1. Mostrar que

$$\sqrt{5+\sqrt{24}} = \sqrt{3}+\sqrt{2} \text{ e } \sqrt{5-\sqrt{24}} = \sqrt{3}-\sqrt{2}.$$

2. Sejam R um domínio e F um subcorpo de R. Mostrar que se R é um espaço vetorial de dimensão finita sobre F, então R é um corpo.

3. Existem números algébricos sobre $\mathbb{Q}$, α e β tais que

$$\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q} \text{ e } [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] < [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}].$$

4. Seja E/F uma extensão. Mostrar que:

   (a) $\alpha \in E$ é algébrico sobre F se, e somente se, $\alpha^{-1} \in F[\alpha]$.

   (b) E/F é algébrica se, e somente se, qualquer anel R com $F \subseteq R \subseteq E$ é um corpo.

5. Suponhamos que $\alpha, \beta \in \mathbb{C}$ satisfaçam as equações

$$\alpha^3+\alpha+1=0 \text{ e } \beta^2+\beta-3=0.$$

Determinar $\text{irr}(\alpha+\beta, \mathbb{Q})$ e $\text{irr}(\alpha\beta, \mathbb{Q})$.

6. Sejam $p_1, p_2, p_3, \ldots$ a seqüência de números primos e

$$E_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}) \subseteq \mathbb{R}.$$

Mostrar que $\sqrt{p_{n+1}} \notin E_n$ e $[E_{n+1} : E_n] = 2$, para todo $n \in \mathbb{N}$. Conclua que $[E_n : \mathbb{Q}] = 2^n$, para todo $n \in \mathbb{N}$.

7. Determinar um corpo de decomposição $E \subseteq \mathbb{C}$ e $[E : \mathbb{Q}]$ para o polinômio

$$p = x^4+x^2+1.$$

8. Seja E/F uma extensão. Mostrar que se $[F(\alpha) : F]$ é um número ímpar, então $F(\alpha^2) = F(\alpha)$.

9. Responda se o número real $\alpha = \pi^6 + 5\pi^3 - 1$ é algébrico ou transcendente sobre $\mathbb{Q}$.

10. Seja L um corpo de decomposição sobre $\mathbb{Q}$ para o polinômio

$$p = (x^2-1)(x^5+x^4+1).$$

Então L possui um elemento primitivo. (Justifique)

2 Suponhamos que R seja um espaço vetorial de dimensão finita sobre F, então $[R:F]=n$, $n\in\mathbb{N}$. Dado $a\in R$, $a\neq 0$, definimos a seguinte função

$$\begin{aligned}\varphi_a : R &\longrightarrow R\\ x &\longmapsto ax.\end{aligned}$$

φ_a é uma transformação linear. De fato,

$$\varphi_a(\alpha x) = a(\alpha x) = \alpha(ax) = \alpha\varphi_a(x),\ \forall \alpha\in F \text{ e } \forall x\in R$$

$$\varphi_a(x+y) = a(x+y) = ax+ay = \varphi_a(x)+\varphi_a(y),\ \forall x,y\in R.$$

Além disso, φ_a é injetora, pois

$$\varphi_a(x)=0 \Rightarrow ax=0 \text{ e como } a\neq 0 \Rightarrow x=0.$$

Logo, $N(\varphi_a)=\{0\}$. Sendo $[R:F]<\infty$ e φ_a injetora $\Rightarrow \varphi_a$ bijetora.
Portanto, existe $b\in R$ tal que $\varphi_a(b)=1$, isto é,

$$ab=1.$$

Como $a\in R$ foi escolhido de modo arbitrário, temos que R é um corpo.

---

3. Seja $p(x)=x^3-2$, temos que $\alpha=\sqrt[3]{2}$ e $\beta=\omega\sqrt[3]{2}$, onde ω é a raiz da unidade, são raízes de p. Então, $\mathbb{Q}(\alpha)\simeq\mathbb{Q}(\beta)$ e $[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\beta):\mathbb{Q}]=3$.

O seguinte diagrama é válido:

$$\begin{array}{c}\mathbb{Q}(\alpha,\beta)\\ |\ 2\\ \mathbb{Q}(\alpha)\\ |\ 3\\ \mathbb{Q}\end{array}$$

Logo, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=6$ e, portanto,

$$6=[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]<[\mathbb{Q}(\alpha):\mathbb{Q}][\mathbb{Q}(\beta):\mathbb{Q}]=3.3=9$$

Note que, $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$, pois $\beta\in\mathbb{C}$, $\alpha\in\mathbb{R}$ e $\alpha\neq\beta$.

4. (a) ($\Rightarrow$) Suponhamos que $\alpha \in E$ seja algébrico sobre F. Então, $F[\alpha] = F(\alpha)$ é um corpo e, portanto, $\alpha^{-1} \in F[\alpha]$.

($\Leftarrow$) Se $\alpha^{-1} \in F[\alpha]$, então existem escalares $a_0, a_1, \ldots, a_n \in F$ tais que

$$\alpha^{-1} = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Assim,

$$a_0\alpha + a_1\alpha^2 + \ldots + a_n\alpha^{n+1} - 1 = 0$$

e, dessa forma, temos que α é raiz de um polinômio pertencente a $F[x]$. Logo, α é algébrico sobre F.

(b) ($\Rightarrow$) Sejam R um anel, com $F \subseteq R \subseteq E$, e $\alpha \in R$. Então, $\alpha \in E$ e existe $p(x) \in F[x]$ tal que

$$p(\alpha) = a_n\alpha^n + \ldots + a_0 = 0,$$

pois, por hipótese, E/F é algébrica. Assim,

$$\alpha(a_n\alpha^{n-1} + \ldots + a_1) = -a_0$$

$$\alpha[(a_n\alpha^{n-1} + \ldots + a_1)(-a_0)^{-1}] = 1$$

e determinamos $\alpha^{-1} = [(a_n\alpha^{n-1} + \ldots + a_1)(-a_0)^{-1}] \in R$. Logo, R é um corpo.

($\Leftarrow$) Seja E/F uma extensão tal que qualquer anel R com $F \subseteq R \subseteq E$ é um corpo, então dado $\alpha \in E$ temos que $F \subseteq F[\alpha] \subseteq E$. Logo, $F[\alpha]$ é um corpo e, por isso, $\alpha^{-1} \in F[\alpha]$. Portanto, pelo item (a), $\alpha \in E$ é algébrico sobre F. Desta forma, concluímos que E/F é algébrica.

8. É claro que $F(\alpha^2) \subseteq F(\alpha)$, pois $F \subseteq F(\alpha)$ e $F(\alpha)$ é corpo e $\alpha \in F(\alpha)$, então $\alpha^2 \in F(\alpha)$. Assim, concluímos que α^2 é algébrico sobre F. Suponhamos que $[F(\alpha):F] = n$ ímpar, $[F(\alpha^2):F] = m$ e $g = irr(\alpha^2, F)$.

$$g(x) = a_0 + a_1 x + \dots + a_m x^m \text{ e } g(\alpha^2) = a_0 + a_1 \alpha^2 + \dots + a_m \alpha^{2m}$$

Definimos, a partir de g, $h(x) \in F[x]$

$$h(x) = a_0 + a_1 x^2 + \dots + a_m x^{2m} \Rightarrow h(\alpha) = 0 = g(\alpha^2).$$

Logo, $n \mid 2m$ e n ímpar $\Rightarrow mdc(n,2) = 1 \Rightarrow n \mid m \Rightarrow n \leq m$ (1).

Como $F \subseteq F(\alpha^2) \subseteq F(\alpha) \Rightarrow m \leq n$ (2). De (1) e (2), temos $m = n$.

Portanto,

$$[F(\alpha):F] = [F(\alpha):F(\alpha^2)][F(\alpha^2):F] \Rightarrow 1 = [F(\alpha):F(\alpha^2)] \Rightarrow F(\alpha) = F(\alpha^2).$$

---

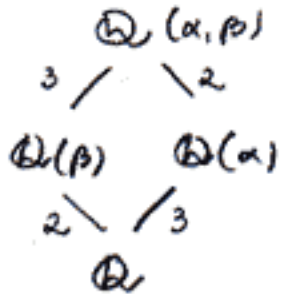
9. $\alpha \in \mathbb{Q}(\pi)$. Então, temos o diagrama

$\mathbb{Q}(\pi)$
|
$\mathbb{Q}(\alpha)$
|
$\mathbb{Q}$

Suponha, por absurdo, que α seja algébrico sobre $\mathbb{Q}$. É claro que π é algébrico sobre $\mathbb{Q}(\alpha)$, pois $p(x) = x^6 + 5x^3 - 1 - \alpha \in \mathbb{Q}(\alpha)[x]$ e $p(\pi) = 0$. Logo, $\mathbb{Q}(\pi)/\mathbb{Q}(\alpha)$ é algébrica, $\mathbb{Q}(\alpha)/\mathbb{Q}$ é algébrica (por hipótese) e daí, concluímos que $\mathbb{Q}(\pi)/\mathbb{Q}$ é algébrica, o que é impossível, porque π é transcendente sobre $\mathbb{Q}$.

5. Sejam $p(x) = x^3 + x + 1$, $q(x) = x^2 + x - 3 \in \mathbb{Q}[x]$, temos $p(\alpha) = 0$ e $q(\beta) = 0$.

Pelo diagrama



temos que $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 6$. Sabemos que $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ é uma base de $\mathbb{Q}(\alpha,\beta)$ sobre $\mathbb{Q}$. Definimos $T_{\alpha+\beta} : \mathbb{Q}(\alpha,\beta) \longrightarrow \mathbb{Q}(\alpha,\beta)$ por

$$T_{\alpha+\beta}(s) = (\alpha+\beta)s.$$

Então,

$$T_{\alpha+\beta}(1) = \alpha+\beta = 0.1 + 1.\alpha + 0.\alpha^2 + 1.\beta + 0.\alpha\beta + 0.\alpha^2\beta$$

$$T_{\alpha+\beta}(\alpha) = \alpha^2 + \alpha\beta = 0.1 + 0.\alpha + 1.\alpha^2 + 0.\beta + 1.\alpha\beta + 0.\alpha^2\beta$$

$$T_{\alpha+\beta}(\alpha^2) = \alpha^3 + \alpha^2\beta = -\alpha - 1 + \alpha^2\beta = (-1).1 + (-1).\alpha + 0.\alpha^2 + 0.\alpha\beta + 1.\alpha^2\beta$$

$$T_{\alpha+\beta}(\beta) = \alpha\beta + \beta^2 = \alpha\beta - \beta + 3 = 3.1 + 0.\alpha + 0.\alpha^2 + (-1).\beta + 1.\alpha\beta + 0.\alpha^2\beta$$

$$T_{\alpha+\beta}(\alpha\beta) = \alpha^2\beta + \alpha\beta^2 = \alpha^2\beta + \alpha(-\beta+3) = 0.1 + 3.\alpha + 0.\alpha^2 + 0.\beta + (-1).\alpha\beta + 1.\alpha^2\beta$$

$$T_{\alpha+\beta}(\alpha^2\beta) = \alpha^3\beta + \alpha^2\beta^2 = (-\alpha-1)\beta + \alpha^2(-\beta+3) = 0.1 + 0.\alpha + 3\alpha^2 + (-1).\beta + (-1)\alpha\beta + (-1)\alpha^2\beta.$$

e

$$[T_{\alpha+\beta}] = A = \begin{bmatrix} 0 & 0 & -1 & 3 & 0 & 0 \\ 1 & 0 & -1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 1 & -1 \end{bmatrix}.$$

Assim, $r(x) = \det(Ix - A) = x^6 - 3x^5 - 4x^4 + 11x^3 + 25x^2 - 52x - 39$ e como $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha+\beta)$ temos que $in(\alpha+\beta, \mathbb{Q}) = r(x)$.

[Continuação]

5. Utilizando o mesmo artifício temos

$$[T_{\alpha\beta}] = B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 3 & 0 & -3 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & -1 & 0 & 0 & -3 \\ 1 & 0 & -1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 & 0 \end{bmatrix}$$

e

$$h(x) = \det(I_x - B) = x^6 + 7x^4 + 6x^3 + 9x^2 + 45x - 27.$$

Como $\partial(p) = 3$, $\partial(q) = 2$ e $mdc(2,3) = 1$, então, $\partial(\text{im}(\alpha\beta; \mathbb{Q})) = 6$.

Sabemos que $\text{im}(\alpha\beta, \mathbb{Q}) \mid h(x)$ e $\partial(h) = 6$, logo, $\text{im}(\alpha\beta, \mathbb{Q}) = h(x)$.

---

7. Observe que

$$p(x) = x^4 + x^2 + 1 = (x-\alpha)(x-\bar{\alpha})(x-\beta)(x-\bar{\beta}),$$

onde $\alpha = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\bar{\alpha} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$, $\beta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\bar{\beta} = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \in \mathbb{C}$.

Logo, $E = \text{Gal}(p, \mathbb{Q}) = \mathbb{Q}(i\sqrt{3})$, pois $\alpha, \bar{\alpha}, \beta, \bar{\beta} \in \mathbb{Q}(i\sqrt{3})$. Como $\text{im}(i\sqrt{3}, \mathbb{Q}) = x^2 + 3$, então $[E : \mathbb{Q}] = \partial(\text{im}(i\sqrt{3}, \mathbb{Q})) = 2$.

1. Suponha, por absurdo, que

$$\sqrt{5+\sqrt{24}} \neq \sqrt{3}+\sqrt{2},$$

então,

$$\left(\sqrt{5+\sqrt{24}}\right)^2 \neq \left(\sqrt{3}+\sqrt{2}\right)^2 \Rightarrow 5+\sqrt{24} \neq 3+2.\sqrt{6}+2 \Rightarrow 5+\sqrt{24} \neq 5+\sqrt{24},$$

o que é um absurdo. Logo, $\sqrt{5+\sqrt{24}} = \sqrt{3}+\sqrt{2}$. De modo análogo, mostra-se que $\sqrt{5-\sqrt{24}} = \sqrt{3}-\sqrt{2}$.

Note que $\sqrt{5+\sqrt{24}}$, $\sqrt{3}+\sqrt{2}$, $\sqrt{5-\sqrt{24}}$, $\sqrt{3}-\sqrt{2}$ são números positivos.

---

10. L corpo de decomposição de p. Então, $[L:\mathbb{Q}] \leq \delta(p)$ e, portanto, $L/\mathbb{Q}$ é algébrica. $L/\mathbb{Q}$ também é separável, pois toda extensão algébrica de um corpo de característica zero é separável. Assim, como L é separável finita, temos que L possui um elemento primitivo, isto é, $L = K(\delta)$, $\gamma \in \mathbb{C}$.

6. Seja $q(x) = x^2 - p_{n+1} \in E_n[x]$. Temos que $q(x)$ é irredutível sobre E_n, pois $q(x) = (x - \sqrt{p_{n+1}})(x + \sqrt{p_{n+1}})$ e $\sqrt{p_{n+1}} \notin E_n$. Como $q(x) = \text{irr}(\sqrt{p_{n+1}}, E_n)$, então $[E_{n+1} : E_n] = 2 = \partial(q)$.

Sabemos que $[E_2 : \mathbb{Q}] = 2$. Suponhamos válido para $n-1$, $[E_{n-1} : \mathbb{Q}] = 2^{n-1}$.

Logo,

$$[E_n : \mathbb{Q}] = [E_n : E_{n-1}][E_{n-1} : \mathbb{Q}] = 2 \cdot 2^{n-1} = 2^n.$$

Resta provarmos que $\sqrt{p_{n+1}} \notin E_n$.