1(f) *Seja* $(A,+,\cdot)$ *um anel com identidade 1. Averigúe se o conjunto* A *tem estrutura de anel para as seguintes operações (em caso afirmativo, verifique se tem identidade, divisores de zero e estrutura de corpo):*

$$a \oplus b = a+b+1, \qquad a \otimes b = a+b+a\cdot b, \qquad \forall a,b \in A.$$

Resolução:

1. $\oplus$ é uma operação associativa: Por um lado,

   $$(a\oplus b)\oplus c = (a+b+1)\oplus c = a+b+a+c+1 = a+b+c+1+1$$

   (porque estamos num grupo comutativo $(A,+)$); por outro lado,

   $$a\oplus(b\oplus c) = a+(b+c+1) = a+b+c+1+1.$$

2. $\oplus$ é comutativa: $a\oplus b = a+b+1 = b+a+1) = b\oplus a$.

3. $\oplus$ tem elemento neutro $\mathbb{0}$: Uma vez que $a\oplus(-1) = a+(-1)+1 = a+0 = a$ para qualquer $a\in A$, o elemento -1 (o simétrico da identidade do anel original) é o elemento neutro de $\oplus$.

   Solução alternativa: Mais uma vez porque estamos num grupo $(A,+)$ temos, para qualquer $a\in A$,

   $$a\oplus x = a \Leftrightarrow \cancel{a}+x+1 = \cancel{a} \Leftrightarrow x+1 = 0 \Leftrightarrow x = -1.$$

   Portanto, $\mathbb{0} = -1$.

4. $(A,\oplus)$ é um grupo comutativo: Falta só verificarmos a existência de simétrico de qualquer elemento para a operação $\oplus$:

   $$a\oplus x = -1 \Leftrightarrow a+x+1 = -1 \Leftrightarrow x = -a-1-1.$$

5. $\otimes$ é uma operação associativa: Usando as propriedades de anel de $(A,+\cdot)$ obtemos

   $$(a\otimes b)\otimes c = (a+b+ab)\otimes c = a+b+ab+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$$

   e

   $$a\otimes(b\otimes c) = a\otimes(b+c+bc = a+b+c+bc+ab+ac+abc,$$

   que são iguais pois $+$ é uma operação comutativa em A.

6. $\otimes$ é uma operação distributiva relativamente a $\oplus$:

   $$a\otimes(b\oplus c) = a\otimes(b+c+1) = a+b+c+1+a(b+c+1) = a+b+c+1+ab+ac+a$$

   enquanto

   $$(a\otimes b)\oplus(a\otimes c) = (a+b+ab)\oplus(a+c+ac) = a+b+ab+a+c+ac+1,$$

   que são iguais pois $+$ é uma operação comutativa em A.

Em conclusão,

$$(A, \oplus, \otimes) \text{ \emph{é um anel.}}$$

Propriedades adicionais de $(A, \oplus, \otimes)$:

7. <u>$\otimes$ é comutativa sse $\cdot$ o for</u>: Como $a \otimes b = a + b + ab$ e $b \otimes a = b + a + ba = a + b + ba$, então

$$a \otimes b = b \otimes a \Leftrightarrow ab = ba.$$

8. <u>$\otimes$ tem elemento neutro $\mathbb{1}$</u>: $a \otimes x = a \Leftrightarrow \cancel{a} + x + ax = \cancel{a} \Leftrightarrow x + ax = 0 \Leftrightarrow (1 + a)x = 0$. Para $a = -1$, a solução para x pode ser arbitrária mas para $a = 0$ a solução terá que ser necessariamente $x = 0$. Assim,

$$\forall a \in A, a \otimes x = a \Leftrightarrow \forall a \in A, (1 + a)x = 0 \Leftrightarrow x = 0$$

($\Leftarrow$ é evidente pela propriedade do zero de um anel relativamente à segunda operação do anel; $\Rightarrow$ segue do caso particular $a = 0$)

Portanto, $\mathbb{1} = 0$.

9. <u>$a \in A$ é um divisor de zero de $(A, \oplus, \otimes)$ sse $a + 1$ for um divisor de zero de $(A, +, \cdot)$</u>: Por definição, um elemento $a \in A$ é um divisor de zero à esquerda do anel $(A, \oplus, \otimes)$ se e só se $a \neq \mathbb{0}$ e existe $b \neq \mathbb{0}$ tal que $a \otimes b = \mathbb{0}$, isto é,

$$a \neq -1, \ \exists\, b \neq -1 \colon a + b + ab = -1.$$

Mas $a + b + ab = -1 \Leftrightarrow a + b + ab + 1 = 0 \Leftrightarrow (a + 1)(b + 1) = 0$. Portanto,

$$\begin{aligned} & a \text{ é um divisor de zero à esquerda em } (A, \oplus, \otimes) \\ \Leftrightarrow\ & a \neq -1, \ \exists\, b \neq -1 \colon (a + 1)(b + 1) = 0 \\ \Leftrightarrow\ & a + 1 \neq 0, \ \exists\, b' \neq 0 \colon (a + 1)b' = 0 \\ \Leftrightarrow\ & a + 1 \text{ é um divisor de zero à esquerda em } (A, +, \cdot). \end{aligned}$$

A conclusão é análoga para divisores de zero à direita e, consequentemente, para divisores de zero.

(Note que $b' = b + 1$, isto é, $b = b' - 1$, pelo que o par b de a em $(A, \oplus, \otimes)$ é dado por $b' - 1$ onde b' é o par do divisor de zero $a + 1$ em $(A, +, \cdot)$).

Em conclusão,

$$(A, \oplus, \otimes) \text{ \emph{é um domínio de integridade se e só se} } (A, +, \cdot) \text{ \emph{o for.}}$$

10. <u>$a \in A$ é uma unidade de $(A, \oplus, \otimes)$ sse $a + 1$ for uma unidade de $(A, +, \cdot)$</u>: Um elemento a de A é invertível em $(A, \oplus, \otimes)$ à esquerda se e só se existe $x \in A$ tal que $a \otimes x = \mathbb{1}$, isto é, $a + x + ax = 0$. Mas

$$a + x + ax = 0 \Leftrightarrow a + x + ax + 1 = 1 \Leftrightarrow (a + 1)(x + 1) = 1.$$

Portanto,

$$\begin{aligned} & a \text{ é invertível à esquerda em } (A, \oplus, \otimes) \\ \Leftrightarrow\ & \exists\, x\colon (a+1)(x+1) = 1 \\ \Leftrightarrow\ & a+1 \text{ é invertível à esquerda em } (A, +, \cdot). \end{aligned}$$

A conclusão é análoga para unidades à direita e, consequentemente, para unidades.

(Note que sendo x o inverso de a em $(A, \oplus, \otimes)$, o inverso $(a+1)^{-1}$ de $a+1$ em $(A, +, \cdot)$ é dado pelo elemento $x+1$. Portanto, $x = (a+1)^{-1} - 1$).

Em conclusão,

$$(A, \oplus, \otimes) \textit{ é um corpo se e só se } (A, +, \cdot) \textit{ o for.}$$

Resumindo, temos a seguinte tabela:

anel	$(A, +, \cdot)$	$(A, \oplus, \otimes)$
zero	0	-1
simétrico de a	$-a$	$-a-1-1$
identidade	1	0
divisor de zero (caso exista)	a	$a-1$
unidade (caso exista)	a	$a-1$
inverso de a (caso exista)	a^{-1}	$(a+1)^{-1}-1$

Será ilustrativo aplicarmos a construção deste exercício a exemplos particulares de anéis $(A, +, \cdot)$:

(1) $(A, +, \cdot) = (\mathbb{Z}_6, +_6, \times_6)$:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

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

$\mathbb{0} = 5$
simétrico de 5: é o 5
simétrico de 0: é o 4
simétrico de 1: é o 3
simétrico de 2: é o 2

$\times_6$	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

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

$\mathbb{1} = 0$
inverso de 0: é o 0
inverso de 4: é o 4

anel	$(\mathbb{Z}_6, +_6, \times_6)$	$(\mathbb{Z}_6, \oplus, \otimes)$
zero	0	5
simétrico de a	$(6-a) \mod 6$	$(4-a) \mod 6$
identidade	1	0
divisores de zero	2,3,4	1,2,3
unidades	1,5	0,4
inversos	1,5	0,4

(2) $(A, +, \cdot) = (\mathbb{Z}, +, \cdot)$:

$+$	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-3	$\cdots$	-6	-5	-4	-3	-2	-1	0	$\cdots$
-2	$\cdots$	-5	-4	-3	-2	-1	0	1	$\cdots$
-1	$\cdots$	-4	-3	-2	-1	0	1	2	$\cdots$
0	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
1	$\cdots$	-2	-1	0	1	2	3	4	$\cdots$
2	$\cdots$	-1	0	1	2	3	4	5	$\cdots$
3	$\cdots$	0	1	2	3	4	5	6	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

$\oplus$	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-3	$\cdots$	-5	-4	-3	-2	-1	0	1	$\cdots$
-2	$\cdots$	-4	-3	-2	-1	0	1	2	$\cdots$
-1	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
0	$\cdots$	-2	-1	0	1	2	3	4	$\cdots$
1	$\cdots$	-1	0	1	2	3	4	5	$\cdots$
2	$\cdots$	0	1	2	3	4	5	6	$\cdots$
3	$\cdots$	1	2	3	4	5	6	7	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

$\times$	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-3	$\cdots$	9	6	3	0	-3	-6	-9	$\cdots$
-2	$\cdots$	6	4	2	0	-2	-4	-6	$\cdots$
-1	$\cdots$	3	2	1	0	-1	-2	-3	$\cdots$
0	$\cdots$	0	0	0	0	0	0	0	$\cdots$
1	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
2	$\cdots$	-6	-4	-2	0	2	4	6	$\cdots$
3	$\cdots$	-9	-6	-3	0	3	6	9	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

$\otimes$	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
-3	$\cdots$	3	1	-1	-3	-5	-7	-9	$\cdots$
-2	$\cdots$	1	0	-1	-2	-3	-4	-5	$\cdots$
-1	$\cdots$	-1	-1	-1	-1	-1	-1	-1	$\cdots$
0	$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
1	$\cdots$	-5	-3	-1	1	3	5	7	$\cdots$
2	$\cdots$	-7	-4	-1	2	5	8	11	$\cdots$
3	$\cdots$	-9	-5	-1	3	7	11	15	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

anel	$(\mathbb{Z}, +, \cdot)$	$(\mathbb{Z}, \oplus, \otimes)$
zero	0	-1
simétrico de a	$-a$	$-a-2$
identidade	1	0
divisores de zero	não há	não há
unidades	$1, -1$	$0, -2$
inversos	$1, -1$	$0, -2$