MAT0231 - Álgebra II para Licenciatura

Prova P3

1.- Mostre que o número real

$$\alpha = 119 + \sqrt[9871]{11} + 888\sqrt[9871]{11^{750}} + 333\sqrt[9871]{11^{5775}} + 999\sqrt[9871]{11^{8777}}$$

é algébrico sobre $\mathbb{Q}$ e que $\partial\,\mathrm{irr}(\alpha,\mathbb{Q}) \leq 9871$. **(1.5 pontos)**

Resposta:
O número real $\gamma := \sqrt[9871]{11}$ é algébrico sobre $\mathbb{Q}$ pois ele é raiz, por exemplo, do polinômio $p(x) = x^{9871} - 11 \in \mathbb{Q}[x]$. Por Eisenstein aplicado ao primo 11, obtemos então que $p(x)$ é irredutível sobre $\mathbb{Q}$ e portanto, $p(x) = \mathrm{irr}(\sqrt[9871]{11}, \mathbb{Q})$. Isso implica que $[\mathbb{Q}[\sqrt[9871]{11}] : \mathbb{Q}] = 9871$. Observa que α é uma combinação linear sobre $\mathbb{Q}$ de potências do elemento γ. Portanto $\alpha \in \mathbb{Q}[\sqrt[9871]{11}]$. Como a extensão de corpos $\mathbb{Q}[\sqrt[9871]{11}]$ de $\mathbb{Q}$ é finita temos que qualquer elemento de $\mathbb{Q}[\sqrt[9871]{11}]$ é algébrico sobre $\mathbb{Q}$. Assim α é algébrico sobre $\mathbb{Q}$ e o corpo $\mathbb{Q}[\alpha]$ é um subespaço de $\mathbb{Q}[\sqrt[9871]{11}]$ sobre $\mathbb{Q}$. Logo $[\mathbb{Q}[\alpha] : \mathbb{Q}] \leq 9871$. Como $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \partial\,\mathrm{irr}(\alpha, \mathbb{Q})$ obtemos o resultado desejado.

2.- Sejam $K \subset L$ uma extensão de corpos e $\alpha \in L$ algébrico sobre K. Mostre que se $[K[\alpha] : K]$ é um número ímpar, então $K[\alpha] = K[\alpha^2]$. **(1.5 pontos)**

Resposta:
O elemento $\alpha^2 \in K[\alpha]$ e portanto também é algébrico sobre K, $K[\alpha^2]$ é um corpo extensão de K e $K[\alpha^2] \subseteq K[\alpha]$. Assim estamos na situação $K \subseteq K[\alpha^2] \subseteq K[\alpha]$ e

$$[K[\alpha] : K] = [K[\alpha] : K[\alpha^2]] \cdot [K[\alpha^2] : K].$$

Como $\alpha^2 \in K[\alpha^2]$, temos que $\partial\,\mathrm{irr}(\alpha, K[\alpha^2]) \leq 2$ e portanto $[K[\alpha] : K[\alpha^2]] \leq 2$. Não pode ser 2 porque isso implicaria que 2 divide o número ímpar $[K[\alpha] : K]$. Logo $[K[\alpha] : K[\alpha^2]] = 1$. Isso implica que $K[\alpha] = K[\alpha^2]$.

3.- Seja γ uma raiz do polinômio $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ e considere o corpo $\mathbb{Z}_2[\gamma]$.

(a) Encontre $a, b, c \in \mathbb{Z}_2$ tais que

$$(\gamma^2 + \gamma)(\gamma^2 + 1) = a + b\gamma + c\gamma^2.$$

(b) Se δ for uma outra raiz de $f(x)$, acontece que $(\delta^2 + \delta)(\delta^2 + 1) = a + b\delta + c\delta^2$ para os mesmos a, b, c anteriores?

(1.5 pontos)

Resposta:

(a) Como γ é raiz de $x^3 + x^2 + 1$, temos que $\gamma^3 + \gamma^2 + 1 = 0$. Então temos que

$$(\gamma^2 + \gamma)(\gamma^2 + 1) = \gamma^4 + \gamma^3 + \gamma + \gamma^2 = \gamma(\gamma^3 + \gamma^2 + 1) + \gamma^2 = \gamma^2.$$

Logo temos que $a = b = \bar{0}$, $c = \bar{1}$.
Também poderíamos dividir $x^4 + x^3 + x^2 + x$ entre $x^3 + x^2 + 1$ e obteríamos

$$x^4 + x^3 + x^2 + x = x(x^3 + x^2 + 1) + x^2.$$

Isso implica que $\gamma^4 + \gamma^3 + \gamma^2 + \gamma = \gamma^2$. Lembra que $\frac{\mathbb{Z}_2[x]}{(x^3+x^2+1)\mathbb{Z}_2[x]} \cong \mathbb{Z}_2[\gamma]$, onde o isomorfismo leva $\overline{x} \mapsto \gamma$.

(b) Observa que $\delta^3 + \delta^2 + 1 = 0$, e portanto podemos fazer o mesmo que antes, obtendo que $(\delta^2 + \delta)(\delta^2 + 1) = \delta^2$. Logo os a, b, c são os mesmos que antes.

4.- Considere o polinômio $f(x) = x^7 - 11 \in \mathbb{Q}[x]$.

(a) Encontre $\beta, \xi \in \mathbb{C}$ tais que $\mathrm{Gal}(f(x), \mathbb{Q}) = \mathbb{Q}[\beta, \xi]$. **(1 ponto)**

(b) Calcule $[\mathrm{Gal}(f(x), \mathbb{Q}) \colon \mathbb{Q}]$. **(1.5 pontos)**

Resposta:

(a) Consideremos o número real $\beta = \sqrt[7]{11}$ e ξ uma raiz sétima primitiva da unidade. Por exemplo $\xi = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$. Então as raízes do polinômio $x^7 - 11$ são $\beta, \beta\xi, \beta\xi^2, \beta\xi^3, \beta\xi^4, \beta\xi^5, \beta\xi^6$. Logo por definição $\mathrm{Gal}(f(x), \mathbb{Q})$ é o corpo $\mathbb{Q}[\beta, \beta\xi, \beta\xi^2, \beta\xi^3, \beta\xi^4, \beta\xi^5, \beta\xi^6]$. Claramente temos a inclusão de corpos $\mathbb{Q}[\beta, \beta\xi, \beta\xi^2, \beta\xi^3, \beta\xi^4, \beta\xi^5, \beta\xi^6] \subseteq \mathbb{Q}[\beta, \xi]$ pois todos os elementos $\beta\xi^i$ pertencem ao corpo $\mathbb{Q}[\beta, \xi]$. Por outro lado, se um corpo contém $\beta, \beta\xi$, então ele contém também β^{-1} e $\beta^{-1}(\beta\xi) = \xi$. Isso implica que $\mathbb{Q}[\beta, \xi] \subseteq \mathbb{Q}[\beta, \beta\xi, \beta\xi^2, \beta\xi^3, \beta\xi^4, \beta\xi^5, \beta\xi^6]$ e portanto $\mathrm{Gal}(f(x), \mathbb{Q}) = \mathbb{Q}[\beta, \xi]$.

(b) Observa que

$$[\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}] = [\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}[\beta]] \cdot [\mathbb{Q}[\beta] \colon \mathbb{Q}]$$

e também

$$[\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}] = [\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}[\xi]] \cdot [\mathbb{Q}[\xi] \colon \mathbb{Q}].$$

Por outro lado $[\mathbb{Q}[\beta] \colon \mathbb{Q}] = 7$ pois o polinômio $x^7 - 11$ é irredutível sobre $\mathbb{Q}$ por Eisenstein aplicado ao primo 11 e assim $\mathrm{irr}(\beta, \mathbb{Q}) = x^7 - 11$. Por outro lado temos que $[\mathbb{Q}[\xi] \colon \mathbb{Q}] = 6$ pois como 7 é primo o polinômio $\mathrm{irr}(\xi, \mathbb{Q}) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Então isso, junto com o anterior, implica que $6 \mid [\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}]$ e $7 \mid [\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}]$ e portanto $42 \mid [\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}]$. Agora como, por exemplo, $[\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}[\beta]] \leq [\mathbb{Q}[\xi] \colon \mathbb{Q}]$, pois $\partial\,\mathrm{irr}(\xi, \mathbb{Q}[\beta]) \leq \partial\,\mathrm{irr}(\xi, \mathbb{Q})$, temos que $[\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}] \leq 42$. Tudo isso implica que $[\mathbb{Q}[\beta, \xi] \colon \mathbb{Q}] = 42$.

5.- Considere o corpo $K = \mathbb{Q}\left[\sqrt[3]{7}, \sqrt{2}\right]$.

(a) Calcule $[K \colon \mathbb{Q}]$. **(1.5 pontos)**

(b) Encontre uma base de K sobre $\mathbb{Q}$. **(1 ponto)**

(c) Calcule $\left[\mathbb{Q}\left[\sqrt[3]{7} + \sqrt{2}\right] \colon \mathbb{Q}\right]$. **(1.5 pontos)**

(d) Encontre $\mathrm{irr}\left(\sqrt[3]{7} + \sqrt{2}, \mathbb{Q}\right)$. **(1 ponto)**

Resposta:

(a)

$$[K \colon \mathbb{Q}] = [K \colon \mathbb{Q}[\sqrt[3]{7}]] \cdot [\mathbb{Q}[\sqrt[3]{7}] \colon \mathbb{Q}] = [K \colon \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] \colon \mathbb{Q}].$$

Por um lado temos que $[\mathbb{Q}[\sqrt[3]{7}] \colon \mathbb{Q}] = 3$ pois $\mathrm{irr}(\sqrt[3]{7}, \mathbb{Q}) = x^3 - 7$ já que o polinômio $x^3 - 7$ é irredutível sobre $\mathbb{Q}$ por Eisenstein aplicado ao primo 7. Por outro lado temos que $[\mathbb{Q}[\sqrt{2}] \colon \mathbb{Q}] = 2$ pois $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ já que o polinômio $x^2 - 2$ é irredutível sobre $\mathbb{Q}$ por Eisenstein aplicado ao primo 2. Assim temos que $3 \mid [K \colon \mathbb{Q}]$ e $2 \mid [K \colon \mathbb{Q}]$ e portanto $6 \mid [K \colon \mathbb{Q}]$.
Agora podemos argumentar como no exercício 4(b) ou da seguinte forma: como $[\mathbb{Q}[\sqrt[3]{7}] \colon \mathbb{Q}]$ e $[\mathbb{Q}[\sqrt{2}] \colon \mathbb{Q}]$ tem máximo divisor comum igual a 1, então $[\mathbb{Q}[\sqrt[3]{7}, \sqrt{2}] \colon \mathbb{Q}[\sqrt{2}]] = 3$ e portanto $[K \colon \mathbb{Q}] = 3 \cdot 2 = 6$.

(b) Uma base de $\mathbb{Q}[\sqrt{2}]$ sobre $\mathbb{Q}$ é $\{1, \sqrt{2}\}$. Uma base de $\mathbb{Q}[\sqrt{2}, \sqrt[3]{7}]$ sobre $\mathbb{Q}[\sqrt{2}]$ é $\{1, \sqrt[3]{7}, \sqrt[3]{7^2}\}$ pois observa que o anterior implica que $[\mathbb{Q}[\sqrt{2}, \sqrt[3]{7}] : \mathbb{Q}[\sqrt{2}]] = 3$. Portanto uma base de $[K \colon \mathbb{Q}]$ é o conjunto obtido como produto dos elementos das duas bases. Assim uma base $\mathcal{B}$ de K sobre $\mathbb{Q}$ é

$$1, \sqrt{2}, \sqrt[3]{7}, \sqrt[3]{7^2}, \sqrt{2}\sqrt[3]{7}, \sqrt{2}\sqrt[3]{7^2} = ()_{\mathcal{B}}.$$

(c) Temos que $\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}] \subseteq K$ e então $6 = [K\colon \mathbb{Q}] = [K\colon \mathbb{Q}[\sqrt[3]{7}+\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}]\colon \mathbb{Q}]$. Logo $[\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}]\colon \mathbb{Q}] = 1, 2, 3$ ou 6. Também sabemos que uma base de $\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}$ sobre $\mathbb{Q}$ é da forma $1, \sqrt[3]{7}+\sqrt{2}, (\sqrt[3]{7}+\sqrt{2})^2, \ldots, (\sqrt[3]{7}+\sqrt{2})^n$ onde $n = \operatorname{irr}(\sqrt[3]{7}+\sqrt{2}, \mathbb{Q})$. Consideremos os elementos $1, \sqrt[3]{7}+\sqrt{2}, (\sqrt[3]{7}+\sqrt{2})^2, (\sqrt[3]{7}+\sqrt{2})^3$ e expressemos eles em termos da base $\mathcal{B}$. Assim obtemos que $1 = (1,0,0,0,0,0)_{\mathcal{B}}$, $\sqrt[3]{7}+\sqrt{2} = (0,1,1,0,0,0)_{\mathcal{B}}$, $(\sqrt[3]{7}+\sqrt{2})^2 = 2+\sqrt[3]{7^2}+2\sqrt{2}\sqrt[3]{7} = (2,0,0,1,2,0)_{\mathcal{B}}$ e $(\sqrt[3]{7}+\sqrt{2})^3 = 7+2\sqrt{2}+6\sqrt[3]{7}+\sqrt{2}\sqrt[3]{7}+3\sqrt{2}\sqrt[3]{7^2} = (7,2,6,0,1,3)_{\mathcal{B}}$. Escalonando a matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 2 & 0 \\ 7 & 2 & 6 & 0 & 1 & 3 \end{pmatrix}$$

é fácil ver que esses quatro elementos de $\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}]$ são linearmente independentes sobre $\mathbb{Q}$. Isso implica que a dimensão de $\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}]$ sobre $\mathbb{Q}$ é pelo menos 4, e como as possibilidades eram $1, 2, 3, 6$ temos que $[\mathbb{Q}[\sqrt[3]{7}+\sqrt{2}\colon \mathbb{Q}] = 6$.

(d) Por um lado, se fazemos $\alpha = \sqrt[3]{7}+\sqrt{2}$, obtemos que $\alpha - \sqrt{2} = \sqrt[3]{7}$, e elevando ao cubo temos que $\alpha^3 + 6\alpha^{-}7 = 2 \cdot (2+3\alpha^2)$. Agora elevando ao quadrado obtemos que $\alpha^6 - 6\alpha^4 - 14\alpha^3 + 12\alpha^2 - 84\alpha + 41 = 0$. Logo $\sqrt[3]{7}+\sqrt{2}$ é raiz do polinômio $x^6 - 6x^4 - 14x^3 + 12x^2 - 84x + 41 \in \mathbb{Q}[x]$ que pode ser complicado provar que é irredutível em $\mathbb{Q}[x]$ com os métodos de irredutibilidade que conhecemos.
Mas, sabemos que $\operatorname{irr}(\sqrt[3]{7}+\sqrt{2}, \mathbb{Q})$ é mônico de grau 6 e que divide a qualquer polinômio de $\mathbb{Q}[x]$ do qual $\sqrt[3]{7}+\sqrt{2}$ seja raiz. Isso implica que $\operatorname{irr}(\sqrt[3]{7}+\sqrt{2}, \mathbb{Q}) = x^6 - 6x^4 - 14x^3 + 12x^2 - 84x + 41$.