

Elementos da Teoria de Anéis

lcc :: lmat :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

generalidades

Definição. Seja A um conjunto não vazio e duas operações binárias, que representamos por $+$ e por \cdot , nele definidas. O triplo $(A, +, \cdot)$ diz-se um *anel* se

1. $(A, +)$ é um grupo comutativo (também chamado *módulo*);
2. (A, \cdot) é um semigrupo;
3. A operação \cdot é *distributiva* em relação à operação $+$, i.e., para todos $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

O anel A diz-se *comutativo* se a multiplicação for comutativa.

Observação. Referimo-nos sempre à primeira operação (i.e., à operação para a qual temos um grupo) como *adição*. À segunda operação (i.e., à operação para a qual temos um semigrupo) chamamos *multiplicação*.

Definições. Seja $(A, +, \cdot)$ um anel.

- Ao elemento neutro do grupo chamamos *zero do anel* e representamos por 0_A .
- Quando existe, ao elemento neutro do semigrupo chamamos *identidade do anel* e representamos por 1_A .
- Ao elemento oposto de $a \in A$ para a adição chamamos *simétrico de a* e representamos por $-a$ (note-se que, sendo $(A, +)$ grupo, qualquer elemento do anel admite um único simétrico).
- No caso de o anel ter identidade, podem existir elementos que admitem elemento oposto para a multiplicação. Quando existe, referimo-nos ao elemento oposto de $a \in A$ para a multiplicação como o *inverso de a* . Neste caso, representamos o inverso de a por a^{-1} .

Observação. Se não houver ambiguidade, falamos no anel A quando nos referimos ao anel $(A, +, \cdot)$ e omitimos o sinal da multiplicação na escrita de expressões.

Exemplo 1. Seja $A = \{a\}$. Então, $(A, +, \cdot)$, onde $a + a = a$ e $a \cdot a = a$, é um anel comutativo com identidade, ao qual se chama *anel nulo*. Representa-se por $A = \{0_A\}$.

Exemplo 2. $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$ são anéis comutativos com identidade.

Exemplo 3. Dado $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \times)$ é um anel comutativo com identidade.

Exemplo 4. Dado o natural $n \geq 2$, $(n\mathbb{Z}, +, \times)$ é um anel comutativo sem identidade.

Exemplo 5. $(\mathcal{M}_2(\mathbb{R}), +, \times)$ é um anel não comutativo com identidade.

Proposição. Seja A um anel. Então, para todo $x \in A$, $0_A x = x 0_A = 0_A$.

Demonstração. Seja $x \in A$. Então, pela distributividade, temos que $0_A x + 0_A x = (0_A + 0_A) x$. Mas,

$$\begin{aligned} 0_A x + 0_A x &= (0_A + 0_A) x && \Leftrightarrow 0_A x + 0_A x = 0_A x \\ &&& \Leftrightarrow 0_A x + 0_A x = 0_A x + 0_A \\ &&& \Leftrightarrow 0_A x = 0_A. \end{aligned}$$

Logo, $0_A x = 0_A$. Analogamente, de

$$x 0_A + x 0_A = x (0_A + 0_A)$$

e de

$$x 0_A + x 0_A = x (0_A + 0_A) \Leftrightarrow x 0_A = 0_A,$$

obtemos $x 0_A = 0_A$. □

Proposição. Se $A \neq \{0_A\}$ é um anel com identidade 1_A , então $1_A \neq 0_A$.

Demonstração. Se 0_A fosse a identidade do anel, então, para $x \neq 0_A$, teríamos $x = 0_A x$. Mas, pela proposição anterior, $0_A x = 0_A$, pelo que $x = 0_A$. □

Proposição. Sejam A um anel e $x, y \in A$. Então:

1. $(-x)y = x(-y) = -xy$;
2. $(-x)(-y) = xy$.

Demonstração. Sejam $x, y \in A$. Então,

1. $(-x)y$ é o simétrico de xy já que

$$(-x)y + xy = (-x + x)y = 0_A y = 0_A$$

e $x(-y)$ é também o simétrico de xy pois

$$x(-y) + xy = x(-y + y) = x0_A = 0_A;$$

Logo, $-xy = (-x)y = x(-y)$.

2. $(-x)(-y)$ é o simétrico de $(-xy)$ já que

$$\begin{aligned} (-x)(-y) + (-xy) &= (-x)(-y) + (-x)y \\ &= (-x)(-y + y) = (-x)0_A = 0_A. \end{aligned}$$

Como o simétrico de $-xy$ é, de facto, xy , obtemos o resultado pretendido. □

Proposição. Sejam A um anel, $n \in \mathbb{N}$ e $a, b_1, b_2, \dots, b_n \in A$. Então,

1. $a(b_1 + b_2 + \dots + b_n) = ab_1 + ab_2 + \dots + ab_n$;
2. $(b_1 + b_2 + \dots + b_n)a = b_1a + b_2a + \dots + b_na$.

Observação. A propriedade apresentada na última proposição é conhecida, em Teoria de Anéis, como *propriedade distributiva generalizada*.

Seja $(A, +, \cdot)$ um anel. Então, $(A, +)$ é grupo, pelo que podemos falar nos múltiplos de expoente **inteiro** de $a \in A$. Assim, temos

- i. $0a = 0_A$;
- ii. $(n + 1)a = na + a$, para todo $n \in \mathbb{N}_0$;
- ii. $na = -(-na)$, para todo $n \in \mathbb{Z}^-$.

Proposição. Sejam A , um anel, $a, b \in A$ e $m, n \in \mathbb{Z}$. Então,

1. $(m + n)a = ma + na$;
2. $n(ma) = (nm)a$;
3. $n(a + b) = na + nb$.

Proposição. Sejam A um anel, $a, b \in A$ e $n \in \mathbb{Z}$. Então,

$$n(ab) = (na)b = a(nb).$$

Demonstração. Temos de considerar três casos:

(i) $n = 0$. A demonstração é trivial.

(ii) $n > 0$. Resulta da propriedade distributiva generalizada:

$$(na)b = \underbrace{(a + a + \cdots + a)}_{n \times} b = \underbrace{ab + ab + \cdots + ab}_n \times = n(ab)$$

e

$$a(nb) = a \underbrace{(b + b + \cdots + b)}_{n \times} = \underbrace{ab + ab + \cdots + ab}_n \times = n(ab).$$

(iii) $n < 0$. Para $a, b \in A$, temos que

$$n(ab) = -[(-n)(ab)] = -[((-n)a)b] = [-(-(na))]b = (na)b$$

e

$$n(ab) = -[(-n)(ab)] = -[a((-n)b)] = a[-(-n)b] = a(nb).$$

Seja $(A, +, \cdot)$ um anel. Então, (A, \cdot) é semigrupo, pelo que podemos falar nas potências de expoente **natural** de $a \in A$. Assim, temos

- i. $a^1 = a$;
- ii. $a^{n+1} = a^n \cdot a$, para todo $n \in \mathbb{N}$.

Proposição. Sejam A um anel, $a \in A$ e $m, n \in \mathbb{N}$. Então,

- 1. $(a^n)^m = a^{nm}$;
- 2. $a^n a^m = a^{n+m}$.

□

Observação. Tendo em conta que estamos a trabalhar num anel e, portanto, a trabalhar com duas operações simultaneamente, distinguiremos as duas potências a^n e na (com $a \in A$ e $n \in \mathbb{N}$) falando em *múltiplo de a* para na e em *potência de a* para a^n .

Definição. Seja A um anel com identidade 1_A . Um elemento $a \in A$ diz-se uma *unidade* se admite um inverso em A . Representa-se por \mathcal{U}_A o conjunto das unidades de um anel com identidade.

Exemplo 6. No anel $(\mathbb{Z}, +, \times)$, temos que $\mathcal{U}_A = \{-1, 1\}$.

Exemplo 7. No anel $(\mathbb{R}, +, \times)$, temos que $\mathcal{U}_A = \mathbb{R} \setminus \{0\}$.

Exemplo 8. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, temos que

$$\mathcal{U}_A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{R}) \mid ad - bc \neq 0 \right\}.$$

Quem são as unidades em $(\mathbb{Z}_n, +, \times)$, para $n \in \mathbb{N}$? São os elementos $[x]_n$, com $\text{m.d.c.}(x, n) = 1$.

Definição. Seja A um anel. Um elemento $a \in A$ diz-se *simplificável* se, para todos $x, y \in A$

$$xa = ya \quad \text{ou} \quad ax = ay \implies x = y.$$

Exemplo 9. Nos anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$, qualquer elemento não nulo é simplificável.

Exemplo 10. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, o elemento $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$ não é simplificável. De facto,

$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}$$

e

$$\begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}.$$

Observação. Num anel A , toda a unidade é simplificável, mas nem todo o elemento simplificável é uma unidade.

Definição. Seja A um anel. Um elemento $a \in A$ diz-se um *divisor de zero* se existe $b \in A \setminus \{0_A\}$ tal que

$$ab = 0_A \quad \text{ou} \quad ba = 0_A.$$

Observação. O elemento zero de um anel A só não é divisor de zero se $A = \{0_A\}$.

Exemplo 11. Nos anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$, o único divisor de zero existente é o elemento 0.

Exemplo 12. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, qualquer matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ tal que $ad - bc = 0$ é divisor de zero.

Quem são os divisores de zero em $(\mathbb{Z}_n, +, \times)$, para $n \in \mathbb{N}$?

Exemplo 13.

- Os divisores de zero do anel $(\mathbb{Z}_6, +, \times)$ são os elementos $[0]_6$, $[2]_6$, $[3]_6$ e $[4]_6$ pois
 $[0]_6 \times [1]_6 = [0]_6$, $[2]_6 \times [3]_6 = [0]_6$ e $[4]_6 \times [3]_6 = [0]_6$.
- No anel $(\mathbb{Z}_7, +, \times)$, o único elemento divisor de zero é $[0]_7$.

Proposição. No anel $(\mathbb{Z}_n, +, \times)$, os divisores de zero são os elementos $[x]_n$, onde $\text{m.d.c.}(x, n) \neq 1$.

Demonstração. Se $1 \neq d = \text{m.d.c.}(x, n)$, então, existem $a, b \in \mathbb{Z}$ tais que $d = ax + bn$ e existe $n = kd$. Assim, em \mathbb{Z}_n , $[d]_n = [a]_n[x]_n + [0]_n(*)$ e, portanto, $[0]_n = [kd]_n = [ka]_n[x]_n$ com $[ka]_n \neq [0]_n$. □

característica de um anel

Sejam A um anel e $a \in A$. Considerando os múltiplos de a , i.e., os elementos da forma na com $n \in \mathbb{Z}$, temos duas situações a considerar:

$$(i) (\exists m \in \mathbb{Z} \setminus \{0\}) (\forall a \in A) \quad ma = 0_A;$$

$$(ii) (\forall m \in \mathbb{Z} \setminus \{0\}) (\exists b \in A) \quad mb \neq 0_A \\ (\text{i.e., } nb = 0_A \ (\forall b \in A) \Rightarrow n = 0).$$

Exemplo 14. São exemplos da situação (ii) o anel dos reais e o anel dos inteiros.

Exemplo 15. É exemplo da situação (i) o anel $(\mathbb{Z}_4, +, \cdot)$.

Definição. Seja A um anel.

1. Se

$$nb = 0_A, \forall b \in A \Rightarrow n = 0,$$

A diz-se um anel de *característica* 0 e escreve-se $c(A) = 0$;

2. Se

$$(\exists m \in \mathbb{Z} \setminus \{0\}) (\forall a \in A) \quad ma = 0_A,$$

A diz-se um anel de *característica* q onde

$q = \min\{n \in \mathbb{N} : na = 0_A \forall a \in A\}$. Escreve-se $c(A) = q$.

Observação. A segunda parte da definição faz todo o sentido, pois se A é um anel que satisfaz 2., temos que, sendo

$$M = \{m \in \mathbb{Z} : ma = 0_A, \quad \forall a \in A\},$$

$(M, +)$ é um subgrupo do grupo cíclico $(\mathbb{Z}, +)$ e, portanto, é ele próprio um grupo cíclico e o seu gerador é o menor inteiro positivo de M .

Como $(A, +)$ é grupo, podemos falar da ordem de qualquer elemento de A .

Se A é um anel de característica q e $x \in A$ é tal que a ordem de x no grupo $(A, +)$ é $o(x) = p$, qual a relação de p com q ?

A resposta é obviamente $p \mid q$. De facto, se q é a característica de A , temos que $qa = 0_A$, para todo $a \in A$. Em particular, para $a = x$ temos que $qx = 0_A$. Logo, como $p = o(x)$, vem, como consequência da definição de ordem de um elemento, que $p \mid q$.

Assim, podemos concluir que a característica de um anel finito A é o m.m.c. entre as ordens de todos os elementos de A .

Proposição. Sejam $A \neq \{0_A\}$ um anel com identidade 1_A e $n \in \mathbb{N}$. Então, a característica de A é n se e só se a ordem de 1_A é n .

Demonstração. $[\Rightarrow]$. Por hipótese, temos que $c(A) = n$, i.e., temos que:

$$(i) \quad \forall a \in A \quad na = 0_A;$$

$$(ii) \quad (\exists p \in \mathbb{N} \forall a \in A \quad pa = 0_A) \implies n \mid p.$$

Queremos provar que $o(1_A) = n$, i.e., queremos provar que:

$$(a) \quad n1_A = 0_A;$$

$$(b) \quad (\exists p \in \mathbb{N} : p1_A = 0_A) \implies n \mid p.$$

A condição (a) resulta naturalmente da condição (i). Para provarmos a condição (b) supomos que existe $p \in \mathbb{N}$ tal que $p1_A = 0_A$. Para aplicarmos (ii), temos que provar que $pa = 0_A$ para todo $a \in A$. De facto, $pa = p(1_A a) = (p1_A)a = 0_A a = 0_A$. Assim, por (ii), temos que $n \mid p$. Logo, verifica-se a condição (b).

$[\Leftarrow]$. Suponhamos agora que $p(1_A) = n$, i.e., que (a) e (b) são satisfeitos. Queremos provar que o anel satisfaz (i) e (ii):

(i) Para todo $a \in A$, temos que

$$na = n(1_A a) = (n1_A)a = 0_A a = 0_A.$$

(ii) Seja $p \in \mathbb{N}$ tal que, para todo $a \in A$, $pa = 0_A$. Em particular, como $1_A \in A$, temos que $p1_A = 0_A$. Então, por (b), concluímos que $n \mid p$, o que termina a nossa demonstração.

□

Exemplo 16. Seja $n \in \mathbb{N}$. Como, em \mathbb{Z}_n , $o(\bar{1}) = n$, concluímos que $c(\mathbb{Z}_n) = n$.

Exemplo 17. O anel dos números inteiros e o anel dos números reais são anéis de característica 0, uma vez que, nestes anéis, $o(1)$ é infinita.