Anéis e corpos

1. Averigúe se os seguintes conjuntos têm estrutura de anel para as operações indicadas. Em caso afirmativo, verifique se têm identidade, divisores de zero e estrutura de corpo.

   (a) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ sendo $Z_n = \{0, 1, \ldots, n-1\}$ com n número natural fixo, $\oplus_n$ e $\otimes_n$ adição e multiplicação módulo n.

   (b) $(\mathcal{M}_n(\mathbb{K}), +, \times)$ sendo $\mathcal{M}_n(\mathbb{K})$, com n número natural fixo, o conjunto das matrizes quadradas de ordem n com elementos num corpo $\mathbb{K}$, $+$ e $\times$ adição e multiplicação usuais de matrizes.

   (c) $(\mathcal{P}(X), \Delta, \cap)$ sendo $\mathcal{P}(X)$ o conjunto das partes de X, $X \neq \emptyset$ e $A\Delta B = (A \cup B) \setminus (A \cap B)$, $\forall A, B \in \mathcal{P}(X)$.

   (d) $(\mathcal{P}(X), \cup, \cap)$ sendo $\mathcal{P}(X)$ o conjunto das partes de X para $X \neq \emptyset$.

   (e) $(\mathbb{Q} \setminus \{0\}, \times, +)$ sendo $\times$ e $+$ a multiplicação e adição usuais de números racionais.

   (f) $(A, \oplus, \otimes)$ sendo $(A, +, .)$ um anel com identidade que designamos por 1 e

   $$a \oplus b = a + b + 1, \forall a, b \in A,$$

   $$a \otimes b = a + b + a.b, \forall a, b \in A.$$

   (g) $(G, +, \times)$ sendo $G = \{a + ib \mid a, b \in \mathbb{Z}\}$, o conjunto dos inteiros de Gauss, $+$ e $\times$ a adição e a multiplicação usuais de números complexos.

2. Quais das seguintes propriedades são válidas em qualquer anel A? E em qualquer anel comutativo?

   (a) $a^m a^n = a^{m+n}, \forall a \in A, \forall m, n \in \mathbb{N}$

   (b) $(a^m)^n = a^{mn}, \forall a \in A, \forall m, n \in \mathbb{N}$

   (c) $(ab)^m = a^m b^m, \forall a, b \in A, \forall m \in \mathbb{N}$

3. Seja A um anel com identidade 1 e não tendo divisores de zero. Para $a, b \in A$ verifique que:

   (a) $ab = 1$ se e só se $ba = 1$.

   (b) Se $a^2 = 1$ então ou $a = 1$ ou $a = -1$.

4. Sejam a e b dois elementos de um anel comutativo R com identidade. Se $n \in \mathbb{Z}^+$, deduza a expressão binomial

   $$(a+b)^n = \sum_{i=0}^{n} C_i^n a^{n-i} b^i, \qquad \text{onde} \qquad C_i^n = \frac{n!}{i!(n-i)!} \ .$$

5. Sendo A um anel comutativo e $a \in A \setminus \{0\}$, prove que

   $$(ab = ac \Rightarrow b = c) \Leftrightarrow a \text{ não é um divisor de zero.}$$

6. Um elemento a de um anel R diz-se *idempotente* se $a^2 = a$ e *nilpotente* se $a^n = 0$ para algum $n \in \mathbb{N}$. Mostre que:

   (a) Um elemento idempotente diferente de zero não pode ser nilpotente.

   (b) Qualquer elemento nilpotente diferente de zero é um divisor de zero.

7. Seja $(A, +, .)$ um anel. Suponha que existe $a \in A \setminus \{0\}$ tal que a não é divisor de zero e, além disso, $a^k = a$ para algum $k \in \mathbb{N} \setminus \{1\}$. Prove que o anel A tem identidade.

8. Averigue quais dos seguintes conjuntos são subanéis ou ideais dos anéis indicados. Sempre que possível determine o anel quociente.

   (a) O conjunto dos inteiros pares em $(\mathbb{Z}, +, \times)$.

   (b) O conjunto dos inteiros ímpares em $(\mathbb{Z}, +, \times)$.

   (c) O conjunto dos números reais de forma $a + b\sqrt{2}$, com $a, b \in \mathbb{Z}$, em $(\mathbb{R}, +, \times)$.

   (d) O conjunto dos números complexos da forma ib, com $b \in \mathbb{R}$, em $(\mathbb{C}, +, \times)$.

   (e) O conjunto dos números inteiros em $(\mathbb{Q}, +, \times)$.

9. Chama-se *centro* de um anel A ao conjunto $\{x \in A \mid xa = ax, \forall a \in A\}$. Mostre que o centro de A é um subanel do anel A. Será um ideal?

10. Verifique que $\mathbb{Z} \times \{0\}$ é um subanel de $(\mathbb{Z} \times \mathbb{Z}, +, .)$ e que $\mathbb{Z} \times \{0\}$ tem identidade diferente da identidade de $(\mathbb{Z} \times \mathbb{Z}, +, .)$.

11. Seja A um anel. Dados dois ideais I e J de A, considere o conjunto $I + J = \{a + b : a \in I \text{ e } b \in J\}$.

    (a) Mostre que $I + J$ é um ideal de A.

    (b) Prove que se N é um subanel de A que contém I e J, então N contém $I + J$.

12. Determine os ideais do anel $\mathbb{Z}_n$ para

    (a) $n = 4$; (b) $n = 11$; (c) $n = 12$; (d) $n = 16$.

13. Prove que a intersecção de qualquer família de subanéis (resp., ideais) de um anel A é um subanel (resp., ideal) de A.

14. (a) Qual é o menor subanel de $\mathbb{Z}$ que contém o 3? E o menor ideal?

    (b) Qual é o menor subanel de $\mathbb{R}$ que contém o $\frac{1}{2}$? E o menor ideal?

15. Mostre que $(a) + (b) = (a, b)$ para quaisquer dois elementos a e b de um anel.

16. (a) Mostre que $\mathcal{P}(S)$ é um ideal de $(\mathcal{P}(X), \Delta, \cap)$ (exercício 1.(c))para qualquer subconjunto S de X.

    (b) Determine o anel quociente $\mathcal{P}(X)/\mathcal{P}(S)$ e compare-o com o anel com $(\mathcal{P}(X \setminus S), \Delta, \cap)$.

17. Averigúe quais das seguintes aplicações são homomorfismos de anéis.

    (a) $\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & a & \longmapsto & 5a \end{array}$

    (b) $\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ & a & \longmapsto & \text{resto da divisão de } a \text{ por } n \end{array}$

    (c) $\begin{array}{rccc} f: & G & \longrightarrow & \mathbb{Z} \\ & a+ib & \longmapsto & a^2+b^2, \end{array}$ sendo G o anel dos inteiros de Gauss (exercício 1.(g)).

18. Seja $f : A \longrightarrow B$ um homomorfismo de anéis. Prove que se I é um ideal de A então $f(I)$ é um ideal de $f(A)$.

19. Considere os seguintes subanéis de $\mathbb{R}$:

$$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \quad \text{e} \quad S = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.$$

    (a) Verifique que $\theta : R \longrightarrow S$ definida por $\theta(a + b\sqrt{2}) = a + b\sqrt{3}$ não é um isomorfismo de anéis.

    (b) Mostre que os anéis R e S não são isomorfos.

20. Seja f um homomorfismo de um domínio de integridade D num domínio de integridade S. Prove que $f(D) = \{0\}$ ou $f(1_D) = 1_S$.

21. Determine a característica dos anéis com identidade do exercício 1.

22. Considere o anel $\mathbb{Z}$ dos números inteiros.

    (a) Prove que o ideal gerado por $p \in \mathbb{N} \setminus \{1\}$ é um ideal primo se e só se p é um número primo.

    (b) Determine o ideal gerado por $\{a, b\} \subset \mathbb{N}$, com $m.d.c.(a, b) = 1$.

23. Sejam $A = \{\frac{m}{n} \in \mathbb{Q} \mid m.d.c.(m, n) = 1 \text{ e } n \text{ é ímpar}\}$,

$B = \{\frac{m}{n} \in \mathbb{Q} \mid m.d.c.(m, n) = 1, n \text{ é ímpar e } m \text{ é par}\}$.

    Prove que:

    (a) A é um anel para as operações usuais de adição e multiplicação de números racionais.

    (b) B é um ideal maximal de A.

24. Seja A um anel comutativo com identidade.

    (a) Mostre que para qualquer ideal I, $1 \in I$ se e só se $A = I$.

    (b) Se I é um ideal de A, então $J_a = \{xa + y \mid x \in A,\ y \in I\}$ é um ideal de A.

25. Sejam D um domínio de integridade e a e b elementos de D. Mostre que $(ab) \subseteq (a)$ e indique uma condição necessária e suficiente para que $(ab) = (a)$.

26. Considere no conjunto $F = \{0, 1, \alpha, \beta\}$ as operações $+$ e $\cdot$ definidas pelas seguintes tabelas:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

    (a) Prove que $(F, +, \cdot)$ é um corpo.

    (b) Determine todos os subcorpos de F. Verifique se são ideais?

    (c) Indique a característica de F.

27. Considere o corpo $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$ com $n \in \mathbb{N}$ fixo.

    Averigúe se as seguintes aplicações estão bem definidas e, nesse caso, se são homomorfismos:

$$f: \begin{array}{ccc} \mathbb{Q}(\sqrt{n}) & \longrightarrow & \mathbb{Q}(\sqrt{n}) \\ a + b\sqrt{n} & \longrightarrow & a - b\sqrt{n} \end{array} \qquad g: \begin{array}{ccc} \mathbb{Q}(\sqrt{n}) & \longrightarrow & \mathbb{Q}(\sqrt{m}) \\ a + b\sqrt{n} & \longrightarrow & a + b\sqrt{m}. \end{array}$$

28. Seja A um anel comutativo com identidade.

    (a) Mostre que se $n1 = 0$, então para qualquer $a \in A$, $na = 0$.

    (b) Se A é um corpo, então, para todo o $a \in A$, $n1 = 0$ se e só se $na = 0$.

    (c) Prove que se F é um corpo de característica $p \neq 0$ e a um elemento não nulo de F, então $na = 0$ se e só se n é um múltiplo de p.

29. Sejam a e b elementos de um anel comutativo com identidade de característica $p \neq 0$. Prove que:

    (a) $(a + b)^{p^n} = a^{p^n} + b^{p^n}$;

    (b) $(a - b)^{p^n} = a^{p^n} - b^{p^n}$.

30. Seja A um anel comutativo com identidade de característica $n \neq 0$. Prove que a aplicação $\Pi : A \to A$, definida por $\Pi(x) = x^n$ para qualquer $x \in A$, é um homomorfismo.

31. Considere os ideais $(2), (4), (5)$ do anel $\mathbb{Z}$. Determine o anel quociente respectivo e diga se é um corpo.

32. Seja f um homomorfismo não nulo de um anel comutativo A num domínio de integridade D. Prove que $Nuc\, f$ é um ideal primo de A.

33. Considere o subconjunto $A = \{5n + 5mi \mid n, m \in \mathbb{Z}\}$ dos inteiros de Gauss (ex. 1.(g)).

    (a) Mostre que A é um ideal.

    (b) Averigúe se A é principal, primo ou maximal.

34. Diga quais dos seguintes anéis quociente são corpos. Determine os elementos que os constituem e a sua característica.

    (a) $G/(5)$;

    (b) $G/(1 - i)$;

    (c) $G/(2i)$.

35. Averigúe se os ideais (x) e $(2, x)$ do domínio $\mathbb{Z}[x]$ são principais, primos ou maximais.

Anéis de polinómios

36. Determine o produto dos polinómios f e g do anel $A[x]$, sendo:
    (a) $f = 2x^5 + 1$, $g = 2x^5 + 1$ e $A = \mathbb{Z}_4$;
    (b) $f = 2x^2 + 2x - 2$, $g = 3x - 3$ e $A = \mathbb{Z}_6$;
    (c) $f = 2x^2 - 4x + 3$, $g = 4x - 5$ e $A = \mathbb{Z}_8$.

37. Mostre que se A é subanel de B, então $A[x]$ é subanel de $B[x]$.

38. Prove que o conjunto dos polinómios homogéneos num anel A,
    $\{\sum_{i=1}^{n} a_i x^i \mid n \in \mathbb{N},\ a_i \in A\}$, é um ideal de $A[x]$.

39. Sejam A um anel comutativo e a um elemento fixo de A. Considere a aplicação

$$\begin{array}{rccc} \phi_a : & A[x] & \longrightarrow & A \\ & f & \longmapsto & f(a) \end{array},$$

    denotando por $f(a)$ o valor da função polinomial associada a f no ponto a.
    (a) Mostre que ϕ_a é um homomorfismo de anéis.
    (b) Determine o núcleo de ϕ_a.

40. (a) Sejam D um domínio de integridade e f um elemento não nulo de $D[x]$. Prove que f é invertível se e só se $\text{gr}(f) = 0$ e f for invertível considerado como elemento de D. Conclua que se $\mathbb{K}$ for um corpo, então os únicos elementos invertíveis de $\mathbb{K}[x]$ são os polinómios de grau zero.
    (b) O resultado da alínea anterior é válido se D for um anel comutativo qualquer?

41. Sendo f e g elementos de $\mathbb{K}[x]$, determine o quociente e o resto da divisão de f por g , para
    (a) $f = x^4 + 4x^2 + 4$, $g = x^2$ e $\mathbb{K} = \mathbb{Q}$;
    (b) $f = x^3 + 2x^2 - x + 2$, $g = x + 2$ e $\mathbb{K} = \mathbb{Z}_3$;
    (c) $f = x^7 - 4x^6 + x^3 - 3x + 5$, $g = 2x^3 - 2$ e $\mathbb{K} = \mathbb{Z}_7$.

42. (a) Sendo f um elemento não nulo de $\mathbb{R}[x]$, indique os elementos associados a f.
    (b) Determine $d = m.d.c.(f, g)$ e também u, $v \in \mathbb{R}[x]$ tais que

$$d = uf + vg,$$

    para
    - $f = x^3 + 1$ e $g = x^4 + x^3 + 2x^2 + x + 1$;
    - $f = x^3 + 2x^2 + 4x - 5$ e $g = x^2 + x - 2$;
    - $f = x^3 + 3x^2 + 2x + 8$ e $g = x^4 - 4$.

43. Sejam p um inteiro positivo primo e f um polinómio irredutível de $\mathbb{Z}_p[x]$ de grau n. Prove que o corpo $\mathbb{Z}_p[x]/(f)$ tem exactamente p^n elementos.

44. Em $\mathbb{Z}_5[x]$ determine $c \in \mathbb{Z}_5$ de tal forma que $x - 2$ seja um divisor de $x^4 + 2x^2 + c$.

45. Sendo C um corpo, prove que se $f \in C[x]$ é de grau 2 ou 3 e não tem raízes em C então f é irredutível sobre C. Mostre que a recíproca é válida para polinómios de grau ≥ 2.

46. Dê exemplos de polinómios redutíveis sobre um corpo mas que não tenham nenhuma raiz nesse corpo.

47. Seja C um corpo finito. Mostre que $C[x]$ contém polinómios irredutíveis de grau tão grande quanto se queira.

    (Sugestão: Imite a prova de Euclides da existência de um número infinito de primos).

48. Seja $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ com $a_0 \neq 0$. Mostre que, se $\frac{p}{q}$ (número racional expresso como quociente de inteiros primos entre si) for raiz de f, então $p \mid a_0$ e $q \mid a_n$. Conclua que se f for mónico então as suas raízes racionais são inteiras e, além disso, dividem a_0.

49. Averigúe quais dos seguintes polinómios de $\mathbb{Z}[x]$ são irredutíveis sobre $\mathbb{Q}$. Em caso negativo, factorize-os como produto de polinómios irredutíveis.

    (a) $x^3 - x + 1$;
    (b) $x^3 - 2x - 1$
    (c) $x^3 - 2x^2 + x + 15$.

50. Determine todas as raízes racionais dos seguintes elementos de $\mathbb{Q}[x]$:

    (a) $x^{50} - x^{20} + x^{10} - 1$;
    (b) $2x^2 - 3x + 4$;
    (c) $\frac{1}{2}x^3 - 5x + 2$;
    (d) $x^3 - 7x + 3$.

51. Mostre que $A[x]/(x^4 + x^3 + x + 1)$ não é um corpo, qualquer que seja o anel comutativo com identidade A que consideremos.

52. Determine $\mathbb{K}[x]/(f)$ e escreva as respectivas tabelas de anel para:

    (a) $\mathbb{K} = \mathbb{Z}_2$ e $f = x$;
    (b) $\mathbb{K} = \mathbb{Z}_2$ e $f = x^2 + x + 1$;
    (c) $\mathbb{K} = \mathbb{Z}_3$ e $f = x^2 + 2$.

53. Quais dos conjuntos $J \subseteq \mathbb{Q}[x]$ são ideais de $\mathbb{Q}[x]$. Em caso afirmativo, calcule $p(x)$ mónico tal que $J = (p(x))$. Quais desses ideais são maximais?

    (a) $J = \{f(x) \in \mathbb{Q}[x] \mid f(1) = f(7) = 0\}$;
    (b) $J = \{f(x) \in \mathbb{Q}[x] \mid f(2) = 0 \text{ e } f(5) \neq 0\}$;
    (c) $J = \{f(x) \in \mathbb{Q}[x] \mid f(\sqrt{3}) = 0\}$;
    (d) $J = \{f(x) \in \mathbb{Q}[x] \mid f(4) = 0 \text{ e } f(0) = f(1)\}$.

54. Se $p > 2$ é um número primo, mostre que há exactamente dois elementos $a \in \mathbb{Z}_p$ tais que $a^2 = 1$.

55. Utilizando o critério de Eisenstein, investigue se são irredutíveis sobre $\mathbb{Q}$ os seguintes polinómios com coeficientes racionais:

    (a) $x^7 + 11x^3 + 33x + 22$;
    (b) $x^5 + 2$;
    (c) $x^3 + 2x^2 + 10$;
    (d) $2x^5 - 6x^3 + 9x^2 - 15$;
    (e) $2x^2 + 27$;
    (f) $\frac{2}{9}x^5 + \frac{5}{3}x^4 + \frac{1}{3}$.

56. Utilize o critério de Eisenstein para demonstrar que, se $n > 1$ e $p_1, p_2, \ldots, p_k$ são números primos distintos dois a dois, então $\sqrt[n]{p_1 p_2 \ldots p_k}$ é um número irracional. Será indispensável exigir que os números $p_1, p_2, \ldots, p_k$ sejam todos distintos?

57. Averigúe se $x^2 + 1$ é irredutível sobre:
    (a) $\mathbb{Z}_3$; (b) $\mathbb{Z}_2$.

58. Mostre que se $f \in \mathbb{Z}[x]$, $f(0)$ e $f(1)$ são ímpares, então f não tem raízes em $\mathbb{Z}$.

59. Prove que os polinómios de $\mathbb{Z}[x]$ (a) $f = x^3 - x^2 + 1$ (b) $g = x^4 + 15x^3 + 7$ são irredutíveis sobre $\mathbb{Q}$. (Sugestão: Estude f sobre $\mathbb{Z}_2$ e g sobre $\mathbb{Z}_5$).

60. Resolva os seguintes sistemas de equações lineares:
    (a) $\begin{cases} 2x + 3y = 1 \\ 4x + 5y = 3 \end{cases}$ sobre $\mathbb{Z}_7$; (b) $\begin{cases} x + iy = -i \\ ix - y = 2 \end{cases}$ sobre $\mathbb{Z}[i]/(2 + i)$.

Extensões de corpos e Teoria de Galois

61. Sejam F_1, F_2, F_3 três corpos tais que $F_1 \subseteq F_2 \subseteq F_3$ e $\theta \in F_3$. Verifique que se θ é algébrico sobre F_1 então é algébrico sobre F_2. Mostre que a proposição recíproca é falsa.

62. Sejam F_1 um subcorpo de um corpo F e α, β elementos de F. Prove que $F_1(\alpha, \beta) = F_1(\alpha)(\beta)$. Generalize para o caso de n elementos $\alpha_1, \ldots, \alpha_n \in F$.

63. Sejam F_1 um subcorpo de um corpo F e α um elemento de F. Prove que:

    (a) se α é algébrico sobre F_1, o mesmo sucede a $\alpha + c$ e a $c\alpha$, qualquer que seja $c \in F_1$;

    (b) se α é algébrico sobre F_1, o mesmo sucede a α^2 e reciprocamente.

    Conclua que $\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$.

64. Averigúe quais dos seguintes elementos são algébricos ou transcendentes sobre o corpo $\mathbb{Q}$:

    (a) $\sqrt{7}$ (b) $\sqrt[3]{2}$ (c) π^2 (d) $e + 3$ (e) $1 + i$.

65. Sejam F_1 um subcorpo de um corpo F e α um elemento de F. Prove que se α é algébrico sobre F_1 então $F_1(\alpha) = F_1[\alpha]$, justificando pormenorizadamente os seguintes passos:

    (a) $F_1[\alpha]$ é um domínio de integridade.

    (b) Sendo $f(\alpha)$ um elemento não nulo de $F_1[\alpha]$ e m o polinómio mínimo de α sobre F_1, então: f não é múltiplo de m; existem $t, s \in F_1[x]$ tais que $tf + sm = 1$; $t(\alpha).f(\alpha) = 1$.

    (c) $F_1[\alpha]$ é um corpo.

66. Averigúe se os seguintes anéis quociente são corpos e, nos casos afirmativos, determine os elementos que os constituem e a sua característica:

    (a) $\mathbb{Z}_5[x]/(x^2 + 4)$;

    (b) $\mathbb{Q}[x]/(x^3 - 2)$;

    (c) $\mathbb{R}[x]/(x^2 + 1)$.

67. Determine o inverso de cada um dos seguintes elementos nas extensões simples $\mathbb{Q}(\alpha)$ indicadas:

    (a) $1 - 2\alpha + 3\alpha^2$, com α raiz do polinómio $x^3 - x + 1$;

    (b) $-\alpha^2 + 2\alpha - 3$, com $\alpha = \sqrt[3]{2}$;

    (c) $\alpha + 1$ e $\alpha^2 - 6\alpha + 8$, com $\alpha \neq 0$ tal que $\alpha^4 - 6\alpha^3 + 9\alpha^2 + 3\alpha = 0$.

68. Sejam F e E dois corpos tais que $F \subseteq E$. Sabendo que, se α, $\beta \in E$ são elementos algébricos sobre F, $[F(\alpha, \beta) : F]$ é finita, prove que os elementos de E algébricos sobre F formam um subcorpo de E.

69. Seja F uma extensão dum corpo F_1 e $\alpha \in F$ um elemento algébrico de grau n sobre F_1. Prove que todo o elemento de $F_1(\alpha)$ se pode exprimir de modo único na forma $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ com $a_i \in F_1$ $(i = 0, ..., n - 1)$.

70. Exprima na forma referida no exercício anterior os seguintes elementos das extensões algébricas $\mathbb{Q}(\alpha)$ indicadas:

    (a) α^4, α^2, α^5 e $\alpha^5 - \alpha^4 + 2$, com α raíz do polinómio $x^3 - 6x^2 + 9x + 3$.

    (b) $(\alpha^3 + 2)(\alpha^3 + 3\alpha)$, $\alpha^4(\alpha^4 + 3\alpha^2 + 7\alpha + 5)$ e $\frac{\alpha+2}{\alpha^2+3}$, sendo α uma solução da equação $x^5 + 2x + 2 = 0$.

71. Determine o polinómio mínimo sobre $\mathbb{Q}$ dos seguintes elementos:

    (a) $2 + \sqrt{3}$ (b) $\theta^2 - 1$, com $\theta^3 = 2\theta + 2$ (c) $\theta^2 + \theta$, com $\theta^3 = -3\theta^2 + 3$.

72. Prove que $\sqrt{7} \notin \mathbb{Q}(\sqrt{3})$, $i \notin \mathbb{Q}(\sqrt{5})$ e $\sqrt{5} \notin \mathbb{Q}(i)$.

73. Seja F uma extensão finita de F_1. Prove que:

    (a) se $[F : F_1]$ é um número primo, então F é uma extensão simples de F_1;

    (b) se $\theta \in F$, então o grau de θ é um divisor de $[F : F_1]$; conclua que se tem $F = F_1(\theta)$ se e só se o grau de θ coincidir com $[F : F_1]$;

    (c) se $f \in F_1[x]$ é irredutível em $F_1[x]$ e o grau de f é um número primo com $[F : F_1]$ e maior do que 1, então f não tem raízes em F.

74. Seja p um número primo e c um elemento do corpo C. Prove que $x^p - c$ é irredutível sobre C se e só se $x^p - c$ não tem raízes em C.

75. Sejam F,F_1 e F_2 corpos com $F \subseteq F_i$, para $i = 1, 2$. Se F_1 e F_2 são extensões finitas de F tais que $[F_1 : F]$ e $[F_2 : F]$ são primos entre si, então $F_1 \cap F_2 = F$.

76. Determine o grau sobre $\mathbb{Q}$ e uma base de cada uma das seguintes extensões de $\mathbb{Q}$:
    (a) $\mathbb{Q}(\sqrt{3}, i)$; (b) $\mathbb{Q}(\sqrt{18}, \sqrt[4]{2})$;
    (c) $\mathbb{Q}(\sqrt[3]{2}, \theta)$, com $\theta^4 + 6\theta + 2 = 0$;
    (d) $\mathbb{Q}(\sqrt{7}, \theta)$, com $\theta^3 + 3 = 0$;
    (e) $\mathbb{Q}(\alpha, \beta)$, com $\alpha^3 - \alpha + 1 = 0$ e $\beta^2 - \beta = 1$.

77. Determine o grau e uma base da extensão $\mathbb{Q}(\sqrt{\pi})$ de $\mathbb{Q}(\pi)$.

78. Sejam $\alpha^3 = 2$, w uma raiz cúbica da unidade e $\beta = w.\alpha$. Determine a dimensão e uma base de $\mathbb{Q}(\alpha, \beta)$ sobre $\mathbb{Q}$.

79. Mostre que $x^2 + 1$ é irredutível sobre $\mathbb{Z}_3$. Sendo u uma raíz deste polinómio determine o número de elementos de $\mathbb{Z}_3(u)$ e as tabelas de adição e multiplicação.

80. Averigúe se os seguintes polinómios são irredutíveis sobre o corpo indicado:
    (a) $x^2 + 2$ sobre $\mathbb{Q}(\sqrt{5})$; (b) $x^2 - 2x + 2$ sobre $\mathbb{Q}(\sqrt{-3})$;
    (c) $x^3 - 3x + 3$ sobre $\mathbb{Q}(\sqrt[4]{2})$.

81. Determine para quais dos seguintes polinómios $f \in F[x]$ existem extensões $F(\alpha)$ tais que f é o polinómio mínimo de α:
    (a) $x^2 - 4$, $F = \mathbb{Q}$; (b) $x^3 + x + 2$, $F = \mathbb{Z}_3$; (c) $x^2 + 1$, $F = \mathbb{Z}_5$.

82. Para cada uma das expressões de $\mathbb{Q}$ indicadas averigúe se θ gera a mesma extensão:
    (a) $\theta = 2 + \sqrt[3]{4}$, $\mathbb{Q}(\sqrt[3]{2})$; (b) $\theta = \sqrt{2} + \sqrt{3}$, $\mathbb{Q}(\sqrt{2})$;
    (c)$\theta = u^2 + u + 1$, $\mathbb{Q}(u)$, com $u^2 + 5u - 5 = 0$.

83. Considere o polinómio $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Seja α uma raiz de f.
    (a) Determine o inverso de $\alpha + 1$ em $\mathbb{Q}(\alpha)$, escrevendo-o como polinómio em α de coeficientes racionais.
    (b) Considere $u = \alpha^2 + 1$. As extensões $\mathbb{Q}(u)$ e $\mathbb{Q}(\alpha)$ coincidem?

84. Determine o inverso de $2 + \sqrt[3]{4}$ em $\mathbb{Q}(\sqrt[3]{2})$.

85. Determine a dimensão e uma base da extensão:
    (a) $\mathbb{Q}(\sqrt{2}, \alpha)$ sobre $\mathbb{Q}$, onde $3\alpha^3 + 7\alpha^2 = 14\alpha - 56$;
    (b) $\mathbb{Q}(\sqrt{7}, \theta)$ sendo θ uma raiz do polinómio $x^3 + 2x^2 + 2x - 4$ tal que $[\mathbb{Q}(\theta) : \mathbb{Q}] > 1$.

86. Seja θ uma raiz não nula do polinómio $x^4 - x^3 + x^2 - 2x \in \mathbb{Q}[x]$. Determine $\frac{\theta^2}{\theta^2+1}$ e exprima o resultado como combinação linear dos elementos duma base do espaço vectorial $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$.

87. Considere $\mathbb{Z}_5(\alpha)$, sendo $\alpha^2 + 3 = 0$, e determine:
    (a) a expressão geral dos elementos desse corpo e o seu cardinal;
    (b) o polinómio mínimo de $\beta = \alpha + 1$;
    (c) o inverso de β.

88. Mostre que é impossível construir com régua e compasso:
    (a) um cubo com volume igual ao de uma esfera dada;
    (b) o ponto $(\sqrt{5\sqrt{5} - 3} + \sqrt{2 - \sqrt[3]{2}}, 0)$ a partir dos pontos $(0, 0)$ e $(1, 0)$.

89. Observe que a fórmula de Cardano-Tartaglia não é conveniente para resolver as equações:

    (a) $x^3 - 19x + 30 = 0$;

    (b) $x^3 + 3x - 14 = 0$.

90. Determine a extensão de decomposição de:

    (a) $x^2 - 5$ sobre $\mathbb{Q}$;

    (b) $x^2 + 1$ sobre $\mathbb{R}$;

    (c) $x^5 - 2x^4 - 10x^3 + 20x^2 + 25x - 50$ sobre $\mathbb{Q}$.

91. Seja L uma extensão de $\mathbb{Q}$. Determine os $\mathbb{Q}$-automorfismos de L para:

    (a) $L = \mathbb{Q}(\sqrt{2})$;

    (b) $L = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, com $\alpha^5 = 7$;

    (c) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;

    (d) L a extensão de decomposição de $t^4 - 4t^2 - 5$.

92. (a) Para as extensões do exercício anterior, calcule os respectivos grupos de Galois.

    (b) Diga em quais dos casos é que a correspondência de Galois entre os subgrupos do grupo de Galois e as subextensões de L é uma bijecção.

93. Seja γ uma raiz de $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Mostre que $\sigma : \mathbb{Z}_2(\gamma) \to \mathbb{Z}_2(\gamma)$ definida por $\sigma(a + b\gamma) = a + b + b\gamma$, com $a, b \in \mathbb{Z}_2$, é um $\mathbb{Z}_2$-automorfismo de $\mathbb{Z}_2(\gamma)$.

94. Determine o grupo de Galois associado a cada uma das extensões do exercício 76.

95. Mostre que $Gal(K; L) = 1$ não implica $K = L$.

    (Sugestão: Considere $L = \mathbb{Q}$ e K a extensão de L gerada pela única raiz real de um polinómio irredutível sobre $\mathbb{Q}$).

96. (a) Determine os corpos intermédios entre $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

    (b) Calcule o respectivo grupo de Galois e compare os resultados.

97. Seja F uma extensão algébrica simples de K, $\alpha \in F - K$ e σ um elemento do grupo de Galois. Mostre que α e $\sigma(\alpha)$ têm o mesmo polinómio mínimo sobre K.

98. Calcule o grupo de Galois do polinómio $f(x)$ sobre o corpo K nos seguintes casos:

    (a) $f(x) = x^2 + 1$, $K = \mathbb{R}$;

    (b) $f(x) = x^4 - 2$, $K = \mathbb{Q}$;

    (c) $f(x) = x^3 - x + 1$, $K = \mathbb{Q}$; (ver Ex.67)

    (d) $f(x) = x^4 - 4x^2 - 5$, $K = \mathbb{Q}(i)$.

99. Calcule o grupo de Galois para os polinómios e os corpos considerados no Exercício 80.

100. Sejam C um corpo e E uma extensão de C. Prove que se $\alpha \in E$ é algébrico sobre C, de grau n, então $|Gal(C(\alpha); C)| \leq n$.

101. Sejam n um número natural e K um corpo que contém as raízes de índice n da unidade.

    (a) Se n for primo e α raiz do polinómio $x^n - a$, $a \in K$, então $Gal(K(\alpha); K)$ é um grupo cíclico de ordem 1 ou de ordem n.

    (b) Se β é raiz de $x^n - a$, $a \in K$, então $Gal(K(\beta); K)$ é cíclico.

102. (a) Sejam p um número primo e K um corpo que contém as raízes de índice p da unidade. Mostre que $x^p - a$, $a \in K$, é irredutível sobre K se e só se não tem raízes sobre K.

    (b) Prove que a hipótese de K conter as raízes de índice p da unidade não é necessária.

103. Seja C um corpo de característica diferente de 2, e K uma extensão de C tal que $[K : C] = 2$. Mostre que $K = C(\sqrt{a})$ para algum $a \in C$ e que K é de Galois sobre C.

104. Mostre que se f é um polinómio irredutível de grau 3, então $Gal(f,\mathbb{Q}) \cong \mathcal{A}_3$ ou $Gal(f,\mathbb{Q}) \cong \mathcal{S}_3$.

105. Considere um polinómio irredutível de grau 3 escrito na sua forma reduzida $x^3 + px + q$, e as suas três raízes complexas distintas a, b, e c.

(a) Verifique que $\begin{cases} a+b+c=0 \\ ab+ac+bc=p \\ abc=-q \end{cases}$.

(b) A partir da alínea anterior, mostre que $((a-b)(a-c)(b-c))^2 = -4p^3 - 27q^2 = D$.

(c) Prove que se $\sqrt{D} \in \mathbb{Q}$ e $\varphi \in Gal(f,\mathbb{Q})$, então $\varphi(\sqrt{D}) = \sqrt{D}$ e portanto $Gal(f,\mathbb{Q}) \cong \mathcal{A}_3$.

(d) Prove que se $\sqrt{D} \notin \mathbb{Q}$, então $\mathbb{Q}(\sqrt{D})$ está na extensão de decomposição de f, e portanto $Gal(f,\mathbb{Q}) \cong \mathcal{S}_3$.

106. Mostre que se os grupos A e B são resolúveis, então $A \times B$ também é resolúvel. Conclua que se os factores irredutíveis de um polinómio são resolúveis por radicais, então ele também é resolúvel por radicais.

107. Para cada um dos seguintes grupos, mostre que são resolúveis e indique um polinómio de coeficientes racionais cuja a resolubilidade por radicais resulte desse facto.

(a) $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$. (b) $\mathbb{Z}_2^n$. (c) $\mathcal{S}_3$. (d) $\mathcal{S}_4$. (e) $\mathbb{Z}_2 \oplus \mathcal{S}_3$.

108. (a) Mostre que, se um grupo resolúvel não tem subgrupos normais próprios, então é um grupo cíclico de ordem prima.

(b) Sabendo que o grupo $\mathcal{A}_5$ não tem subgrupos normais próprios, conclua que ele é resolúvel.

(c) A partir da alínea anterior, mostre que $\mathcal{S}_n$ não é resolúvel para $n \geq 5$.

109. Sejam p um número primo, e $f \in \mathbb{Q}[x]$ um polinómio irredutível de grau p. Mostre que:

(a) se f tem exactamente duas raízes complexas, então o grupo de Galois de f sobre $\mathbb{Q}$ é o grupo simétrico $\mathcal{S}_p$ e portanto não é resolúvel por radicais;

(b) se f tem exactamente quatro raízes complexas, então não é resolúvel por radicais.

110. Mostre que os seguintes polinómios $f \in \mathbb{Q}[x]$ não são resolúveis por radicais:

(a) $f = 2x^5 - 10x + 5$;
(b) $f = 2x^5 - 5x^4 + 20$;
(c) $f = x^5 - 6x^2 + 5$;
(d) $f = x^7 - 10x^5 + 15x + 5$.

111. Resolva as equações por meio de radicais.

(a) $x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 8 = 0$. (Sugestão: $y = x - 1$.)

(b) $x^3 + 2x^2 - 5x + 9 - \frac{5}{x} + \frac{2}{x^2} + \frac{1}{x^3} = 0$. (Sugestão: $y = x + \frac{1}{x}$.)

112. Determine a extensão a radical sobre $\mathbb{Q}$ que contém os seguintes elementos de $\mathbb{C}$:

(a) $\sqrt[3]{8} + \sqrt{2}$; (b) $\dfrac{\sqrt[7]{13+\sqrt{2}}}{\sqrt[3]{5}}$.

113. Verifique que apesar de $x^3 - 3x + 1$ ser resolúvel por radicais, a sua extensão de decomposição não é uma extensão radical. (ver Exercício 105)

Corpos finitos

114. Seja F a extensão de decomposição de $x^2 - 2 \in \mathbb{Z}_3[x]$.

(a) Descreva o corpo F e indique um gerador de $F^* = F \setminus \{0\}$.

(b) Qual é o subcorpo primo de F?

115. Seja F a extensão de decomposição de $f = x^{p^n} - x$ sobre $\mathbb{F}_p$.

(a) Mostre que $R = \{a \in F \mid a^{p^n} = a\}$, o conjunto das raízes de f, é um subcorpo de F.

(b) Prove directamente, a partir a definição de raiz dupla, que todas as raízes de f são simples.

(c) Conclua que $R = F$.

116. Seja C um corpo com 81 elementos.

(a) Determine a característica de C, indique o seu o corpo primo e determine $[C : \mathbb{Z}_p]$.

(b) Justifique a afirmação *O único subcorpo próprio de C é o seu subcorpo primo.*

117. Construa um corpo finito de ordem 16 e determine todos os geradores do seu grupo multiplicativo.

118. Indique, justificando, o número de corpos não isomorfos de ordem inferior a 100.

119. Determine todos os subcorpos de um corpo com 32 e 64 elementos, respectivamente.

120. Usando resultados sobre corpos finitos, mostre que se p é um número primo e r divide n, então $p^r - 1$ divide $p^n - 1$.

121. Através de um comando à distância de uma televisão podem ser efectuadas 20 operações: escolher entre 18 canais diferentes (0–17), aumentar (A) ou diminuir (D) o volume. A tabela indica três códigos decimais para transmitir essa informação.

	0	1	2	$\cdots$	9	10	11	$\cdots$	17	A	D
C_1	00	01	02	$\cdots$	09	10	11	$\cdots$	17	18	19
C_2	0000	0101	0202	$\cdots$	0909	1010	1111	$\cdots$	1717	1818	1919
C_3	00000	01011	02022	$\cdots$	09099	10109	11118	$\cdots$	17172	18181	19190

(a) Determine a distância mínima de cada um dos três códigos.

(b) Diga quais dos códigos detectam e/ou corrigem erros singulares.

(c) Um receptor de televisão recebe informação do comando utilizando o terceiro código. Sempre que possível diga o efeito gerado pela recepção das seguintes mensagens: 15154, 13144, 19191.

122. As matrizes H_1, H_2 e H_3 determinam três códigos lineares binários.

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad H_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Para cada um deles responda às perguntas.

(a) Determine o comprimento do código e o número de dígitos de controlo.

(b) Calcule a distância mínima e descreva o conjunto das mensagens.

(c) Poderão estes códigos ser usados para detectar e/ou corrigir erros singulares?

(d) Supondo que os três últimos dígitos da mensagem são 011. Diga se esta mensagem pode pertencer ao código e determine a mensagem completa.

123. Calcule a matriz dos códigos do Exercício 121.

124. Usando os códigos do Exercício 122, determine os sintomas e, se possível, corrija os erros das mensagens.

(a) Código 1; mensagens: 00000, 11111, 01010.

(b) Código 2; mensagens: 11011, 10011.

(c) Código 3; mensagens: 1000000, 1110101.

125. Considere $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, com $\alpha^4 = \alpha + 1$, e a matriz do código BCH

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}.$$

(a) Faça uma estimativa para a distância mínima deste código.

(b) Codifique a mensagem 1010101 e descodifique 110010110100110 e 100111000000000.

(c) Mostre que se uma mensagem recebida r tem apenas um erro e esse erro é na posição i então $H.r = [\alpha^{(i-1)} \;\; \alpha^{3(i-1)}]^t$.