1. (a) Uma função $f\colon \{1,2,3\} \to \mathbb{Z}_6$ é completamente determinada pela sucessão

$$(f(1), f(2), f(3)) \in \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_6$$

das suas imagens em $\mathbb{Z}_6$. Podemos então representar cada elemento f do anel A por um triplo $(a_1, a_2, a_3) \in \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_6$. Nesta representação, as operações do anel A correspondem a operar triplos coordenada a coordenada com as operações de $\mathbb{Z}_6$ (formalmente, isto significa que o anel A é isomorfo ao anel produto $\mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_6$).

$(a_1, a_2, a_3) = (f(1), f(2), f(3)) \in A$ é um divisor de zero se e só se $(a_1, a_2, a_3) \neq (0,0,0)$ e existe $(x_1, x_2, x_3) = (g(1), g(2), g(3)) \neq (0,0,0)$ em A tal que $(a_1, a_2, a_3) \cdot (x_1, x_2, x_3) = (0,0,0)$.
Por exemplo, a função $(0,1,1)$ é um divisor de zero pois $(0,1,1) \cdot (1,0,0) = (0,0,0)$.
É evidente que há muitos mais exemplos análogos a este, mesmo com as três imagens todas diferentes de zero: $(2,1,1) \cdot (3,0,0) = (0,0,0)$, $(2,4,1) \cdot (3,3,0) = (0,0,0)$, etc.

(b) $(a_1, a_2, a_3) \cdot (b_1, b_2, b_3) = (1,1,1) \iff (a_1 \times_6 b_1, a_2 \times_6 b_2, a_3 \times_6 b_3) = (1,1,1) \iff a_1 \times_6 b_1 = 1, a_2 \times_6 b_2 = 1, a_3 \times_6 b_3 = 1$. Portanto, os elementos invertíveis de A são precisamente as funções (a_1, a_2, a_3) com $a_1, a_2, a_3 \in \{1,5\}$, uma vez que 1 e 5 são os únicos elementos invertíveis de $\mathbb{Z}_6$. São, ao todo, oito:

$$(1,1,1),\ (1,1,5),\ (1,5,1),\ (1,5,5),\ (5,1,1),\ (5,1,5),\ (5,5,1),\ (5,5,5).$$

(c) Como $(0,0,0) \in I$, para que I seja um subgrupo para a primeira operação basta que $(a_1, a_2, a_3) - (b_1, b_2, b_3) \in I$ sempre que $(a_1, a_2, a_3), (b_1, b_2, b_3) \in I$, o que é evidente:

$$(a_1, 0, 0) - (b_1, 0, 0) = (a_1 - b_1, 0, 0) \in I.$$

Finalmente, sejam $(x, y, z) \in A$ e $(a_1, 0, 0) \in I$. Então $(x, y, z) \cdot (a_1, 0, 0) = (x \times_6 a_1, 0, 0) \in I$, o que mostra que I é um ideal de A.
Este ideal é claramente principal:

$$I = \{(a_1, 0, 0) \mid a_1 \in \mathbb{Z}_6\} = \{(a_1, a_2, a_3) \cdot (1,0,0) \mid (a_1, a_2, a_3) \in A\} = \langle (1,0,0) \rangle.$$

Este ideal não é primo uma vez que, por exemplo, para quaisquer $(a, 2, 0), (b, 3, 0)$, se tem $(a, 2, 0) \cdot (b, 3, 0) = (a \times_6 b, 0, 0) \in I$ mas nem $(a, 2, 0)$ nem $(b, 3, 0)$ pertencem a I.

(d) À partida existem $6 \times 6 \times 6 = 216$ classes laterais definidas por I em A. Como

$$(x, y, z) + I = (x', y', z') + I \Leftrightarrow (x, y, z) - (x', y', z') \in I \Leftrightarrow y - y' = z - z' = 0 \Leftrightarrow y = y', z = z',$$

então o que distingue duas classes laterais $(x, y, z) + I$ e $(x', y', z') + I$ é o valor das coordenadas 2 e 3 dos respectivos triplos representantes. Assim, para cada par $y, z \in \mathbb{Z}_6$, é evidente que

$$(0, y, z) + I = (1, y, z) + I = (2, y, z) + I = (3, y, z) + I = (4, y, z) + I = (5, y, z) + I$$

e basta escolhermos uma delas para representar as seis. Por exemplo, escolhendo a primeira, concluímos que as classes

$$(0, y, z) + I, \quad y, z \in \mathbb{Z}_6$$

formam um conjunto representativo de todas as classes laterais. Existem assim $6 \times 6 = 36$ classes distintas.

2. (a) Uma vez que a não é divisor de zero, temos

$$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b-c) = 0 \Rightarrow a = 0 \text{ ou } b - c = 0.$$

Como $a \neq 0$ então, necessariamente, $b = c$.

(b) Pela propriedade distributiva dos anéis tem-se

$$na = a + a + \cdots + a = 1_A \cdot a + 1_A \cdot a + \cdots + 1_A \cdot a = \underbrace{(1_A + 1_A + \cdots + 1_A)}_{=x \in A} \cdot a = x \cdot a.$$

Num anel sem identidade já não temos a identidade disponível para realizar estes cálculos com a propriedade distributiva. Por exemplo, no anel $(2\mathbb{Z}, +, \cdot)$ dos inteiros pares, para $a = 2$ e $n = 1$ ou $n = 3$ tal é impossível: os elementos 2 e $6 = 2 + 2 + 2$ para se escreverem na forma $x \cdot 2$ com $x \in 2\mathbb{Z}$ teriam que ser múltiplos de 4 !

(c) Pela definição de ideal maximal, teremos que mostrar que se J é um ideal de A contendo I estritamente, então $J = A$. Seja então J um ideal de A tal que $I \subset J$. Isto significa que existe $a \in J \setminus I$. Usando a propriedade do ideal I, podemos concluir da existência de $b \in A$ tal que $ab - 1 \in I$. Mas então $ab - 1 \in J$, pois I está contido em J, e $ab \in J$, pois $a \in J$. Consequentemente, $ab - (ab - 1) = 1$ também tem que pertencer a J. Assim, $1 \in J$, o que implica imediatamente $J = A$ (uma vez que, para qualquer $a \in A$, $a = a \cdot 1 \in J$).
