1. Diga, justificando, se as expressões seguintes definem operações binárias nos conjuntos indicados:

   (a) $x * y = x - y$ em $\mathbb{Z} \setminus \{0\}$
   (b) $x * y = x|y|$ em $\mathbb{Z}$
   (c) $x * y = x + y + xy$ em $\mathbb{R} \setminus \{-1\}$
   (d) $x * y = \frac{x+y}{2}$ em $\mathbb{N}$

   Quais das operações binárias encontradas são comutativas?

2. Seja X um conjunto com 2 elementos. Quantas operações binárias é possível definir em X? Quantas destas são comutativas? E se X tiver n elementos com $n \geq 1$?

3. Para cada um dos seguintes casos, verifique se $(\mathbb{R}, *)$ é um semigrupo.

   (a) $x * y = \frac{x+y}{2}$
   (b) $x * y = x + y - 1$
   (c) $x * y = |x + y|$
   (d) $x * y = |x|y$

   Quais dos semigrupos encontrados são monóides?

4. Seja $(G, *)$ um grupóide com elemento neutro tal que

   $$\forall a, b, c, d \in G \quad (a * b) * (c * d) = (a * d) * (b * c).$$

   Mostre que G é um monóide comutativo.

5. Seja S um conjunto com pelo menos dois elementos. Considere a operação $*$ definida em $S \times S$ por $(a, b) * (c, d) = (a, d)$. Mostre que $(S \times S, *)$ é um semigrupo sem elemento neutro.

6. Sejam S um semigrupo e $a, b \in S$ tais que $ab = ba$. Mostre que para qualquer inteiro $n \geq 1$, $a^n b = ba^n$ e $(ab)^n = a^n b^n$.

7. Dê exemplo de um semigrupo S no qual existem dois elementos a e b tais que $(ab)^2 \neq a^2 b^2$.

8. Considere o grupóide $(M, *)$ em que $M = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 1\}$ e a operação $*$ é dada por

   $$(x, y, z) * (a, b, c) = (xa, b + ya, c + za).$$

   Mostre que $(M, *)$ é um monóide e que um elemento $(x, y, z) \in M$ é invertível se e só se $x \neq 0$. Se $(x, y, z) \in M$ é invertível, qual é o seu inverso?

9. Sejam M um monóide e $a, b \in M$. Diga, justificando, quais das seguintes afirmações são verdadeiras e quais são falsas:

   (a) Se a é invertível e $ab = e$, então $b = a^{-1}$.
   (b) Se a é invertível à esquerda, então para quaisquer dois elementos $x, y \in M$, $ax = ay \Rightarrow x = y$.
   (c) Se para quaisquer dois elementos $x, y \in M$, $ax = ay \Rightarrow x = y$, então a é invertível à esquerda.

10. Verifique quais dos grupóides seguintes são grupos:

(a) $(\mathbb{N}, *)$ onde $a * b = 2^{ab}$

(b) $(\mathbb{R} \setminus \{-1\}, *)$ onde $a * b = a + b + ab$

(c) $(\mathbb{Q}, *)$ onde $a * b = ab + a + b + 1$

11. Mostre que existe no máximo uma estrutura de grupo no conjunto $V = \{e, a, b, c\}$ tal que e é o elemento neutro e $a^2 = b^2 = e$. Se existir, será um grupo abeliano? Nota-se que existe um tal grupo, é chamado *grupo de Klein.*

12. Diga quais das aplicações seguintes são homomorfismos de grupos e, nesses casos, classifique-os.

    (a) $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $f(x) = x + 3$

    (b) $g\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $g(x) = 4x$

    (c) $h\colon (\mathbb{R}, +) \to (\mathbb{R}, +)$, $h(x) = x^2$

    (d) $\ln\colon (]0, +\infty[, \cdot) \to (\mathbb{R}, +)$

    (e) $\det : (GL_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$

13. Considere a operação binária $*$ definida em $\mathbb{Z}$ por $x * y = x + y - 3$. Mostre que:

    (a) $(\mathbb{Z}, *)$ é um grupo

    (b) A aplicação $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}, *)$ definida por $f(x) = x + 3$ é um isomorfismo.

14. Sejam G um grupo e $n \in \mathbb{Z}$. Considere a aplicação $f\colon G \to G$ definida por $f(x) = x^n$. Mostre que, se G é abeliano, então a aplicação f é um endomorfismo de G.

15. Quais dos seguintes conjuntos é um subgrupo do grupo $(\mathrm{GL}_2(\mathbb{R}), \cdot)$?

    (a) $C = \{\begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} : a \in \mathbb{R} \setminus \{-1, +1\}\}$.

    (b) $C = \{\begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} : a \neq 0,\ b \in \mathbb{R}\}$.

    (c) $O(2) = \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) : A \cdot A^T = A^T \cdot A = I_2\}$.

16. Sejam G um grupo e $a \in G$. Mostre que o conjunto $C(a) = \{x \in G \mid xa = ax\}$ é um subgrupo de G. O conjunto $C(a)$ é chamado *centralizador* de a.

17. Seja G um grupo. Seja $H \neq \emptyset$ um subconjunto finito de G tal que para quaisquer $x, y \in H$, tem-se $xy \in H$.

    (a) Justifique que H é um semi-grupo.

    (b) Justifique que H é subgrupo de G.

18. Considere o grupo simétrico S_3. Seja H o subgrupo gerado pela permutação σ dada por $\sigma(1) = 2$, $\sigma(2) = 1$ e $\sigma(3) = 3$ e seja K o subgrupo gerado pela permutação τ dada por $\tau(1) = 1$, $\tau(2) = 3$ e $\tau(3) = 2$. Determine HK. É um subgrupo de S_3?

19. Sejam G um grupo e H e K subgrupos de G. Mostre que HK é um subgrupo de G se e só se $HK = KH$.

20. Sejam G um grupo, H um subgrupo de G e $x \in G$. Mostre que as três seguintes afirmações são equivalentes:

    (a) Hx é subgrupo de G

    (b) $x \in H$

    (c) $Hx = H$

21. Seja G um grupo finito tal que $|G|$ é primo. Usando o Teorema de Lagrange, mostre que para todo o $a \in G \setminus \{e\}$ tem-se $G = \langle a \rangle$. Podemos concluir que G é abeliano?

22. Sejam G um grupo e H e K dois subgrupos finitos de G tais que $|H|$ e $|K|$ são primos entre si. Mostre que $H \cap K = \{e\}$.

23. Sejam G um grupo e H um subgrupo de índice 2. Prove que para todo o $x \in G$, $x^2 \in H$.

24. Seja G um grupo e sejam H e K subgrupos finitos de G. Mostre que se $H \cap K = \{e\}$ então a aplicação $f : H \times K \to HK$ dada por $f(h, k) = hk$ é bijetiva.

25. Seja G um grupo de ordem 20 e sejam H e K subgrupos de G de ordem 5. Mostre que $H = K$ (*Sugestão:* Usando o exercício anterior, comece por mostrar que $|H \cap K| = 5$.). Qual o índice de H em G?

26. Considere o grupo simétrico S_3 e o subgrupo $H = \langle \sigma \rangle$ gerado pela permutação σ dada por $\sigma(1) = 2$, $\sigma(2) = 1$ e $\sigma(3) = 3$.

    (a) Qual a ordem de σ? Qual o índice $|S_3 : H|$?

    (b) Usando a permutação τ dada por $\tau(1) = 1$, $\tau(2) = 3$ e $\tau(3) = 2$, mostre que H não é normal em S_3.

27. Seja G um grupo. Mostre que o centro de G dado por $Z(G) = \{x \in G \ : \ \forall g \in G, gx = xg\}$ é um subgrupo normal de G.

28. Sejam G um grupo e H e K normais de G tais que $H \cap K = \{e\}$. Mostre que para todos os $h \in H$ e $k \in K$, $hk = kh$.

29. 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 $|H| = |G : K|$.

30. 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 $|O(2) : SO(2)| = 2$.

31. Seja $f \colon G \to G'$ um epimorfismo de grupos em que G e G' são finitos. Mostre que a ordem de G' divide a ordem de G.

32. 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.

33. Seja G um grupo finito e $a \in G$. Mostre que $a^{|G|} = e$.

34. Seja $G = \langle a \rangle$ um grupo cíclico de ordem 15.

    (a) Mostre que G admite exactamente 8 geradores distintos.

    (b) Indique todos os subgrupos de G.

35. 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.

36. 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 σ_1 e σ_2 em cíclos dois a dois disjuntos.

   (b) Determine as permutações σ_1^{-1}, $\sigma_1\sigma_2$, $\sigma_1\sigma_3$, σ_2^2, σ_2^3 e $\sigma_2^2\sigma_3$ e factorize-os em cíclos dois a dois disjuntos.

   (c) Indique a ordem e a paridade de cada uma das permutações da alínea anterior.

37. 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 σ.

   (b) Determine σ^{339}.

38. 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.

39. Considere o seguinte subconjunto de $\mathcal{M}_{2\times 2}(\mathbb{R})$:

$$D = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;:\; a, b \in \mathbb{R} \right\}.$$

   (a) Mostre que D é um subanel de $\mathcal{M}_{2\times 2}(\mathbb{R})$.

   (b) Mostre que a aplicação $f : \mathbb{C} \to D$ dada por $f(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ é um isomorfismo de anéis.

   (c) Seja $A \in D$ com $\det A \neq 0$. Calculando $A \cdot A^T$, verifique que $A^{-1} \in D$.

   (d) Mostre que todo o elemento não nulo de $\mathbb{C}$ é invertível (uma unidade do anel $\mathbb{C}$) e indique o seu inverso.

40. Determine todos os endomorfismos do anel $\mathbb{Z}$.

41. Mostre que os anéis $\mathbb{Z}_6$ e $\mathbb{Z}_2 \times \mathbb{Z}_3$ são isomorfos.

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

43. Seja $n \geq 1$ um inteiro. Mostre que $[k]_n \in \mathbb{Z}_n \setminus \{[0]_n\}$ é uma unidade do anel $\mathbb{Z}_n$ se e só se k e n são primos entre si.

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

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

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

47. 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 $a, b \in A$.

48. Sejam A um anel e d um divisor de zero. Prove que d não é invertível.

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

    (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.

50. 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.

51. 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.

52. 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) $\mathrm{car}(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$.

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

53. Sejam p um número primo, A um anel comutativo de característica p e $a, b \in A$. Mostre que $(a + b)^p = a^p + b^p$.

54. Seja $f\colon A \to B$ um isomorfismo de anéis. Mostre que $\mathrm{car}(A) = \mathrm{car}(B)$.

55. Seja A um domínio de integridade e sejam $a, b \in A$. Mostre que a e b são associados (isto é, $a|b$ e $b|a$) se e só se existir $u \in A$ invertível tal que $a = bu$.

56. Considere o seguinte subconjunto de $\mathbb{C}$:

$$\mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3} \ : \ a, b, \in \mathbb{Z}\}.$$

    (a) Mostre que $\mathbb{Z}[i\sqrt{3}]$ é um subanel de $\mathbb{C}$ (e, portanto, um domínio de integridade).

    (b) Mostre que a aplicação $N : \mathbb{Z}[i\sqrt{3}] \to \mathbb{N}$ dada por $N(a + ib\sqrt{3}) = a^2 + 3b^2$ satisfaz $N(zw) = N(z)N(w)$ para todos os $z, w \in \mathbb{Z}[i\sqrt{3}]$.

    (c) Determine as unidades de $\mathbb{Z}[i\sqrt{3}]$.

    (d) Mostre que o elemento $1 + i\sqrt{3}$ é irredutível mas não é primo (para mostrar que não é primo, considere o produto $(1 + i\sqrt{3})(1 - i\sqrt{3})$).

57. Seja A um domínio de integridade. Suponha que A é um *domínio de ideais principais* isto é todo o ideal de A é um ideal principal. Sejam $a, b \in A \setminus \{0\}$.

    (a) Justifique que existe $d \in A$ tal que $(a) + (b) = (d)$ e que este elemento é único a menos de um fator invertível.

    (b) Mostre que o elemento d da alínea anterior é um *máximo divisor comum* de a e b, isto é:

$$d|a, \ d|b \text{ e, } \forall x \in A, \ x|a \text{ e } x|b \Rightarrow x|d.$$