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) $(\forall m \in \mathbb{Z} \setminus \{0\})\,(\exists b \in A) \quad mb \neq 0_A$
(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.

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.

anéis especiais

Definição. Um anel comutativo com identidade A diz-se um *domínio* (ou *anel*) *de integridade* se admitir como único divisor de zero o elemento zero do anel.

Exemplo 18. Os anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$ são domínios de integridade.

Exemplo 19. O anel das matrizes quadradas de ordem 2 não é um domínio de integridade.

Observação. Se A é um domínio de integridade, então, $A \neq \{0_A\}$.

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A \setminus \{0_A\} \neq \emptyset$ e todo o elemento de $A \setminus \{0_A\}$ é simplificável.

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A \setminus \{0_A\} \neq \emptyset$ e $A \setminus \{0_A\}$ é subsemigrupo de A relativamente ao produto.

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A \setminus \{0_A\} \neq \emptyset$ e, se as equações $ax = b$ e $xa = b$ $(a \neq 0_A)$ tiverem solução, então, a solução é única.

Definição. Um anel A diz-se um *anel de divisão* se $(A \setminus \{0_A\}, \cdot)$ é um grupo. Um anel de divisão comutativo diz-se um *corpo*.

Resulta da definição que qualquer corpo é um domínio de integridade, mas o recíproco não é verdadeiro.

Exemplo 20. O domínio de integridade $(\mathbb{Z}, +, \times)$ não é um anel de divisão, pois $(\mathbb{Z} \setminus \{0\}, \times)$ não é grupo.

Exemplo 21. O domínio de integridade $(\mathbb{R}, +, \times)$ é um corpo e, portanto, um anel de divisão.

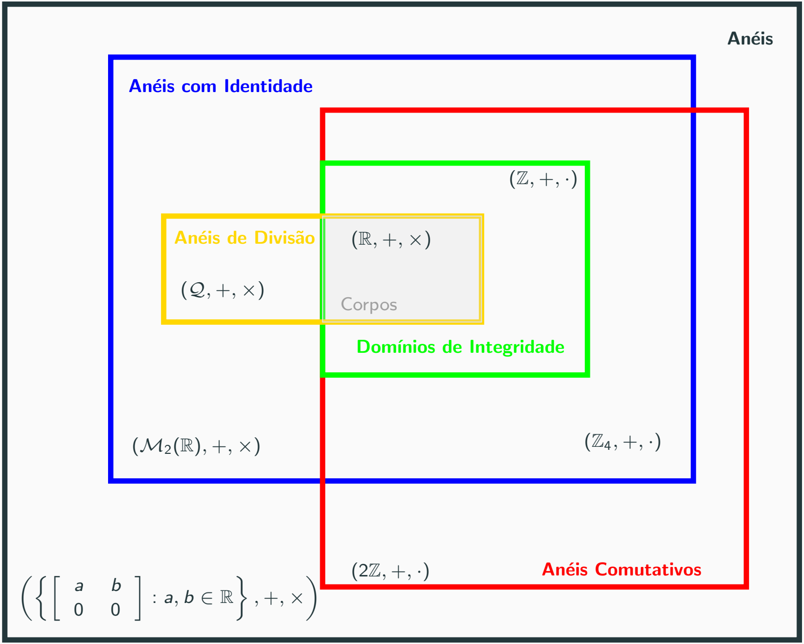
Exemplo 22. Seja $\mathcal{Q} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, onde $i^2 = j^2 = k^2 = -1$, $ij = -ji = k, ki = -ik = j, jk = -kj = i$. Considere em $\mathcal{Q}$ as operações $+$ e $\times$ definidas por

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k)$$
$$= a + a' + (b + b')i + (c + c')j + (d + d')k$$

e

$$(a + bi + cj + dk) \times (a' + b'i + c'j + d'k) =$$
$$aa' - bb' - cc' - dd' + (ab' + a'b + cd' - c'd)i+$$
$$(ac' - bd' + a'c + b'd)j + (ad' + bc' - b'c + a'd)k.$$

Então, $(\mathcal{Q}, +, \times)$ é um anel de divisão não comutativo. Este anel designa-se por *Anel dos Quarteniões.*


Anéis
Anéis com Identidade
$(\mathbb{Z}, +, \cdot)$
Anéis de Divisão
$(\mathbb{R}, +, \times)$
$(\mathcal{Q}, +, \times)$
Corpos
Domínios de Integridade
$(\mathcal{M}_2(\mathbb{R}), +, \times)$
$(\mathbb{Z}_4, +, \cdot)$
$(2\mathbb{Z}, +, \cdot)$
Anéis Comutativos
$\left(\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R}\right\}, +, \times\right)$