Soluções

1. 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 α é uma raiz de $x^3 - x + 1$. Como este polinómio é mónico e irredutível sobre $\mathbb{Q}$, será o polinómio mínimo de α sobre $\mathbb{Q}$.

3. Pela alínea anterior, a extensão $\mathbb{Q}(\alpha)$ tem dimensão 3 sobre o corpo $\mathbb{Q}$ e a sua base é $\{1, \alpha, \alpha^2\}$. Assim,

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

4. Uma vez que $\alpha^3 - \alpha + 1 = 0$ então $1 = \alpha - \alpha^3 = \alpha(1 - \alpha^2)$. Portanto, $1 - \alpha^2$ é o inverso de α em $\mathbb{Q}(\alpha)$.

5. Uma vez que $t(x) \in \mathbb{Q}[x]$, não tem raízes racionais e o seu grau é um número primo com a dimensão de $\mathbb{Q}(\alpha)$, então continua a não ter raízes em $\mathbb{Q}(\alpha)$ (por um resultado provado nas aulas). Como é de grau 2, é então irredutível sobre $\mathbb{Q}(\alpha)$. Portanto, $t(x)$ é o polinómio mínimo de β sobre $\mathbb{Q}(\alpha)$.

6. Pelas alíneas anteripres, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$ sendo

$$\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

uma base do espaço vectorial $\mathbb{Q}(\alpha, \beta)$ sobre o corpo $\mathbb{Q}$. Logo

$$\mathbb{Q}(\alpha, \beta) = \{a_1 + a_2\alpha + a_3\alpha^2 + a_4\beta + a_5\alpha\beta + a_6\alpha^2\beta \mid a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{Q}\}.$$

7. $t(x)$ tem uma raiz em $\mathbb{Q}(\beta)$. Aplicando a regra de Ruffini ou fazendo a divisão directamente obtemos $t(x) = (x - \beta)(x + \beta + 1)$. É claro que $x + \beta + 1 \in \mathbb{Q}(\beta)[x]$ pelo que $\mathbb{Q}(\beta)$ é a extensão de decomposição de $t(x)$.

Solução alternativa: Pela fórmula resolvente da equação de grau 2 podemos obter as duas raízes de $x^2 + x + 1$, complexas conjugadas:

$$-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i.$$

Assim, o corpo de decomposição de $t(x)$ é a menor extensão de $\mathbb{Q}$ que contém os números $\frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2}i$, ou seja, $\mathbb{Q}(\frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2}i) = \mathbb{Q}(\frac{\sqrt{3}}{2}i) = \mathbb{Q}(\sqrt{3}\,i)$. Portanto, o corpo de decomposição de $t(x)$ é o corpo

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

8. Pela alínea anterior, $\mathrm{Gal}(t(x),\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\beta),\mathbb{Q})$. Calculemo-lo:

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

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

   Uma vez que $t(x)$ tem duas raízes distintas em $\mathbb{C}$, $\mathrm{Gal}(\mathbb{Q}(\beta),\mathbb{Q})$ pode ser apresentado como um subgrupo de S_2. Para isso, basta identificarmos as duas raízes $\beta, -1-\beta$ de $t(x)$ por 1,2 e observar como cada Φ actua nesse conjunto de raízes:

   $$\Phi_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1), \quad \Phi_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (12).$$

   Assim, $\mathrm{Gal}(t(x),\mathbb{Q}) = \{(1),(12)\} \cong S_2$.

9. $t(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ é irredutível sobre $\mathbb{Z}_2$, uma vez que não tem raízes em $\mathbb{Z}_2$. Pelo Teorema de Kronecker, $t(x)$ terá uma raiz na extensão

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

   constituída pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em $\mathbb{Z}_2[x]$ por $t(x)$.

   Denotando $0 + \langle t(x)\rangle$ por 0, $1 + \langle t(x)\rangle$ por 1, $x + \langle t(x)\rangle$ por a e $1 + x + \langle t(x)\rangle$ por b, as tabelas das operações de L são as seguintes:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

   Por exemplo,

   $$a + b = (x + \langle t(x)\rangle) + (1 + x + \langle t(x)\rangle) = 1 + \langle t(x)\rangle = 1$$

   e

   $$ab = x(1 + x) + \langle t(x)\rangle = x + x^2 + \langle t(x)\rangle = 1 + \langle t(x)\rangle = 1.$$

   O Teorema de Kronecker garante-nos ainda que a é uma raiz de $t(x)$. Portanto, em L já o polinómio $t(x)$ é redutível. De facto,

   $$x^2 + x + 1 = (x - a)(x - b).$$

   Em conclusão, L é a extensão de decomposição de $t(x)$ e $(x-a)(x-b)$ a sua factorização em factores lineares.

10. Da primeira alínea sabemos que $(x-1)(x^3-x+1)$ é a factorização de $p(x)$ em factores irredutíveis de $\mathbb{Q}[x]$. Como nos dizem que $p(x)$ tem pelo menos uma raiz não real, isso significa que o polinómio x^3-x+1 terá duas raízes não reais (conjugadas uma da outra) e uma raiz irracional. Seja θ esta última raiz. Aplicando a regra de Ruffini ou fazendo a divisão directamente obtemos

$$x^3-x+1=(x-\theta)(x^2+\theta x+\theta^2-1).$$

Como $\mathbb{Q}(\theta)\subseteq\mathbb{R}$ e as duas raízes de $x^2+\theta x+\theta^2-1$ não são reais então este último polinómio é irredutível sobre $\mathbb{Q}(\theta)$. Seja λ uma raiz de $x^2+\theta x+\theta^2-1$. É claro que $\mathbb{Q}(\theta,\lambda)$ será a extensão de decomposição de $p(x)$:

$$p(x)=(x-1)(x-\theta)(x-\lambda)(x+\theta+\lambda).$$

Além disso,

$$[\mathbb{Q}(\theta,\lambda):\mathbb{Q}]=[\mathbb{Q}(\theta,\lambda):\mathbb{Q}(\theta)]\times[\mathbb{Q}(\theta):\mathbb{Q}]=2\times 3=6.$$
