Anéis - Ideais

José Antônio O. Freitas

MAT-UnB

5 de outubro de 2020

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

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

$$I_1 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$$
$$I_2 = \{\overline{0}, \overline{4}\}$$

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, $x - z = (x-z) + (y-z) \in I$, 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 $\dfrac{A}{I_1} = \{x + I \mid x \in A\}$, logo existem tantas classes de equivalência quantos forem os elementos de A.

ii) Para $I_2 = A$ temos:

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

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

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,* $\dfrac{\mathbb{Z}}{I} = \mathbb{Z}_m$.

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 a unidade do produto é $1_A + I$.