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

Duração: 1h30m 28/05/2021

Soluções

1. (a) As possíveis raízes racionais de $p(x)$ são os divisors de 4. Verificando, observamos que, de facto, -1 e 2 são raízes. Dividindo $p(x)$ por $(x+1)(x-2)$ obtemos

$$p(x) = (x+1)(x-2)(x^2-2x+2).$$

Como x^2-2x+2 é irredutível sobre $\mathbb{Q}$ (critério de Eisenstein com $p=2$), esta é a factorização de $p(x)$ em $\mathbb{Q}[x]$.

(b) Pela fórmula resolvente da equação de grau 2 podemos obter as duas raízes de x^2-2x+2, complexas conjugadas: $1 \pm i$. Assim, o corpo de decomposição de $p(x)$ é a menor extensão de $\mathbb{Q}$ que contém os números $-1, 2, 1+i, 1-i$, ou seja, $\mathbb{Q}(1+i, 1-i) = \mathbb{Q}(1+i)$, porque $1-i$ já pertence a $\mathbb{Q}(1+i)$. De facto, $2i = (1+i)^2 \in \mathbb{Q}(1+i)$, logo $i \in \mathbb{Q}(1+i)$, logo $1-i \in \mathbb{Q}(1+i)$.

Nota: Ainda podemos simplificar mais a apresentação do corpo: $\mathbb{Q}(1+i) = \mathbb{Q}(i)$ pois $i = 1+i-1 \in \mathbb{Q}(1+i)$ e $1+i \in \mathbb{Q}(i)$. Portanto, o corpo de decomposição de $p(x)$ é o corpo

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

(c) Pela alínea anterior, $\mathrm{Gal}(p(x), \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(i), \mathbb{Q})$. Calculemo-lo:

Seja Φ um $\mathbb{Q}$-automorfismo de $\mathbb{Q}(i)$. Por um lado, Φ é determinado pela sua imagem em i. Por outro lado, Φ é um prolongamento da função $\mathrm{id}\colon \mathbb{Q} \to \mathbb{Q}$ a $\mathbb{Q}(i)$. Como x^2+1 é o polinómio mínimo de i sobre $\mathbb{Q}$ então, por uma proposição estudada nas aulas, $\Phi(i)$ só pode tomar o valor de qualquer uma das raízes de x^2+1 em $\mathbb{Q}(i)$, ou seja, $\pm i$. Assim, o grupo $\mathrm{Gal}(\mathbb{Q}(i), \mathbb{Q})$ é formado pelos automofismos

$$\Phi_1\colon a+bi \mapsto a+bi \quad \text{e} \quad \Phi_2\colon a+bi \mapsto a-bi.$$

Uma vez que $p(x)$ tem 4 raízes distintas em $\mathbb{C}$, $\mathrm{Gal}(\mathbb{Q}(i), \mathbb{Q})$ pode ser apresentado como um subgrupo de S_4. Para isso, basta identificarmos as 4 raízes $-1, 2, 1+i, 1-i$ de $p(x)$ por 1,2,3,4 e observar como cada Φ actua nesse conjunto de raízes:

$$\Phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1), \quad \Phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34).$$

Assim, $\mathrm{Gal}(p(x), \mathbb{Q}) = \{(1), (34)\} \subseteq S_4$.

2. (a) Sim, como é evidente: π é raiz do polinómio $x^3 - \pi^3 \in \mathbb{Q}(\pi^3)[x]$.

[Números como este, para os quais existe uma sua potência que pertence a um corpo K, são sempre algébricos sobre K.]

(b) Pode observar logo de início que, sendo $\sqrt{6}\sqrt{10} = \sqrt{60} = 2\sqrt{15}$, então $\sqrt{15} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$ pelo que

$$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$$

e bastará calcular esta extensão dupla. Senão, acabará por descobrir isso no final da aplicação do Teorema da Torre:

$$[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}(\sqrt{6},\sqrt{10})]\,[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}(\sqrt{6})]\,[\mathbb{Q}(\sqrt{6}):\mathbb{Q}].$$

$[\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2$ pois x^2-6 é o polinómio mínimo de $\sqrt{6}$ sobre $\mathbb{Q}$.

Qual é o polinómio mínimo de $\sqrt{10}$ sobre $\mathbb{Q}(\sqrt{6}) = \{a+b\sqrt{6} \mid a,b \in \mathbb{Q}\}$? $\sqrt{10}$ é raiz de $x^2-10 \in \mathbb{Q}[x]$. Será que este polinómio é irredutível sobre $\mathbb{Q}(\sqrt{6})$? Sim, pois as suas duas raízes $\pm\sqrt{10} = \pm\sqrt{2}\,\sqrt{5}$ não pertencem a $\mathbb{Q}(\sqrt{6})$:

Com efeito, $\pm\sqrt{10} = a+b\sqrt{6}$ para algum par a,b de racionais implicaria $10 = a^2+6b^2+2ab\sqrt{6}$, ou seja, $\sqrt{6} = \frac{10-a^2-6b^2}{2ab} \in \mathbb{Q}$ (no caso $a,b \neq 0$) ou $10 = 6b^2$ (no caso $a=0$) ou $10 = a^2$ (no caso $b=0$), uma contradição, em qualquer um dos três casos.

Portanto, x^2-10 é o polinómio mínimo de $\sqrt{10}$ sobre $\mathbb{Q}(\sqrt{6})$, pelo que $[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}(\sqrt{6})] = 2$, sendo $\{1,\sqrt{10}\}$ uma base de $\mathbb{Q}(\sqrt{6},\sqrt{10})$ sobre $\mathbb{Q}(\sqrt{6})$. Consequentemente, $[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}] = 4$ e, pela demonstração do Teorema da Torre, $\{1,\sqrt{6},\sqrt{10},\sqrt{60}\} = \{1,\sqrt{2}\sqrt{3},\sqrt{2}\sqrt{5},2\sqrt{3}\sqrt{5}\}$ constitui uma base de $\mathbb{Q}(\sqrt{6},\sqrt{10})$ sobre $\mathbb{Q}$. Assim, $\mathbb{Q}(\sqrt{6},\sqrt{10}) = \{a+b\sqrt{6}+c\sqrt{10}+d\sqrt{15} \mid a,b,c,d \in \mathbb{Q}\}$. Finalmente, como $\sqrt{15} \in \mathbb{Q}(\sqrt{6},\sqrt{10})$ então $[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}(\sqrt{6},\sqrt{10})] = 1$. Em conclusão, $[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}] = 4$ e

$$\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) = \mathbb{Q}(\sqrt{6},\sqrt{10}) = \{a+b\sqrt{6}+c\sqrt{10}+d\sqrt{15} \mid a,b,c,d \in \mathbb{Q}\}.$$

3. (a) É óbvio que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ pois, evidentemente, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Quanto à inclusão recíproca, note que

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

Portanto, $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, logo $\sqrt{2}+\sqrt{3}+\sqrt{3}-\sqrt{2} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, pelo que $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Analogamente, $\sqrt{2}+\sqrt{3}-(\sqrt{3}-\sqrt{2}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ pelo que $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Solução alternativa: Temos a cadeia $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ e, de modo análogo ao exercício anterior, é evidente que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$. Bastará então mostrar que $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$ também é igual a 4. Para isso, denotemos $\sqrt{2}+\sqrt{3}$ por θ. Temos $\theta^2 = 5+2\sqrt{6}$ pelo que $(\theta^2-5)^2 = 24$, isto é, θ é raiz do polinómio x^4-10x^2+1. Teremos então que mostrar que este é o polinómio mínimo de θ sobre $\mathbb{Q}$.

Este polinómio não tem raízes racionais, pelo que a única possibilidade de não ser irredutível em $\mathbb{Q}$ é poder-se factorizar como produto de dois polinómios em $\mathbb{Q}$ de grau 2, $(x^2+ax+b)(x^2+cx+d)$. Mas, resolvendo o respectivo sistema de equações em $\mathbb{Q}$, pode concluir-se que é impossível.

Solução alternativa: Podemos evitar resolver esse sistema de equações fazendo $y = x^2$ e calculando explicitamente as raízes r_1,r_2,r_3,r_4 do polinómio x^4-10x^2+1:

$$y^2-10y+1 = 0 \Leftrightarrow y = \frac{10 \pm \sqrt{96}}{2} = 5 \pm 2\sqrt{6}$$

pelo que $r_1 = \sqrt{5+2\sqrt{6}}, r_2 = \sqrt{5-2\sqrt{6}}, r_3 = -\sqrt{5+2\sqrt{6}}, r_4 = -\sqrt{5-2\sqrt{6}}$ e $x^4-10x^2+1 = (x-r_1)(x-r_2)(x-r_3)(x-r_4)$. Uma vez que $(x-r_i)(x-r_j) = x^2+(-r_i-r_j)x+r_ir_j$ em nenhum caso terá coeficientes racionais, como é evidente, podemos então concluir que será impossível factorizar x^4-10x^2+1 na forma $(x^2+ax+b)(x^2+cx+d)$ em $\mathbb{Q}[x]$.

(b) Se $\theta = \sqrt{2+\sqrt{2}}$ pertencesse a $\mathbb{Q}(\sqrt{2})$ teríamos $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{2})$ o que implicaria $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Mas $\theta^2 - 2 = \sqrt{2}$ pelo que $(\theta^2-2)^2 = 2$, isto é, θ é raiz de $x^4 - 4x^2 + 2$. Trata-se de um polinómio irredutível sobre $\mathbb{Q}$ (critério de Eisenstein, $p = 2$) pelo que é o polinómio mínimo de θ sobre $\mathbb{Q}$, o que mostra que $[\mathbb{Q}(\sqrt{2+\sqrt{2}}) : \mathbb{Q}] = 4$.

Solução alternativa: Uma vez que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, bastará mostrar que não existem racionais a, b tais que $\sqrt{2+\sqrt{2}} = a + b\sqrt{2}$. Suponhamos, por contradição que existiam. Então, elevando ao quadrado e isolando os termos com $\sqrt{2}$ do lado esquerdo, teríamos

$$(1 - 2ab)\sqrt{2} = a^2 + 2b^2 - 1. \qquad (*)$$

Caso 1: $1 - 2ab \neq 0$. Neste caso, teríamos $\sqrt{2} = \frac{a^2+2b^2-1}{1-2ab} \in \mathbb{Q}$, um absurdo.

Caso 2: $1 - 2ab = 0$ (isto é, $2ab = 1$; em particular, $a, b \neq 0$). Neste caso, $(*)$ resume-se a $a^2 + 2b^2 - 1 = 0$, que, em conjunto com $2ab = 1$, nos dá $\frac{1}{4b^2} + 2b^2 = 1$, ou seja, $8b^4 - 4b^2 + 1 = 0$. Esta condição é também absurda pois o polinómio $8x^4 - 4x^2 + 1$ não tem raízes racionais, como é fácil de verificar.

[As possíveis raízes racionais são $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$; como o polinómio só tem termos de grau par, basta verificar nas positivas, nenhuma é! Ainda mais rápido: se b é raiz racional do polinómio então b^2 seria raiz racional do polinómio $8y^2 - 4y + 1$; mas as duas raízes deste polinómio são irracionais.]

4. Um corpo é primo se não contém nenhum subcorpo próprio. Vimos um resultado que nos diz que qualquer corpo primo é isomorfo a $\mathbb{Q}$ ou a algum $\mathbb{Z}_p$ (p primo). Basta então calcularmos $Aut(\mathbb{Q})$ e $Aut(\mathbb{Z}_p)$. O primeiro calculámo-lo nas últimas aulas:

   Seja $\Phi\colon \mathbb{Q} \to \mathbb{Q}$ um automorfismo. Como é um homomorfismo, então $\Phi(0) = 0$. Como Φ é injectivo, não pode ser a aplicação nula, logo $\Phi(1) = 1$ (como observámos nas aulas). Daqui segue então o seguinte:

   (a) $\Phi(-1) = -1$, pois $0 = \Phi(0) = \Phi(1-1) = \Phi(1) + \Phi(-1) = 1 + \Phi(-1)$.

   (b) Para cada inteiro a, $\Phi(a) = a$: se $a \geq 1$ então

   $$\Phi(a) = \Phi(\underbrace{1 + 1 + \cdots + 1}_{a \text{ vezes}}) = \Phi(1) + \Phi(1) + \cdots + \Phi(1) = 1 + 1 + \cdots + 1 = a$$

   e se $a \leq -1$ então $\Phi(a)$ é igual a

   $$\Phi(\underbrace{(-1) + (-1) + \cdots + (-1)}_{-a \text{ vezes}}) = \Phi(-1) + \Phi(-1) + \cdots + \Phi(-1) = (-1) + (-1) + \cdots + (-1) = a.$$

   (c) Para cada inteiro a, $\Phi(a^{-1}) = a^{-1}$. De facto, como $1 = \Phi(1) = \Phi(a \cdot a^{-1}) = \Phi(a)\Phi(a^{-1})$, então $\Phi(a^{-1}) = 1/\Phi(a) = 1/a$.

   (d) Finalmente, para cada racional $\frac{a}{b}$, $\Phi(\frac{a}{b}) = \Phi(a \cdot b^{-1}) = \Phi(a)\Phi(b^{-1}) = a \cdot b^{-1} = \frac{a}{b}$.

   Em conclusão, Φ é a aplicação identidade pelo que $Aut(\mathbb{Q}) = \{\mathrm{id}\}$.

   Fazendo uma analise análoga para $\Phi\colon \mathbb{Z}_p \to \mathbb{Z}_p$ (basta nesse caso ir até à primeira parte de (b)), conclui-se também que $Aut(\mathbb{Z}_p) = \{\mathrm{id}\}$, pelo que ambos os grupos são o grupo trivial só com o elemento neutro.