DMat-FCTUC Exame de Corpos e Equações Algébricas

Duração: 2h30m 21/06/2019

Soluções

1. (a) V

   (b) V

   (c) V

2. (a) Pelo critério das raízes racionais de um polinómio de coeficientes inteiros, todas as raízes racionais do polinómio $p(x)$ indicado são inteiras e divisoras de 1. Portanto as únicas possibilidades são 1 e -1. Verifiquemos se alguma delas é de facto raiz:

   - n é par:

     $p(1) = (-1)^n 1^n + (-1)^{n-1}1^{n-1} + \cdots + 1^2 - 1 + 1 = \not{1} - \not{1} + \cdots + \not{1} - \not{1} + 1 = 1 \neq 0$

     $p(-1) = (-1)^n(-1)^n + (-1)^{n-1}(-1)^{n-1} + \cdots + (-1)^2 - (-1) + 1 = 1+1+\cdots+1+1+1 = n+1 \neq 0.$

   - n é ímpar:

     $p(1) = (-1)^n 1^n + (-1)^{n-1}1^{n-1} + \cdots + 1^2 - 1 + 1 = -\not{1} + \not{1} + \cdots - \not{1} + \not{1} - \not{1} + \not{1} = 0$

     $p(-1) = (-1)^n(-1)^n + (-1)^{n-1}(-1)^{n-1} + \cdots + (-1)^2 - (-1) + 1 = 1+1+\cdots+1+1+1 = n+1 \neq 0.$

   Em conclusão, se n é par, o polinómio não tem raízes racionais; se n é ímpar, tem uma única raiz racional, 1.

   (b) Não: Em primeiro lugar, como $(\sqrt{3}\ i)^2 = -3$, então $\sqrt{3}\ i$ é raiz de $x^2 + 3$, e este é claramente o polinómio mínimo de $\sqrt{3}\ i$ sobre os racionais. Portanto $[\mathbb{Q}(\sqrt{3}\ i)\colon \mathbb{Q}] = 2$. Assim, se $\sqrt{3}$ pertencesse a $\mathbb{Q}(\sqrt{3}\ i)$ teríamos

   $$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}\ i)$$

   e, consequentemente, pelo Teorema da Torre, $[\mathbb{Q}(\sqrt{3}\ i)\colon \mathbb{Q}(\sqrt{3})] = 1$, ou seja, $\mathbb{Q}(\sqrt{3}\ i) = \mathbb{Q}(\sqrt{3})$, um absurdo, pois $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$.

   (c) Sim: $\sqrt{18} = 3\sqrt{2}$ e $\sqrt{2} = \sqrt[4]{4} = (\sqrt[4]{2})^2 \in \mathbb{Q}(\sqrt[4]{2})$.

   (d) Sim: $x^3 - 2$ é o polinómio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, logo $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e

   $$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

   Denotemos $2 + \sqrt[3]{4}$ por θ. É evidente que $\theta \in \mathbb{Q}(\sqrt[3]{2})$, pelo que

   $$\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2}).$$

   Por outro lado, como $\theta - 2 = \sqrt[3]{4}$, então $(\theta - 2)^3 = 4$, ou seja, θ é raiz do polinómio $x^3 - 6x^2 + 12x - 12$. Como este polinómio é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein), é o polinómio mínimo de θ sobre $\mathbb{Q}$,o que mostra que também $[\mathbb{Q}(\theta) : \mathbb{Q}]$ é igual a 3.

   Concluindo, como $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$ e $\dim \mathbb{Q}(\theta) = \dim \mathbb{Q}(\sqrt[3]{2})$, as duas extensões coincidem.

(e) Sim: $f(x) = x^3 - 3x + 3$ é irredutível sobre $\mathbb{Q}$ (critério de Eisenstein: $p = 3$). Como $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ (pois $x^4 - 2$ é o polinómio mínimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}$) e o grau de $f(x)$ é um número maior do que 1 primo com $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$, podemos concluir por um resultado usado nas aulas que $f(x)$ não tem raízes em $\mathbb{Q}(\sqrt[4]{2})$. Como é de grau 3, pelo critério das raízes é de facto irredutível sobre $\mathbb{Q}(\sqrt[4]{2})$.

3. (a) As possíveis raízes racionais de $p(x)$ são $\pm 1, \pm 2$. Uma vez que 1 é de facto uma raiz, $x - 1$ é um divisor de $p(x)$. Fazendo a divisão obtemos

$$x^3 - x^2 + 2x - 2 = (x - 1)(x^2 + 2)$$

que é a factorização de $p(x)$ em factores irredutíveis sobre $\mathbb{Q}$ uma vez que $x^2 + 2$ é irredutível sobre $\mathbb{Q}$ (critério de Eisenstein $p = 2$).

(b) Da alínea anterior podemos concluir que

$$x^3 - x^2 + 2x - 2 = (x - 1)(x^2 + 2) = (x - 1)(x - i\sqrt{2})(x + i\sqrt{2}).$$

Portanto, $\mathbb{Q}(i\sqrt{2})$ é a extensão de decomposição de $p(x)$. Determinemo-la. Como $(\sqrt{2}\ i)^2 = -2$, então $\sqrt{2}\ i$ é raiz de $x^2 + 2$, e este é claramente o polinómio mínimo de $\sqrt{2}\ i$ sobre os racionais (critério de Eisenstein: $p = 2$). Portanto $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$ pelo que

$$\mathbb{Q}(i\sqrt{2}) = \{a + b\sqrt{2}\ i \mid a, b \in \mathbb{Q}\}.$$

(c) Uma vez que $\mathbb{Q}(i\sqrt{2})$ é a extensão de decomposição do polinómio, o grupo de Galois deste polinómio é o grupo $Gal(\mathbb{Q}(i\sqrt{2}), \mathbb{Q})$. O elemento $i\sqrt{2}$ tem polinómio mínimo x^2+2 sobre $\mathbb{Q}$. Uma vez que qualquer $\mathbb{Q}$-automorfismo $\Phi : \mathbb{Q}(i\sqrt{2}) \to \mathbb{Q}(i\sqrt{2})$ transforma necessariamente raízes deste polinómio em raízes do mesmo polinómio, só poderão existir no máximo dois $\mathbb{Q}$-automorfismos:

$$\begin{array}{rccc} \Phi_1 : & \mathbb{Q}(i\sqrt{2}) & \to & \mathbb{Q}(i\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & i\sqrt{2} & \mapsto & i\sqrt{2} \end{array} \quad \text{e} \quad \begin{array}{rccc} \Phi_2 : & \mathbb{Q}(i\sqrt{2}) & \to & \mathbb{Q}(i\sqrt{2}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & i\sqrt{2} & \mapsto & -i\sqrt{2}. \end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento $a + bi\sqrt{2}$ de $\mathbb{Q}(i\sqrt{2})$ em $a - bi\sqrt{2}$. Portanto, $Gal(\mathbb{Q}(i\sqrt{2}), \mathbb{Q}) = \{\Phi_1, \Phi_2\}$, onde

$$(\Phi_2 \circ \Phi_2)(a + bi\sqrt{2}) = \Phi_2(a - bi\sqrt{2}) = a + bi\sqrt{2} = \Phi_1(a + bi\sqrt{2}).$$

Portanto, a tabela deste grupo é:

$\circ$	Φ_1	Φ_2
Φ_1	Φ_1	Φ_2
Φ_2	Φ_2	Φ_1

4. (a) $\mathrm{Nuc}(f)$ é um ideal de A:

- $\mathrm{Nuc}(f) \neq \emptyset$ pois em qualquer homomorfismo de anéis, $f(0) = 0$, ou seja, $0 \in \mathrm{Nuc}(f)$.
- Sejam $a, b \in \mathrm{Nuc}(f)$. Então $f(a) = f(b) = 0$ logo $f(a-b) = f(a) - f(b) = 0 - 0 = 0$. Portanto, $a - b \in \mathrm{Nuc}(f)$.

- Sejam $a \in A$ e $b \in \text{Nuc}(f)$. Então $f(a \cdot b) = f(a) \cdot f(b) = f(a) \cdot 0 = 0$. Portanto, $a \cdot b \in \text{Nuc}(f)$.

Além disso, é primo:

- Sejam $a, b \in A$ tais que $a \cdot b \in \text{Nuc}(f)$. Então $0 = f(a \cdot b) = f(a) \cdot f(b) \in D$. Como D é um domínio, podemos concluir que necessariamente $f(a) = 0$ ou $f(b) = 0$, ou seja, $a \in \text{Nuc}(f)$ ou $b \in \text{Nuc}(f)$.

(b) Um corpo A só admite os ideais triviais A e $\{0\}$. De facto, se $I \neq \{0\}$ é um ideal de A, seja x um elemento em I diferente de 0. Então, pela definição de ideal, $1 = x \cdot x^{-1} \in I$ e, consequentemente, $a = 1 \cdot a \in I$ para qualquer $a \in A$. Logo $I = A$.

Agora, usando a alínea anterior, podemos concluir que $\text{Nuc}(f) = \{0\}$ ou $\text{Nuc}(f) = A$. Como por hipótese, f não é a aplicaçã nula, $\text{Nuc}(f) \neq A$ donde $\text{Nuc}(f) = \{0\}$ e f será a aplicação nula. De facto,

$$f(a) = f(b) \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a - b) = 0 \Leftrightarrow a - b \in \text{Nuc}(f) \Rightarrow a - b = 0 \Leftrightarrow a = b.$$

(c) Como f não é a aplicação nula, existe $x \in A$ tal que $f(x) = b \neq 0$. Então

$$f(1) \cdot b = f(1) \cdot f(x) = f(1 \cdot x) = f(x) = b = 1 \cdot b.$$

Como estamos num corpo e $b \neq 0$, a lei do corte é válida para b e podemos então concluir que $f(1) = 1$.

5. Ver os Apontamentos.
