DMat-FCTUC **2ª Frequência de Corpos e Equações Algébricas**

*Duração: 1h30m* 3/06/2019

# Soluções

1. (a) $\alpha$ é raiz de $x^4 - 2x - 2 \in \mathbb{Q}[x]$, que é mónico e irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 2$). Portanto, este é o polinómio mínimo de $\alpha$ sobre $\mathbb{Q}$. Logo $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, $\{1, \alpha, \alpha^2, \alpha^3\}$ é uma base do espaço vectorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ e

$$\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a, b, c, d \in \mathbb{Q}\}$$

(onde $\alpha^4 = 2\alpha + 2$).

(b) Determinemos primeiro o inverso de $\alpha^2 + 2$ em $\mathbb{Q}(\alpha)$. Pelo algoritmo de Euclides temos

$$\begin{aligned} x^4 - 2x - 2 &= (x^2 + 2)(x^2 - 2) + (2 - 2x) \\ x^2 + 2 &= (2 - 2x)\left(-\frac{x}{2} - \frac{1}{2}\right) + 3. \end{aligned}$$

Portanto, denotando $x^4 - 2x - 2$ por $p(x)$ e $x^2 + 2$ por $q(x)$, temos

$$\begin{aligned} 3 &= q(x) + \left(\frac{x}{2} + \frac{1}{2}\right)[p(x) - (x^2 - 2)q(x)] \\ \Leftrightarrow 3 &= q(x) + \left(\frac{x}{2} + \frac{1}{2}\right)p(x) - \left(\frac{x}{2} + \frac{1}{2}\right)(x^2 - 2)q(x) \\ \Leftrightarrow 1 &= \left[\frac{1 - \left(\frac{x}{2} + \frac{1}{2}\right)(x^2 - 2)}{3}\right] q(x) + \frac{\left(\frac{x}{2} + \frac{1}{2}\right)}{3} p(x). \end{aligned}$$

Como $\alpha$ é raiz de $p(x)$, então

$$(\alpha^2 + 2)^{-1} = q(\alpha)^{-1} = \frac{1 - \left(\frac{\alpha}{2} + \frac{1}{2}\right)(\alpha^2 - 2)}{3} = \frac{1}{3} - \left(\frac{\alpha}{6} + \frac{1}{6}\right)(\alpha^2 - 2) = \frac{2}{3} + \frac{\alpha}{3} - \frac{\alpha^2}{6} - \frac{\alpha^3}{6}.$$

Finalmente,

$$\frac{\alpha + 2}{\alpha^2 + 2} = (\alpha + 2)\left(\frac{2}{3} + \frac{\alpha}{3} - \frac{\alpha^2}{6} - \frac{\alpha^3}{6}\right) = \cdots = 1 + \alpha - \frac{1}{2}\alpha^3.$$

Alternativa: Uma vez que $\{1, \alpha, \alpha^2, \alpha^3\}$ é uma base do espaço vectorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$, existem escalares (racionais) únicos $a, b, c, d$ tais que

$$\frac{\alpha + 2}{\alpha^2 + 2} = a + b\alpha + c\alpha^2 + d\alpha^3.$$

Isto é equivalente a

$$\begin{aligned} \alpha + 2 &= a\alpha^2 + b\alpha^3 + c(\underbrace{2\alpha + 2}_{\alpha^4}) + d(\underbrace{2\alpha^2 + 2\alpha}_{\alpha^5}) + 2a + 2b\alpha + 2c\alpha^2 + 2d\alpha^3 \\ \Leftrightarrow (-2 + 2c + 2a) &+ \alpha(-1 + 2c + 2d + 2b) + \alpha^2(a + 2d + 2c) + \alpha^3(b + 2d) = 0. \end{aligned}$$

Finalmente, como $1, \alpha, \alpha^2, \alpha^3$ são vectores linearmente independentes, isto é ainda equivalente ao sistema de equações

$$\begin{cases} 2a + 2c = 2 \\ b + c + d = \frac{1}{2} \\ a + 2c + 2d = 0 \\ b + 2d = 0 \end{cases} \Leftrightarrow \cdots \Leftrightarrow \begin{cases} a = 1 \\ b = 1 \\ c = 0 \\ d = -\frac{1}{2} \end{cases}$$

Portanto,

$$\frac{\alpha + 2}{\alpha^2 + 2} = 1 + \alpha - \frac{1}{2}\alpha^3.$$

2. (a) Sim: $f(x) = x^3 - 3x + 3$ é irredutível sobre $\mathbb{Q}$ (critério de Eisenstein: $p = 3$). Como $[\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}] = 4$ (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 $[\mathbb{Q}(\sqrt[4]{2})\colon \mathbb{Q}]$, 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, é de facto irredutível sobre $\mathbb{Q}(\sqrt[4]{2})$.

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

   (c) Não: Em primeiro lugar, 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. Portanto $[\mathbb{Q}(\sqrt{2}\ i)\colon \mathbb{Q}] = 2$. Assim, se $\sqrt{2}$ pertencesse a $\mathbb{Q}(\sqrt{2}\ i)$ teríamos $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}\ i)$ e, consequentemente, pelo Teorema da Torre, $[\mathbb{Q}(\sqrt{2}\ i)\colon \mathbb{Q}(\sqrt{2})] = 1$, ou seja, $\mathbb{Q}(\sqrt{2}\ i) = \mathbb{Q}(\sqrt{2})$, um absurdo, pois $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$.

3. (a) Uma vez que $p(x)$ não tem raízes em $\mathbb{Z}_2$ (de facto, $0^2 + 0 + 1 = 1$ e $1^2 + 1 + 1 = 1$), $p(x)$ é o polinómio mínimo de $\theta$ sobre $\mathbb{Z}_2$. Assim, $[\mathbb{Z}_2(\theta)\colon \mathbb{Z}_2] = 2$ pelo que

$$\mathbb{Z}_2(\theta) = \{a + b\theta \mid a, b \in \mathbb{Z}_2\} = \{0, 1, \theta, 1 + \theta\}$$

onde $\theta^2 = 1 + \theta$ (pois $\theta$ é raiz de $p(x)$). Denotando o elemento $1 + \theta$ por $\delta$ obtemos imediatamente as tabelas da extensão $\mathbb{Z}_2(\theta)$:

| $+$ | $0$ | $1$ | $\theta$ | $\delta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\theta$ | $\delta$ |
| $1$ | $1$ | $0$ | $\delta$ | $\theta$ |
| $\theta$ | $\theta$ | $\delta$ | $0$ | $1$ |
| $\delta$ | $\delta$ | $\theta$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\theta$ | $\delta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\theta$ | $\delta$ |
| $\theta$ | $0$ | $\theta$ | $\delta$ | $1$ |
| $\delta$ | $0$ | $\delta$ | $1$ | $\theta$ |

Observe que $\delta$ é a outra raiz de $p(x)$ em $\mathbb{Z}_2(\theta)$ e, portanto,

$$p(x) = (x - \theta)(x - \delta) = (x + \theta)(x + \delta)$$

em $\mathbb{Z}_2(\theta)$.

Alternativa: Como provámos nas aulas,

$$\begin{aligned} \mathbb{Z}_2(\theta) \cong \frac{\mathbb{Z}_2[x]}{\langle p(x) \rangle} &= \{a_0 + a_1 x + \langle p(x) \rangle \mid a_0, a_1 \in \mathbb{Z}_2\} \\ &= \{0 + \langle p(x) \rangle, 1 + \langle p(x) \rangle, x + \langle p(x) \rangle, 1 + x + \langle p(x) \rangle\} \end{aligned}$$

é constituído pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em $\mathbb{Z}_2[x]$ por $p(x)$ (onde $\theta$ corresponde à classe $x + \langle p(x)\rangle$). Denotando $0 + \langle p(x)\rangle$ por 0, $1 + \langle p(x)\rangle$ por 1, $x + \langle p(x)\rangle$ por $\theta$ e $1 + x + \langle p(x)\rangle$ por $\delta$, obtemos exactamente as tabelas acima das operações de $\mathbb{Z}_2(\theta)$.

(b) Basta observar que $\Phi(a) = a$ para qualquer $a \in \mathbb{Q}$ (portanto, $\Phi$ é um prolongamento da função identidade em $\mathbb{Q}$) e que $\Phi(\theta) = 1 + \theta = \delta$ é a outra raiz de $p(x)$ em $\mathbb{Z}_2(\theta)$.

(c) O que fizemos na alínea (a) mostra que $\mathbb{Z}_2(\theta)$ é precisamente a extensão de decomposição de $p(x)$. Portanto,

$$\mathrm{Gal}(p(x), \mathbb{Z}_2) = \mathrm{Gal}(\mathbb{Z}_2(\theta), Z_2),$$

isto é, o grupo de Galois de $p(x)$ sobre $\mathbb{Z}_2$ é o grupo dos $\mathbb{Z}_2$-automorfismos de $\mathbb{Z}_2(\theta)$. Calculemo-los (claro que um deles será o $\Phi$ da alínea anterior): Como sabemos cada $\mathbb{Z}_2$-automorfismo

$$\varphi\colon \mathbb{Z}_2(\theta) \to \mathbb{Z}_2(\theta)$$

terá que satisfazer as condições $\varphi(a) = a$ (para qualquer $a \in \mathbb{Q}$) e $\varphi(\theta)$ igual a uma qualquer das raízes de $p(x)$ em $\mathbb{Z}_2(\theta)$. Portanto, $\varphi(\theta) = \theta$ ou $\varphi(\theta) = \delta = 1 + \theta$. Assim, $\varphi$ será a identidade ou o automorfismo $\Phi$ da alínea anterior. Concluindo, $\mathrm{Gal}(p(x), \mathbb{Z}_2)$ é o grupo $\{\mathrm{id}, \Phi\}$ (com a composição de funções), isomorfo a $S_2$.

(d) $\Phi(\theta) = \delta$ é raiz de $p(x)$ (que já observámos ser irredutível sobre $\mathbb{Z}_2$). Portanto, $p(x)$ é, além de polinómio mínimo de $\theta$, também o polinómio mínimo de $\Phi(\theta)$.

4. $[K\colon \mathbb{Q}] = 2$ implica $\mathbb{Q} \subset K$. Seja $\theta \in K \setminus \mathbb{Q}$. Uma vez que $\mathbb{Q} \subseteq \mathbb{Q}(\theta) \subseteq K$, então

$$2 = [K\colon \mathbb{Q}] = [K\colon \mathbb{Q}(\theta)][\mathbb{Q}(\theta)\colon \mathbb{Q}].$$

Como 2 é primo e $[\mathbb{Q}(\theta)\colon \mathbb{Q}] > 1$, necessariamente $[\mathbb{Q}(\theta)\colon \mathbb{Q}] = 2$ e $[K\colon \mathbb{Q}(\theta)] = 1$, isto é, $K = \mathbb{Q}(\theta)$. Portanto, $K$ é de facto uma extensão simples de $\mathbb{Q}$. Falta só mostrar que $\theta = \sqrt{a}$ para algum racional $a$, ou seja, $\theta^2 \in \mathbb{Q}$.

Como $2 = [\mathbb{Q}(\theta)\colon \mathbb{Q}]$ então o polinómio mínimo de $\theta$ sobre $\mathbb{Q}$ é de grau 2, da forma

$$x^2 + bx + c \in \mathbb{Q}[x].$$

Então, pela fórmula resolvente das equações do segundo grau,

$$\theta = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{ou} \quad \theta = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Daqui decorre que $(2\theta + b)^2 = b^2 - 4c \in \mathbb{Q}$. Como $\mathbb{Q}(\theta) = \mathbb{Q}(2\theta + b)$, fica provado que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a})$ onde $a = b^2 - 4c \in \mathbb{Q}$.