ÁLGEBRA MINIMAL PARA A GRADUAÇÃO

Problemas

1. Com o uso da lei de associatividade mostre que $(a \cdot b) \cdot \big(c \cdot (d \cdot f)\big) = \Big(\big(a \cdot (b \cdot c)\big) \cdot d\Big) \cdot f$.

2. Seja G um grupo finito e seja $g \in G$. Mostre que $g^n = 1$ para algum $n > 0$ apropriado.

3. Calcule a ordem de Σ_n.

4. Mostre que o grupo Σ_3 possui um único subgrupo próprio $\big\{\binom{123}{123}, \binom{123}{231}, \binom{123}{312}\big\}$.

5. Descreva todos os subgrupos de $(\mathbb{Z}, +)$.

6. Seja $0 < n \in \mathbb{N}$. Mostre que os números inteiros módulo n formam, relativamente a adição, um grupo cíclico de ordem n. Quantas escolhas há para um gerador deste grupo?

7. Seja M um conjunto e seja G um grupo. Defina no conjunto $G^M = \{f : M \to G\}$ de todas as funções de M para G uma estrutura de grupo (e verifique os axiomas). Qual é ordem de G^M caso M e G sejam finitos?

8. Quantos elementos têm os grupos D_3 e D_4 ?

9. Descreva o núcleo do homomorfismo $|\ | : \mathbb{C}^* \to \mathbb{R}^{>0}$.

10. Seja G um grupo comutativo. Mostre que $h : g \mapsto g^{2015}$ é um homomorfismo $h : G \to G$. Será que tal h é sempre injetivo?

11. Seja $h : G_1 \to G_2$ um homomorfismo de grupos e seja $H \leqslant G_1$. Mostre que $hH \leqslant G_2$.

12. Seja G um grupo e seja $g \in G$. Mostre que a função $()^g : G \to G$, $()^g : x \mapsto g \cdot x \cdot g^{-1}$, é um homomorfismo. Descreva o seu núcleo e a sua imagem.

13. Sejam G_1 e G_2 grupos. Mostre que as funções

$$\pi_1 : G_1 \times G_2 \to G_1, \quad \pi_1 : (g_1, g_2) \mapsto g_1; \qquad \pi_2 : G_1 \times G_2 \to G_2, \quad \pi_2 : (g_1, g_2) \mapsto g_2;$$

$$j_1 : G_1 \to G_1 \times G_2, \quad j_1 : g_1 \mapsto (g_1, 1); \qquad j_2 : G_2 \to G_1 \times G_2, \quad j_2 : g_2 \mapsto (1, g_1)$$

são homomorfismos. Descreva os homomorfismos $\pi_1 \circ j_1$, $\pi_2 \circ j_1$, $\pi_1 \circ j_2$, $\pi_2 \circ j_2$, $j_1 \circ \pi_1$, $j_2 \circ \pi_2$ e indique os seus núcleos e as suas imagens.

14. Seja G um grupo finito. Definamos $h : G \to \Sigma G$ pela regra $hg : G \to G$, onde $hg : g' \mapsto g \cdot g'$ (verifique que $hg \in \Sigma G$). Mostre que h é um homomorfismo injetivo. (Portanto, todo grupo finito é um subgrupo de um grupo simétrico.)

15. Mostre que todo grupo de ordem 4 é comutativo.

16. Seja G um grupo sem subgrupos próprios. Mostre que G é comutativo.

17. Mostre que todo grupo de ordem prima é comutativo.

18*. Suponhamos que um grupo G satisfaz $g^{-1} = g$ para todo $g \in G$. Mostre que G é abeliano.

19*. Seja G um grupo tal que $g_1^2 \cdot g_2^2 = (g_1 \cdot g_2)^2$ para todos $g_1, g_2 \in G$. Mostre que G é abeliano.

20*. Seja G um grupo e sejam $g_1, g_2 \in G$ tais que $g_1^5 = 1$, $g_2^{g_1} = g_1^2$ e $g_2 \neq 1$. Calcule a ordem de g_2.

21. Seja G um grupo e seja $H \leqslant G$. Mostre que as classes laterais à direita de H em G são exatamente as classes da relação de equivalência definida pela regra $g_1 \sim g_2 \Leftrightarrow g_1 g_2^{-1} \in H$.

22. Seja $h : G_1 \to G_2$ um homomorfismo de grupos. Denotamos $K := h^{-1}1$. Mostre que o subgrupo K é fechado relativamente à conjugação por todos os elementos de G_1, isto é, $k^g \in K$ para todo $k \in K$ e todo $g \in G_1$. (Podemos escrever essa propriedade como $K^g \subset K$ para todo $g \in G_1$, ou seja, como $K^{G_1} \subset K$.)

23. Sejam $H \leqslant S \leqslant G$. Mostre que $|G : H| = |G : S| \cdot |S : H|$.

24. Mostre que um subgrupo $N \leqslant G$ é normal se e só se $Ng = gN$ para todo $g \in G$.

25. Mostre que um subgrupo $N \leqslant G$ é normal se e só se o produto de quaisquer duas classes laterais à direita de N em G é uma classe lateral à direita de N em G.

26. Sejam $N_1, N_2 \lhd G$. Mostre que $N_1 N_2 \lhd G$.

27*. Seja G um grupo e seja $H \leqslant G$. Façamos $N_H := \{g \in G \mid H^g \subset H\}$. Mostre que $H \lhd N_H \leqslant G$.

28*. Seja G um grupo e seja $H \leqslant G$. Façamos $N_H := \{g \in G \mid H^g = H\}$. Mostre que $H \lhd N_H \leqslant G$.

29. Seja $N \leqslant G$ um único subgrupo de G de índice n. Mostre que N é normal.

30. Mostre que qualquer subgrupo de índice 2 é normal.

31. Sejam $N_1, N_2 \lhd G$ subgrupos normais tais que $N_1 \cap N_2 = 1$ e $G = N_1 N_2$. Mostre que $G \simeq N_1 \times N_2$.

32. Sejam $H, S \leqslant G$. Mostre que $HS \leqslant G$ se e só se $HS = SH$.

33*. Mostre que todo grupo finito de ordem par contém um elemento de ordem 2.

34. Para $a, b \in \mathbb{R}$, definamos $f_{a,b} : \mathbb{R} \to \mathbb{R}$ pela regra $f_{a,b} : r \mapsto ar+b$. Seja $G = \{f_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$. Mostre que G munido da composição de funções é um grupo e que $h : G \to \mathbb{R}^*$, $h : f_{a,b} \mapsto a$, é um homomorfismo. Descreva o núcleo de h. É G comutativo?

35*. Mostre que a interseção de dois subgrupos de índice finito é um subgrupo de índice finito. (Dica: se $H, S \leqslant G$ com $|G : H|, |G : S| < \infty$, então $|H : H \cap S| \leqslant |G : S|$.)

36*. Seja G um grupo e H um subgrupo em G de índice finito, $H \leqslant G$, $|G : H| < \infty$. Mostre que G possui um subgrupo normal N de índice finito tal que $N \subset H$.

37*. Sejam $H, S \leqslant G$. Mostre que $|HS| \cdot |H \cap S| = |H| \cdot |S|$. Aplique este fato a um grupo G de ordem pq, onde p e q são primos tais que $p > q$. Mostre que existe no máximo um subgrupo de G de ordem p.

38. Qual é a paridade de um ciclo de comprimento k ?

39. Seja σ uma permutação cuja decomposição em produto de ciclos disjuntos consiste nos ciclos de comprimentos $k_1, k_2, \ldots, k_r$. Qual é a ordem (= período) de σ ?

40*. Sejam $\sigma, \theta \in \Sigma_n$ permutações cujas decomposições em produto de ciclos disjuntos consistem nos ciclos de comprimentos $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_r$ e $l_1 \leqslant l_2 \leqslant \cdots \leqslant l_s$, respectivamente. Quando σ e θ são conjugados em Σ_n ?

41. Sejam A_1 e A_2 dois grupos abelianos. Mostre que $\operatorname{Hom}(A_1, A_2)$, munido da operação definida pela regra $(h_1 + h_2)a_1 := h_1 a_1 + h_2 a_1$, $a_1 \in A_1$, é um grupo abeliano. Sejam A_1, A_2, A_3 grupos abelianos. Verifique que a composição $\circ : \operatorname{Hom}(A_2, A_3) \times \operatorname{Hom}(A_1, A_2) \to \operatorname{Hom}(A_1, A_3)$ é aditiva em todo argumento, isto é, $(h_2 + h_2') \circ h_1 = h_2 \circ h_1 + h_2' \circ h_1$ e $h_2 \circ (h_1 + h_1') = h_2 \circ h_1 + h_2 \circ h_1'$ para todos $h_1, h_1' \in \operatorname{Hom}(A_1, A_2)$ e $h_2, h_2' \in \operatorname{Hom}(A_2, A_3)$.

42. Seja A um grupo abeliano. Mostre que a fórmula $H_1 \cap (H_2 + H_3) = H_1 \cap H_2 + H_1 \cap H_3$ é válida para quaisquer subgrupos $H_1, H_2, H_3 \leqslant A$ tais que dois dentre H_1, H_2, H_3 são incluídos um em outro?

43. Seja A um grupo abeliano finitamente gerado sem torção. Será que a fórmula $H_1 \cap (H_2 + H_3) = H_1 \cap H_2 + H_1 \cap H_3$ é válida para quaisquer subgrupos $H_1, H_2, H_3 \leqslant A$? (Considere também o caso particular de $H_2 \cap H_3 = 0$.)

44. Seja G um grupo abeliano finito. Suponhamos que mdc $\big(|G|, n\big) = 1$. Mostre que $g \mapsto g^n$ é um automorfismo de G.

45*. Seja A um grupo abeliano finitamente gerado tal que todo endomorfismo não-nulo de A é um automorfismo. Mostre que A é cíclico.

46*. Indique um grupo abeliano não-cíclico A tal que todo endomorfismo não-nulo de A é um automorfismo.

47*. Sejam A_1 e A_2 grupos cíclicos. Mostre que o grupo abeliano $A := \mathrm{Hom}(A_1, A_2)$ é cíclico. Calcule $|A|$ a partir de $|A_1|$ e $|A_2|$.

48*. Indique grupos abelianos finitos A_1 e A_2 tais que $\mathrm{Hom}(A_1, A_2) = 0$ e $\mathrm{Hom}(A_2, A_1) \neq 0$ ou mostre que esta situação é impossível.

49*. Indique grupos abelianos finitamente gerados A_1 e A_2 tais que $\mathrm{Hom}(A_1, A_2) = 0$ e $\mathrm{Hom}(A_2, A_1) \neq 0$ ou mostre que esta situação é impossível.

50. Quantos (a menos de isomorfismo) grupos abelianos de ordem 216 existem?

51*. Seja A um grupo finito abeliano tal que $p(A) = |A|$, onde $p(A)$ denota o período de A, isto é, o número mínimo $0 < p \in \mathbb{N}$ tal que $pa = 0$ para todo $a \in A$. Mostre que A é cíclico.

52*. Sejam A_1 e A_2 grupos finitos abelianos, sejam $p_1, \ldots, p_k \in \mathbb{N}$ primos distintos por pares e sejam $l_1, \ldots, l_k \in \mathbb{N}$, $l_1, \ldots, l_k > 0$. Façamos $n := p_1^{l_1} \cdot \ldots \cdot p_k^{l_k}$ e $m := p_1 \cdot \ldots \cdot p_k$. Suponhamos que $|A_1| = |A_2| = n$ e $p(A_1) = p(A_2) = m$. (Onde $p(A)$ denota o período do grupo A, isto é, o número mínimo $0 < p \in \mathbb{N}$ tal que $pa = 0$ para todo $a \in A$.) Mostre que os grupos A_1 e A_2 são isomorfos.

53*. Seja A um grupo abeliano finito que tem exatamente 2 automorfismos. Quantos elementos pode ter A ?

54. É o conjunto $\mathbb{N}[i] := \{a + bi \mid a, b \in \mathbb{N}\}$ munido das operações usuais (induzidas pelas operações $+$ e $\cdot$ em $\mathbb{C}$) um corpo? um domínio euclidiano? um domínio? um anel? Por que?

55. Mostre que qualquer ideal não-nulo no anel dos inteiros de Gauss $\mathbb{Z}[i]$ contém um número natural positivo.

56. Seja A um anel comutativo. Mostre que o conjunto formado por todos elementos nilpotentes é um ideal de A. (Um elemento $a \in A$ se chama *nilpotente* se $a^n = 0$ para algum $n > 0$.)

57. Descreva da maneira mais simples possível o corpo de frações para o domínio $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

58. Verifique que o conjunto $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ munido das operações usuais e da função $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{N}$, $\varphi : a + b\sqrt{2} \mapsto |a^2 - 2b^2|$, é um domínio euclidiano.

59. Seja K um corpo. Definimos

$$I := \big\{f \in K[x, y] \mid \text{todo monômio de } f \text{ com o coeficiente não-nulo é divisível ou por } x^2 \text{ ou por } y^3\big\}.$$

É I um ideal principal de $K[x, y]$? um ideal de $K[x, y]$? um anel? Por que?

60. Quantos elementos inversíveis tem o anel $\mathbb{Z}/9^{999}\mathbb{Z}$?

61. Será que $1 + 5i$ e $5 - i$ são associados em $\mathbb{Z}[i]$?

62. Seja D um domínio e sejam $a, b, c \in D$. Complete a frase (usando os conceitos de divisibilidade, tais como: "divide", "divisor", "múltiplo", "divisor comum", "maior divisor comum", "múltiplo comum", "menor múltiplo comum", "elemento inversível", "elementos associados", "elemento irredutível") e mostre a afirmação obtida:

- $Da = D$ se e só se ...
- $Da \subset Db$ se e só se ...
- $Da = Db$ se e só se ...

- $Da + Db \subset Dc$ se e só se ...
- $Da + Db = Dc$ se e só se ...
- $Da \cap Db \supset Dc$ se e só se ...
- $Da \cap Db = Dc$ se e só se ...
- Seja $a \neq 0$. O ideal Da é primo em D se e só se ...

63. O conjunto $\mathbb{Z}[i\sqrt{7}] = \{a + bi\sqrt{7} \mid a, b \in \mathbb{Z}\}$ munido das operações usuais é um domínio e existe uma função norma multiplicativa $N : \mathbb{Z}[i\sqrt{7}] \to \mathbb{N}$, $N : a \mapsto a \cdot \overline{a}$. Por exemplo, para $a = 3 + i\sqrt{7}$, temos $Na = a \cdot \overline{a} = (3 + i\sqrt{7})(3 - i\sqrt{7}) = 16$. Procure todos os elementos inversíveis com respeito à multiplicação no anel $\mathbb{Z}[i\sqrt{7}]$. É $\mathbb{Z}[i\sqrt{7}]$ um domínio fatorial?

64. Dados um domínio D arbitrário e um elemento não-inversível $0 \neq a \in D$. Mostre que $\mathrm{mdc}(a, x) = 1$ em $D[x]$. Mostre que não existem $f, g \in D[x]$ tais que $af + xg = 1$. Pode $D[x]$ ser um domínio principal?

65. Será que todo domínio de fatoração única é principal?

66. Ache o maior divisor comum de $3 + 2i, 2 - i \in \mathbb{Z}[i]$.

67. Ache o maior divisor comum dos polinômios $13x^3 + (3 - 2i)x, (2 + 3i)x^2 - 13 \in \mathbb{Z}[i][x]$.

68. É o polinômio $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ irredutível em $\mathbb{Z}[x]$?

69. Seja $f \in \mathbb{Z}[x]$ um polinômio mônico e seja $n > 0$. Considerando f como polinômio sobre o anel $\mathbb{Z}/n\mathbb{Z}$, obtemos o polinômio $\overline{f} \in (\mathbb{Z}/n\mathbb{Z})[x]$. Mostre que f é irredutível em $\mathbb{Z}[x]$ caso $\overline{f}$ seja irredutível em $(\mathbb{Z}/n\mathbb{Z})[x]$.

70. Sejam $p_1, \ldots, p_m \in \mathbb{N}$ números primos distintos por pares, $m > 0$. Mostre que $\sqrt[n]{p_1 \ldots p_m} \notin \mathbb{Q}$ para $n > 1$.

71. Ache a decomposição de $(x^5 + 1)/(x^3 - 1)$ em frações parciais sobre $\mathbb{Q}$.

72. Seja K um corpo. Mostre que o polinômio $x^3 + x^2 + x + 1$ não é irredutível em $K[x]$.

73. Procure o polinômio de menor grau em uma variável sobre $\mathbb{R}$ que tem valores 3, 2, 1 para $x = 1, 2, 3$.

74. Sejam K um corpo, $f \in K[x]$ e $a \in K$. Mostre que $(x - a)^2$ divide f se, e só se, $f(a) = f'(a) = 0$.

75. Determine a multiplicidade da raiz $x = 1$ no polinômio $x^{2015} - x^{2011} - 4x + 4 \in \mathbb{Q}[x]$.

76. Indique um polinômio não-nulo em uma variável sobre um anel que tem um número infinito de raízes.

77. Indique um polinômio não-nulo em uma variável sobre um anel A que tem um número infinito de raízes e ao mesmo tempo A satisfaz a propriedade seguinte: $a^2 = 0 \Rightarrow a = 0$ para todo $a \in A$.

78. Seja K um corpo finito de característica p. Mostre que $\Phi : x \mapsto x^p$ é um automorfismo de K.

79. Seja K um corpo finito de característica p. Calcule a ordem do automorfismo de Frobenius de K em termos de $|K|$.

80. Seja K um corpo finito de característica p e seja $F \subset K$ um subcorpo. Sejam $|F| = p^m$ e $|K| = p^n$. Mostre que m divide n.

81. Encontre um corpo K e polinômios distintos $f, g \in K[x]$ tais que f e g são iguais como funções $K \to K$.

82. Seja $A = \mathbb{Z}/17\mathbb{Z}$ e seja $f := x^{289} + \overline{5} \in A[x]$. Quantas raízes em A tem o polinômio f ?

83. Seja D um domínio tal que $d^5 = d$ para todo $d \in D$. Quantos elementos pode ter D ?

84*. Escreva uma expressão $f(a, b)$ tal que $f(a, b) = 0$ se e só se o polinômio $x^3 + ax + b \in \mathbb{C}[x]$ tem pelo menos duas raízes iguais.

85*. Seja $f_0 := 0$, $f_1 := 1$ e $f_{n+2} = f_{n+1} + f_n$ para $n \in \mathbb{N}$. Encontre uma fórmula explícita para f_n.

86*. Seja $f := x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$ um polinômio sobre um corpo K. Mostre que o discriminante $\operatorname{discr} f \in K[a_1, \ldots, a_n]$ é um polinômio irredutível.

87*. Sejam $c_1, \ldots, c_n \in \mathbb{C}$. Mostre que o sistema $\begin{cases} x_1 + \cdots + x_n = c_1 \\ x_1^2 + \cdots + x_n^2 = c_2 \\ \quad\vdots \\ x_1^n + \cdots + x_n^n = c_n \end{cases}$ admite uma solução em números complexos e mostre que essa solução é única a menos de permutação de $x_1, \ldots, x_n$.

Um presente de gregos antigos

88. É 2001 a soma de dois quadrados de números naturais? É $3 \cdot 23 \cdot 2001$ a soma de dois quadrados de números naturais?

89. Sejam $a := \sqrt[3]{7} \in \mathbb{R}$ e $b := -\sqrt[3]{7} \cdot (\frac{1}{2} + \frac{\sqrt{3}}{2}i) \in \mathbb{C}$. Mostre que $\mathbb{Q}[a]$ e $\mathbb{Q}[b]$ são isomorfos.

90. Seja $a := \cos\frac{2\pi}{7} + i \cdot \operatorname{sen}\frac{2\pi}{7} \in \mathbb{C}$. Calcule o grau da extensão $\mathbb{Q} \subset \mathbb{Q}[a]$.

91. Calcule o grau da extensão $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}][i]$.

92. É o ângulo de $7°$ construtível? É o ângulo de $18°$ construtível?

93. Sejam $a := \cos\frac{2\pi}{7} + i \cdot \operatorname{sen}\frac{2\pi}{7} \in \mathbb{C}$ e $b := \cos\frac{2\pi}{5} + i \cdot \operatorname{sen}\frac{2\pi}{5} \in \mathbb{C}$. Pode ser válida uma igualdade do tipo $b = f(a)$, onde $f \in \mathbb{Q}[x]$?

94. Seja $\mathbb{Q} \subset K$ uma extensão de corpos de grau 15, onde $K \subset \mathbb{C}$. Mostre que $\sqrt{2} \notin K$.

95. Usando o fato que o pentágono é construtível, mostre que o polígono regular de 60 lados é construtível. (Dica: $1/15 = 2/5 - 1/3$.)

96. Seja $K \subset L$ uma extensão de corpos de grau 2, onde $L \subset \mathbb{C}$. Mostre que $L = K[\sqrt{a}]$ para algum $a \in K$ apropriado.

97. Procure todos os $n > 0$ tais que o número $\sqrt[n]{2}$ é construtível.