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

Duração: 1h30m 18/05/2023

Soluções

1. Uma vez que o polinómio é mónico, as possíveis raízes racionais de $p(x)$ são os divisores de 1. Verificando, observamos que, de facto, só 1 é raiz. Aplicando a regra de Ruffini ou fazendo a divisão directamente obtemos
$$p(x) = (x-1)(x^3 - x + 1).$$
Como 1 é raiz de multiplicidade um de $p(x)$, pois já não é raiz de $x^3 - x + 1$, este último polinómio não tem raízes racionais e, sendo de grau 3, é irredutível sobre $\mathbb{Q}$. Assim, $(x-1)(x^3 - x + 1)$ é a factorização de $p(x)$ em factores irredutíveis de $\mathbb{Q}[x]$.

2. Portanto θ é uma raiz de $x^3 - x + 1$. Como este polinómio é mónico e irredutível sobre $\mathbb{Q}$, será o polinómio mínimo de θ sobre $\mathbb{Q}$. Logo, a extensão $\mathbb{Q}(\theta)$ tem dimensão 3 sobre o corpo $\mathbb{Q}$ e a sua base é $\{1, \theta, \theta^2\}$. Assim,
$$\mathbb{Q}(\theta) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\}.$$

3. Resolvendo a equação $(a + b\theta + c\theta^2)(1 + \theta^2) = 1$ $(a, b, c \in \mathbb{Q})$, sabendo que $\theta^3 = \theta - 1$, obtemos
$$\begin{aligned} 0 &= a + b\theta + c\theta^2 + a\theta^2 + b\theta^3 + c\theta^4 - 1 = a + b\theta + c\theta^2 + a\theta^2 + b(\theta - 1) + c(\theta^2 - \theta) - 1 \\ &= (a - b - 1) + (2b - c)\theta + (a + 2c)\theta^2. \end{aligned}$$
Uma vez que $1, \theta, \theta^2$ são vectores linearmente independentes, teremos
$$\begin{cases} a - b - 1 = 0 \\ 2b - c = 0 \\ a + 2c = 0 \end{cases} \Leftrightarrow \begin{cases} b = a - 1 \\ 2a - 2 + \frac{a}{2} = 0 \\ c = -\frac{a}{2} \end{cases} \Leftrightarrow \begin{cases} b = -\frac{1}{5} \\ a = \frac{4}{5} \\ c = -\frac{2}{5} \end{cases}$$
Portanto, $\frac{4}{5} - \frac{1}{5}\theta - \frac{2}{5}\theta^2$ é o inverso de $\theta^2 + 1$ em $\mathbb{Q}(\theta)$.

4. Teremos que começar por obter um polinómio em $\mathbb{Q}[x]$ que tenha a raiz λ. Para isso, como $\lambda \in \mathbb{Q}(\theta)$ está num espaço de dimensão 3, os vectores $1, \lambda, \lambda^2, \lambda^3$ são linearmente dependentes, pelo que existirão racionais a, b, c tais que $a+b\lambda+c\lambda^2+\lambda^3 = 0$ e o polinómio $a+bx+cx^2+x^3$ terá raiz λ. Determinemo-los:
$$\begin{aligned} 0 &= a + b(\theta^2 + 1) + c(\theta^2 + 1)^2 + (\theta^2 + 1)^3 = a + b(\theta^2 + 1) + c(\theta^4 + 2\theta^2 + 1) + (\theta^6 + 3\theta^4 + 3\theta^2 + 1) \\ &= (a + b + c + 2) + (-c - 5)\theta + (b + 3c + 7)\theta^2 \end{aligned}$$
pelo que
$$\begin{cases} a + b + c + 2 = 0 \\ -c - 5 = 0 \\ b + 3c + 7 = 0 \end{cases} \Leftrightarrow \begin{cases} a + b = 3 \\ c = -5 \\ b = 8 \end{cases} \Leftrightarrow \begin{cases} a = -5 \\ c = -5 \\ b = 8 \end{cases}$$
Portanto λ é raiz do polinómio $x^3 - 5x^2 + 8x - 5$. Como é de grau 3 e não tem raízes em $\mathbb{Q}$ (nenhuma das possibilidades $\pm 1, \pm 5$ o é), este é o polinómio mínimo de λ sobre $\mathbb{Q}$ e $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 3$.

Sobre as extensões, é evidente que $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\theta)$ pois $\lambda = \theta^2 + 1 \in \mathbb{Q}(\theta)$. Por outro lado, como $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ (pela alínea 2) e $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 3$, necessariamente $[\mathbb{Q}(\theta) : \mathbb{Q}(\lambda)] = 1$, pelo Teorema da Torre, pelo que as extensões $\mathbb{Q}(\lambda)$ e $\mathbb{Q}(\theta)$ coincidem.

5. Uma vez que $q(x)$ tem a raiz 1, $q(x) = (x-1)q_2(x) = (x+1)(x^2+x+1)$. É evidente que x^2+x+1 é irredutível sobre $\mathbb{Z}_2$ (pois nem 0 nem 1 são raízes) pelo que, pelo Teorema de Kronecker,

$$L = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle \cong \mathbb{Z}_2(\alpha) = \{a+b\alpha \colon a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1+\alpha\}$$

pois x^2+x+1 é o polinómio mínimo de α sobre $\mathbb{Z}_2$. As operações de L são dadas pelas fórmulas $(a+b\alpha)+(c+d\alpha) = (a+c)+(b+d)\alpha$ e $(a+b\alpha)(c+d\alpha) = ac+(ad+bc)\alpha+bd\alpha^2 = (ac+bd)+(ad+bc+bd)\alpha$ (onde as operações nos coeficientes são as operações de $\mathbb{Z}_2$. Em L, x^2+x+1 já tem a raiz α. Claro que a outra raiz também está em L; não estando em $\mathbb{Z}_2$, terá que ser α ou $1+\alpha$; é fácil de verificar que é $1+\alpha$. Em conclusão, $q(x) = (x+1)(x+\alpha)(x+1+\alpha)$.

6. $\mathrm{Gal}(q(x), \mathbb{Z}_2) = \mathrm{Gal}(L, \mathbb{Z}_2) = \mathrm{Gal}(\mathbb{Z}_2(\alpha), \mathbb{Z}_2)$. Cada $\mathbb{Z}_2$-automorfismo de $\mathbb{Z}_2(\alpha)$, sendo um prolongamento da função $\mathrm{id}\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, terá que aplicar cada elemento de $\mathbb{Z}_2$ nele próprio; por outro lado, pelo teroema estudado nas aulas, terá que aplicar α numa raiz de x^2+x+1 em $\mathbb{Z}_2(\alpha)$. Assim, existem exactamente dois $\mathbb{Z}_2$-automorfismos de $\mathbb{Z}_2(\alpha)$, nomeadamente

$$\Phi_1\colon a \in \mathbb{Z}_2 \mapsto a,\ \alpha \mapsto \alpha; \qquad \Phi_2\colon a \in \mathbb{Z}_2 \mapsto a,\ \alpha \mapsto 1+\alpha.$$

Então $\Phi_1(a+b\alpha) = a+b\alpha$ enquanto $\Phi_2(a+b\alpha) = a+b(1+\alpha) = a+b+b\alpha$ e $\mathrm{Gal}(q(x), \mathbb{Z}_2) = (\{\Phi_1, \Phi_2\}, \circ) \cong \mathcal{S}_2$.

7. Pelo Teorema da Torre, $[\mathbb{Z}_2(\alpha,\beta) : \mathbb{Z}_2] = [\mathbb{Z}_2(\alpha,\beta) : \mathbb{Z}_2(\alpha)] \times [\mathbb{Z}_2(\alpha) : \mathbb{Z}_2]$. Pela alínea 5, $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 2$ sendo $\{1, \alpha\}$ a base da extensão $\mathbb{Z}_2(\alpha)$. Por outro lado, $[\mathbb{Z}_2(\alpha,\beta) : \mathbb{Z}_2(\alpha)] = 3$ pois $r(x)$ é o polinómio mínimo de β sobre $\mathbb{Z}_2(\alpha)$: como não tem raízes em $\mathbb{Z}_2$ é irredutível em $\mathbb{Z}_2$, e como tem coeficientes em $\mathbb{Z}_2$ e o seu grau é primo com a dimensão $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 2$, continua a não ter raízes em $\mathbb{Z}_2(\alpha)$, pelo que será também irredutível em $\mathbb{Z}_2(\alpha)$.

[Claro que aqui, como $\mathbb{Z}_2(\alpha)$ é um corpo muito pequeno, não era necessário argumentar desta maneira, bastava alternativamente verificar directamente que nem α nem $1+\alpha$ são raízes de $r(x)$.]

Em conclusão, $[\mathbb{Z}_2(\alpha,\beta) : \mathbb{Z}_2] = 6$, sendo $\{1, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$ uma base do espaço vectorial $\mathbb{Z}_2(\alpha,\beta)$ sobre o corpo $\mathbb{Z}_2$. Portanto,

$$\mathbb{Z}_2(\alpha,\beta) = \{a_1+a_2\alpha+a_3\beta+a_4\beta^2+a_5\alpha\beta+a_6\alpha\beta^2 \mid a_1,a_2,a_3,a_4,a_5,a_6 \in \mathbb{Z}_2\} \cong \mathbb{F}_{2^6}.$$

8. (a) Claro que $0 \in A_{\mathbb{Q}}$ e para quaisquer $x, y \in A_{\mathbb{Q}}$, $x-y, xy^{-1} \in \mathbb{Q}(x,y)$. Como x e y são algébricos sobre $\mathbb{Q}$, sabemos pelo Teorema da Torre que $[\mathbb{Q}(x,y)\colon \mathbb{Q}] < \infty$ pelo que a extensão $\mathbb{Q}(x,y)$ é algébrica, isto é, todos os elementos de $\mathbb{Q}(x,y)$ são algébricos sobre $\mathbb{Q}$. Portanto, $x-y, xy^{-1} \in A_{\mathbb{Q}}$.

   (b) $\Leftarrow$: A conclusão segue imediatamente da alínea anterior, uma vez que a, b e i são algébricos sobre $\mathbb{Q}$.

   $\Rightarrow$: Se $a+ib$ é algébrico sobre $\mathbb{Q}$ então é raiz de algum $p(x) \in \mathbb{Q}[x]$. Sabemos que então $a-ib$ também é raiz de $p(x)$ pelo que também é algébrico sobre $\mathbb{Q}$. Logo, pela alínea anterior, $\frac{1}{2}[(a+ib)+(a-ib)] = a$ também é algébrico sobre $\mathbb{Q}$. Aplicando novamente a alínea anterior, $i(a-(a+ib)) = b$ também é algébrico sobre $\mathbb{Q}$.