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

2. Sejam K um subcorpo de um corpo L e θ um elemento de L. Prove que se θ é algébrico sobre K, o mesmo sucede a $\theta + c$ e a $c\theta$, qualquer que seja $c \in K$.

3. 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) $1+i$.

4. π é algébrico sobre $\mathbb{Q}(\pi^3)$?

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

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

   (a) $2 + \sqrt{3}$.
   (b) $\sqrt{3} + \sqrt{5}$.
   (c) $\theta^2 - 1$, sendo θ uma raiz do polinómio $x^3 - 2x - 2$.
   (d) $\theta^2 + \theta$, onde $\theta^3 = -3\theta^2 + 3$.

7. Qual é o polinómio mínimo do número real $\theta = \sqrt{\sqrt{2}+2}$ sobre o corpo $\mathbb{Q}$? E sobre o corpo $\mathbb{Q}(\sqrt{2})$?

8. Sejam K um subcorpo de um corpo L e θ um elemento de L. Prove que θ é algébrico sobre K se e só se o mesmo sucede a θ^2.

9. Prove que:

   (a) $\sqrt{7} \notin \mathbb{Q}(\sqrt{3})$.
   (b) $i \notin \mathbb{Q}(\sqrt{5})$.
   (c) $\sqrt{5} \notin \mathbb{Q}(i)$.
   (d) $\sqrt{2+\sqrt{2}} \notin \mathbb{Q}(\sqrt{2})$.

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

    (a) $2 + \sqrt[3]{4}$ em $\mathbb{Q}(\sqrt[3]{2})$.
    (b) $1 - 2\theta + 3\theta^2$, onde θ é raiz do polinómio $x^3 - x + 1$.
    (c) $-\theta^2 + 2\theta - 3$, para $\theta = \sqrt[3]{2}$.
    (d) $\theta + 1$ e $\theta^2 - 6\theta + 8$, onde $\theta \neq 0$ é tal que $\theta^4 - 6\theta^3 + 9\theta^2 + 3\theta = 0$.

11. Exprima os seguintes elementos das extensões algébricas $\mathbb{Q}(\theta)$ indicadas em função da sua base:

    (a) θ^4, θ^5 e $\theta^5 - \theta^4 + 2$, onde θ é raiz do polinómio $x^3 - 6x^2 + 9x + 3$.
    (b) $(\theta^3 + 2)(\theta^3 + 3\theta)$, sendo θ uma raiz do polinómio $x^5 + 2x + 2 = 0$.
    (c) $\dfrac{\theta^2}{\theta^2+1}$, onde θ é uma raiz não nula do polinómio $x^4 - x^3 + x^2 - 2x$.

12. Seja L uma extensão finita de K. Prove que:

   (a) Se $[L : K]$ é um número primo, então L é uma extensão simples de K.

   (b) Se $\theta \in L$, então o grau de θ é um divisor de $[L : K]$. Conclua que se tem $L = K(\theta)$ se e só se o grau de θ coincidir com $[L : K]$.

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

13. 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 $\mathbb{Q}(\sqrt[4]{2})$.

14. 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) $\mathbb{Q}(\sqrt[3]{2}, \theta)$, onde $\theta^4 + 6\theta + 2 = 0$.

   (d) $\mathbb{Q}(\sqrt{7}, \theta)$, onde $\theta^3 + 3 = 0$.

   (e) $\mathbb{Q}(\alpha, \beta)$, onde $\alpha^3 - \alpha + 1 = 0$ e $\beta^2 - \beta = 1$.

   (f) $\mathbb{Q}(\sqrt{2}, \alpha)$, onde $3\alpha^3 + 7\alpha^2 = 14\alpha - 56$.

   (g) $\mathbb{Q}(\sqrt{7}, \theta)$ sendo θ uma raiz do polinómio $x^3 + 2x^2 + 2x + 4$ tal que $[\mathbb{Q}(\theta) : \mathbb{Q}] > 1$.

15. Será que $[\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) : \mathbb{Q}]$ é igual a 8?

16. Seja p um inteiro primo positivo. Determine $[\mathbb{Q}(\sqrt{p + \sqrt{p}}) : \mathbb{Q}]$.

17. 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.

18. 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.

19. Para cada uma das extensões de $\mathbb{Q}$ indicadas averigúe se θ gera a mesma extensão:

   (a) $\theta = 2 + \sqrt[3]{4}$, $\quad \mathbb{Q}(\sqrt[3]{2})$.

   (b) $\theta = \sqrt{2} + \sqrt{3}$, $\quad \mathbb{Q}(\sqrt{2})$.

   (c) $\theta = u^2 + u + 1$, $\quad \mathbb{Q}(u)$, com $u^2 + 5u - 5 = 0$.

20. Considere o polinómio $f(x) = x^3 - x + 1 \in \mathbb{Q}[x]$. Seja θ uma raiz de $f(x)$.

   (a) Determine o inverso de $\theta + 1$ em $\mathbb{Q}(\theta)$, escrevendo-o como polinómio em θ de coeficientes racionais.

   (b) Considere $u = \theta^2 + 1$. As extensões $\mathbb{Q}(u)$ e $\mathbb{Q}(\theta)$ coincidem?

21. Prove que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

22. Considere o polinómio $p(x) = 8x^3 - 6x - 1$ sobre $\mathbb{Q}$.
    (a) Mostre que $p(x)$ é irredutível sobre $\mathbb{Q}$.
    (b) Construa uma extensão de decomposição de $p(x)$ e determine a sua dimensão.
23. 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 $\mathbb{Q}$.
24. Determine o grupo dos automorfismos de $\mathbb{Q}$ e de $\mathbb{Z}_p$ (p primo).
25. Determine os $\mathbb{Q}$-automorfismos de L para:
    (a) $L = \mathbb{Q}(\sqrt{2})$.
    (b) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
26. Seja θ uma raiz de $x^2+x+1 \in \mathbb{Z}_2[x]$. Mostre que $\Phi : \mathbb{Z}_2(\theta) \to \mathbb{Z}_2(\theta)$ definido por $\Phi(a+b\theta) = a+b+b\theta$, para quaisquer $a, b \in \mathbb{Z}_2$, é um $\mathbb{Z}_2$-automorfismo de $\mathbb{Z}_2(\theta)$.
27. Considere o polinómio $p(x) = x^4 - 3x^3 + 2x^2 + 2x - 4 \in \mathbb{Q}[x]$. Determine:
    (a) A factorização de $p(x)$ em factores irredutíveis em $\mathbb{Q}[x]$.
    (b) O corpo de decomposição de $p(x)$.
    (c) O grupo de Galois de $p(x)$ sobre $\mathbb{Q}$. Apresente-o como subgrupo de S_4.
28. Seja θ a raiz real do polinómio $x^5 - 7$. Determine o grupo de Galois da extensão $\mathbb{Q}(\theta)$ de $\mathbb{Q}$.
29. Calcule o grupo de Galois do polinómio $f(x)$ sobre o corpo K nos seguintes casos:
    (a) $f(x) = x^2 + 1, \qquad K = \mathbb{R}$.
    (b) $f(x) = x^3 - x + 1, \qquad K = \mathbb{Q}$.
30. (a) Para as extensões L de $\mathbb{Q}$ do Exercício 25, calcule os respectivos grupos de Galois, $Gal(L, \mathbb{Q})$.
    (b) Verifique em quais desses casos a correspondência de Galois entre os subgrupos do grupo de Galois e as extensões intermédias (entre $\mathbb{Q}$ e L) é uma bijecção.
31. Considere a extensão $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subseteq \mathbb{R}$ de $\mathbb{Q}$.
    (a) Como se define o grupo de Galois de L (sobre $\mathbb{Q}$)? Determine-o.
    (b) Indique todas as extensões intermédias de $\mathbb{Q}$ em L.
    (c) L é uma extensão de Galois de $\mathbb{Q}$? Justifique.

Exercícios mais avançados

1*. Sejam K,K_1 e K_2 corpos com $K \subseteq K_i$ ($i = 1, 2$). Se K_1 e K_2 são extensões finitas de K tais que $[K_1 : K]$ e $[K_2 : K]$ são primos entre si, então $K_1 \cap K_2 = K$.

2*. 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 $\mathbb{Q}$.

3*. (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.

4*. Seja L uma extensão algébrica simples de K, $\alpha \in L - K$ e $\Phi \in Gal(L, K)$. Mostre que α e $\Phi(\alpha)$ têm o mesmo polinómio mínimo sobre K.

5*. Calcule o grupo de Galois do polinómio $x^4 - 2$ sobre o corpo $\mathbb{Q}$.

6*. Considere um polinómio $f(x)$ 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 $((a - b)(a - c)(b - c))^2 = -4p^3 - 27q^2$.

(c) Seja D o número $-4p^3 - 27q^2$ da alínea anterior. Prove que se $\sqrt{D} \in \mathbb{Q}$ e $\Phi \in Gal(f(x), \mathbb{Q})$, então $\Phi(\sqrt{D}) = \sqrt{D}$ e portanto $Gal(f(x), \mathbb{Q}) \cong \mathcal{A}_3$.

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

7*. 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.

8*. Sejam $p \geq 5$ um número primo, e $f(x) \in \mathbb{Q}[x]$ um polinómio irredutível de grau p. Mostre que:

(a) se $f(x)$ tem exactamente duas raízes complexas não reais, então $Gal(f(x), \mathbb{Q})$ é o grupo simétrico $\mathcal{S}_p$ e portanto $f(x)$ não é resolúvel por radicais.

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

9*. Mostre que os seguintes polinómios $f(x) \in \mathbb{Q}[x]$ 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) $f = x^7 - 10x^5 + 15x + 5$.