Miscelânea algébrica
by ET

1 Grupos

1. Mostre que $GL_2(\mathbb{F}_2) \cong S_3$.

2. Determine a cardinalidade da órbita da matriz $\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}$ na ação por conjugação em $GL_2(\mathbb{F}_5)$.

3. Seja $\mathbb{F}_q$ um corpo finito com q elementos. Mostre que

$$|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1})$$

e que

$$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{q-1}$$

4. Mostre que $SL_2(\mathbb{F}_3)$ e S_4 possuem mesmas ordens, mas não são isomorfos. Dica: considere $\begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{2} \end{pmatrix} \in SL_2(\mathbb{F}_3)$.

5. Seja p um primo. Na ação $GL_n(\mathbb{F}_p) \curvearrowright \mathbb{F}_p^n$, determine a ordem do estabilizador de um vetor não nulo.

6. Seja k um corpo e considere a ação $PGL_2(k) \curvearrowright \mathbb{P}^1_k$.

(a) Determine $\mathrm{Stab}(\infty)$ em que $\infty = (0:1) \in \mathbb{P}^1_k$.

(b) Mostre que se $T \in PGL_2(k)$ fixa os pontos $(1:0)$, $(1:1)$ e $(0:1)$ então T é a identidade.

(c) Mostre que, dados quaisquer três pontos distintos $P, Q, R \in \mathbb{P}^1_k$, existe uma única $T \in PGL_2(k)$ tal que $T(P) = (1:0)$, $T(Q) = (1:1)$ e $T(R) = (0:1)$.

7. Determine os seguintes quocientes (ou seja, encontre explicitamente grupos conhecidos que são isomorfos a estes quocientes):

(a) $\mathbb{C}^\times/\mathbb{R}_{>0}$

(b) $\mathbb{R}^\times \times \mathbb{R}^\times/\langle(1,-1)\rangle$

(c) $S^1/\{\pm 1, \pm i\}$

(d) $\mathbb{C}^\times/\{\pm 1, \pm i\}$

8. Prove: todo subgrupo finitamente gerado de $(\mathbb{Q}, +)$ é cíclico.

9. Seja G um grupo. Se $g \in G$ é um elemento de ordem ímpar, mostre que g e g^2 têm mesma ordem.

10. Seja G um grupo de ordem par. Mostre que existe um elemento $a \neq e$ tal que $a^2 = e$.

11. Prove: se um grupo G possui um único elemento a de ordem 2, então $a \in Z(G)$ (aqui $Z(G)$ denota o centro de G).

12. Seja G um grupo em que a intersecção de todos os subgrupos distintos de $\{e\}$ é um subgrupo distinto de $\{e\}$. Prove que todo elemento de G tem ordem finita.

13. Seja G um grupo abeliano finito.

(a) Suponha que $a, b \in G$ têm ordens m e n respectivamente. Mostre que a e b geram um subgrupo de ordem $\mathrm{mmc}(m, n)$.

(b) Seja $g \in G$ um elemento de ordem máxima n. Mostre que a ordem de qualquer elemento em G divide n.

14. Se $a > 1$ é um inteiro, prove que $n \mid \varphi(a^n - 1)$ para todo n inteiro positivo, em que φ é a função de Euler.

15. Sejam M e N subgrupos normais de G com $M \cap N = \{e\}$. Prove que $mn = nm$ para quaisquer $m \in M$, $n \in N$.

16. Mostre que se G é um grupo contendo dois subgrupos normais de ordens 3 e 5 então G possui um elemento de ordem 15.

17. Seja A qualquer conjunto com mais de 2 elementos. Dado $a \in A$, considere o subgrupo $H(a) = \{\sigma \in S_A \mid \sigma(a) = a\}$ do grupo simétrico S_A de A. Prove que $H(a)$ não pode ser normal em S_A.

18. Seja $Z(G)$ o centro do grupo G.

(a) Se existe $H \leqslant Z(G)$ tal que G/H é cíclico, então G é abeliano.

(b) Dê um exemplo de grupo G tal que $G/Z(G)$ é abeliano mas G não é abeliano.

19. Sejam G e H grupos finitos com $\mathrm{mdc}(|G|, |H|) = 1$ e seja $\phi\colon G \to H$ um morfismo de grupos. Mostre que ϕ é trivial.

20. Seja G um grupo finito e $N \trianglelefteq G$ um subgrupo normal. Mostre que se $\mathrm{mdc}(|\operatorname{Aut}(N)|, |G|) = 1$ então $N \leqslant Z(G)$.

21. Seja G um grupo finito.

(a) Se $|G|$ é ímpar e $N \trianglelefteq G$ com $|N| = 5$, então $N \leqslant Z(G)$.

(b) Seja p o menor primo que divide $|G|$ e seja $N \trianglelefteq G$ com $|N| = p$. Prove que $N \leqslant Z(G)$.

22. Mostre que se $\operatorname{Aut}(G)$ é cíclico então G é abeliano.

23. Seja G um grupo de ordem ímpar. Prove: se $g, g^{-1} \in G$ são conjugados entre si, então $g = e$.

24. Seja G um grupo finito e seja H um subgrupo. Mostre que existe um conjunto S de elementos de G que é, simultaneamente, um conjunto de representantes de classe tanto à direita quanto à esquerda.
Warning: este é um problema de grafos, não de álgebra! Vide teorema dos casamentos de Hall para grafos bipartidos.

25. Seja G um grupo e seja p o menor primo que divide $|G|$. Suponha que H seja um subgrupo de G com $[G : H] = p$. Mostre que $H \trianglelefteq G$.

26. (Teorema do Ponto Fixo para p-grupos) Seja p um primo e seja P um p-grupo. Seja $P \curvearrowright X$ uma ação de P sobre um conjunto finito X. Sendo

$$X^P \stackrel{\text{def}}{=} \{x \in X \mid gx = x \text{ para todo } g \in P\}$$

o conjunto dos pontos fixos desta ação, prove:

$$|X^P| \equiv |X| \pmod{p}$$

Em particular, se $p \nmid |X|$ então existe pelo menos um ponto $x \in X$ fixo por todo $g \in P$.

27. (Teorema de Cauchy) Seja p um primo e seja G um grupo abeliano finito. Mostre que se $p \mid |G|$ então G possui um elemento de ordem p. Para isto, seja $X = \{(a_1, a_2, \ldots, a_p) \in G^p \mid a_1 a_2 \ldots a_p = e\}$ e considere a ação de $\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ dada por shifts circulares à esquerda (i.e., $\overline{1}$ leva a tupla $(a_1, a_2, \ldots, a_p)$ em $(a_2, a_3, \ldots, a_p, a_1)$). Aplique o teorema do ponto fixo para p-grupos.

28. (Putnam) Seja p um primo e suponha que um grupo finito tenha exatamente n elementos de ordem p. Mostre que $n = 0$ ou $n + 1$ é um múltiplo de p.

29. Seja p um primo e seja G um p-grupo. Seja $H \trianglelefteq G$. Mostre que se H é não trivial, o mesmo ocorre com $H \cap Z(G)$.

30. Seja p primo e seja H um p-subgrupo do grupo finito G. Mostre que

$$[N(H) : H] \equiv [G : H] \pmod{p}$$

em que $N(H)$ denota o normalizador de H em G.

31. Seja $G \leqslant S_n$ um subgrupo transitivo. Mostre: $|G| \equiv 0 \pmod{n}$.

32. Seja G um grupo finito e seja $G \curvearrowright S$ uma ação transitiva com $|S| \geqslant 2$. Mostre que existe $g \in G$ sem pontos fixos.

33. Seja X um conjunto qualquer e seja $G \leqslant S_X$. Suponha que G seja abeliano e que G aja transitivamente sobre X. Mostre que $\mathrm{Stab}(x)$ é trivial para todo $x \in X$.

34. Seja $N \in \mathbb{N}_{>0}$ e seja

$$\Gamma(N) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{array}{rl} a, d \equiv 1 & \pmod N, \\ b, c \equiv 0 & \pmod N \end{array} \right\}$$

o subgrupo de $SL_2(\mathbb{Z})$ formado pelas matrizes "congruentes a identidade" módulo N. Sejam ainda

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{array}{rl} a, d \equiv 1 & \pmod N, \\ c \equiv 0 & \pmod N \end{array} \right\}$$

os subgrupos $SL_2(\mathbb{Z})$ formado pelas matrizes "triangulares superiores e unipotentes" módulo N.

(a) Mostre que $\Gamma(N)$, $\Gamma_0(N)$ e $\Gamma_1(N)$ possuem índice finito em $SL_2(\mathbb{Z})$.

(b) Mostre que $\Gamma_1(N) \lhd \Gamma_0(N)$ e que $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

(c) Sejam $A_1, \ldots, A_r$ representantes das classes laterais à direita de $\Gamma_0(N)$ em $SL_2(\mathbb{Z})$. Se $D \subseteq \mathbb{H}$ é um domínio fundamental para a ação $SL_2(\mathbb{Z}) \curvearrowright \mathbb{H}$ por transformações de Möbius, mostre que

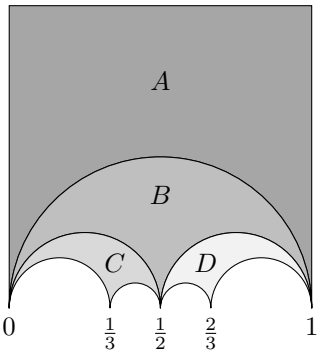
$$D' = A_1 \cdot D \cup A_2 \cdot D \cup \cdots \cup A_r \cdot D$$

é um domínio fundamental para a ação $\Gamma_0(N) \curvearrowright \mathbb{H}$.

35. Seja $\Gamma_0(N)$ como no exercício anterior. Temos que $\Gamma_0(N)$, como subgrupo de $SL_2(\mathbb{R})$, age sobre o semiplano de Poincaré $\mathbb{H}$ via transformações de Möbius.

(a) Mostre que $\Gamma_0(11)$ possui índice 12 em $SL_2(\mathbb{Z})$.

(b) Mostre que, na figura a seguir, cada uma das regiões A, B, C, D são a união de três domínios fundamentais para $SL_2(\mathbb{Z})$.

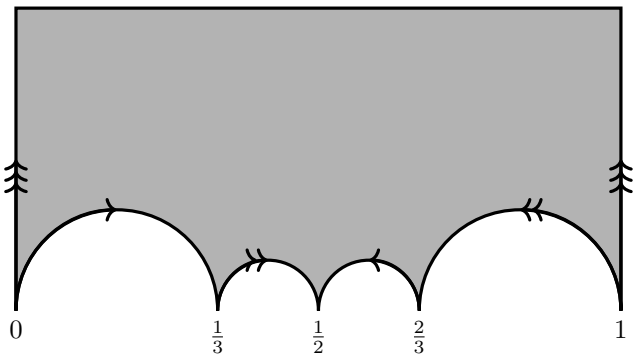


(c) Mostre que a região $A \cup B \cup C \cup D$ contém um domínio fundamental para a ação $\Gamma_0(11) \curvearrowright \mathbb{H}$.

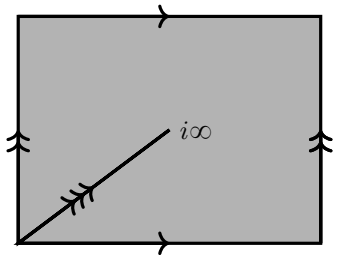
(d) Considere os seguintes elementos de $\Gamma_0(11)$:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad U = \begin{pmatrix} 7 & -2 \\ 11 & -3 \end{pmatrix} \qquad V = \begin{pmatrix} 8 & -3 \\ 11 & -4 \end{pmatrix}$$

Mostre que T é uma translação por 1 para a direita e, na figura a seguir, U leva o interior da circunferência de diâmetro dado pelo intervalo real $[0, \frac{1}{3}]$ no exterior da circunferência de diâmetro $[\frac{1}{2}, \frac{2}{3}]$, enquanto V leva o interior da circunferência de diâmetro $[\frac{1}{3}, \frac{1}{2}]$ no exterior da de diâmetro $[\frac{2}{3}, 1]$, com as orientações indicadas nas fronteiras.



Interprete geometricamente o quociente de $\mathbb{H}$ pela ação de $\Gamma_0(11)$ como um toro menos um ponto $i\infty$:



(e) Mostre que $\Gamma_0(11)$ é gerado pelas matrizes T, U, V.

36. Sejam $f\colon A \to B$ e $g\colon B \to C$ dois morfismos de grupos abelianos. Mostre que existe uma sequência exata

$$0 \longrightarrow \ker(f) \longrightarrow \ker(g \circ f) \xrightarrow{f} \ker(g) \longrightarrow \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(g \circ f) \longrightarrow \operatorname{coker}(g) \longrightarrow 0$$

37. (Lema da Serpente) Considere o seguinte diagrama comutativo de grupos abelianos, em que as linhas são sequências exatas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

(a) Mostre que existe um morfismo de grupos $\delta\colon \ker h \to \operatorname{coker} f$ definido da seguinte forma: dado $c \in \ker h$, escolha qualquer $b \in B$ tal que $b \mapsto c$; então $g(b) \in B'$ é a imagem de um único elemento $a' \in A'$ e definimos $\delta(c) = a'$.

(b) Mostre que temos uma sequência exata

$$0 \longrightarrow \ker f \longrightarrow \ker g \longrightarrow \ker h \xrightarrow{\delta} \operatorname{coker} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h \longrightarrow 0$$

38. Seja $n \geqslant 5$.

(a) Seja $A_n \curvearrowright X$ uma ação de A_n sobre um conjunto finito X com $|X| < n$. Mostre que esta ação é trivial.

(b) Seja $H < A_n$. Prove: $[A_n : H] \geqslant n$.

39. Seja G um grupo. Um subgrupo $H \leqslant G$ é dito **característico** em G se $\varphi(H) \leqslant H$ para qualquer $\varphi \in \operatorname{Aut}(G)$. Mostre que:

(a) se H é característico em G então $H \trianglelefteq G$.

(b) se $K \trianglelefteq G$ e se H é característico em K então $H \trianglelefteq G$.

(c) se $K \trianglelefteq G$ e $\operatorname{mdc}(|K|, |G/K|) = 1$ então K é característico em G.

(d) se $P \trianglelefteq G$ é o único p-Sylow de G (p primo) então P é característico em G.

40. Neste exercício, apresentamos uma outra demonstração dos dois primeiros teoremas de Sylow. Seja p um primo.

(a) Prove: todo grupo finito G é isomorfo a um subgrupo de $GL_n(\mathbb{Z}/p\mathbb{Z})$ para algum $n \geqslant 1$. Dica: utilize o teorema de Cayley e matrizes de permutação.

(b) Seja G um grupo cuja ordem é um múltiplo de p e suponha que G possua um p-Sylow P. Seja $K \leqslant G$ um subgrupo qualquer cuja ordem é um múltiplo de p. Mostre que existe um conjugado gPg^{-1} ($g \in G$) de P tal que $gPg^{-1} \cap K$ é um p-Sylow de K. Para isto, considere a ação de translação à esquerda $K \curvearrowright G/P$ de K sobre o conjunto das classes laterais à esquerda de P; mostre que $\operatorname{Stab}(gP) = gPg^{-1} \cap K$ e conclua que $gPg^{-1} \cap K$ é um p-Sylow de K para algum $g \in G$.

(c) Utilizando os itens anteriores, mostre que se $|G|$ é divisível por p então G possui um p-Sylow.

(d) Utilizando o item (b), mostre que qualquer p-subgrupo de G está contido em algum p-Sylow e que todos os p-Sylows são conjugados entre si.

41. (Complexidade) Seja G um grupo finito. Mostre:

(a) se $|G| = pq$ com p, q primos, então G é solúvel.

(b) se $p < q < r$ são números primos e $|G| = pqr$ então G não é simples. Mostre ainda que G é solúvel.

(c) se $|G| = p^e a$ com p primo e $1 \leqslant a < p$, então G não é simples.

(d) se $|G| = p^2 q$ com p, q primos, então G não é simples.

(e) se H é um subgrupo próprio de G tal que $|G| > r!$, em que $r = [G : H]$, então G não é simples. Dica: considere a ação de translação à esquerda $G \curvearrowright G/H$ de G sobre o conjunto das classes laterais à esquerda de H, que define um morfismo de grupos $\phi\colon G \to S_r$.

(f) Mostre que, com exceção dos grupos de ordem prima, todo grupo de ordem estritamente menor do que 60 não é simples. Mostre que todo grupo de ordem estritamente menor do que 60 é solúvel. Dentre estes, quais são necessariamente nilpotentes?

42. Determine o número de p-Sylows em $GL_3(\mathbb{F}_p)$.

43. Mostre:

(a) não existem grupos simples com as seguintes ordens:

$12 = 2^2 \cdot 3$	$30 = 2 \cdot 3 \cdot 5$	$56 = 2^3 \cdot 7$
$80 = 2^4 \cdot 5$	$105 = 3 \cdot 5 \cdot 7$	$132 = 2^2 \cdot 3 \cdot 11$
$306 = 2 \cdot 3^2 \cdot 17$	$351 = 3^3 \cdot 13$	$380 = 2^2 \cdot 5 \cdot 19$
$495 = 3^2 \cdot 5 \cdot 11$	$616 = 2^3 \cdot 7 \cdot 11$	$858 = 2 \cdot 3 \cdot 11 \cdot 13$
$870 = 2 \cdot 3 \cdot 5 \cdot 29$	$992 = 2^5 \cdot 31$	$1365 = 3 \cdot 5 \cdot 7 \cdot 13$
$1722 = 2 \cdot 3 \cdot 7 \cdot 41$	$3875 = 5^3 \cdot 31$	$5103 = 3^6 \cdot 7$
$8883 = 3^3 \cdot 7 \cdot 47$		

(b) não existem grupos simples com as seguintes ordens:

$24 = 2^3 \cdot 3$	$36 = 2^2 \cdot 3^2$	$48 = 2^4 \cdot 3$
$96 = 2^5 \cdot 3$	$108 = 2^2 \cdot 3^3$	$160 = 2^5 \cdot 5$
$192 = 2^6 \cdot 3$	$320 = 2^6 \cdot 5$	$324 = 2^2 \cdot 3^4$
$384 = 2^7 \cdot 3$	$520 = 2^3 \cdot 5 \cdot 13$	$640 = 2^7 \cdot 5$
$648 = 2^3 \cdot 3^4$	$750 = 2 \cdot 3 \cdot 5^3$	$768 = 2^8 \cdot 3$
$972 = 2^2 \cdot 3^5$	$1280 = 2^8 \cdot 5$	$1536 = 2^9 \cdot 3$
$2560 = 2^9 \cdot 5$	$2862 = 2 \cdot 3^3 \cdot 53$	$8505 = 3^5 \cdot 5 \cdot 7$

(c) não existem grupos simples com as seguintes ordens:

$72 = 2^3 \cdot 3^2$	$150 = 2 \cdot 3 \cdot 5^2$	$216 = 2^3 \cdot 3^3$
$270 = 2 \cdot 3^3 \cdot 5$	$300 = 2^2 \cdot 3 \cdot 5^2$	$392 = 2^3 \cdot 7^2$
$450 = 2 \cdot 3^2 \cdot 5^2$	$600 = 2^3 \cdot 3 \cdot 5^2$	$784 = 2^4 \cdot 7^2$
$945 = 3^3 \cdot 5 \cdot 7$	$2835 = 3^4 \cdot 5 \cdot 7$	$3159 = 3^5 \cdot 13$
$3393 = 3^2 \cdot 13 \cdot 29$	$4125 = 3 \cdot 5^3 \cdot 11$	$5145 = 3 \cdot 5 \cdot 7^3$
$9477 = 3^6 \cdot 13$		

44. Seja G um grupo de ordem n.

(a) Mostre que se $n = p \cdot q$ com $p < q$ primos e $q \not\equiv 1 \pmod{p}$ então G é cíclico.

(b) Mostre que se n é um dos números a seguir, então G é abeliano.

1	2	3	4	5	7	9	11	13
15	17	19	23	25	29	31	33	35
37	41	43	45	47	49	51	53	59
61	65	67	69	71	73	77	79	83
85	87	89	91	95	97	99	101	103
107	109	113	115	119	121	123	127	131
133	137	139	141	143	145	149	151	153
157	159	161	163	167	169	173	175	177
179	181	185	187	191	193	197	199	

(c) Para quais valores de n do item anterior G é necessariamente cíclico?

(d) Prove: dados dois primos p e q tais que $q \mid p-1$, prove que existe um grupo G não abeliano de ordem pq.

45.

(a) Quantos elementos de ordem 5 há em um grupo de ordem 20?

(b) Mostre que nenhum grupo de ordem 224 é simples.

46. Seja G um grupo simples de ordem 168. Quantos elementos de ordem 7 há em G?

47. Seja G um grupo abeliano tal que $|G| \equiv 2 \pmod{4}$. Mostre que existe um **único** elemento de ordem 2 em G.

48. Seja P um p-Sylow de G. Mostre: se $H \geqslant N(P)$ então $[G:H] \equiv 1 \pmod{p}$.

49. Seja P um p-Sylow de G. Prove: se $H \trianglelefteqslant G$ e $P \trianglelefteqslant H$ então $P \trianglelefteqslant G$.

50. Seja G um grupo e seja $\sigma \in \mathrm{Aut}(G)$ um automorfismo de ordem 2 cujo único ponto fixo é $e \in G$.

(a) Mostre que a seguinte função é injetora:

$$\begin{aligned} G &\hookrightarrow G \\ x &\mapsto \sigma(x) \cdot x^{-1} \end{aligned}$$

(b) Se G é finito, mostre que $\sigma(x) = x^{-1}$ para todo $x \in G$. Conclua que G é abeliano.

2 Polinômios

51. Sejam $a_1, \ldots, a_n$ inteiros distintos. Prove: $(x-a_1)^2 (x-a_2)^2 \cdot \ldots \cdot (x-a_n)^2 + 1$ é irredutível em $\mathbb{Z}[x]$.

52. Mostre que o polinômio $(x^2+x)^{2^n}+1$ é irredutível em $\mathbb{Q}[x]$ para todo inteiro positivo n. Dica: analisando módulo 2, mostre que possíveis fatores deste polinômio são da forma $(x^2+x+1)^k + 2p(x)$ para algum $p(x) \in \mathbb{Z}[x]$. Agora substitua $x = \omega$.

53. Mostre que o polinômio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Q}$ se a_0 é um número primo e $|a_0| > |a_1| + |a_2| + \cdots + |a_n|$.

54. Dados polinômios $f_1(x), f_2(x), \ldots, f_n(x) \in \mathbb{Z}[x]$, mostre que existe um polinômio $g(x)$ redutível em $\mathbb{Z}[x]$ tal que $g(x) + f_i(x)$ é irredutível em $\mathbb{Z}[x]$ para todo $1 \leqslant i \leqslant n$.

55. (OBM) Prove que o polinômio $f(x) = x^5 - x^4 - 4x^3 + 4x^2 + 2$ não admite raízes da forma $\sqrt[n]{r}$ com $r \in \mathbb{Q}$ e $n \in \mathbb{N}$, $n > 1$.

56. Seja $f(n)$ o número de coeficientes ímpares de $(x^2+x+1)^n$. Mostre que, para todo $m \in \mathbb{N}$, $f(2^m) = 3$ e

$$f(2^m - 1) = \frac{2^{m+2} + (-1)^{m+1}}{3}$$

57. Seja $f(x) \in K[x]$ um polinômio irredutível de grau p primo e sejam $\theta_1, \ldots, \theta_p$ as raízes de $f(x)$. Suponha que $\theta_2 \in K(\theta_1)$. Mostre que $K(\theta_1)$ é o corpo de raízes de $f(x)$.

58. Sejam $M(x)$ e $N(x)$ polinômios mônicos e irredutíveis em $\mathbb{Q}[x]$. Suponha que $M(x)$ e $N(x)$ tenham raízes α e β, respectivamente, tais que $\alpha + \beta \in \mathbb{Q}$. Prove que $M(x)^2 - N(x)^2$ possui uma raiz racional.

59. Seja $f(x) \in \mathbb{Q}[x]$ e seja $\alpha \in \mathbb{R}$ tal que $\alpha^3 - 1992\alpha = (f(\alpha))^3 - 1992 \cdot f(\alpha) = -33$. Prove que, para todo $n \geqslant 1$,

$$\left(f^{(n)}(\alpha)\right)^3 - 1992 \cdot f^{(n)}(\alpha) = -33,$$

em que $f^{(n)}(\alpha) = \underbrace{f(f(\ldots f}_{n \text{ vezes}}(\alpha)))$ e n é um inteiro positivo.

60. Mostre que o polinômio $x^4 + \overline{1}$ é redutível sobre $\mathbb{F}_p$ para todo primo p.

61. (Último Teorema de Fermat—versão baby) Seja $n \in \mathbb{N}_{>0}$ com $n \geqslant 3$. Mostre que não existem polinômios $a(x), b(x), c(x) \in \mathbb{C}[x]$, todos não constantes, tais que

$$\big(a(x)\big)^n + \big(b(x)\big)^n = \big(c(x)\big)^n$$

Dica: fatore o lado esquerdo como $\prod_{0 \leqslant j < n} (a(x) + \zeta^j b(x))$ em que $\zeta = e^{2\pi i/n}$.

62. Sejam p um primo p e $f(x) \in \mathbb{F}_p[x]$ um polinômio irredutível de grau n. Seja $r \in \mathbb{F}_p^{\mathrm{alg}}$ uma raiz de $f(x)$. Mostre que as raízes de $f(x)$ são precisamente $r, r^p, r^{p^2}, \ldots, r^{p^n} = r$.

63. Seja p um primo. Mostre que há $\binom{p}{2}$ polinômios mônicos irredutíveis de grau 2 em $\mathbb{F}_p[x]$ e que o produto destes polinômios é

$$(x^p - x)^{p-1} + \overline{1}$$

64. Seja $\alpha = \zeta + \zeta^3 + \zeta^9$ em que $\zeta = e^{2\pi i/13}$. Seja $f(x) = x^4 + x^3 + 2x^2 - 4x + 3$.

(a) Mostre que $f(x)$ é o polinômio minimal de α sobre $\mathbb{Q}$.

(b) Se $f(x)$ possui raiz em $\mathbb{F}_p$, p primo, então $p \equiv 0, 1, 3, 9 \pmod{13}$.

65. Sejam p um primo e $f(x) \in \mathbb{F}_p[x]$ um polinômio separável. Mostre que existe um $n \in \mathbb{N}$ tal que $f(x) \mid x^{p^n} - x$.

66. Seja q uma potência de primo. Defina a **função zeta** como

$$Z(t) = \frac{1}{1-t} \prod_f \frac{1}{1-t^{\deg f}}$$

em que f percorre o conjunto dos polinômios mônicos irredutíveis em $\mathbb{F}_q$. Prove que $Z(t)$ é uma função racional (i.e., $Z(t) \in \mathbb{Q}(t) = \operatorname{Frac} \mathbb{Q}[t]$) e determine-a explicitamente.

67. Seja k um corpo. Dado $f(x) \in k[x]$, mostre que existe um múltiplo $g(x)$ de $f(x)$ tal que todos os expoentes dos monômios não nulos de $g(x)$ são primos. Por exemplo, se $f(x) = x^4 + 20x - 2$ em $\mathbb{Q}[x]$, então podemos tomar $g(x) = x^{11} - 4x^7 - 400x^5 + 4x^3$.

3 Anéis e Corpos

68. Seja $L \supseteq K$ uma extensão algébrica de corpos. Suponha que A seja um anel tal que $L \supseteq A \supseteq K$ (como subanel de L). Mostre que A é um corpo.

69. Seja R um domínio que é uma $\mathbb{C}$-álgebra de dimensão finita (i.e., R tem dimensão finita como $\mathbb{C}$-espaço vetorial). Mostre que $R = \mathbb{C}$.

70. Mostre que o anel $K = \mathbb{F}_3[x]/(x^3 + \overline{2}x + \overline{1})$ é um corpo com 3^3 elementos e que $\overline{x} \in K$ é um gerador do grupo cíclico $K^\times$. Mostre ainda que $L = \mathbb{F}_3[x]/(x^3 + \overline{2}x + \overline{2})$ também é um corpo com 3^3 elementos e portanto isomorfo a K. Escreva explicitamente este isomorfismo. Verifique que $\overline{x} \in K$ não gera $L^\times$ e encontre um gerador deste grupo.

71. Mostre:

(a) $\mathbb{Z}[i]/(a+bi) \cong \mathbb{F}_p$ em que p é um primo da forma $4k+1$ ou $p = 2$ e $a^2 + b^2 = p$, $a, b \in \mathbb{Z}$.

(b) $\mathbb{Z}[i]/(p)$ é uma extensão de grau 2 de $\mathbb{F}_p$ se p é um primo da forma $4k+3$.

72. Em $\mathbb{Z}[i]$, mostre que

(a) $\alpha^9 - \alpha$ é múltiplo de 3 para todo $\alpha \in \mathbb{Z}[i]$.

(b) $\alpha^5 - \alpha$ é múltiplo de $2+i$ para todo $\alpha \in \mathbb{Z}[i]$.

Você consegue generalizar os resultados acima?

73. Sejam $a_1, \ldots, a_n \in \mathbb{N}$ e $\alpha = \sqrt{a_1} + \cdots + \sqrt{a_n}$. Se $\alpha \notin \mathbb{Z}$, mostre que α é irracional.

74. Seja $\omega = e^{2\pi i/3}$ e considere o corpo $K = \mathbb{Q}[\omega \sqrt[3]{2}]$. Prove: a equação $x^2 + y^2 = -1$ não tem solução com $x, y \in K$.

75. Seja q uma potência de um primo p. Determine os autovalores e autovetores do automorfismo de Frobenius $\Phi\colon \mathbb{F}_q \xrightarrow{\approx} \mathbb{F}_q$, visto como aplicação $\mathbb{F}_p$-linear.

76. Seja $\mathbb{F}_q$ um corpo finito e sejam $a, b \in \mathbb{F}_q^\times$. Mostre que

(a) qualquer elemento em $\mathbb{F}_q$ é soma de dois quadrados perfeitos em $\mathbb{F}_q$.

(b) existem $x, y \in \mathbb{F}_q$ tais que $ax^2 + by^2 = -1$.

77. Seja q uma potência de primo. Em $\mathbb{F}_q$, mostre que

(a) (Teorema de Wilson) $\prod_{a \in \mathbb{F}_q^\times} a = -1$

(b) $\sum_{a \in \mathbb{F}_q} a^n = \begin{cases} -1 & \text{se } q-1 \mid n \\ 0 & \text{caso contrário} \end{cases}$

78. (Miklós-Schweitzer) Seja $p > 3$ um primo satisfazendo $p \equiv 3 \pmod 4$. Prove:

$$\prod_{1 \leqslant x \neq y \leqslant (p-1)/2} (x^2 + y^2) \equiv 1 \pmod p$$

79. Seja $K \supseteq \mathbb{Q}$ uma extensão de corpos de grau 15. Prove que $\sqrt{2} \notin K$.

80. Sejam $\alpha = e^{2\pi i/17}$ e $\beta = e^{2\pi i/23}$. É possível que $\beta = f(\alpha)$ para algum $f(x) \in \mathbb{Q}[x]$?

81. Seja $K = \mathbb{Q}(\alpha)$ onde α é raiz de $x^3 + 2x + 1$. O polinômio $x^3 + x + 1$ possui raiz em K?

82. Seja p um número primo e seja $\alpha = \sqrt[p]{2}$. Seja $g(x) \in \mathbb{Q}[x]$ um polinômio com $\deg g(x) < p$. Mostre que $\alpha \in \mathbb{Q}(g(\alpha))$. Por outro lado, mostre que existe um polinômio $g(x) \in \mathbb{Q}[x]$ com $\deg g(x) < 4$ tal que $\sqrt[4]{2} \notin \mathbb{Q}(g(\sqrt[4]{2}))$.

83. Seja $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$. Mostre que se $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é ímpar, então $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$.

84. Seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível de grau n e seja $L \supset \mathbb{Q}$ uma extensão de grau m onde $\operatorname{mdc}(m, n) = 1$. Prove que $p(x)$ também é irredutível em $L[x]$. Conclua que $x^3 - 2$ e $x^3 - 3$ são irredutíveis sobre $\mathbb{Q}(i)$.

85. Seja $f(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau n e seja $g(x) \in \mathbb{Q}[x]$ um polinômio qualquer. Mostre que todo fator irredutível de $f(g(x))$ tem grau divisível por n.

86. Seja $B \supseteq A$ uma extensão de anéis comutativos. Um elemento $\beta \in B$ é dito **integral** sobre A se β é raiz de um polinômio **mônico** $f(x) \in A[x]$.

(a) Mostre que se A e B são corpos, então $\beta \in B$ é integral sobre A se, e só se, β é algébrico sobre A.

(b) Mostre que $\beta \in B$ é integral sobre A se, e só se, o subanel $A[\beta] \subseteq B$ é um A-módulo finitamente gerado.

87. Seja $L \supseteq K$ uma extensão de corpos e suponha que K seja **algebricamente fechado** em L, ou seja, se $\beta \in L$ é algébrico sobre K então $\beta \in K$. Mostre que se $f(x) \in K[x]$ é um polinômio irredutível em $K[x]$, então $f(x)$ é irredutível também em $L[x]$.

88. Mostre que $\mathbb{C}[x, y, z, w]/(xw - yz)$ é domínio, mas não um DFU.

89. Prove que o anel quociente

$$\frac{\mathbb{C}[x, y]}{(x^2 + y^2 - 1)}$$

é um DFU.

90. Seja $A = \{f\colon [0,1] \to \mathbb{R} \mid f \text{ é contínua}\}$ o anel de funções contínuas e seja $P \in [0,1]$. Defina

$$I_P = \{f \in A \mid f(P) = 0\}$$

(a) Mostre que I_P é um ideal maximal de A.

(b) Descreva $A^\times$.

(c) Mostre que todo ideal maximal $\mathfrak{m}$ de A é da forma I_P para algum P. Para isto, suponha por contradição que para cada ponto $P \in [0,1]$, existe uma função $g_P \in \mathfrak{m}$ tal que $g_P(P) \neq 0$. Usando compacidade, exiba uma função em $\mathfrak{m}$ que não se anula em todo $[0,1]$.

91.

(a) Determine o kernel dos seguintes morfismos:

$$\alpha\colon \mathbb{Z}[x] \to \mathbb{R} \qquad \beta\colon \mathbb{C}[x,y] \to \mathbb{C}[t]$$
$$f(x) \mapsto f(1+\sqrt{2}) \qquad f(x,y) \mapsto f(t^2,t^3)$$

$$\gamma\colon \mathbb{C}[x,y] \to \mathbb{C}[t]$$
$$f(x,y) \mapsto f(t^2-t, t^3-t^2)$$

(b) Mostre que $\operatorname{im}\beta$ é o conjunto dos polinômios $p(t)$ tais que $p'(0) = 0$.

(c) Mostre que $\operatorname{im}\gamma$ é o conjunto dos polinômios $p(t)$ tais que $p(0) = p(1)$. Dê uma interpretação geométrica.

92. Mostre que o morfismo de anéis

$$\frac{\mathbb{C}[x,y]}{(xy, x^2+y^2-1)} \xrightarrow{\approx} \mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}$$
$$\overline{f(x,y)} \mapsto \big(f(1,0); f(0,1); f(-1,0); f(0;-1)\big)$$

é um isomorfismo. Interprete geometricamente em termos de funções polinomiais de curvas no plano.

93. Para qualquer quatérnion $q \in \mathbb{H}$, denote por $\overline{q}$ o seu conjugado.

(a) Um **quatérnion puro** u é um quatérnion tal que $u = -\overline{u}$, i.e., um quatérnion com parte real 0: $u = x\mathbf{i}+y\mathbf{j}+z\mathbf{k}$ para $x,y,z \in \mathbb{R}$. Sejam u e v dois quatérnions puros. Mostre que

$$uv = u\times v - u\cdot v, \quad u\times v = \frac{uv-vu}{2} \quad u\cdot v = -\frac{uv+vu}{2}$$

em que $u \times v$ denota o produto vetorial e $u \cdot v \in \mathbb{R}$, o produto escalar de u e v (interpretados como vetores em $\mathbb{R}^3$).

(b) Mostre que, para qualquer $q \in \mathbb{H}^\times$, se v é um quatérnion puro então qvq^{-1} também é um quatérnion puro. Interpretando v como um vetor em $\mathbb{R}^3$, mostre que a conjugação $v \mapsto qvq^{-1}$ é uma transformação $\mathbb{R}$-linear que preserva ângulos, comprimentos e orientação, logo pertence a $SO_3(\mathbb{R})$.

(c) Mostre que $SU_2(\mathbb{C}) = \mathbb{H}^\times \cap SL_2(\mathbb{C})$ e que todo $q \in SU_2(\mathbb{C})$ se escreve como $q = \cos(\frac{\theta}{2}) + \operatorname{sen}(\frac{\theta}{2})u$ com u um quatérnion puro de norma 1. Usando $u = (q-\overline{q})/2$, mostre que $quq^{-1} = u$. Portanto, se v é um quatérnion puro, $v \mapsto qvq^{-1}$ é uma rotação em $\mathbb{R}^3$ em torno da reta determinada por u.

(d) Mostre que o ângulo da rotação $v \mapsto qvq^{-1}$ do item anterior é θ. Dica: sendo e um quatérnion puro de norma 1 que é perpendicular a u (como vetor no $\mathbb{R}^3$), basta calcular o produto vetorial $e \times qeq^{-1}$; utilize $e^2 = u^2 = -1$.

(e) Mostre que o mapa $\phi\colon SU_2(\mathbb{C}) \to SO_3(\mathbb{R})$ que leva $q \in SU_2(\mathbb{C})$ na rotação $v \mapsto qvq^{-1}$ é um morfismo de grupos com kernel ± 1. Interpretando $SU_2(\mathbb{C})$ como S^3 (a esfera real de dimensão 3), conclua que $SO_3(\mathbb{R})$ é homeomorfo a $\mathbb{P}^3_{\mathbb{R}}$ (com a topologia quociente de $\mathbb{R}^4$).

4 Espaços vetoriais

Nos exercícios a seguir, a menos de menção contrária, k denota um corpo, V e W denotam k-espaços vetoriais.

94. Para $d \in \mathbb{N}$, seja $k[x_1,\dots,x_n]_d$ o conjunto de todos os polinômios $f(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$ que são homogêneos de grau d, juntamente com 0 (um polinômio é dito **homogêneo** se é uma combinação linear de monômios de mesmo grau; por exemplo, $x^2-3xy+y^2$ é homogêneo de grau 2, mas x^3+2xy não é homogêneo). Sejam $f(x), g(x) \in k[z]$ dois polinômios de graus m, n, respectivamente. Mostre que

$$T\colon k[x,y]_{\leqslant d} \to k[x]_{\leqslant (m+n)d}$$
$$p(x,y) \mapsto p(f(z),g(z))$$

é uma transformação linear. Mostre que T não é injetora para d suficientemente grande e conclua que existe um polinômio não nulo $p(x,y) \in k[x,y]$ tal que $p(f(z),g(z)) = 0$

95. Seja X um conjunto qualquer e seja

$$V = \{f\colon X \to k \mid f \text{ é função}\}$$

o conjunto de todas as funções de X para k.

(a) Verifique que V é um k-espaço vetorial e que $\dim_k V = |X|$ se X é finito.

(b) Se $x_1,\dots,x_n \in X$ e $f_1,\dots,f_n \in V$ são tais que $f_i(x_i) \neq 0$ para $i = 1,\dots,n$ e $f_i(x_j) = 0$ se $i \neq j$, então $f_1,\dots,f_n$ são linearmente independentes sobre k.

(c) Se $\pi\colon X \to X$ é uma função qualquer, verifique que o mapa

$$T_\pi\colon V \to V$$
$$f \mapsto f\circ\pi$$

é uma transformação linear de V em V. Encontre os autovalores e autovetores correspondentes de T_π no caso em que $k = \mathbb{C}$, $X = \{1,2,3\}$ e $\pi\colon X \to X$ é a permutação circular $\pi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

96. Seja $n \geqslant 2$ um inteiro. Mostre que qualquer base do espaço vetorial $M_n(k)$ deve conter duas matrizes A e B tais que $AB \neq BA$.

97. Considere os seguintes vetores em $\mathbb{R}^n$:

$$\begin{aligned} v_1 &= (a_{11}, a_{12}, \ldots, a_{1n}) \\ v_2 &= (a_{21}, a_{22}, \ldots, a_{2n}) \\ &\vdots \\ v_n &= (a_{n1}, a_{n2}, \ldots, a_{nn}) \end{aligned}$$

Suponha que $a_{ii} > 0$, $a_{ij} < 0$ para $i \neq j$ e que $\sum_{1 \leqslant k \leqslant n} a_{ik} > 0$ para todo $1 \leqslant i, j \leqslant n$ (i.e., a matriz $(a_{ij})_{1 \leqslant i,j \leqslant n}$ tem diagonal e soma das linhas positivas e entradas fora da diagonal negativas). Mostre que os vetores $v_1, \ldots, v_n$ são linearmente independentes sobre $\mathbb{R}$.

98. Sejam V e W dois $\mathbb{F}_q$-espaços vetoriais com $\dim_{\mathbb{F}_q} V = m$ e $\dim_{\mathbb{F}_q} W = n$. Determine

(a) $|V|$ e $|V^\vee|$

(b) a quantidade de subespaços de dimensão 1 em V

(c) a quantidade de subespaços de dimensão d em V

(d) $|\operatorname{Hom}_{\mathbb{F}_q}(V, W)|$

(e) a quantidade de isomorfismos $T\colon V \xrightarrow{\approx} V$

99. Mostre que

(a) $\mathbb{R}$, quando visto como um espaço vetorial sobre $\mathbb{Q}$, não possui dimensão finita.

(b) o conjunto

$$\{\ln(p) \in \mathbb{R} \mid p \in \mathbb{N} \text{ é primo}\}$$

é linearmente independente sobre $\mathbb{Q}$.

(c) existe no máximo um número primo p para o qual $\ln(p)$ é racional.

100. Suponha que $\dim_k V < \infty$ e seja $T\colon V \to V$ uma transformação linear. Prove: existe $n_0 \in \mathbb{N}$ tal que, para todo $n \geqslant n_0$,

$$\ker T^n = \ker T^{n+1} \qquad \text{e} \qquad \operatorname{im} T^n = \operatorname{im} T^{n+1}$$

101. (Dedekind) Seja G um grupo. Seja

$$V = \{f\colon G \to k \mid f \text{ é função}\}$$

o k-espaço vetorial de todas as funções de G em k. Sejam $f_1, \ldots, f_n\colon G \to k^\times$ morfismos de grupos, dois a dois distintos. Mostre que $f_1, \ldots, f_n\colon G \to k^\times$, vistos como elementos de V, são k-linearmente independentes (Dica: utilize indução sobre n.)

102. Seja k um corpo.

(a) Mostre que um polinômio $f(x) \in k[x]$ de grau n possui no máximo n raízes em k.

(b) Mostre que $f(x) = x^2 - \overline{1} \in \mathbb{Z}/8\mathbb{Z}[x]$ possui 4 raízes no anel $\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{7}\}$ (inteiros módulo 8).

(c) Se k é infinito e $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ é um polinômio não nulo, mostre existe $(a_1, \ldots, a_n) \in k^n$ tal que $f(a_1, \ldots, a_n) \neq 0$ (Dica: indução em n).

(d) Seja p um número primo. Encontre $f(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ não nulo tal que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$ (Dica: pelo pequeno teorema de Fermat, então $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$).

103. Sejam k um corpo e V um k-espaço vetorial com $\dim_k V < \infty$.

(a) Se $W \subsetneq V$ é um k-subespaço vetorial próprio de V (i.e., $W \neq V$), mostre que existe $\ell \in V^\vee$ não nulo tal que $\ell(w) = 0$ para todo $w \in W$.

(b) Mostre que se k é infinito então V não é uma união de uma quantidade finita de subespaços vetoriais de dimensão estritamente menor do que $\dim_k V$. Por exemplo, para $k = \mathbb{R}$ e $V = \mathbb{R}^2$, temos que $\mathbb{R}^2$ não pode ser escrito como uma união finita de retas passando pela origem (Dica: use o item (a) juntamente com o exercício anterior).

(c) Por outro lado, mostre que se $k = \mathbb{F}_q$ e $\dim_{\mathbb{F}_q} V \geqslant 2$, então V é uma união finita de subespaços de dimensão 1 (faça um desenho para $k = \mathbb{F}_5$ e $V = \mathbb{F}_5^2$ ilustrando este fato).

104. Seja V um k-espaço vetorial de dimensão finita.

(a) Mostre que

$$\begin{aligned} \phi\colon \operatorname{Hom}_k(V, V) &\to \operatorname{Hom}_k(V^*, V^*) \\ T &\mapsto T^t \end{aligned}$$

é um isomorfismo. Aqui, T^t denota a **transposta** de T, isto é, o mapa induzido por composição com T:

$$\begin{aligned} T^t\colon V^* &\to V^* \\ \ell &\mapsto \ell \circ T \end{aligned}$$

(b) Dada uma base $\mathcal{B}$ de V e a base dual correspondente $\mathcal{B}^*$, considere os isomorfismos de anéis $\tau_{\mathcal{B}}\colon \operatorname{Hom}_k(V, V) \xrightarrow{\approx} M_n(k)$ e $\tau_{\mathcal{B}^*}\colon \operatorname{Hom}_k(V^*, V^*) \xrightarrow{\approx} M_n(k)$. Descreva ϕ explicitamente em termos de matrizes, i.e., descreva $\tau_{\mathcal{B}^*} \circ \phi \circ \tau_{\mathcal{B}}^{-1}\colon M_n(k) \to M_n(k)$.

105. Seja $P(\mathbb{R})$ o espaço vetorial de todos os polinômios com coeficientes reais. Para números reais a e b fixos, seja $f\colon P(\mathbb{R}) \to \mathbb{R}$ o funcional linear

$$f(p(x)) = \int_a^b p(t)\, dt.$$

Se $D\colon P(\mathbb{R}) \to P(\mathbb{R})$ é o operador de derivação, o que é $D^t(f)$? (D^t denota a transposta de D).

106. No espaço $V = \mathbb{R}[x]_{\leqslant 2}$ (já vimos esta notação antes!), defina os seguintes funcionais lineares:

$$f_1(p(x)) = \int_0^1 p(t)\, dt, \quad f_2(p(x)) = \int_0^2 p(t)\, dt,$$

$$f_3(p(x)) = \int_0^{-1} p(t)\, dt.$$

Mostre que $B = \{f_1, f_2, f_3\}$ é uma base de V^* e exiba uma base de V da qual B é a base dual.

107. Sejam $r \geqslant n$ dois inteiros positivos, k um corpo infinito e V um k-espaço vetorial com $\dim_k V = n$.

(a) Prove: existe um conjunto $S \subseteq V$ com $|S| = r$ vetores com a propriedade de que qualquer subconjunto de S com n vetores é linearmente independente.

(b) Dado $m \in \mathbb{N}$, seja $s = \binom{m}{2} \cdot (n-1) + 1$. Prove: existe um conjunto de s funcionais lineares $\ell_1, \ldots, \ell_s \in V^\vee$ com a seguinte propriedade: para qualquer subconjunto $T \subset V$ com $|T| = m$, existe i com $1 \leqslant i \leqslant s$ tal que $|\ell_i(T)| = m$ (ou seja, pelo menos um dos $\ell_i \in V^\vee$ acima "separa" os pontos de T).

Cuidado: note que da maneira como o problema foi formulado, a escolha dos funcionais **não** pode depender de T! (Dica: pelo item (a), podemos escolher s funcionais de modo que quaisquer n deles são k-linearmente independentes.)

108. (Característica de Euler) Seja k um corpo.

(a) Dada uma sequência exata de k-espaços vetoriais

$$0 \to V_n \to V_{n-1} \to \cdots \to V_1 \to V_0 \to 0$$

mostre que

$$\dim_k V_0 - \dim_k V_1 + \dim_k V_2 - \cdots + (-1)^n \dim_k V_n = 0$$

(b) Considere a sequência de transformações k-lineares

$$0 \longrightarrow V_n \xrightarrow{f_n} \cdots \longrightarrow V_1 \xrightarrow{f_1} V_0 \xrightarrow{f_0} 0$$

satisfazendo $\operatorname{im} f_i \subseteq \ker f_{i-1}$ para todo i (dizempos que esta sequência é um **complexo** de k-espaços vetoriais). Definimos o seu **i-ésimo grupo de homologia** como sendo o k-espaço vetorial

$$h_i(V_\bullet, f_\bullet) \stackrel{\text{def}}{=} \frac{\ker f_i}{\operatorname{im} f_{i+1}}$$

Mostre que

$$\begin{aligned}\chi(V_\bullet, f_\bullet) &\stackrel{\text{def}}{=} \sum_{0 \leqslant i \leqslant n} (-1)^i \dim_k h_i(V_\bullet, f_\bullet) \\ &= \sum_{0 \leqslant i \leqslant n} (-1)^i \dim_k V_i\end{aligned}$$

Esta soma alternada $\chi(V_\bullet, f_\bullet)$ é a chamada **característica de Euler** do complexo; a igualdade acima é a justificativa algébrica de a fórmula $v - a + f$ (em que v, a, f denotam respectivamente o número de vértices, aresta e faces) para um poliedro concordar com a soma alternada dos números de Betti na homologia simplicial, veja por exemplo Hatcher, theorem 2.44, p.146.

109. Dado $A \in \operatorname{Hom}_k(V, V)$, defina o elemento $\tau_A \in \operatorname{Hom}_k(V, V)^\vee$ dado por

$$\begin{aligned}\tau_A \colon \operatorname{Hom}_k(V, V) &\to k \\ T &\mapsto \operatorname{Tr}(A \circ T)\end{aligned}$$

Mostre que

$$\begin{aligned}\operatorname{Hom}_k(V, V) &\xrightarrow{\approx} \operatorname{Hom}_k(V, V)^\vee \\ A &\mapsto \tau_A\end{aligned}$$

é um isomorfismo de k-espaços vetoriais.

110. Prove os seguintes isomorfismos canônicos:

(a) $\operatorname{Hom}_k(k, V) = V$

(b) $k \otimes V = V$

(c) $\operatorname{Hom}_k(V, \prod_{i \in I} W_i) = \prod_{i \in I} \operatorname{Hom}_k(V, W_i)$

(d) $\operatorname{Hom}_k(\bigoplus_{i \in I} V_i, W) = \prod_{i \in I} \operatorname{Hom}_k(V_i, W)$

(e) $V \otimes W = W \otimes V$

(f) $\left(\bigoplus_{i \in I} V_i\right) \otimes W = \bigoplus_{i \in I} (V_i \otimes W)$

(g) $\operatorname{Hom}_k(U, V) \otimes W = \operatorname{Hom}_k(U, V \otimes W)$

(h) $\operatorname{Hom}_k(V, W) = V^\vee \otimes W$

(i) $(V \otimes W)^\vee = V^\vee \otimes W^\vee$

(j) $\operatorname{Hom}_k(V/U, W) = \{T \in \operatorname{Hom}_k(V, W) \mid T(U) = 0\}$

(k) $\operatorname{Hom}_k(U \otimes V, W) = \operatorname{Hom}_k(U, \operatorname{Hom}_k(V, W))$

111. Sejam $v_1, \ldots, v_r$ e $w_1, \ldots, w_r$ dois conjuntos de vetores LI (em algum espaço vetorial V). Mostre que estes conjuntos geram o mesmo subespaço se, e só se, $v_1 \wedge \ldots \wedge v_r = \lambda \cdot w_1 \wedge \ldots \wedge w_r$ para algum $\lambda \in k^\times$.

112. Seja R um anel comutativo e seja F um R-módulo livre de posto finito. Mostre que o mapa

$$\begin{aligned}\delta \colon F^r \times (F^\vee) &\to R \\ (\mathbf{v}, \hat{\mathbf{w}}) &\mapsto \det(\hat{w}_i(v_j))\end{aligned}$$

é R-multilinear e alternado, logo define um mapa $\delta \colon \bigwedge^r F \times \bigwedge^r (F^\vee) \to R$, que por sua vez induz um isomorfismo

$$\left(\bigwedge^r F\right)^\vee = \bigwedge^r (F^\vee)$$

113. Seja $A \in M_n(k)$ e seja $\ell_A \in M_n(k)^\vee$ o funcional linear dado por $X \mapsto \operatorname{Tr}(AX)$. Mostre que $A \mapsto \ell_A$ é um isomorfismo entre $M_n(k)$ e $M_n(k)^\vee$.

114. Se U é um subespaço de V, prove que existe um subespaço W de V tal que $V = U \oplus W$.

115. Se U_1 e U_2 são subespaços de dimensão finita do espaço V, prove que

$$\dim_k(U_1 + U_2) = \dim_k(U_1) + \dim_k(U_2) - \dim_k(U_1 \cap U_2).$$

116. Seja V um espaço vetorial de dimensão finita sobre o corpo infinito k. Se U_1 e U_2 são subespaços de V tais que $\dim_k U_1 = \dim_k U_2$, prove que existe um subespaço W de V tal que $V = U_1 \oplus W = U_2 \oplus W$.

117. Seja V um espaço de dimensão finita e $T \colon V \to V$ uma transformação linear. Se $T \circ T = 0$, prove que $2 \dim_k \operatorname{im}(T) \leqslant \dim_k V$.

118. Se $N \in M_3(\mathbb{C})$ é uma matriz nilpotente, prove que $A = I + \frac{1}{2}N - \frac{1}{8}N^2$ satisfaz $A^2 = I + N$, isto é, A é uma raiz quadrada de $I + N$. Use a expansão em série da função $f(z) = (1+z)^{1/2}$ para obter uma fórmula similar para a raiz quadrada de $I + N$ quando N é uma matriz nilpotente de ordem n.

119. Inspirado(a) pelo exercício anterior, mostre que a matriz $\lambda I + N$ possui uma raiz quadrada quando $N \in M_n(\mathbb{C})$ é nilpotente e $\lambda \neq 0$. Então use a forma canônica de Jordan para mostrar que toda matriz complexa inversível possui uma raiz quadrada.

120. Seja $n \geqslant 2$ um inteiro positivo e seja $N \in M_n(\mathbb{R})$ uma matriz tal que $N^n = 0$ mas $N^{n-1} \neq 0$. Prove que N não possui raiz quadrada, isto é, que não existe uma matriz $A \in M_n(\mathbb{R})$ tal que $A^2 = N$.

121. Seja $A \in M_n(\mathbb{C})$ tal que para todo inteiro $k \geqslant 1$ temos $\mathrm{Tr}(A^k) = 0$. Prove que A é nilpotente.

5 Matrizes e Determinantes

122. Seja θ um número real. Mostre que as matrizes

$$\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

são semelhantes sobre o corpo $\mathbb{C}$ dos números complexos.

123. (Matriz de Vandermonde) Mostre que o determinante da matriz

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$$

é igual a

$$\prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

124. Dizemos que um conjunto de pontos $X \subseteq k^n$ está em **posição geral** se não existe um subconjunto $S = \{v_1, \ldots, v_{n+1}\} \subseteq X$ de $n+1$ pontos em X contidos em um hiperplano de k^n (i.e., se $v_2 - v_1, v_3 - v_1, \ldots, v_{n+1} - v_1$ são linearmente independentes sobre k). Mostre que os pontos da "curva" $X = \{(t, t^2, \ldots, t^n) \in k^n \mid t \in k\}$ estão em posição geral.

125. Dado $n \in \mathbb{N}$, seja $\omega = e^{2\pi i/n} \in \mathbb{C}$, uma raiz n-ésima da unidade. Considere a matriz em $M_n(\mathbb{C})$

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ & \vdots & & & \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$$

em que cada linha é um "shift circular" da linha anterior. Considere a transformação linear $T\colon \mathbb{C}^n \to \mathbb{C}^n$ dada por A na base standard.

(a) Mostre que os vetores $v_j = (1, \omega^j, \omega^{2j}, \ldots, \omega^{(n-1)j}) \in \mathbb{C}^n$ são autovetores de T para $j = 0, 1, \ldots, n-1$.

(b) Prove:

$$\det A = \prod_{0 \leqslant j \leqslant n-1} (a_1 + a_2\omega^j + a_3\omega^{2j} + \cdots + a_n\omega^{(n-1)j})$$

126. Se M é uma matriz quadrada de números complexos, mostre que o traço de M é a soma dos autovalores de M (cada um contado com sua multiplicidade algébrica).

127. Se $\lambda_1, \ldots, \lambda_n$ são números reais não nulos, mostre que o determinante da matriz

$$\begin{pmatrix} 1+\lambda_1 & 1 & \cdots & 1 \\ 1 & 1+\lambda_2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1+\lambda_n \end{pmatrix}$$

é igual a $(\lambda_1\lambda_2\cdots\lambda_n)\left(1 + \frac{1}{\lambda_1} + \cdots + \frac{1}{\lambda_n}\right)$.

128. Se $A \in M_n(\mathbb{R})$ é uma matriz anti-simétrica (isto é, $A^t = -A$) e n é ímpar, prove que $\det(A) = 0$.

129. Seja $A \in M_n(\mathbb{Z})$ uma matriz cujas entradas são todas iguais a 1 ou -1. Prove que $\det(A)$ é divisível por 2^{n-1}.

130. Ana e Beto jogam o seguinte jogo: no início, existe uma matriz quadrada de ordem n vazia. Alternadamente, Ana e Beto escrevem números reais em cada uma das n^2 posições da matriz, sendo que Ana começa o jogo. Ao final, o determinante da matriz obtida é calculado. Se o determinante for diferente de zero, Ana vence. Se o determinante for igual a zero, o vencedor é Beto.

(a) Se n é par, mostre que Beto possui uma estratégia vencedora.

(b) (jogo da velha nível hard) Se $n = 3$, qual jogador possui a estratégia vencedora?

131. Seja F_n o n-ésimo número de Fibonacci, isto é, $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$ para $n \geqslant 0$.

(a) Determine uma transformação linear $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ tal que $T(F_{n-1}, F_n) = (F_n, F_{n+1})$ para todo $n \geqslant 1$.

(b) Seja A a matriz de T na base canônica de $\mathbb{R}^2$. Determine $P \in M_2(\mathbb{R})$ inversível tal que $P^{-1}AP$ seja uma matriz diagonal.

(c) Calcule A^n para todo $n \geqslant 0$ e deduza que

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

para todo $n \geqslant 0$.

6 Polinômios minimal e característico

132. Encontre o polinômio característico da multiplicação por $\sqrt{2} + \sqrt{3}$ em $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

133. Seja N uma matriz quadrada de ordem 2 sobre os complexos. Se $N^2 = 0$, prove que $N = 0$ ou que N é semelhante sobre $\mathbb{C}$ à matriz

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

134. Sejam $S \in \mathrm{Hom}_k(V,V)$ e $T \in \mathrm{Hom}_k(W,W)$ com polinômios característicos $p(x), q(x) \in k[x]$, respectivamente. Mostre que

(a) o polinômio característico de $S \oplus T \in \mathrm{Hom}_k(V \oplus W, V \oplus W)$ é dado por $p(x) \cdot q(x)$.

(b) o polinômio característico de $S \otimes T \in \mathrm{Hom}_k(V \otimes W, V \otimes W)$ é igual a $\prod_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} (x - \alpha_i \beta_j)$ em que α_i e β_j denotam as raízes de $p(x)$ e $q(x)$ (listadas com multiplicidade).

135. (OBM) Definimos $SL(2,\mathbb{Z})$ como o conjunto das matrizes 2×2 com coeficientes inteiros e determinante 1. Seja $A \in SL(2,\mathbb{Z})$ uma matriz tal que existe $n > 0$ inteiro com $A^n = I$. Prove que existe $X \in SL(2,\mathbb{Z})$ tal que $X^{-1}AX$ é igual a uma das matrizes:

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

136. Considere o seguinte diagrama comutativo com linhas exatas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V_1 & \longrightarrow & V_2 & \longrightarrow & V_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle T_1} & & \downarrow{\scriptstyle T_2} & & \downarrow{\scriptstyle T_3} & & \\ 0 & \longrightarrow & V_1 & \longrightarrow & V_2 & \longrightarrow & V_3 & \longrightarrow & 0 \end{array}$$

(a) Determine o polinômio característico de T_2 em função dos polinômios característicos de T_1 e T_3.

(b) Mostre que $\operatorname{Tr} T_2^r = \operatorname{Tr} T_1^r + \operatorname{Tr} T_3^r$ para todo $r \in \mathbb{N}$.

137. Seja $A \in M_n(\mathbb{Z})$ e seja $\lambda \in \mathbb{Q}$ um autovalor de A. Mostre que $\lambda \in \mathbb{Z}$.

138. Seja $A \in M_n(\mathbb{C})$. Mostre que as matrizes A e A^t são conjugadas.

139. Seja $A \in M_n(k)$. Verifique a seguinte identidade no anel de séries formais $M_n(k)[\![t]\!]$:

$$\frac{1}{\det(I_n - A \cdot t)} = \exp\left(\sum_{n \geqslant 1} \operatorname{Tr}(A^n) \cdot \frac{t^n}{n} \right)$$

140. Se $\dim_K(V) = n$ e $T \in \mathrm{Hom}_k(V,V)$ possui n autovalores distintos, prove que T é diagonalizável.

141. Seja $T \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^2, \mathbb{C}^2)$ um operador com apenas um autovalor e tal que $T^k = \mathrm{id}_{\mathbb{C}^2}$ para algum natural $k \neq 0$. Mostre que T é diagonalizável.

142. Se um operador T sobre um espaço de dimensão finita satisfaz $T^2 = T$, prove que T é diagonalizável.

143. Sejam $A, B \in M_n(k)$ tais que $AB = BA$. Prove: se A é diagonalizável, o mesmo vale para B.

144. Seja $S \subseteq \mathrm{Hom}_k(V,V)$ um conjunto de transformações lineares tais que $AB = BA$ para quaisquer $A, B \in S$. Prove que existe uma base de k^n que diagonaliza todo $A \in S$ simultaneamente.

7 Espaços com produto interno

145. Seja $A \in M_n(\mathbb{C})$. Mostre:

(a) Existe $U \in U_n(\mathbb{C})$ tal que UAU^{-1} é triangular superior.

(b) Se, além disso, $AA^* = A^*A$ então existe $U \in U_n(\mathbb{C})$ tal que UAU^{-1} é diagonal.

146. (Berlekamp) Em Oddtown, existem n pessoas e m clubes $C_1, \ldots, C_m$. Esses clubes satisfazem:

1. $|C_i|$ é ímpar para qualquer i.
2. $|C_i \cap C_j|$ é par para quaisquer $i \neq j$.

Mostre que $m \leqslant n$.

147. (Berkelamp) Em Eventown, existem n pessoas e uma família F de m clubes. Esses clubes satisfazem:

1. $|C|$ é par para qualquer $C \in F$.
2. $|C \cap D|$ é par para quaisquer $C, D \in F$.

Prove que

(a) A família F tem $m \leqslant 2^{\lfloor n/2 \rfloor}$ clubes.

(b) Se a família F tem menos de $2^{\lfloor n/2 \rfloor}$ clubes, então existe um clube C que pode ser adicionado à família sem violar as regras de Eventown.

148. Seja $V = M_n(\mathbb{C})$, com produto interno dado por $\langle A, B \rangle = \operatorname{Tr}(AB^*)$. Determine o complemento ortogonal do subespaço das matrizes diagonais.

149. Seja V o espaço vetorial real das funções reais contínuas definidas no intervalo $[-1,1]$, com produto interno

$$\langle f, g \rangle = \int_{-1}^{1} f(t) g(t)\, dt.$$

Seja W o subespaço das funções ímpares, isto é, funções que satisfazem $f(-t) = -f(t)$ para todo $t \in [-1,1]$. Determine o complemento ortogonal de W.

150. Seja W um subespaço de V, um espaço de dimensão finita com produto interno, e seja E a projeção ortogonal de V sobre W. Prove que $\langle E(u), v \rangle = \langle u, E(v) \rangle$ para todos u, $v \in V$.

151. Em um espaço vetorial V com produto interno e dimensão finita, mostre que a composição de dois operadores autoadjuntos é autoadjunto se, e somente se, estes operadores comutam.

152. Seja V um espaço com produto interno e dimensão finita. Se dois operadores normais comutam, prove que sua composição também é um operador normal.

153. Prove que um operador normal em um espaço vetorial complexo (com produto interno e de dimensão finita) é autoadjunto se, e somente se, todos os seus autovalores são reais.

154. Suponha que V é um espaço vetorial complexo com produto interno e dimensão finita e $T \in L(V)$ é um operador normal tal que $T^9 = T^8$. Prove que T é autoadjunto e $T^2 = T$.

155. Seja V um espaço vetorial complexo com produto interno e $T \in L(V)$ um operador autoadjunto. Mostre que:

(a) $\|u + iT(u)\| = \|u - iT(u)\|$ para todo $u \in V$.

(b) $u + iT(u) = v + iT(v)$ se, e somente se, $u = v$.

(c) $I + iT$ é inversível.

(d) $I - iT$ é inversível.

156. Prove que toda matriz simétrica real possui uma raiz cúbica.

157. Prove que um operador normal e nilpotente é o operador nulo.

158. Seja V um espaço vetorial com produto interno e dimensão finita. Um operador $T \in L(V)$ é *não negativo* se $T = T^*$ e $\langle T(u), u\rangle \geqslant 0$ para todo $u \in V$. Se T é um operador não negativo, prove que existe um operador não negativo S tal que $S^2 = T$.

159. Se $A \in M_n(\mathbb{C})$ é uma matriz positiva (isto é, A é a matriz de uma forma sesquilinear positiva relativa a alguma base), prove que todos os elementos da diagonal principal de A são positivos.

160. Seja f uma forma bilinear em um espaço de dimensão finita V. Seja W o subespaço de todos os vetores $v \in V$ tais que $f(u, v) = 0$ para todo $u \in V$. Prove que

$$\text{posto}(f) = \dim_k V - \dim_k W.$$

8 Teorema de Estrutura de Módulos sobre Domínios Euclidianos

161. Encontre a forma normal de Smith da seguinte matriz com entradas em $\mathbb{Q}[x]$:

$$\begin{pmatrix} 14x^4 - 73x^3 + 119x^2 - 48x - 20 & 2x^2 - 7x + 6 \\ 7x^3 - 26x^2 + 20x + 8 & x - 2 \end{pmatrix}$$

162. Quantos grupos abelianos de ordem 24 existem (a menos de isomorfismo)? E de ordem 400?

163. (Cayley-Hamilton) Seja $T \in \text{Hom}_k(V, V)$. Mostre que $p(T) = 0$ em que $p(x) \in k[x]$ é o polinômio característico de T.

164. Seja $T \in \text{Hom}_{\mathbb{R}}(\mathbb{R}^3, \mathbb{R}^3)$ o operador linear que é representado na base canônica de $\mathbb{R}^3$ pela matriz

$$\begin{pmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{pmatrix}.$$

(a) Expresse o polinômio minimal $p(x)$ de T na forma $p(x) = p_1(x)p_2(x)$, em que $p_1(x)$ e $p_2(x)$ são mônicos e irredutíveis sobre $\mathbb{R}$.

(b) Seja W_i o núcleo de $p_i(T)$ $(i \in \{1, 2\})$. Determine bases B_i de para os espaços W_i e escreva a matriz de T na base $B_1 \cup B_2$.

165. Para cada uma das matrizes a seguir, determine

1. os polinômios característicos e minimais.
2. a forma canônica de Jordan.

(a) $T = \begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 3 \\ -1 & -2 & -2 \end{pmatrix}$

(b) $T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \\ -1 & 1 & 0 & 0 & 1 \end{pmatrix}$

(c) $T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

166. Determine a forma racional da matriz

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

167. Mostre que $A \in M_n(k)$ é diagonalizável se, e só se, seu polinômio minimal é **separável** (i.e., possui raízes distintas).

168. Seja V um espaço de dimensão finita e $T\colon V \to V$ um operador linear tal que $\dim(\text{im}(T)) = 1$. Prove que T é diagonalizável ou nilpotente, mas não ambos.

169. Seja T um operador linear no espaço de dimensão finita V, seja $p(x) = p_1(x)^{r_1} \cdots p_k(x)^{r_k}$ seu polinômio minimal, e seja $V = W_1 \oplus \cdots \oplus W_k$ a decomposição primária de T, isto é, $W_i = \ker(p_i(T)^{r_i})$. Se W é um subespaço de V invariante por T, prove que

$$W = (W \cap W_1) \oplus (W \cap W_2) \oplus \cdots \oplus (W \cap W_k).$$

170.

(a) Se A e B são matrizes quadradas de ordem 3 que possuem o mesmo polinômio característico e o mesmo polinômio minimal, prove que A e B são semelhantes.

(b) Exiba duas matrizes quadradas de ordem 4 que possuem o mesmo polinômio característico e o mesmo polinômio minimal, mas não são semelhantes.

171. Seja V um espaço vetorial de dimensão n, e seja $T \in \text{Hom}_k(V, V)$ um operador diagonalizável. Se T possui um vetor cíclico, isto é, se existe $u \in V$ tal que $\{u, T(u), T^2(u), \ldots, T^{n-1}(u)\}$ é uma base de V, prove que T possui n autovalores distintos.

172. Sejam K e L corpos tais que $K \subset L$, e sejam A e $B \in M_n(K)$. Prove que A e B são semelhantes sobre K se, e somente se, A e B são semelhantes sobre L.

173. Seja A uma matriz quadrada de ordem n com entradas complexas. Se todos os autovalores de A são reais, prove que A é semelhante a uma matriz com entradas reais.

174. Seja $A \in M_n(\mathbb{R})$ uma matriz tal que $A^2 + I_n = 0$. Prove que n é par e que, se $n = 2k$, a matriz A é semelhante sobre o corpo dos reais à matriz

$$\begin{pmatrix} 0 & -I_k \\ I_k & 0 \end{pmatrix}.$$

175. Seja A uma matriz complexa de ordem 5 cujo polinômio característico é $f(x) = (x - 2)^3(x + 7)^2$ e cujo polinômio minimal é $p(x) = (x - 2)^2(x + 7)$. Qual é a forma de Jordan de A?