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

Duração: 1h30m 25/05/2018

Soluções

1. (a) θ é raiz de $p(x) = x^2 + 3x - 3 \in \mathbb{Q}[x]$, que é mónico e irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$). Portanto $p(x)$ é o polinómio mínimo de θ sobre $\mathbb{Q}$.

   (b) Quanto a θ^2:

   `[Método geral]` Como $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$, os elementos 1, θ^2 e θ^4 são linearmente dependentes pelo que existem escalares racionais não todos nulos, a_0, a_1, a_2 tais que $a_0 + a_1\theta^2 + a_2\theta^4 = 0$. Como queremos um polinómio mónico podemos supor $a_2 = 1$. Uma vez que $\theta^2 = -3\theta + 3$, podemos escrever então

$$\begin{aligned} 0 &= a_0 + a_1(-3\theta + 3) + (-3\theta + 3)^2 \\ &= a_0 + a_1(-3\theta + 3) + (9 - 18\theta + 9\theta^2) \\ &= a_0 - 3a_1\theta + 3a_1 + 9 - 18\theta + 9(-3\theta + 3) \\ &= a_0 + 3a_1 + 36 + (-3a_1 - 45)\theta. \end{aligned}$$

   Por sua vez $\{1, \theta\}$ constitui uma base de $\mathbb{Q}(\theta)$ donde

$$\begin{cases} a_0 + 3a_1 + 36 = 0 \\ 3a_1 + 45 = 0. \end{cases} \Leftrightarrow \begin{cases} a_0 = 9 \\ a_1 = -15. \end{cases}$$

   Concluímos que $9 - 15\theta^2 + \theta^4 = 0$, isto é, θ^2 é raiz do polinómio $x^2 - 15x + 9$. Este polinómio é mónico e irredutível sobre $\mathbb{Q}$ (as suas duas raízes, que podem ser calculadas pela fórmula resolvente, são irracionais) pelo que é o polinómio mínimo de θ^2 sobre $\mathbb{Q}$.
   `[Alternativa]` Se θ é raiz de $p(x) = x^2 + 3x - 3$ e $\theta^2 = -3\theta + 3$ (isto é, $\theta = \frac{\theta^2 - 3}{-3}$), então $0 = p(\theta) = p\left(\frac{\theta^2-3}{-3}\right)$. Portanto θ^2 é raiz de

$$p\left(\frac{x-3}{-3}\right) = \left(\frac{x-3}{-3}\right)^2 + 3\left(\frac{x-3}{-3}\right) - 3 = \cdots = x^2 - 15x + 9.$$

2. (a) Basta observar que o polinómio não tem raízes em $\mathbb{Z}_2$: $0^2 + 0 + 1 = 1$ e $1^2 + 1 + 1 = 1$.

   (b) Basta aplicar o algoritmo, fornecido pela demonstração do Teorema de Kronecker, ao polinómio $p(x)$.

   Seja então L a extensão

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

   constituída pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em $\mathbb{Z}_2[x]$ por $p(x)$. Denotando $0 + \langle p(x)\rangle$ por 0, $1 + \langle p(x)\rangle$ por 1, $x + \langle p(x)\rangle$ por α e $1 + x + \langle p(x)\rangle$ por β, as tabelas das operações de L são as seguintes:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

O Teorema garante-nos agora que α é uma raiz de $p(x)$. Portanto, em L já o polinómio $p(x)$ é redutível. De facto,

$$x^2 + x + 1 = (x - \alpha)(x - \beta).$$

Assim, L é a extensão de decomposição de $p(x)$.

3. (a) As possíveis raízes racionais de $q(x)$ são $\pm 1, \pm 2, \pm 4$. Verificando, confirma-se que -2 é a única.

   (b) Uma vez que $q(x) = (x + 2)r(x)$, fazendo a divisão obtemos $q(x) = (x + 2)(x^2 + 2)$. Portanto, θ é raiz de $x^2 + 2$, ou seja, $\theta \in \{\sqrt{2}i, -\sqrt{2}i\} \subseteq \mathbb{C}$. Pelo Teorema da Torre,

   $$[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})] \times 2$$

   pois $x^2 - 3$ é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$.

   Qual é o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{3})$? θ é raiz de $x^2 + 2 \in \mathbb{Q}[x]$. Será que este polinómio é irredutível sobre $\mathbb{Q}(\sqrt{3})$? Sim, pois as suas duas raízes não pertencem a $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, uma vez que são complexas. Portanto, $x^2 + 2$ é o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{3})$, pelo que $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})] = 2$, sendo $\{1, \theta\}$ uma base de $\mathbb{Q}(\sqrt{3}, \theta)$ sobre $\mathbb{Q}(\sqrt{3})$.

   Em conclusão, $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = 4$ e $\{1, \sqrt{3}, \theta, \sqrt{3}\,\theta\}$ constitui uma base de $\mathbb{Q}(\sqrt{3}, \theta)$ sobre $\mathbb{Q}$. Assim,

   $$\mathbb{Q}(\sqrt{3}, \theta) = \{a + b\sqrt{3} + c\theta + d\sqrt{3}\,\theta \mid a, b, c, d \in \mathbb{Q}\}.$$

   (c) Seja $L = \mathbb{Q}(\sqrt{3}, \theta)$. Teremos então que determinar todos os $\mathbb{Q}$-automorfismos de L.

   Cada $\mathbb{Q}$-automorfismo $\Phi\colon L \to L$ é completamente determinado pela sua acção no conjunto $\{\sqrt{3}, \theta\}$. A respectiva restrição $\Phi|_{\mathbb{Q}(\sqrt{3})}\colon \mathbb{Q}(\sqrt{3}) \to L$ é um homomorfismo injectivo que mantém fixos os elementos de $\mathbb{Q}$ (ou seja, é um prolongamento do isomorfismo $id\colon \mathbb{Q} \to \mathbb{Q}$). Estes podem ser determinados com o auxílio do resultado estudado nas aulas (Proposição 3.15):

   O elemento $\sqrt{3}$ tem polinómio mínimo $x^2 - 3$ sobre $\mathbb{Q}$, Então o isomorfismo $id\colon \mathbb{Q} \to \mathbb{Q}$ pode ser prolongado a um homomorfismo injectivo $\phi\colon \mathbb{Q}(\sqrt{3}) \to L$ se e só se $x^2 - 3$ tem uma raiz em L, e o número desses prolongamentos é igual ao número de raízes distintas de $x^2 - 3$ em L, ou seja dois:

   $$\begin{array}{rccc} \phi_1\colon & \mathbb{Q}(\sqrt{3}) & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \begin{array}{rccc} \phi_2\colon & \mathbb{Q}(\sqrt{3}) & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

   Estes são pois os únicos homomorfismos injectivos $\mathbb{Q}(\sqrt{3}) \to L$ que prolongam $id\colon \mathbb{Q} \to \mathbb{Q}$ e, consequentemente, os $\Phi\colon L \to L$ que procuramos, quando restritos a $\mathbb{Q}(\sqrt{3})$, coincidem necessariamente com um dos ϕ_i $(i = 1, 2)$. Dito de outro modo, claramente equivalente,

os $\Phi\colon L \to L$ que procuramos são os prolongamentos a L de cada um dos seguintes isomorfismos de corpos:

$$\begin{array}{rccc} \tilde{\phi}_1\colon & \mathbb{Q}(\sqrt{3}) & \to & \mathbb{Q}(\sqrt{3}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \begin{array}{rccc} \tilde{\phi}_2\colon & \mathbb{Q}(\sqrt{3}) & \to & \mathbb{Q}(\sqrt{3}) \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

$x^2+2 \in \mathbb{Q}[x]$ é o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{3})$. Como cada um dos $\tilde{\phi}_i$ mantém fixos os coeficientes de x^2+2 e este polinómio tem duas raízes distintas em L, podemos concluir que cada um dos isomorfismos $\tilde{\phi}_i$ vai ter dois prolongamentos a homomorfismos injectivos de extensões $L \to L$, um que transforma θ em θ e o outro transforma θ na outra raiz $-\theta$.

Começando com $\tilde{\phi}_1$

$$\begin{array}{ccccc} & & L & \overset{\Phi=?}{\dashrightarrow} & L \\ & & \uparrow & & \uparrow \\ \boxed{x^2+2} & & \mathbb{Q}(\sqrt{3}) & \xrightarrow{\tilde{\phi}_1 = id} & \mathbb{Q}(\sqrt{3}) \qquad \boxed{x^2+2} \end{array}$$

obtemos

$$\begin{array}{rccc} \Phi_1\colon & L & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & \sqrt{3} \\ & \theta & \mapsto & \theta \end{array} \qquad \begin{array}{rccc} \Phi_2\colon & L & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & \sqrt{3} \\ & \theta & \mapsto & -\theta. \end{array}$$

Φ_1 é simplesmente a identidade e Φ_2 é o isomorfismo definido por

$$a_0 + a_1\sqrt{3} + a_2\theta + a_3\sqrt{3}\theta \;\mapsto\; a_0 + a_1\sqrt{3} - a_2\theta - a_3\sqrt{3}\theta.$$

Fazendo o mesmo para $\tilde{\phi}_2$ obtemos

$$\begin{array}{rccc} \Phi_3\colon & L & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & -\sqrt{3} \\ & \theta & \mapsto & \theta \end{array} \qquad \begin{array}{rccc} \Phi_4\colon & L & \to & L \\ & a \in \mathbb{Q} & \mapsto & a \\ & \sqrt{3} & \mapsto & -\sqrt{3} \\ & \theta & \mapsto & -\theta \end{array}$$

Portanto, $Gal(\mathbb{Q}(\sqrt{3},\theta),\mathbb{Q}) = \{\mathrm{id}, \Phi_2, \Phi_3, \Phi_4\}$.

(d) Uma vez que a operação do grupo de Galois é a composição de funções obtemos:

$\circ$	id	Φ_2	Φ_3	Φ_4
id	id	Φ_2	Φ_3	Φ_4
Φ_2	Φ_2	id	Φ_4	Φ_3
Φ_3	Φ_3	Φ_4	id	Φ_2
Φ_4	Φ_4	Φ_3	Φ_2	id

(e) $Gal(\mathbb{Q}(\sqrt{3},\theta),\mathbb{Q})$ pode ser descrito como um subgrupo de $\mathcal{S}_4$:

$$\Phi_1 = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \theta & -\theta \\ \sqrt{3} & -\sqrt{3} & \theta & -\theta \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$$

$$\Phi_2 = \begin{pmatrix} \sqrt{3} & -\sqrt{3} & \theta & -\theta \\ \sqrt{3} & -\sqrt{3} & -\theta & \theta \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34)$$

$$\Phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12), \quad \Phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34).$$

Em conclusão:

$$\boxed{Gal(\mathbb{Q}(\sqrt{3},\theta),\mathbb{Q}) = \Big\{id, (12), (34), (12)(34)\Big\}}$$
