---

1. (a) Evidentemente, a implicação $\Leftarrow$ de $(*)$ é verdadeira para qualquer a. Quanto a $\Rightarrow$, uma vez que $a+1$ não é divisor de zero, tem-se

$$a^2 = 1 \Leftrightarrow a^2 - 1 = 0 \Leftrightarrow (a+1)(a-1) = 0 \Rightarrow a+1 = 0 \text{ ou } a-1 = 0 \Leftrightarrow a = -1 \text{ ou } a = 1.$$

Teremos que procurar um contra-exemplo num anel com divisores de zero. Tentemos os $\mathbb{Z}_n$ com n não primo: em $\mathbb{Z}_8$, $3^2 = 1$, $3 \neq 1$ e $3 \neq -1 = 7$.

(b) Um ideal I de A diz-se *maximal* se $I \neq A$ e, para qualquer outro ideal J, $I \subset J \subseteq A \Rightarrow J = A$. No anel $\mathbb{Z}$, o ideal $\mathbb{Z}$ não é, por definição, e $4\mathbb{Z}$ também não porque nem sequer é primo ($2 \times 2 = 4 \in 4\mathbb{Z}$ mas $2 \notin 4\mathbb{Z}$). Resta assim $5\mathbb{Z}$.

2. (a) $-(1,3) = (4,3)$ pois $(1,3) + (4,3) = (0,0)$; $(1,5)^{-1} = (1,5)$ pois $(1,5) \cdot (1,5) = (1,5)$.

(b) Pela alínea anterior, $(1,5)(x,y) = (2,3) \Leftrightarrow (1,5)^{-1}(1,5)(x,y) = (1,5)^{-1}(2,3) \Leftrightarrow (x,y) = (1,5)(2,3) = (2,3)$.

(c) $(a,b) \in A$ é um divisor de zero se e só se $(a,b) \neq (0,0)$ e existe $(x,y) \neq (0,0)$ em A tal que $(a,b) \cdot (x,y) = (0,0)$. Portanto, se e só se

$$(a \neq 0 \text{ ou } b \neq 0) \text{ e } (\exists (x,y) \neq (0,0) : ax = 0, by = 0).$$

Em $\mathbb{Z}_5$, $ax = 0$ sse $a = 0$ ou $x = 0$, mas em $\mathbb{Z}_6$, como há divisores de zero, $by = 0$ sse $b = 0$ ou $y = 0$ ou $b = 2, y = 3$ ou $b = 3, y = 2$ ou etc. Por exemplo, $(0,1)$ é um divisor de zero pois $(0,1) \cdot (1,0) = (0,0)$ mas há muitos mais exemplos análogos a este, mesmo com ambas as coordenadas diferentes de zero: $(1,2) \cdot (0,3) = (0,0)$, $(2,4) \cdot (0,3) = (0,0)$, etc.

Assim, qualquer elemento da forma $(0,b)$, $b \in \mathbb{Z}_6 \setminus \{0\}$, e da forma $(a,0)$, $a \in \mathbb{Z}_5 \setminus \{0\}$ é um divisor de zero. Além destes, também (a,b) com $a \neq 0$ e $b \in \{2,3,4\}$ é divisor de zero. São assim, ao todo, $5+4+4\times 3 = 21$ divisores de zero.

(d) $(a,b) \cdot (c,d) = (1,1) \Leftrightarrow (a \times_5 c, b \times_6 d) = (1,1) \Leftrightarrow a \times_5 c = 1, b \times_6 d = 1$. Portanto, os elementos invertíveis de A são precisamente os pares (a,b), $a \in \mathbb{Z}_5 \setminus \{0\}$, $b \in \{1,5\} \subseteq \mathbb{Z}_6$, uma vez que 1 e 5 são os únicos elementos invertíveis de $\mathbb{Z}_6$. Em conclusão, A tem oito elementos invertíveis: $(1,1)$, $(1,5)$, $(2,1)$, $(2,5)$, $(3,1)$, $(3,5)$, $(4,1)$, $(4,5)$.

(e) $I = A$ pois $(1,5)$ é invertível. Como A é um anel comutativo com identidade, $\langle x \rangle = \{ax \mid a \in A\}$. Portanto,

$$J = \{(a,b)(1,3) \mid (a,b) \in A\} = \{(a,3b) \mid a \in \mathbb{Z}_5, b \in \mathbb{Z}_6\} = \{(a,b) \mid a \in \mathbb{Z}_5, b = 0,3\}.$$

J é primo pois $(a,b)(c,d) = (ac,bd) \in J \Leftrightarrow bd \in \{0,3\} \Leftrightarrow b,d \in \{0,3\} \Leftrightarrow (a,b),(c,d) \in J$.

(f) $A/J = \{a + J \mid a \in A\}$. À partida existem $5 \times 6 = 30$ classes laterais definidas por J em A. Como

$$(x,y) + J = (x',y') + J \Leftrightarrow (x,y) - (x',y') \in J \Leftrightarrow y - y' \in \{0,3\} \Leftrightarrow y' = y \text{ ou } y' = y+3.$$

Assim, para cada $y \in \mathbb{Z}_6$, é evidente que

$$(0,y) + J = (1,y) + J = (2,y) + J = (3,y) + J = (4,y) + J$$

e, além disso,

$$(0,0) + J = (0,3) + J,\ (0,1) + J = (0,4) + J,\ (0,2) + J = (0,5) + J.$$

Existem assim 3 classes distintas: $\overline{0} = (0,0) + J$, $\overline{1} = (0,1) + J$, $\overline{2} = (0,2) + J$. Escrevendo as tabelas do anel, conclui-se imediatamente que $A/J \cong (\mathbb{Z}_3, +_3, \times_3)$.

Comentários e soluções alternativas:

1(a) Em $\mathbb{Z}_4$ ou $\mathbb{Z}_6$ não há (porque aí não há nenhum a tal que $a+1$ e $a-1$ são divisores de zero) mas em $\mathbb{Z}_8$ já temos $3^2 = 1$ e $3 \neq 1$ e $3 \neq -1 = 7$ (porque, neste caso, quer $a+1 = 4$ quer $a-1 = 2$ são divisores de zero).

De facto, a prova de $(*)$ mostra que
Se $a+1$ não é divisor de zero **ou** *$a-1$ não é divisor de zero,* **então** *$(*)$ é verdadeira.*

1(b) A prova directa que $5\mathbb{Z}$ é maximal é simples: se J é um ideal de $\mathbb{Z}$ tal que $5\mathbb{Z} \subset J$, então existe $d \in J$ que não é múltiplo de 5 pelo que $\text{mdc}(5, d) = 1$. Logo existem inteiros r, s tais que $1 = 5r + ds$ e, consequentemente, como $5r, ds \in J$, então $1 \in J$, isto é, $J = A$.

Alternativa: Vimos nas aulas que em $\mathbb{Z}$, um ideal é maximal sse é primo e que $n\mathbb{Z}$ é primo sse n é primo.

2(c) Podia-se também observar que neste anel, qualquer elemento que não é invertível, com excepção do $(0,0)$, é automaticamente divisor de zero e responder a esta questão depois da alínea seguinte onde são calculados os invertíveis. Em conclusão, o anel A, com 30 elementos, além do seu zero (o par $(0,0)$) tem 8 elementos invertíveis e 21 divisores de zero.

2(e) Uma maneira rápida de concluir que, em $\mathbb{Z}_6$,

$$bd \in \{0,3\} \iff b, d \in \{0,3\}$$

é olhar para a tabela da multiplicação:

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2(f) $A/J = \{\overline{0}, \overline{1}, \overline{2}\}$. Fazendo as contas obtem-se

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

e

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$