

1. (a) Verdadeira:

$\Rightarrow$: $ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0$. Como $a \neq 0$ e a não é divisor de zero à esquerda, então $b - c = 0$, isto é, $b = c$.

$\Leftarrow$: Se a fosse um divisor de zero à esquerda, existiria $b \neq 0$ tal que $ab = 0$. Mas então teríamos $ab = a0$ com $b \neq 0$, contrariando a hipótese.

- (b) É falsa. O anel $\mathbb{Z}$ dos inteiros é um contra-exemplo: não contém divisores de zero mas só os inteiros $1, -1$ são invertíveis.
- (c) É falsa: num anel onde existam elementos a e b tais que $ab \neq ba$ tem-se $ba - ab \neq 0$ pelo que $(a + b)(a - b) = a^2 + ba - ab - b^2 \neq a^2 - b^2$. Por exemplo, no anel das matrizes quadradas de ordem 2 com coeficientes inteiros, para

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

A afirmação só é verdadeira se nos restringirmos aos anéis comutativos. Nesse caso, de facto, $(a + b)(a - b) = (a + b)a + (a + b)(-b) = a^2 + ba - ab - b^2 = a^2 + ab - ab - b^2 = a^2 - b^2$.

2. (a) A identidade de $\mathcal{A}$ é o triplo $(1, 1, 1)$, uma vez que $(a_1, a_2, a_3) \cdot (1, 1, 1) = (a_1, a_2, a_3)$ para quaisquer $a_1, a_2, a_3 \in \mathbb{Z}_6$.

O inverso de $x = (1, 5, 1)$ é o próprio x pois $1 \otimes 1 = 1$ e $5 \otimes 5 = 1$.

- (b) O exemplo da alínea anterior mostra imediatamente que os elementos invertíveis de $\mathcal{A}$ são precisamente os triplos cujas coordenadas estão contidas em $\{1, 5\}$, pois 1 e 5 são os únicos elementos invertíveis de $\mathbb{Z}_6$. São assim todas as sequências com repetição de comprimento 3 que podemos formar com os números 1 e 5, pelo que, ao todo, temos $2^3 = 8$ elementos invertíveis.
- (c) Excluamos à partida o elemento $(0, 0, 0)$ que não é nem divisor de zero nem invertível. Dos restantes elementos de $\mathcal{A}$, qualquer elemento que não é invertível será divisor de zero. De facto, se em $(a, b, c) \neq (0, 0, 0)$ um dos elementos não pertencer a $\{1, 5\}$, ou seja, se for um dos elementos $0, 2, 3, 4$, (a, b, c) será sempre divisor de zero. Por exemplo, para $a = 0, 2, 3, 4$:

$$(0, \dots, \dots) \cdot (1, 0, 0) = (0, 0, 0), \quad (2, \dots, \dots) \cdot (3, 0, 0) = (0, 0, 0),$$

$$(3, \dots, \dots) \cdot (2, 0, 0) = (0, 0, 0), \quad (4, \dots, \dots) \cdot (3, 0, 0) = (0, 0, 0).$$

Em conclusão, (a, b, c) é divisor de zero se $(a, b, c) \neq (0, 0, 0)$ e pelo menos uma das coordenadas a, b, c não está no conjunto $\{1, 5\}$. Como $\mathcal{A}$ tem $6^3 = 216$ elementos, o número de divisores de zero será igual a $216 - 1 - 2^3 = 207$.

- (d) $\mathcal{S}_{(x,y)}$ é claramente não vazio. Para que seja um subanel, é necessário que

$$(a_1, a_2, a_3) - (b_1, b_2, b_3) \in \mathcal{S}_{(x,y)}$$

sempre que $(a_1, a_2, a_3), (b_1, b_2, b_3) \in \mathcal{S}_{(x,y)}$, isto é, $a_1 - b_1 = x$ e $a_3 - b_3 = y$ sempre que $a_1 = b_1 = x$ e $a_3 = b_3 = x$. Mas, nestas condições, $a_1 - b_1 = x - x = 0$ e $a_3 - b_3 = y - y = 0$ pelo que,

$$(a_1, a_2, a_3) - (b_1, b_2, b_3) \in \mathcal{S}_{(x,y)} \Leftrightarrow x = y = 0.$$

É agora fácil verificar que nessas condições ($x = y = 0$) a outra condição que caracteriza os subanéis é automaticamente verdadeira: para quaisquer $(0, a, 0), (0, b, 0) \in \mathcal{S}_{(0,0)}$, $(0, a, 0) \cdot (0, b, 0) = (0, ab, 0) \in \mathcal{S}_{(0,0)}$. Portanto, $\mathcal{S}_{(x,y)}$ é um subanel de $\mathcal{A}$ se e só se $x = y = 0$.

- (e) Sejam $(a_1, a_2, a_3) \in \mathcal{A}$ e $(0, b, 0) \in \mathcal{S}_{(0,0)}$. Como $(a_1, a_2, a_3) \cdot (0, b, 0) = (0, a_2b, 0) \in \mathcal{S}_{(0,0)}$, então $\mathcal{S}_{(0,0)}$ é mesmo um ideal de $\mathcal{A}$. Este ideal não é primo uma vez que, por exemplo, $(2, 2, 2) \cdot (3, 3, 3) = (0, 0, 0) \in \mathcal{S}_{(0,0)}$ mas nem $(2, 2, 2)$ nem $(3, 3, 3)$ pertencem a $\mathcal{S}_{(0,0)}$.

Não sendo primo, também não pode ser maximal (pois maximal $\Rightarrow$ primo).

- (f) Como $I = \mathcal{S}_{(0,0)} = \{(0, b, 0) \mid b \in \mathbb{Z}_6\}$, então

$$(a_1, a_2, a_3) + I = (b_1, b_2, b_3) + I \Leftrightarrow (a_1, a_2, a_3) - (b_1, b_2, b_3) \in I \Leftrightarrow a_1 = b_1, a_3 = b_3.$$

Assim, o que distingue duas classes laterais $(a_1, a_2, a_3) + I$ e $(b_1, b_2, b_3) + I$ é o valor das coordenadas 1 e 3 dos respectivos representantes (a_1, a_2, a_3) e (b_1, b_2, b_3) . É então evidente que $(a_1, a_2, a_3) + I = (a_1, 0, a_3) + I$ para qualquer $a_2 \in \mathbb{Z}_6$. Assim,

$$\mathcal{A}/I = \{(a, 0, c) + I \mid a, c \in \mathbb{Z}_6\}$$

e aqui já todos os elementos são distintos. As operações deste anel são

$$((a, 0, c) + I) + ((a', 0, c') + I) = (a + a', 0, c + c') + I$$

e

$$((a, 0, c) + I) \cdot ((a', 0, c') + I) = (aa', 0, cc') + I.$$

É evidente que se denotarmos cada elemento $(a, 0, c) + I$ simplesmente por (a, c) o que temos aqui é precisamente o anel $\mathbb{Z}_6 \times \mathbb{Z}_6$, que tem 36 elementos e não é um domínio de integridade, uma vez que tem divisores de zero.

Observação. Temos aqui outro argumento para justificar a resposta à alínea (e): como $\mathcal{A}/I$ não é um domínio de integridade, o ideal I não é primo.

- (g) Basta observar que I está (estritamente) contido no ideal $K = \{(a, b, 0) \mid a, b \in \mathbb{Z}_6\}$, mas como K não é maximal (pois não é primo: $(1, 1, 2) \cdot (1, 1, 3) = (1, 1, 0) \in K$ mas $(1, 1, 2) \notin K$ e $(1, 1, 3) \notin K$) terá que haver um J ainda maior que contenha K . Até há mais do que uma hipótese para J :

$$J = \{(a, b, c) \mid a, b \in \mathbb{Z}_6, c \in \{0, 2, 4\}\} \quad \text{ou} \quad J = \{(a, b, c) \mid a, b \in \mathbb{Z}_6, c \in \{0, 3\}\}.$$

Observação. Isto é consequência do facto de que, como $\mathbb{Z}_6$ não é um corpo, tem, além dos ideais triviais $\langle 0 \rangle = \{0\}$ e $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$, os ideais próprios maximais

$$\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\} \quad \text{e} \quad \langle 3 \rangle = \{0, 3\}.$$

Então, uma vez que

$$I = \{0\} \times \mathbb{Z}_6 \times \{0\} = \langle 0 \rangle \times \langle 1 \rangle \times \langle 0 \rangle,$$

temos as cadeias de inclusões estritas

$$I \subset \langle 1 \rangle \times \langle 1 \rangle \times \langle 0 \rangle \subset \underbrace{\langle 1 \rangle \times \langle 1 \rangle \times \langle 2 \rangle}_J \subset \langle 1 \rangle \times \langle 1 \rangle \times \langle 1 \rangle = \mathcal{A}$$

ou

$$I \subset \langle 1 \rangle \times \langle 1 \rangle \times \langle 0 \rangle \subset \underbrace{\langle 1 \rangle \times \langle 1 \rangle \times \langle 3 \rangle}_J \subset \langle 1 \rangle \times \langle 1 \rangle \times \langle 1 \rangle = \mathcal{A}.$$