

Anéis - Homomorfismos

José Antônio O. Freitas

MAT-UnB

5 de outubro de 2020

Definição

Um homomorfismo do anel $(A, +, \cdot)$ no anel (B, \oplus, \otimes) é uma função $f: A \rightarrow B$ que satisfaz:

i) $f(x + y) = f(x) \oplus f(y)$, para todos $x, y \in A$;

ii) $f(x \cdot y) = f(x) \otimes f(y)$, para todos $x, y \in A$.

Proposição

Sejam $(A, +, \cdot)$ e (B, \oplus, \otimes) anéis e seja $f: A \rightarrow B$ um homomorfismo. Então:

$$i) f(0_A) = 0_B$$

$$ii) f(-x) = -f(x), \text{ para todo } x \in A.$$

Prova:

i) Fazendo $x = y = 0_A$, temos

$$f(0_A) = f(0_A + 0_A) = f(0_A) \oplus f(0_A)$$

Somando $-f(0_A)$ em ambos os lados obtemos

$$f(0_A) \oplus (-f(0_A)) = (f(0_A) \oplus f(0_A)) \oplus (-f(0_A))$$

$$0_B = f(0_A) \oplus 0_B$$

$$f(0_A) = 0_B$$

ii) Temos $0_B = f(0_A) = f(x + (-x)) = f(x) \oplus f(-x)$. Assim somando $-f(x)$ em ambos os lados obtemos

$$\begin{aligned} 0_B \oplus (-f(x)) &= [f(x) \oplus f(-x)] + (-f(x)) \\ -f(x) &= f(-x) \oplus (f(x) \oplus (-f(x))) \\ f(-x) &= -f(x) \end{aligned}$$

como queríamos. ■

Definição

Seja $f: A \rightarrow B$ um homomorfismo, onde A e B são anéis. Dizemos que

- i) f é um epimorfismo se f for sobrejetora.
- ii) f é um monomorfismo se f for injetora.
- iii) f é um isomorfismo se f for bijetora.
- iv) Quando $A = B$ e f é um isomorfismo, então f é um automorfismo.

Definição

Sejam $(A, +, \cdot)$ e (B, \oplus, \otimes) anéis e $f: A \rightarrow B$ um homomorfismo de anéis. Então o subconjunto de A definido por

$$\ker(f) = \{x \in A \mid f(x) = 0_B\}$$

é chamado de **kernel** ou **núcleo** de f .

Proposição

Sejam $(A, +, \cdot)$ e (B, \oplus, \otimes) anéis e $f: A \rightarrow B$ um homomorfismo de anéis. Então:

- i) $\ker(f)$ é um subanel de A .
- ii) f é injetora se, e somente se, $\ker(f) = \{0_A\}$.

Prova:

i) Primeiro note que sendo f é um homomorfismo então $f(0_A) = 0_B$.

Logo $0_A \in \ker(f)$, isto é, $\ker(f) \neq \emptyset$.

Agora dados $x, y \in \ker(f)$ precisamos mostrar que $x - y \in \ker(f)$ e $xy \in \ker(f)$, e para mostrar isso basta mostrar que $f(x - y) = 0_B$ e $f(xy) = 0_B$. Inicialmente como $x, y \in \ker(f)$ daí $f(x) = f(y) = 0_B$. Assim

$$f(x - y) = f(x + (-y)) = f(x) \oplus f(-y) = f(x) \oplus (-f(y)) = 0_B \oplus 0_B = 0_B$$

$$f(xy) = f(x) \otimes f(y) = 0_B \otimes 0_B = 0_B$$

Logo $x - y \in \ker(f)$ e $xy \in \ker(f)$. Portanto $\ker(f)$ é um subanel de A .

- ii) Primeiro suponha que f é injetora e vamos mostrar que $\ker(f) = \{0_A\}$. Para isso seja $x \in \ker(f)$. Então

$$f(x) = 0_B,$$

mas f sendo um homomorfismo temos $f(0_A) = 0_B$. Daí

$$f(x) = 0_B = f(0_A).$$

E como f é injetora, por hipótese, segue que $x = 0_A$. Logo $\ker(f) = \{0_A\}$.

Agora suponha que $\ker(f) = \{0_A\}$ e vamos mostrar que f é injetora.
Para isso sejam $x_1, x_2 \in A$ tais que $f(x_1) = f(x_2)$. Daí

$$f(x_1) = f(x_2)$$

$$f(x_1) \oplus (-f(x_2)) = 0_B$$

$$f(x_1) \oplus f(-x_2) = 0_B$$

$$f(x_1 - x_2) = 0_B$$

Logo $x_1 - x_2 \in \ker(f) = \{0_A\}$. Com isso $x_1 - x_2 = 0_A$, isto é, $x_1 = x_2$.
Portanto f é injetora. ■

Proposição

Sejam $(A, +, \cdot)$ e (B, \oplus, \otimes) anéis e seja $f: A \rightarrow B$ um homomorfismo sobrejetor de anéis.

i) Se A tem unidade, então B tem unidade e

$$f(1_A) = 1_B.$$

ii) Se A tem unidade e $x \in A$ possui inverso multiplicativo, então $f(x)$ tem inverso e

$$[f(x)]^{-1} = f(x^{-1}).$$

Prova:

- i) Inicialmente como num anel a unidade é única, para mostrar que B possui unidade basta mostrar que

$$y \otimes f(1_A) = y = f(1_A) \otimes y$$

para todo $y \in B$. Sendo assim, seja $y \in B$. Como f é sobrejetor então existe $x \in A$ tal que $f(x) = y$. Assim

$$y \otimes f(1_A) = f(x) \otimes f(1_A) = f(x \cdot 1_A) = f(x) = y$$

$$f(1_A) \otimes y = f(1_A) \otimes f(x) = f(1_A \cdot x) = f(x) = y$$

para todo $y \in B$. Portanto B possui unidade e

$$1_B = f(1_A).$$

- ii) Novamente, devido á unicidade do inverso em um anel, para mostrar que $f(x)$ possui inverso basta mostrar que

$$f(x) \otimes f(x^{-1}) = 1_B = f(x^{-1}) \otimes f(x)$$

desde que $x \in A$ possua inverso multiplicativo. Sendo assim suponha que $x \in A$ possui inverso multiplicativo. Seja x^{-1} o inverso multiplicativo de x em A . Temos

$$f(x) \otimes f(x^{-1}) = f(x \cdot x^{-1}) = f(1_A) = 1_B$$

$$f(x^{-1}) \otimes f(x) = f(x^{-1} \cdot x) = f(1_A) = 1_B$$

Portanto $f(x)$ possui inverso multiplicativo e

$$[f(x)]^{-1} = f(x^{-1}),$$

como queríamos.

Definição

Seja $(A, +, \cdot)$ um anel comutativo. Um subconjunto não-vazio $I \subseteq A$ é chamado de **ideal** de A se:

- i) para todos $x, y \in I$, temos $x - y \in I$.
- ii) Para todo $\alpha \in A$ e todo $x \in I$, temos $\alpha \cdot x \in I$.

Observação:

Quando $I = A$ ou $I = \{0_A\}$, dizemos que I é um **ideal trivial**.

Proposição

Seja A um anel comutativo e I um ideal de A . Então:

- i) $0_A \in I$.
- ii) $-x \in I$ para todo $x \in I$.
- iii) Se $1_A \in I$, então $I = A$.

Prova:

- i) Da definição de ideal temos $\alpha \cdot x \in I$ para todo $x \in I$ e todo $\alpha \in A$. Assim dado $x \in I$ $0_A = 0_A \cdot x \in I$.
- ii) Como $0_A \in I$, dado $x \in I$ da definição de ideal segue que $0_A - x \in I$, isto é, $-x \in I$.
- iii) Suponha que $1_A \in I$. Como I é ideal, para todo $\alpha \in A$ e todo $x \in I$ devemos ter $\alpha \cdot x \in I$. Assim, em particular, $1_A \cdot x \in I$ para todo $x \in A$. Logo, $A \subseteq I$ e como $I \subseteq A$, então $I = A$.



Exemplos

- 1) Em \mathbb{Z} todos os ideais não triviais são da forma $m\mathbb{Z}$, $m > 1$.
- 2) No anel \mathbb{Z}_p , onde p é um número primo, os únicos ideais são os triviais $\{\bar{0}\}$ e \mathbb{Z}_p .

De fato, seja $I \subseteq \mathbb{Z}_p$ um ideal, $I \neq \{\bar{0}\}$. Provemos que $I = \mathbb{Z}_p$. Para isso, vamos provar que $\bar{1} \in I$. Seja $\bar{a} \in I$, $\bar{a} \neq \bar{0}$, pois $I \neq \{\bar{0}\}$. Como p é primo, $\text{mdc}(a, p) = 1$, daí existe $\bar{b} \in \mathbb{Z}_p$, $\bar{b} \neq \bar{0}$, tal que $\bar{1} = \bar{a} \otimes \bar{b}$. Mas I é ideal e $\bar{a} \in I$, logo $\bar{1} = \bar{a} \otimes \bar{b} \in I$.

Portanto $I = \mathbb{Z}_p$.

- 3) Os únicos ideais não triviais de $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ são:

$$I_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$$

$$I_2 = \{\bar{0}, \bar{4}\}$$

Definição

Seja I um ideal de um anel $(A, +, \cdot)$. Dados $x, y \in A$ dizemos que x é **congruente a y módulo I** quando $x - y \in I$. Neste caso, escrevemos $x \equiv y \pmod{I}$.

Proposição

A congruência módulo I é uma relação de equivalência em $A \times A$, onde A anel unitário.

Prova: Como $0 = 0_A \in I$ e para todo $x \in I$, $x - x = 0 \in I$, então $x \equiv x \pmod{I}$.

Suponha que $x \equiv y \pmod{I}$. Então $x - y \in I$. Como $-1 \in A$, $y - x = -(x - y) = -[(x - y)1] = (x - y)(-1) \in I$, ou seja, $y \equiv x \pmod{I}$. Agora, se $x \equiv y \pmod{I}$ e $y \equiv z \pmod{I}$, então $x - y \in I$ e $y - z \in I$. Daí, $x - z = (x - y) + (y - z) \in I$, ou seja, $x \equiv z \pmod{I}$.

Logo, é uma relação de equivalência. ■

Seja $y \in A$. A classe de equivalência módulo I de y é

$$C(y) = \{x \in A \mid x \equiv y \pmod{I}\} = \{x \in A \mid x - y \in I\}.$$

Agora, $x - y \in I$ significa que existe $t \in I$, tal que $x - y = t$. Logo, $x = y + t$, onde $t \in I$.

Assim,

$$C(y) = \{y + t \mid t \in I\} = y + I.$$

Observação:

Denotamos por $y + I$ (ou $I + y$) a classe de equivalência módulo I de $y \in A$.

*Denotamos por $\frac{A}{I}$ o conjunto de todas as classes de equivalência, tal conjunto é chamado de **quociente do anel A pelo ideal I** .*

Exemplos

1) Seja A um anel com unidade e $I_1 = \{0\}$ e $I_2 = A$ ideais. Então:

i) Dado $x \in A$:

$$C(x) = x + I_1 = \{x + 0\} = \{x\}.$$

Assim $\frac{A}{I_1} = \{x + I_1 \mid x \in A\}$, logo existem tantas classes de equivalência quantos forem os elementos de A .

ii) Para $I_2 = A$ temos:

$$C(0_A) = 0_A + I_2 = \{0_A + t \mid t \in I_2\}.$$

Como $I_2 = A$, para todo $x \in A$ temos $x \in C(0_A)$ logo existem uma única classe de equivalência e $\frac{A}{I_2} = \{0_A + I_2\}$.

Exemplos

2) Seja $A = \mathbb{Z}$. Sabemos que os ideais de \mathbb{Z} são da forma $m\mathbb{Z}$, $m > 1$. Seja $I = m\mathbb{Z}$ um ideal de \mathbb{Z} . Assim $x \equiv y \pmod{I}$ se, e só se, $x - y \in I$. Mais isso ocorre se, e somente se, $x - y = mk$, para algum $k \in \mathbb{Z}$. Logo $x \equiv y \pmod{I}$ se, e só se, $m \mid (x - y)$. Portanto, $\frac{\mathbb{Z}}{I} = \mathbb{Z}_m$.

Agora seja I ideal e A um anel. Temos

$$\frac{A}{I} = \{y + I \mid y \in A\}$$

onde $y + I = \{y + t \mid t \in I\}$ e $y \in A$.

Vamos definir uma soma \oplus e um produto \otimes em $\frac{A}{I}$ por

$$(x + I) \oplus (y + I) = (x + y) + I$$

$$(x + I) \otimes (y + I) = (xy) + I$$

para $x + I, y + I \in \frac{A}{I}$.

Verifiquemos que a soma e o produto em $\frac{A}{I}$ não dependem do representante da classe de equivalência. Para isso sejam $x_1 + I$, $x_2 + I$, $y_1 + I$, $y_2 + I \in \frac{A}{I}$ tais que

$$x_1 + I = x_2 + I$$

$$y_1 + I = y_2 + I$$

Então

$$(x_1 + I) \oplus (y_1 + I) = (x_1 + y_1) + I$$

$$(x_2 + I) \oplus (y_2 + I) = (x_2 + y_2) + I$$

Como $x_1 + I = x_2 + I$, então $x_1 - x_2 \in I$ e como $y_1 + I = y_2 + I$, então $y_1 - y_2 \in I$. Mas I é ideal, logo

$(x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2) \in I$, ou seja

$$(x_1 + I) \oplus (y_1 + I) = (x_2 + I) \oplus (y_2 + I).$$

Agora,

$$(x_1 + I) \otimes (y_1 + I) = (x_1 y_1) + I$$

$$(x_2 + I) \otimes (y_2 + I) = (x_2 y_2) + I$$

Como $(x_1 - x_2)y \in I$ e $(y_1 - y_2)x_2 \in I$ então

$$(x_1 - x_2)y_1 + (y_1 - y_2)x_2 \in I$$

$$x_1 y_2 - \underbrace{x_2 y_1 + y_1 x_2}_{=0} - y_2 x_2 \in I$$

$$x_1 y_1 - x_2 y_2 \in I,$$

ou seja, $xy + I = x_2 y_2 + I$. Portanto,

$$(x_1 + I) \otimes (y + I) = (x_2 + I) \otimes (y_2 + I).$$

Teorema

Seja $(A, +, \cdot)$ um anel associativo, comutativo e com unidade. Então, se I é um ideal de A , o quociente $\frac{A}{I}$ com as operações \oplus e \otimes é um anel associativo, comutativo e com unidade. O elemento neutro da soma é a classe $0_A + I$ e unidade do produto é $1_A + I$.