anel e B um subconjunto de A . Temos que B é um subanel de A se e somente se são satisfeitas as condições:

(a) A unidade $1 \in B$;

(b) $\forall a, b \in B, a - b \in B$ e $ab \in B$.

Demonstração: ($\Rightarrow$) Se B for um subanel de A , então as condições a) e b) são imediatamente satisfeitas.

($\Leftarrow$) Suponhamos que as condições (a) e (b) são satisfeitas. Como $1 \in B, 0 = 1 - 1 \in B$. Se $x \in B, -x = 0 - x \in B$.

Sejam $a, b \in B$. Como $-b \in B$, logo $a + b = a - (-b) \in B$ e como $ab \in B$, podemos concluir que B é um subanel.

Com esta proposição, podemos verificar de uma forma mais eficaz se um determinado subconjunto de um anel é um subanel.

Exemplos: O conjunto $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ e o conjunto $\mathbb{Z}[\sqrt{2}]$ é um subanel de $\mathbb{R}$.

Inteiros Gaussianos

Um inteiro gaussiano é um elemento da forma $a + bi$, em que $a, b \in \mathbb{Z}$ e $i^2 = -1$. Chamaremos o conjunto $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z} \text{ e } i^2 = -1\}$ de *Anel dos Inteiros Gaussianos*. O termo Anel é justificado pela seguinte proposição.

Exemplos: $(8 + 5i)$ é um inteiro gaussiano, mas $(1,5 + 3i)$ não é, pois $1,5 \notin \mathbb{Z}$.

Obs.: $\mathbb{Z} \subset \mathbb{Z}[i]$, pois $\mathbb{Z} = \{a + 0i \mid a \in \mathbb{Z} \text{ e } i^2 = -1\}$. Como a unidade $(1 + 0i) = 1 \in \mathbb{Z}$ e $\forall (a + 0i), (b + 0i) \in \mathbb{Z}, (a + 0i) + (b + 0i) = a + b \in \mathbb{Z}$ e $(a + 0i)(b + 0i) = ab \in \mathbb{Z}$, podemos concluir que $\mathbb{Z}$ é um subanel de $\mathbb{Z}[i]$.

Proposição: O conjunto $\mathbb{Z}[i]$ é um subanel de $\mathbb{C}$.

Demonstração:

(a) A unidade é $1 = 1 + 0i \in \mathbb{Z}[i]$.

(b) Sejam $(a + bi)$ e $(a' + b'i) \in \mathbb{Z}[i]$, $(a + bi) - (a' + b'i) = (a + a') - (b + b')i \in \mathbb{Z}[i]$.

$(a+bi)(a'+b'i) = aa' + ab'i + ba'i + bb'i^2 = (aa' - bb') + (ab' + a'b)i \in \mathbb{Z}[i]$.

Vamos definir por *função norma* a seguinte função:

$$N: \mathbb{C} \rightarrow \mathbb{R}^+$$

$$(a+bi) \mapsto |a + bi|^2 = a^2 + b^2$$

Geometricamente, a função norma nos fornece o quadrado do comprimento de um vetor $x \in \mathbb{C}$ no plano complexo.

Exemplos: $N(5 + 3i) = 5^2 + 3^2 = 34$ e $N(2,5 + 4i) = (2,5)^2 + 4^2 = 22,25$

Obs.: Se $z = (a + bi) \in \mathbb{Z}[i]$, então $N(z) = (a^2 + b^2) \in \mathbb{Z}^+$.

Proposição: Se $z = (a + bi)$ e $z' = (a' + b'i) \in \mathbb{Z}[i]$, então $N(zz') = N(z)N(z')$.

Demonstração: $N(zz') = N((aa' - bb') + (ab' + a'b)i) = (aa' - bb')^2 + (ab' + a'b)^2 = (aa')^2 - 2aa'bb' + (bb')^2 + (ab')^2 + 2ab'a'b + (a'b)^2 = (aa')^2 + (bb')^2 + (ab')^2 + (a'b)^2 = (a^2 + b^2)(a'^2 + b'^2) = N(z)N(z')$

Exemplo: $N((3 + 5i)(2 + 3i)) = N(6 + 9i + 10i + 15i^2) = N(-9 + 19i) = 9^2 + 19^2 = 442 = 34 \cdot 13 = (9 + 25)(4 + 9) = (3^2 + 5^2)(2^2 + 3^2) = N(3 + 5i)N(2 + 3i)$

Seja $(A, +, \cdot)$ um anél. Dizemos que $a \in A$ é invertível se $\exists b \in A$ tal que $ab = 1$. O elemento b é chamado inverso multiplicativo de a .

Exemplo: $\frac{1}{3}$ é o inverso de 3 em $\mathbb{Q}$, pois $3 \cdot \frac{1}{3} = 1$.

Proposição: Seja $x = (a + bi) \in \mathbb{Z}[i]$. São equivalentes as seguintes afirmações:

(a) x é invertível em $\mathbb{Z}[i]$;

(b) $N(x) = 1$;

(c) $x \in \{1, -1, i, -i\}$

Demonstração:

(a) $\Rightarrow$ (b) Se x é invertível, $\exists x' \in \mathbb{Z}[i]$ tal que $xx' = 1$. Pela proposição anterior, $N(x)N(x') = N(xx') = N(1) = 1$. Como $N(x)$ e $N(x') \in \mathbb{Z}^+$, segue que $N(x) = N(x') = 1$.

(b) $\Rightarrow$ (c) Suponhamos que $N(x) = 1$. Logo $N(x) = N(a + bi) = a^2 + b^2 = 1$, cujas soluções em $\mathbb{Z} \times \mathbb{Z}$ são $(0, \pm 1)$ e $(\pm 1, 0)$. Logo $x \in \{1, -1, i, -i\}$.

(c) $\Rightarrow$ (a) É óbvio que todos os elementos do conjunto $\{1, -1, i, -i\}$ são invertíveis em $\mathbb{Z}[i]$.

Dizemos que um anel $(A, +, \cdot)$ não possui divisores de zero, se $\forall x, y \in A, xy = 0 \Rightarrow x = 0$ ou $y = 0$.

Exemplos: O anel $\mathbb{R}$ não possui divisores de zero, pois se $a, b \in \mathbb{R}, ab = 0 \Rightarrow a = 0$ ou $b = 0$.

O anel das classes de congruência $\mathbb{Z}_8$ possui divisores de zero, pois $\overline{2}, \overline{4} \in \mathbb{Z}_8$, $\overline{2} * \overline{4} = \overline{0}$.

Seja $(A, +, \cdot)$ um anel. Dizemos que $(A, +, \cdot)$ é um corpo se todo elemento de $A - \{0\}$ é invertível e se $(A, +, \cdot)$ é um anel comutativo e que não possui divisores de zero.

Exemplo: O anel $(\mathbb{Q}, +, \cdot)$ é um corpo, pois $\forall a \in \mathbb{Q}$, podemos definir o inverso multiplicativo de a como $(1/a)$, pois se $ab = 1 \Rightarrow b = (1/a)$.

Sejam $(a + bi), (a' + b'i) \in \mathbb{Z}[i]$. Podemos ver que $\mathbb{Z}[i]$ não possui divisores de zero, pois $(a + bi)(a' + b'i) = 0 \Rightarrow (aa' - bb') + (ab' + a'b)i = 0$ nos leva a um sistema cujas soluções são $a = b = 0$ ou $a' = b' = 0$. Apesar disso, podemos o anel $(\mathbb{Z}[i], +, \cdot)$ não é um corpo, pois pela proposição acima, vimos que os únicos elementos de $\mathbb{Z}[i]$ que são invertíveis são $\{1, -1, i, -i\}$.