Em

- $\mathbb{Z}$: $ab = 0 \Rightarrow a = 0$ ou $b = 0$ `[não tem divisores de zero]`
- $\mathbb{Z}_6$: $2 \cdot 3 = 2 \otimes_6 3 = 0$ `[tem divisores de zero]`
- $M_2(\mathbb{Z})$: $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. `[tem divisores de zero]`

Um elemento $a \in A$, diferente de zero, diz-se *divisor de zero à esquerda* (resp. *divisor de zero à direita*) caso exista $b \in A$, diferente de zero, tal que $ab = 0$ (resp. $ba = 0$). Um *divisor de zero* à esquerda e à direita chama-se simplesmente *divisor de zero*.

DOMÍNIO DE INTEGRIDADE

Um *domínio de integridade* é um anel comutativo com identidade sem divisores de zero.

Em

- $\mathbb{Z}$: só 1 e -1 são invertíveis para a operação $\cdot$
- $\mathbb{Q}$: todos os elementos $\neq 0$ têm inverso.

CORPO

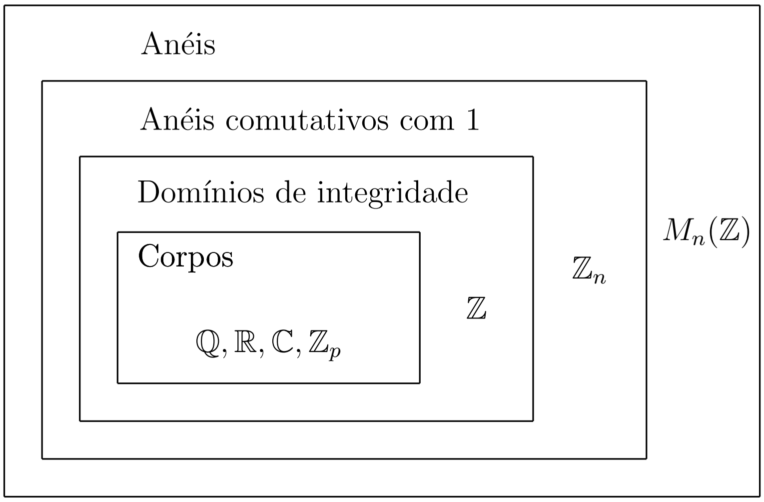
Um *corpo* é um anel comutativo com identidade onde todo o elemento $\neq 0$ possui inverso.

Chama-se *unidade* do anel a qualquer elemento que tenha inverso. Designando por U o conjunto das unidades de A, é evidente que $(U, \cdot)$ constitui um grupo (portanto, se A é um corpo, $U = A \setminus \{0\}$ e $(A \setminus \{0\}, \cdot)$ é um grupo abeliano).

Todo o corpo é um domínio de integridade. Com efeito, se a tem inverso então não é divisor de zero:

$$ab = 0 \Leftrightarrow a^{-1}(ab) = a^{-1} \cdot 0 \Leftrightarrow b = 0.$$

Em conclusão:



n: não primo

p: primo

$\mathbb{Z}$ é um exemplo de domínio de integridade que não é corpo. Nenhum exemplo destes pode ser finito:

Teorema. *Todo o domínio de integridade finito é um corpo.*

Demonstração. Seja $D = \{0, d_1, d_2, \ldots, d_n\}$ um domínio de integridade finito. Para cada $i \in \{1, 2, \ldots, n\}$ consideremos os produtos $d_i d_1, d_2 d_2, \ldots, d_i d_n$. São distintos dois a dois: $d_i d_j = d_i d_k \Leftrightarrow d_i(d_j - d_k) = 0$; como $d_i \neq 0$ e D não tem divisores de zero, necessariamente $d_j - d_k = 0$, isto é, $d_j = d_k$.

Assim, os produtos $d_i d_1, d_2 d_2, \ldots, d_i d_n$ percorrem todos os elementos não nulos de D; em particular, existe j tal que $d_i d_j = 1$, o que significa que d_i é invertível. Portanto, todo o elemento não nulo de D é invertível, logo D é um corpo. ■

SUBANEL
$S \subseteq A$ é um *subanel* de A se S é fechado para $+$ e $\cdot$ e forma um anel para estas operações.

Exemplos: $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, ... são subanéis de $(\mathbb{Z}, +, \cdot)$.

Qualquer anel A possui sempre os *subanéis triviais* $\{0\}$ e o próprio A. Qualquer outro subanel de A diz-se *subanel próprio*.

Proposição. *Um subconjunto S de um anel A é um subanel se e só se as seguintes condições se verificam:*

(1) $S \neq \emptyset$.

(2) *Para cada* $x, y \in S$, $x - y \in S$.

(3) *Para cada* $x, y \in S$, $xy \in S$.

Demonstração. Exercício. ■

Mais exemplos:

- $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ é um subanel de $(\mathbb{C}, +, \cdot)$.
- $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{Z} \right\}$ é um subanel de $M_2(\mathbb{Z})$.

IDEAL
Um subanel I de A diz-se um *ideal* se, para cada $a \in A$ e cada $x \in I$, ax e xa pertencem a I.

Exemplos:

- $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ mas não é um ideal $(1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z})$
- $n\mathbb{Z}$ é um ideal de Z $(n \in \mathbb{N}_0)$.

`[Observe o paralelismo com a teoria dos grupos: os subanéis correspondem aos subgrupos e os ideais correspondem aos subgrupos normais]`

Da proposição anterior decorre imediatamente que:

Proposição. *Um subconjunto* I *de um anel* A *é um ideal se e só se as seguintes condições se verificam:*

(1) $I \neq \emptyset$.

(2) *Para cada* $x, y \in I$, $x - y \in I$.

(3) *Para cada* $a \in A$ *e* $x \in I$, $ax \in I$ *e* $xa \in I$. ■

Mais exemplos: Seja A um anel comutativo e $a \in A$.

- $\{xa \mid x \in A\}$ é um ideal de A. `[pode não conter` a`]`
- O menor ideal de A contendo a é o ideal $(a) := \{xa + na \mid x \in A, n \in \mathbb{Z}\}$. Diz-se o *ideal principal gerado* por a. Se A for também unitário, $(a) = \{xa \mid x \in A\}$.

Seja A um anel comutativo. Um ideal I de A diz-se *principal* se existe algum $a \in A$ tal que $I = (a)$.

Exemplo: Em Álgebra I observaram que os subconjuntos $n\mathbb{Z}$, $n = 0, 1, 2, \ldots$, são os únicos subgrupos de $(\mathbb{Z}, +)$. Portanto, $n\mathbb{Z}$, $n = 0, 1, 2, \ldots$, são os únicos ideais de $(\mathbb{Z}, +, \cdot)$. Como $n\mathbb{Z} = (n)$, são todos principais.

[$\mathbb{Z}$ `diz-se um domínio de ideais principais`]