

Anéis

José Antônio O. Freitas

MAT-UnB

16 de setembro de 2020

Definição

Seja A um conjunto não vazio. Dizemos que A está munido (ou equipado) de uma **operação binária** quando existe uma função

$$\Delta : A \times A \rightarrow A$$

$$(a, b) \mapsto a\Delta b$$

Uma operação binária também é chamada de uma **operação interna** em A .

Exemplos

- 1) *A soma usual nos conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} é uma operação binária.*
- 2) *A multiplicação usual nos conjuntos \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} é uma operação binária.*
- 3) *Seja $m > 1$, $m \in \mathbb{Z}$ fixo. A soma e a multiplicação definidos em $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ são operações binárias.*
- 4) *A operação \div em \mathbb{Q}^* é uma operação binária.*
- 5) *Já em \mathbb{N} , \mathbb{Z} , \mathbb{Z}^* e em \mathbb{Q} a operação \div não é uma operação binária.*

Definição

Seja A um conjunto não vazio A no qual estão definidas duas operações binárias \oplus e \otimes , chamadas soma e produto. Dizemos que (A, \oplus, \otimes) é um **anel** quando as seguintes condições são verdadeiras:

i) **Associatividade**: para todos $x, y, z \in A$ vale que

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$

Essa propriedade é chamada **propriedade associativa da soma**.

ii) **Comutatividade**: Para todos $x, y \in A$ vale

$$x \oplus y = y \oplus x.$$

Definição

- iii) **Elemento Neutro:** Existe em A um elemento denotado por 0 (zero) ou 0_A tal que para todo elemento $x \in A$ vale

$$x \oplus 0_A = x = 0_A \oplus x.$$

Tal elemento 0_A é chamado de **elemento neutro da soma** ou simplesmente **elemento neutro**.

- iv) **Elemento Oposto:** Para cada elemento $x \in A$, existe $y \in A$ tal que

$$x \oplus y = 0_A = y \oplus x.$$

Tal elemento y é chamado de **oposto aditivo** de x ou simplesmente **oposto** de x .

Definição

v) **Associatividade:** Para todos $x, y, z \in A$, vale que

$$(x \otimes y) \otimes z = x \otimes (y \otimes z).$$

vi) **Distributividade:** Para todos $x, y, z \in A$ vale

$$(x \oplus y) \otimes z = x \otimes z \oplus y \otimes z.$$

Essa propriedade é chamada **distributiva da soma em relação ao produto**.

Definição

vii) **Distributividade:** Para todos $x, y, z \in A$ vale

$$x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z.$$

Essa é a propriedade **distributiva do produto em relação à soma**.

Observações:

Seja (A, \oplus, \otimes) uma anel.

1) **Comutatividade:** Se para todos $x, y \in A$ vale

$$x \otimes y = y \otimes x.$$

Dizemos que (A, \oplus, \otimes) é um **anel comutativo**.

2) **Unidade:** Se existe em A um elemento denotado por 1 ou 1_A tal que

$$x \otimes 1 = x = 1 \otimes x,$$

para todo $x \in A$, então dizemos que (A, \oplus, \otimes) é um **anel com unidade** ou um **anel unitário**. O elemento 1_A é chamado de **unidade** de A ou **elemento neutro da multiplicação** de A .

Observações:

- 3) Se um anel (A, \oplus, \otimes) satisfaz as duas propriedades anteriores dizemos que (A, \oplus, \otimes) é um **anel comutativo com unidade** ou um **anel comutativo unitário**.
- 4) Seja (A, \oplus, \otimes) uma anel. Quando não houver chance de confusão com relação às operações envolvidas diremos simplesmente que A é uma anel.

Exemplos

1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_m, \oplus, \otimes)$ são anéis associativos, comutativos e com unidade.

Exemplos

2) Consideremos em $\mathbb{Z} \times \mathbb{Z}$ as operações \oplus e \otimes definidas por

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$(a, b) \otimes (c, d) = (ac - bd, ad + bc).$$

Mostre que $(\mathbb{Z} \times \mathbb{Z}, \oplus, \otimes)$ é um anel comutativo e com unidade.

Observação:

Seja (A, \oplus, \cdot) um anel. Para simplificar a notação vamos denotar a operação \oplus por $+$ e a operação \otimes por \cdot e assim escrever simplesmente que $(A, +, \cdot)$ é um anel.

Proposição

Seja $(A, +, \cdot)$ uma anel. Então:

- i) O elemento neutro é único.*
- ii) Para cada $x \in A$ existe um único oposto.*
- iii) Para todo $x \in A$, $-(-x) = x$.*
- iv) Dados $x_1, x_2, \dots, x_n \in A$, $n \geq 2$, então*

$$-(x_1 + x_2 + \dots + x_n) = (-x_1) + (-x_2) + \dots + (-x_n).$$

Proposição

v) Para todos $a, x, y \in A$, se $a + x = a + y$, então $x = y$.

vi) Para todo $x \in A$, $x \cdot 0_A = 0_A = 0_A \cdot x$.

vii) Para todos $x, y \in A$, temos $x(-y) = (-x)y = -(xy)$.

viii) Para todos $x, y \in A$, $xy = (-x)(-y)$.

Prova:

Prova:

i) Suponha que existam $0_1, 0_2 \in A$ elementos neutros de A . Assim

$$x + 0_1 = x \quad \text{e} \quad x + 0_2 = x$$

para todo $x \in A$. Assim

$$0_1 = 0_1 + 0_2 = 0_2$$

e portanto o elemento neutro é único.

ii) De fato, dado $x \in A$ suponha que existam $y_1, y_2 \in A$ tais que

$$x + y_1 = 0_A \quad \text{e} \quad x + y_2 = 0_A.$$

Daí

$$y_1 = y_2 + 0_A = y_1 + (x + y_2) = (y_1 + x) + y_2 = 0_A + y_2 = y_2.$$

Logo o oposto de x é único e daí será denotado por $-x$.

iii) Dado $x \in A$, então $-x$ é oposto de x , isto é, $x + (-x) = 0_A$. Logo o oposto de $(-x)$ é x , ou seja, $-(-x) = x$.

iv) Segue usando indução sobre n .

v) Suponha que $a + x = a + y$. Seja $-a$ o oposto de a daí

$$\begin{aligned}
 x &= 0_A + x \\
 &= [(-a) + a] + x \\
 &= (-a) + (a + x) \\
 &= (-a) + (a + y) \\
 &= [(-a) + a] + y \\
 &= 0_A + y = y
 \end{aligned}$$

como queríamos.

vi) Temos $0_A + x \cdot 0_A = a \cdot 0_A = a(0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$. Assim do item anterior segue que $x \cdot 0_A = 0_A$.

vii) Provemos que $x(-y) = -(xy)$:

$$x(-y) + xy = x((-y) + y) = x \cdot 0_A = 0_A,$$

portanto $-xy = x(-y)$.

viii) Basta usar o caso anterior.

Definição

Um anel comutativo $(A, +, \cdot)$ é dito ser um **anel de integridade** quando para todos $x, y \in A$, se $xy = 0_A$, então $x = 0_A$ ou $y = 0_A$. Um anel de integridade também é chamado de **domínio de integridade** ou simplesmente de **domínio**.

Observação:

Se x e y são elementos não nulos de um anel A tais que $xy = 0_A$, então x e y são chamados de **divisores próprios de zero**.

Exemplos

- 1) *Os anéis \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} são anéis de integridade.*
- 2) *Em geral \mathbb{Z}_m não é anel de integridade, por exemplo, em \mathbb{Z}_4 , $\bar{2} \neq \bar{0}$, no entanto $\bar{2} \otimes \bar{2} = \bar{4} = \bar{0}$.*

Exemplos

3) $M_n(\mathbb{R})$ não é um anel de integridade, por exemplo, em $M_2(\mathbb{R})$

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

4) Suponha que $m = nk$, $m > n > 1$ e $m > k > 1$. Logo, em \mathbb{Z}_m , $\bar{n} \neq \bar{0}$ e $\bar{k} \neq \bar{0}$ e no entanto $\bar{n} \otimes \bar{k} = \bar{m} = \bar{0}$. Logo, se m não é primo, então \mathbb{Z}_m não é um anel de integridade. Agora, suponha que $m = p$ primo. Sejam $\bar{x}, \bar{y} \in \mathbb{Z}_m$ tais que $\bar{x} \otimes \bar{y} = \bar{0}$, ou seja, $xy \equiv 0 \pmod{p}$. Daí $p \mid xy$. Logo $p \mid x$ ou $p \mid y$. Portanto, $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$. Assim, \mathbb{Z}_m é anel de integridade se, e somente se, m é primo.