Folha4-Ex1 Seja $G$ um grupo tal que, para quaisquer $a, b \in G$, $(ab)^{10} = a^{10}b^{10}$. Sejam $H = \{a^{10} \,|\, a \in G\}$ e $K = \{a \in G \,|\, a^{10} = e\}$.

(a) Mostre que $f : G \to G$ dado por $f(a) = a^{10}$ é um endomorfismo.

(b) Usando o Teorema do Homomorfismo, mostre que $|H| = |G : K|$.

(a) Sejam $a, b \in G$. Como $(ab)^{10} = a^{10}b^{10}$, tem-se $f(ab) = (ab)^{10} = a^{10}b^{10} = f(a)f(b)$ e $f$ é um homomorfismo de grupos. Como o grupo de chegada coincide com o grupo de partida, podemos concluir que $f$ é um endomorfismo.

(b) Aplicando o Teorema do Homomorfismo a $f$, obtemos $G/\mathrm{Ker}(f) \cong \mathrm{Im}f$. Como $\mathrm{Ker}(f) = K$ e $\mathrm{Im}f = H$, obtemos $G/K \cong H$. Logo $|G/K| = |H|$. Como a ordem do grupo quociente é igual ao índice $|G : K|$, podemos concluir que $|G : K| = |H|$.

Folha4-Ex2 Considere o grupo ortogonal $O(2) = \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) : A \cdot A^T = A^T \cdot A = I_2\}$ bem como o seu subgrupo $SO(2) = \{A \in O(2) : \det(A) = 1\}$. Recorrendo ao Teorema do Homomorfismo mostre que $|O(2) : SO(2)| = 2$.

Indicação: aplique o Teorema do Homomorfismo ao homomorfismo $\det : (O(2), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$.

Folha4-Ex4 Seja $G = \langle a \rangle$ um grupo cíclico em que $a \neq e$. Diga, justificando, se é verdadeiro ou falsa cada uma das afirmações seguintes:

(a) Se $|G| = 18$, então $a^{30} = a^{12}$.

(b) Se $a^{30} = a^{12}$, então $|G| = 18$.

(c) Se $a^{25} = a^{38}$, então $|G| = 13$.

(d) Se $G$ é infinito então $G$ admite exactamente dois geradores distintos: $a$ e $a^{-1}$.

(e) Se os geradores distintos de $G$ são exactamente $a$ e $a^{-1}$, então $G$ é infinito.

(a) Verdadeira. Tem-se $a^{18} = e$ e então $a^{30} = a^{18}a^{12} = ea^{12} = a^{12}$.

(b) Falsa, contra-exemplo: se $G = \langle a \rangle$ com $a^2 = e$, tem-se $a^{18} = a^{30}$ mas $|G| = 2$. Equivalentemente, em escrita aditiva, no grupo $G = \mathbb{Z}_2$, $a = [1]_2$ verifica $30a = 12a$ mas $|G| = 2$.

(c) Verdadeira. Tem-se $a^{13} = a^{38}a^{-25} = e$. Logo $|a|$ divide 13. Como $a \neq e$, $|a| \neq 1$. Logo $|G| = |a| = 13$.

(d) Verdadeira. Como $a$ é gerador de $G$, $a^{-1}$ é gerador de $G$ também. Como $G$ é infinito, $a \neq a^{-1}$ pois senão $a^2 = e$ e $|G| = |a| \leq 2$. Não existem outros geradores: Um isomorfismo $f\colon \mathbb{Z} \to G$ é dado por $f(m) = a^m$. Seja $n \in \mathbb{Z}$ tal que $a^n$ é um gerador de $G$. Então $f(nk) = a^{nk} = a = f(1)$ para um certo $k \in \mathbb{Z}$. Logo $nk = 1$, pelo que $n = \pm 1$.

(e) Falsa. Em $\mathbb{Z}_3$, $[1]_3$ e $-[1]_3 = [2]_3$ são os únicos geradores.

Folha4-Ex7 Seja $G = \langle a \rangle$ um grupo cíclico de ordem 15.

(a) Mostre que $G$ admite exatamente 8 geradores distintos.

(b) Indique todos os subgrupos de $G$.

(a) Tem-se $G = \{e, a, \ldots, a^{14}\}$ e $G = \langle a^k \rangle$ se e só se $\mathrm{mdc}(15, k) = 1$. Assim, os geradores de $G$ são: $a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$.

Folha4-Ex7 Seja $G = \langle a \rangle$ um grupo cíclico de ordem 30 e $H = \langle a^{25} \rangle$.

(a) Determine $H$.

(b) Indique, caso existam, os elementos de $H$ que têm ordem 3.

(c) Diga, justificando, se $G$ admite subgrupos de ordem 5 e, em caso afirmativo, indique-os.

(a) $H = \{a^{25}, a^{50} = a^{20}, a^{75} = a^{15}, a^{100} = a^{10}, a^{125} = a^5, a^{150} = a^0 = e\}$.

(b) $a^{20}, a^{10}$.

(c) Como 5 divide 30, $G$ admite um único subgrupo de ordem 5, nomeadamente $\langle a^6 \rangle$.

Folha4-Ex8 Considere em $S_8$ as permutações

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 6 & 8 & 7 & 5 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 1 & 4 & 8 & 2 & 7 \end{pmatrix}$$

e $\sigma_3 = (1,3,6)(2,7,4)(5,8)$.

(a) Decomponha $\sigma_1$ e $\sigma_2$ em cíclos dois a dois disjuntos.

(b) Determine as permutações $\sigma_1^{-1}$, $\sigma_1\sigma_2$, $\sigma_1\sigma_3$, $\sigma_2^2$, $\sigma_2^3$ e $\sigma_2^2\sigma_3$ e factorize-os em cíclos dois a dois disjuntos. Indique a ordem e a paridade de cada permutação.

(a) $\sigma_1 = (1,2)(3,4,6,7,5,8)$, $\sigma_2 = (1,3,5,4)(2,6,8,7)$.

(b) Temos:

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 3 & 7 & 4 & 6 & 5 \end{pmatrix} = (1,2)(3,8,5,7,6,4)$$

Como os cíclos $\tau = (1,2)$ e $\gamma = (3,8,5,7,6,4)$ são disjuntos, temos $|\sigma^{-1}| = \text{mmc}(|\tau|,|\gamma|) = \text{mmc}(2,6) = 6$. Como sgn é um homomorfismo e o sinal de um cíclo de ordem $k$ é $k-1$ temos $\text{sgn}(\sigma_1^{-1}) = \text{sgn}(\tau)\text{sgn}(\gamma) = (-1)^1(-1)^5 = 1$, isto é $\sigma_1^{-1}$ é par. Nota: como o homomorfismo sgn tem valor no grupo multiplicativo $\{+1,-1\}$ poderíamos também dizer que $\text{sgn}(\sigma_1^{-1}) = (\text{sgn}(\sigma_1))^{-1} = \text{sgn}(\sigma_1)$ e utilizar a decomposição em cíclos obtida na alínea anterior para concluir.

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 8 & 2 & 6 & 3 & 1 & 5 \end{pmatrix} = (1,4,2,7)(3,8,5,6),\ |\sigma_1\sigma_2| = 4,\ \text{par}$$

$$\sigma_1\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 7 & 1 & 3 & 2 & 6 & 8 \end{pmatrix} = (1,4)(2,5,3,7,6),\ |\sigma_1\sigma_3| = 10,\ \text{ímpar}$$

$$\sigma_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 4 & 3 & 1 & 7 & 6 & 2 \end{pmatrix} = (1,5)(2,8)(3,4)(6,7),\ |\sigma_2^2| = 2,\ \text{par}$$

$$\sigma_2^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 5 & 3 & 2 & 8 & 6 \end{pmatrix} = (1,4,5,3)(2,7,8,6),\ |\sigma_2^3| = 4,\ \text{par}$$

$$\sigma_2^2\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 8 & 2 & 5 & 3 & 1 \end{pmatrix} = (1,4,8)(2,6,5)(3,7),\ |\sigma_2^2\sigma_3| = 6,\ \text{ímpar}$$

Folha4-Ex9 Considere em $S_9$ a permutação $\sigma = (9,5,7)(3,4,1,5,7,6)(1,2,8,4)(3,4,8)$.

(a) Determine a ordem e a paridade de $\sigma$.

(b) Determine $\sigma^{339}$.

(a) Da apresentação de $\sigma$ deduzimos que $\sigma$ é par. Por outro lado temos

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 7 & 1 & 9 & 3 & 6 & 4 & 5 \end{pmatrix} = (1,2,8,4)(3,7,6)(5,9).$$

Desta decomposição em cíclos dois a dois disjuntos, podemos concluir que $|\sigma| = 12$.

(b) Tem-se $\sigma^{339} = \sigma^{12\cdot 28+3} = \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 3 & 8 & 9 & 6 & 7 & 2 & 5 \end{pmatrix}$.

Folha4-Ex10 Considere o grupo simétrico $S_8$.

(a) Exiba um elemento de $S_8$ de ordem 15.

(b) Mostre que não existe um elemento de $S_8$ de ordem 14.

(a) $(1,2,3)(4,5,6,7,8)$

(b) Suponhamos, por absurdo, que existe um elemento $\sigma \in S_8$ de ordem 14. Então $\sigma$ não é um cíclo (pois a ordem de um cíclo é inferior ou igual a 8). Logo $\sigma$ pode ser factorizado em pelo menos dois cíclos dois a dois disjuntos de $S_8 \setminus \{id\}$ e $|\sigma| = 14$ é o mmc das ordens destes cíclos. Segue-se que a decomposição de $\sigma$ em cíclos dois a dois disjuntos de $S_8 \setminus \{id\}$ contém pelo menos um cíclo de ordem 2 e um cíclo de ordem 7. Logo $\{1,\ldots,8\}$ tem pelo menos $2+7=9$ elementos. Contradição! Logo não existe um elemento de $S_8$ de ordem 14.

Folha5-Ex2 Determine todos os endomorfismos do anel $\mathbb{Z}$.

Seja $f\colon \mathbb{Z} \to \mathbb{Z}$ um endomorfismo de aneis. Então $f$ é um endomorfismo de grupos e $f(1) = 1$. Segue-se que $f = id_{\mathbb{Z}}$. Logo $id_{\mathbb{Z}}$ é o único endomofismo do anel $\mathbb{Z}$.

Folha5-Ex3 Mostre que os aneis $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ são isomorfos.

Como 2 e 3 são primos entre si, um isomorfismo de grupos $f\colon \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ é dado por $f(k + 6\mathbb{Z}) = (k + 2\mathbb{Z}, k + 3\mathbb{Z})$. Como $f(1 + 6\mathbb{Z}) = (1 + 2\mathbb{Z}, 1 + 3\mathbb{Z})$ e para quaisquer $k, l \in \mathbb{Z}$, $f((k + 6\mathbb{Z})(l + 6\mathbb{Z})) = f(kl + 6\mathbb{Z}) = (kl + 2\mathbb{Z}, kl + 3\mathbb{Z}) = (k + 2\mathbb{Z}, k + 3\mathbb{Z})(l + 2\mathbb{Z}, l + 3\mathbb{Z}) = f(k + 6\mathbb{Z})f(l + 6\mathbb{Z})$, $f$ é de facto um isomorfismo de aneis.

Folha5-Ex4 Mostre que o *centro* de um anel $A$, $Z(A) = \{x \in A \,|\, \forall y \in A\ xy = yx\}$, é um subanel de $A$.

Tem-se $1y = y = y1$ para todo o $y \in A$, pelo que $1 \in Z(A)$. Sejam $a, b \in Z(A)$ e $y \in A$. Então $(a - b)y = ay - by = ya - yb = y(a - b)$ e $aby = ayb = yab$. Logo $a - b, ab \in Z(A)$. Segue-se que $Z(A)$ é um subanel de $A$.

Folha5-Ex6 Sejam $A$ um anel e $n \in \mathbb{Z}$. Verifique que $nA = \{nx \,|\, x \in A\}$ é um ideal de $A$.

Tem-se $0 = n0 \in nA$. Como o grupo aditivo de $A$ é abeliano, tem-se para $x, y \in A$, $nx - ny = n(x - y) \in nA$. Logo $nA \leq A$. Sejam $a, x \in A$. Então, pelas leis de distributividade, $a(nx) = n(ax) \in nA$ e $(nx)a = n(xa) \in nA$. Segue-se que $nA$ é um ideal de $A$.

Folha5-Ex7 Seja $A$ um anel comutativo e seja $a \in A$. Verifique que $I = \{x \in A \,|\, ax = 0\}$ é um ideal de $A$.

Tem-se $0 \in I$ pois $a \cdot 0 = 0$. Sejam $x, y \in I$. Tem-se $ax = 0$ e $ay = 0$ pelo que $a(x - y) = ax - ay = 0 - 0 = 0$. Logo $x - y \in I$. Seja $x \in I$ e seja $b \in A$. Como $A$ é comutativo, basta ver que $bx \in I$ e temos $a(bx) = bax$. Como $x \in I$, temos $ax = 0$ e portanto $a(bx) = bax = 0$ e $bx \in I$. Podemos concluir que $I$ é um ideal.

Folha5-Ex8 Sejam $m$ e $n$ dois números inteiros primos entre si. Mostre que o único ideal de $\mathbb{Z}$ que contém $m$ e $n$ é $\mathbb{Z}$.

Seja $I$ um ideal de $\mathbb{Z}$ que contém $m$ e $n$. Como $\text{mdc}(m, n) = 1$, existem, pelo lema de Bézout, $u, v \in \mathbb{Z}$ tais que $um + vn = 1$. Segue-se que $1 \in I$ e então que $I = \mathbb{Z}$.

Folha5-Ex9 Sejam $A$ um anel e $I$ um ideal de $A$. Mostre que o anel quociente $A/I$ é comutativo se e só se $ab - ba \in I$ para todos os $a, b \in A$.

Suponhamos primeiramente que $A/I$ é comutativo. Sejam $a, b \in A$. Então $ab + I = (a + I)(b + I) = (b + I)(a + I) = ba + I$. Logo $ab - ba \in I$. Suponhamos inversamente que $ab - ba \in I$ para todos os $a, b \in A$. Então para todos os $a, b \in A$, $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$. Logo $A/I$ é comutativo.

Folha6-Ex1 Sejam $A$ um anel e $d$ um divisor de zero. Prove que $d$ não é invertível.

Suponhamos, por absurdo que $d$ é invertível. Como $d$ é um divisor de zero, $d \neq 0$ e existe $a \neq 0$ tal que $da = 0$ ou $ad = 0$. Então $a = d^{-1}da = d^{-1}0 = 0$ ou $a = add^{-1} = 0d^{-1} = 0$. Contradição! Logo $d$ não é invertível.

Folha6-Ex2 Um elemento $a$ de um anel $A$ diz-se *nilpotente* se $a^n = 0$ para algum número natural positivo $n$.

(a) Seja $A$ é um domínio de integridade. Mostre que 0 é o único elemento nilpotente de $A$.

(b) Seja $A$ um anel comutativo e sejam $x, y \in A$ tais que $x^2 = 0$ e $y^3 = 0$. Mostre que $x + y$ é um elemento nilpotente de $A$.

(a) Suponhamos, por absurdo, que $a \neq 0$ é nilpotente em $A$. Seja $n$ o menor natural positivo tal que $a^n = 0$. Como $a \neq 0$, temos $n > 1$. Como $aa^{n-1} = a^n = 0$, $a^{n-1} = 0$ pois $A$ é um domínio de integridade. Isto contradiz a minimalidade de $n$. Logo 0 é o único elemento nilpotente de $A$.

(b) Como $A$ é comutativo tem-se $(x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4 = x^2(x^2+4xy+6y^2)+(4x+y)y^3$. Como $x^2 = 0$ e $y^3 = 0$ obtemos $(x + y)^4 = 0(x^2 + 4xy + 6y^2) + (4x + y)0 = 0$.

Folha6-Ex3 Seja $A$ um anel comutativo não nulo tal que $A = (a)$ para todo o $a \in A \setminus \{0\}$. Mostre que $A$ é um corpo.

Seja $a \in A \setminus \{0\}$. Como $A = (a)$, existe $b \in A$ tal que $1 = ba$. Logo $a$ é invertível. Logo $A$ é um corpo.

Folha6-Ex4 Seja $A$ um anel comutativo.

(a) Mostre que qualquer ideal maximal de $A$ é primo.

(b) Mostre que um ideal $I$ de $A$ é maximal se e só se $A/I$ é um corpo.

(c) Mostre que o ideal $2\mathbb{Z} \times \mathbb{Z}$ do anel $\mathbb{Z} \times \mathbb{Z}$ é um ideal maximal.

(d) Mostre que o ideal $\{0\} \times \mathbb{Z}$ do anel $\mathbb{Z} \times \mathbb{Z}$ é um ideal primo que não é maximal.

(a) Seja $I$ um ideal maximal de $A$. Então $I \neq A$. Sejam $a, b \in A$ tais que $ab \in I$. Suponhamos que $a \notin I$, queremos ver que $b \in I$. Consideremos o ideal $J = I + (a)$. Como $a \notin I$, tem-se $J \neq I$. Como $I$ é maximal e $I \subset J$, $I \neq J$, podemos concluir que $J = A$. Logo existe $x \in I, r \in A$ tais que $1 = x + ra$. Multiplicando por $b$ (e usando a comutatividade de $A$), obtemos $b = bx + rab$. Como $I$ é um ideal e $x, ab \in I$ obtemos $bx, rab \in I$ e consequentemente $b \in I$. Podemos concluir que $I$ é primo.

(b) Suponhamos primeiramente que $I$ é maximal. Como $A$ é comutativo, $A/I$ é comutativo. Como $I \neq A$, $A/I$ é não nulo. Seja $a + I$ com $a \in A \setminus I$ um elemento não nulo de $A/I$. Então $(a) + I$ é um ideal de $A$ que contém $I$ como subconjunto próprio. Como $I$ é maximal, $(a) + I = A$. Logo existem $b \in A$ e $x \in I$ tais que $1 = ab + x$. Tem-se $(a + I)(b + I) = ab + I = ab + x + I = 1 + I$, pelo que $a + I$ é uma unidade de $A/I$.

Suponhamos agora que $A/I$ é um corpo. Então $I \neq A$ pois $A/I$ é não nulo. Seja $J$ um ideal de $A$ tal que $I \subseteq J \neq A$. Seja $a \in J$. Suponhamos, por absurdo, que $a \notin I$. Então $a + I$ é uma unidade de $A/I$ e existe $b \in A$ tal que $ab + I = (a + I)(b + I) = 1 + I$. Logo $ab - 1 \in I \subseteq J$. Como $ab \in J$, obtém-se $1 \in J$ e então $J = A$. Contradição! Portanto $a \in I$ e $I$ é maximal.

Nota: podemos deduzir a alínea (a) da aínea (b) pois se $I$ é maximal então, pela alínea (b), $A/I$ é um corpo. Logo $A/I$ é um domínio de integridade e $I$ é um ideal primo.

(c) $2\mathbb{Z}\times\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}\times\mathbb{Z}$. Com efeito, seja $J$ um ideal de $\mathbb{Z}\times\mathbb{Z}$ tal que $2\mathbb{Z}\times\mathbb{Z} \subseteq J \subseteq \mathbb{Z}\times\mathbb{Z}$. Suponhamos que $J \neq 2\mathbb{Z} \times \mathbb{Z}$. Logo existe $(a, b) \in J$ tal que $(a, b) \notin 2\mathbb{Z} \times \mathbb{Z}$. Então $a \notin 2\mathbb{Z}$ e existe $k \in \mathbb{Z}$ tal que $a = 2k + 1$. Então $(a, b) - (2k, b - 1) = (1, 1) \in J$, pelo que $J = \mathbb{Z} \times \mathbb{Z}$. Contradição! Logo $(a, b) \in 2\mathbb{Z} \times \mathbb{Z}$ e $2\mathbb{Z} \times \mathbb{Z}$ é maximal.

(d) $\{0\} \times \mathbb{Z}$ é um ideal primo de $\mathbb{Z} \times \mathbb{Z}$ que não é maximal. Com efeito, sejam $(a, b), (x, y) \in \mathbb{Z} \times \mathbb{Z}$ tais que $(a, b)(x, y) = (ax, by) \in \{0\} \times \mathbb{Z}$. Então $a = 0$ ou $x = 0$ e portanto $(a, b) \in \{0\} \times \mathbb{Z}$ ou $(x, y) \in \{0\} \times \mathbb{Z}$. Logo $\{0\} \times \mathbb{Z}$ é primo. Como $\{0\} \times \mathbb{Z} \subsetneq 2\mathbb{Z} \times \mathbb{Z}$, $\{0\} \times \mathbb{Z}$ não é maximal.

Folha6-Ex5 Diga, justificando, se é verdadeira ou falsa cada uma das seguintes afirmações:

(a) O anel $\mathbb{Z}_2 \times \mathbb{Z}$ é um domínio de integridade.

(b) O anel $\mathbb{Z}_2 \times \mathbb{Z}_3$ é um corpo.

(c) O anel $\mathbb{Z}_7$ contém elementos nilpotentes não nulos.

(d) $\text{car}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$.

(e) $\text{car}(\mathbb{Z}_6 \times \mathbb{Z}_4) = 24$.

(a) Falso pois $([1]_2, 0)([0]_2, 1) = ([0]_2, 0)$.

(b) Falso pois o anel $\mathbb{Z}_2\times\mathbb{Z}_3$ não é um domínio de integridade (tem-se, por exemplo, $([1]_2, [0]_3)([0]_2, [1]_3) = ([0]_2, [0]_3)$).

(c) Falso pois $\mathbb{Z}_7$ é um domínio de integridade.

(d) Verdadeiro pois temos um isomorfismo de anéis $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ e, pelo Ex 7, $\text{car}(\mathbb{Z}_2 \times \mathbb{Z}_3) = \text{car}(\mathbb{Z}_6) = 6$.

(e) Falso. Como $12 \cdot ([1]_6, [1]_4) = ([12]_6, [12]_4) = ([0]_6, [0]_4)$, $\text{car}(\mathbb{Z}_6 \times \mathbb{Z}_4) \leq 12$.