

# Soluções de exercícios

## Folha 3

**5(d).** *Determine o inverso de  $\theta^2 - 6\theta + 8$  na extensão simples  $\mathbb{Q}(\theta)$ , onde  $\theta \neq 0$  é tal que  $\theta^4 - 6\theta^3 + 9\theta^2 + 3\theta = 0$ .*

O polinómio  $x^4 - 6x^3 + 9x^2 + 3x = x(x^3 - 6x^2 + 9x + 3)$ , do qual  $\theta$  é raiz, é redutível sobre  $\mathbb{Q}$ . Como  $\theta \neq 0$ , então  $\theta$  é raiz do factor  $x^3 - 6x^2 + 9x + 3$ . Este polinómio é irreduzível sobre  $\mathbb{Q}$  (pelo critério de Eisenstein,  $p = 3$ ), logo é o polinómio mínimo  $m(x)$  de  $\theta$  sobre  $\mathbb{Q}$ . Seja  $f(x) = x^2 - 6x + 8$ . Uma vez que  $m(x) = xf(x) + x + 3$  e  $f(x) = (x - 9)(x + 3) + 35$  (o que confirma que  $\text{mdc}(m(x), f(x)) = 1$ ), então

$$35 = f(x) - (x - 9)(m(x) - xf(x)) = (x^2 - 9x + 1)f(x) - (x - 9)m(x),$$

ou seja,

$$1 = \frac{1}{35}[(x^2 - 9x + 1)f(x) - (x - 9)m(x)].$$

Substituindo  $x$  por  $\theta$  obtemos  $1 = \frac{1}{35}(\theta^2 - 9\theta + 1)f(\theta)$ , o que mostra que

$$(\theta^2 - 6\theta + 8)^{-1} = f(\theta)^{-1} = \frac{1}{35}(\theta^2 - 9\theta + 1).$$

**7(b).** *Determine o polinómio mínimo sobre  $\mathbb{Q}$  de  $\sqrt{3} + \sqrt{5}$ .*

Seja  $\theta = \sqrt{3} + \sqrt{5} \in \mathbb{R}$ . Como  $\theta^2 = 8 + 2\sqrt{15}$  então  $(\theta^2 - 8)^2 = 60$ . Assim  $\theta^4 - 16\theta^2 + 4 = 0$  pelo que  $\theta$  é raiz de  $x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$ . Este polinómio é irreduzível em  $\mathbb{Q}[x]$  e é assim o polinómio mínimo de  $\theta$  sobre  $\mathbb{Q}$ . De facto:

- Não tem raízes racionais: as únicas possibilidades são  $\pm 1, \pm 2, \pm 4$ , nenhuma o é.
- Portanto, a única possibilidade de ser redutível é factorizar-se na forma

$$x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + a'x + b').$$

Isto será possível precisamente se o sistema

$$\begin{cases} a + a' = 0 \\ b + aa' + b' = -16 \\ ab' + a'b = 0 \\ bb' = 4 \end{cases}$$

tiver solução em  $\mathbb{Q}$ . Resolvendo vem

$$\left\{ \begin{array}{l} a' = -a \\ \hline a(b' - b) = 0 \Leftrightarrow a = 0 \vee b' = b \\ \hline \end{array} \right.$$

O caso  $a = 0$  implica  $b + b' = -16$  e  $bb' = 4$ , ou seja,  $b^2 + 16b + 4 = 0$ , que não tem raízes racionais. Por outro lado, o caso  $b' = b$  implica  $b^2 = 4$ , ou seja,  $b = 2$  ou  $b = -2$ . Substituindo na segunda equação obtemos

$$-a^2 + 4 = -16 \Leftrightarrow a^2 = 20 \quad \text{ou} \quad -a^2 - 4 = -16 \Leftrightarrow a^2 = 12,$$

ambas impossíveis em  $\mathbb{Q}$ .

Em conclusão, o sistema é impossível.

**9.** *Seja  $L$  uma extensão finita de  $K$ . Prove que:*

- (a) *Se  $[L : K]$  é um número primo, então  $L$  é uma extensão simples de  $K$ .*
- (b) *Se  $\theta \in L$ , então o grau de  $\theta$  é um divisor de  $[L : K]$ . Conclua que se tem  $L = K(\theta)$  se e só se o grau de  $\theta$  coincidir com  $[L : K]$ .*
- (c) *Se  $f(x) \in K[x]$  é irredutível sobre  $K$  e o grau de  $f(x)$  é um número primo com  $[L : K]$  e maior do que 1, então  $f(x)$  não tem raízes em  $L$ .*

- (a) Se  $L$  é uma extensão finita de  $K$  todos os seus elementos são algébricos sobre  $K$ . Como  $[L : K] = p > 1$ , existe  $\theta \in L \setminus K$ . Pelo Teorema da Torre,

$$p = [L : K] = [L : K(\theta)][K(\theta) : K]. \quad (1)$$

Como  $\theta \notin K$ ,  $[K(\theta) : K] > 1$ . Mas  $p$  é primo, donde só pode ser  $[K(\theta) : K] = p$  e  $[L : K(\theta)] = 1$ . Esta última igualdade diz-nos que  $L = K(\theta)$ , pelo que  $L$  é uma extensão simples de  $K$ .

- (b) Como, por definição, o grau de  $\theta$  coincide com  $[K(\theta) : K]$ , por (1) este é um divisor de  $[L : K]$  e coincide com  $[L : K]$  se e só se  $[L : K(\theta)] = 1$ , ou seja,  $L = K(\theta)$ .
- (c) Suponhamos, por absurdo, que  $f(x)$  tinha uma raiz  $\theta$  em  $L$ . Seja  $m(x)$  o polinómio mónico associado a  $f(x)$ . Evidentemente, trata-se do polinómio mínimo de  $\theta$  sobre  $K$ . Portanto,  $[K(\theta) : K] = gr(f(x))$  seria um número primo com  $[L : K]$ , o que é absurdo por (1). Logo  $f(x)$  não tem raízes em  $L$ .

**11(e).** *Determine o grau sobre  $\mathbb{Q}$  e uma base da extensão  $\mathbb{Q}(\alpha, \beta)$ , onde  $\alpha^3 - \alpha + 1 = 0$  e  $\beta^2 - \beta = 1$ .*

Pelo Teorema da Torre,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Como  $x^3 - x + 1$  é irreduzível sobre  $\mathbb{Q}$  (pois não tem raízes racionais), trata-se do polinómio mínimo de  $\alpha$  sobre  $\mathbb{Q}$ . Assim,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$  e  $\{1, \alpha, \alpha^2\}$  é uma base desta extensão simples. Portanto,  $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$ . Por outro lado,  $\beta$  é raiz do polinómio  $f(x) = x^2 - x - 1$ . Será que este polinómio é irreduzível sobre  $\mathbb{Q}(\alpha)$ ? Sim, pelo exercício anterior (alínea (c)):  $f(x) \in \mathbb{Q}[x]$  é irreduzível sobre  $\mathbb{Q}$  e o seu grau é um número primo com  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  e maior do que 1, pelo que não tem raízes em  $\mathbb{Q}(\alpha)$ . Como é de grau 2 será irreduzível sobre  $\mathbb{Q}(\alpha)$ . Assim,  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$  e  $\{1, \beta\}$  é uma base desta extensão simples. Concluindo,  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$  e  $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$  é uma base da extensão dupla  $\mathbb{Q}(\alpha, \beta)$  de  $\mathbb{Q}$ .

**12.** *Determine para quais dos seguintes polinómios  $f(x) \in K[x]$  existem extensões  $K(\alpha)$  tais que  $f(x)$  é o polinómio mínimo de  $\alpha$ :*

$$(a) x^2 - 4, \quad K = \mathbb{Q}. \quad (b) x^3 + x + 2, \quad K = \mathbb{Z}_3. \quad (c) x^2 + 1, \quad K = \mathbb{Z}_5.$$

- (a) Como  $x^2 - 4$  é redutível sobre  $\mathbb{Q}$  (pois tem raízes racionais), não existe nenhuma extensão  $\mathbb{Q}(\alpha)$  tal que  $x^2 - 4$  é o polinómio mínimo de  $\alpha$ .
- (b)  $x^3 + x + 2$  também é redutível sobre  $\mathbb{Z}_3$  (pois tem raízes neste corpo), logo não existe nenhuma extensão  $\mathbb{Z}_3(\alpha)$  tal que  $x^3 + x + 2$  é o polinómio mínimo de  $\alpha$ .
- (c)  $x^2 + 1$  também é redutível sobre  $\mathbb{Z}_5$  (pois tem raízes neste corpo), logo não existe nenhuma extensão  $\mathbb{Z}_5(\alpha)$  tal que  $x^2 + 1$  é o polinómio mínimo de  $\alpha$ .

**13.** *Para cada uma das extensões de  $\mathbb{Q}$  indicadas averigúe se  $\theta$  gera a mesma extensão:*

$$(a) \theta = 2 + \sqrt[3]{4}, \quad \mathbb{Q}(\sqrt[3]{2}).$$

$$(b) \theta = \sqrt{2} + \sqrt{3}, \quad \mathbb{Q}(\sqrt{2}).$$

$$(c) \theta = u^2 + u + 1, \quad \mathbb{Q}(u), \text{ com } u^2 + 5u - 5 = 0.$$

(a)  $x^3 - 2$  é o polinómio mínimo de  $\sqrt[3]{2}$  sobre  $\mathbb{Q}$ , logo  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  e

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Então  $\theta \in \mathbb{Q}(\sqrt[3]{2})$ , pelo que  $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$ . Por outro lado, como  $\theta - 2 = \sqrt[3]{4}$ , então  $(\theta - 2)^3 = 4$ , ou seja,  $\theta$  é raiz do polinómio  $x^3 - 6x^2 + 12x - 12$ . Como este polinómio é irreduzível sobre  $\mathbb{Q}$  (pelo critério de Eisenstein), é o polinómio mínimo de  $\theta$  sobre  $\mathbb{Q}$ , o que mostra que também  $[\mathbb{Q}(\theta) : \mathbb{Q}]$  é igual a 3.

Concluindo, como  $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[3]{2})$  e  $\dim \mathbb{Q}(\theta) = \dim \mathbb{Q}(\sqrt[3]{2})$ , as duas extensões coincidem.

(b) Neste caso, as extensões são diferentes, pois  $\theta \notin \mathbb{Q}(\sqrt{2})$ . De facto,  $\theta = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})$  implicaria  $\sqrt{2} + \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ , ou seja,  $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ , o que é um absurdo, pois não existem racionais  $a$  e  $b$  tais que  $\sqrt{3} = a + b\sqrt{2}$ :  $b = 0$  implicaria  $\sqrt{3} \in \mathbb{Q}$ ;  $a = 0$  e  $b \neq 0$  implicariam  $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$  e  $a, b \neq 0$  implicariam  $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ !!!

(c) Claramente  $\theta \in \mathbb{Q}(u)$ , donde  $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(u)$ . Por outro lado,  $\theta = u^2 + u + 1 = 5 - 5u + u + 1 = 6 - 4u$ , ou seja,  $u = \frac{6-\theta}{4} \in \mathbb{Q}(\theta)$ , o que mostra que também  $\mathbb{Q}(\theta) \supseteq \mathbb{Q}(u)$ . Portanto as extensões coincidem.

**15.** *É possível, usando régua (não graduada) e compasso, construir o ponto*

$$\left( \sqrt{5\sqrt{2} - 3} + \sqrt{2 - \sqrt[3]{2}}, 0 \right)$$

*a partir dos pontos  $(0, 0)$  e  $(1, 0)$ ?*

Sejam  $\theta_1 = \sqrt{5\sqrt{2} - 3}$  e  $\theta_2 = \sqrt{2 - \sqrt[3]{2}}$ . É fácil de ver que  $\theta_1$  é raiz de  $p(x) = x^4 + 6x^2 - 41$  e  $\theta_2$  é raiz de  $q(x) = x^6 - 6x^4 + 12x^2 - 6 = 0$ . O polinómio  $q(x)$  é claramente irreduzível sobre  $\mathbb{Q}$  (pelo critério de Eisenstein) pelo que  $[\mathbb{Q}(\theta_2) : \mathbb{Q}] = 6$  e  $\theta_2$  não é construível a partir dos pontos  $(0, 0)$  e  $(1, 0)$ . Quanto ao polinómio  $p(x)$ , também é irreduzível sobre  $\mathbb{Q}$ , mas dá mais trabalho a verificar isso:

Não tem raízes racionais (as únicas possibilidades,  $\pm 1$  e  $\pm 41$ , claramente não o são). Assim, se fosse redutível, a única possibilidade de factorização seria como produto de dois polinómios de grau 2:

$$x^4 + 6x^2 - 41 = (ax^2 + bx + c)(a'x^2 + b'x + c').$$

Desenvolvendo esta igualdade chegaremos a um sistema de equações, impossível em  $\mathbb{Q}$ , o que confirma que  $p(x)$  é, de facto, irreduzível sobre  $\mathbb{Q}$ . Portanto,  $[\mathbb{Q}(\theta_1) : \mathbb{Q}] = 4$ . Como o recíproco do Teorema 3.8 não é verdadeiro (observação feita a

seguir à demonstração do Teorema) não podemos para já concluir da construtibilidade de  $\theta_1$  a partir dos pontos  $(0, 0)$  e  $(1, 0)$ . No entanto, o que afirmámos na Observação ao Teorema 3.8 dá-nos a resposta:  $\sqrt{5\sqrt{2}-3}$  é construível pois obtém-se dos números racionais 2, 3 e 5 por sucessivas aplicações das operações de subtração, multiplicação e raiz quadrada.

Concluindo,  $\theta_1 + \theta_2$  não é construível a partir dos pontos  $(0, 0)$  e  $(1, 0)$  (se fosse, como  $\theta_1$  é, também  $(\theta_1 + \theta_2) - \theta_1 = \theta_2$  seria).

**16.** *Seja  $p$  um inteiro primo positivo.*

- (a) *Determine a dimensão e uma base da extensão  $\mathbb{Q}(\sqrt{p + \sqrt{p}})$  de  $\mathbb{Q}$ .*
- (b) *Será possível construir o ponto  $(\sqrt{p + \sqrt{p}}, \sqrt{p + \sqrt{p}})$  a partir dos pontos  $(0, 0)$  e  $(1, 0)$  ?*
- (a) Denotemos o número  $\sqrt{p + \sqrt{p}}$  por  $\theta$ . Como  $\theta^2 = p + \sqrt{p}$ , então  $(\theta^2 - p)^2 = p$ , pelo que  $\theta$  é raiz do polinómio

$$q(x) = (x^2 - p)^2 - p = x^4 - 2px^2 + p(p - 1) \in \mathbb{Q}[x].$$

Pelo critério de Eisenstein,  $q(x)$  é irredutível sobre  $\mathbb{Q}$  (basta considerar o primo  $p$ ). Portanto,  $q(x)$  é o polinómio mínimo de  $\theta$  sobre  $\mathbb{Q}$ , pelo que  $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$  e  $\{1, \theta, \theta^2, \theta^3\}$  é uma base desta extensão.

- (b) Sim, pela Observação ao Teorema 3.8 (veja o exercício anterior).

**18.** *Considere o polinómio  $p(x) = 2x^7 + 12x^5 + 3x^3 + 6x + 6$  em  $\mathbb{Q}[x]$ .*

- (a) *Prove que  $p(x)$  tem uma raiz real  $\alpha$ .*
- (b) *Justifique se  $\alpha$  é ou não um real construível a partir dos racionais.*
- (a) Em  $\mathbb{C}[x]$ ,  $p(x)$  decompõe-se em 7 factores lineares (pois  $\mathbb{C}$  é um corpo algebricamente fechado) correspondentes às suas 7 raízes em  $\mathbb{C}$ . Além disso, como sabemos, as raízes complexas não reais aparecem aos pares. Então, como 7 é ímpar, uma das 7 raízes raízes é necessariamente real.
- (b) O polinómio  $p(x)$  é irredutível sobre  $\mathbb{Q}[x]$  (pelo critério de Eisenstein,  $p = 3$ ). Então o polinómio mínimo de  $\alpha$  sobre  $\mathbb{Q}$  é o polinómio mónico associado de  $p(x)$ , ou seja, o polinómio  $x^7 + 6x^5 + \frac{3}{2}x^3 + 3x + 3$ . Assim  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ . Como este número não é uma potência de 2, pelo critério algébrico estudado sobre a construtibilidade (por régua e compasso) de números, podemos concluir que  $\alpha$  não é construível a partir dos racionais.

**19.** Mostre que  $x^2 + 1$  é irredutível sobre  $\mathbb{Z}_3$ . Sendo  $u$  uma raiz deste polinómio determine o número de elementos de  $\mathbb{Z}_3(u)$  e as tabelas de adição e multiplicação.

Para mostrar a irredutibilidade basta verificar que nenhum elemento de  $\mathbb{Z}_3$  é raiz de  $x^2 + 1$ .

Pelo que vimos na página 69,

$$\mathbb{Z}_3(u) \cong \frac{\mathbb{Z}_3[x]}{\langle x^2 + 1 \rangle} = \{a_0 + a_1x + \langle x^2 + 1 \rangle \mid a_0, a_1 \in \mathbb{Z}_3\}.$$

Denotando  $0 + \langle x^2 + 1 \rangle$ ,  $1 + \langle x^2 + 1 \rangle$ ,  $2 + \langle x^2 + 1 \rangle$ ,  $x + \langle x^2 + 1 \rangle$ ,  $2x + \langle x^2 + 1 \rangle$ ,  $1 + x + \langle x^2 + 1 \rangle$ ,  $1 + 2x + \langle x^2 + 1 \rangle$ ,  $2 + x + \langle x^2 + 1 \rangle$  e  $2 + 2x + \langle x^2 + 1 \rangle$  por, respectivamente,  $0, 1, 2, u, a, b, c, d, f$ , as tabelas das operações são as seguintes:

+	0	1	2	$u$	$a$	$b$	$c$	$d$	$f$	·	0	1	2	$u$	$a$	$b$	$c$	$d$	$f$	
0	0	1	2	$u$	$a$	$b$	$c$	$d$	$f$	0	0	0	0	0	0	0	0	0	0	0
1	1	2	0	$b$	$c$	$d$	$f$	$u$	$a$	1	0	1	2	$u$	$a$	$b$	$c$	$d$	$f$	1
2	2	0	1	$d$	$f$	$u$	$a$	$b$	$c$	2	0	2	1	$a$	$u$	$f$	$d$	$c$	$b$	2
$u$	$u$	$b$	$d$	$a$	0	$c$	1	$f$	2	$u$	0	$u$	$a$	2	1	$d$	$b$	$f$	$c$	$u$
$a$	$a$	$c$	$f$	0	$u$	1	$b$	2	$d$	$a$	0	$a$	$u$	1	2	$c$	$f$	$b$	$d$	$a$
$b$	$b$	$d$	$u$	$c$	1	$f$	2	$a$	0	$b$	0	$b$	$f$	$d$	$c$	$a$	2	1	$u$	$b$
$c$	$c$	$f$	$a$	1	$b$	2	$d$	0	$u$	$c$	0	$c$	$d$	$b$	$f$	2	$u$	$a$	1	$c$
$d$	$d$	$u$	$b$	$f$	2	$a$	0	$c$	1	$d$	0	$d$	$c$	$f$	$b$	1	$a$	$u$	2	$d$
$f$	$f$	$a$	$c$	2	$d$	0	$u$	1	$b$	$f$	0	$f$	$b$	$c$	$d$	$u$	1	2	$a$	$f$

**21.** Considere o polinómio  $p(x) = 8x^3 - 6x - 1$  sobre  $\mathbb{Q}$ .

(a) Mostre que  $p(x)$  é irredutível sobre  $\mathbb{Q}$ .

(b) Construa uma extensão de decomposição de  $p(x)$  e determine a sua dimensão.

(a) As possíveis raízes racionais de  $p(x)$  são:  $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$ . Nenhuma delas é de facto uma raiz pelo que o polinómio, não tendo raízes em  $\mathbb{Q}$  e sendo de grau 3, é irredutível sobre  $\mathbb{Q}$ .

(b) Como  $p(x)$  é irredutível sobre  $\mathbb{Q}$ ,

$$\begin{aligned} \mathbb{Q}[x]/\langle p(x) \rangle &= \{a(x) + \langle p(x) \rangle \mid a(x) \in \mathbb{Q}[x]\} \\ &= \{a(x) + \langle p(x) \rangle \mid a(x) \in \mathbb{Q}[x], \text{gr}(a(x)) \leq 2\} \\ &\cong \mathbb{Q}(\theta), \end{aligned}$$

onde  $8\theta^3 - 6\theta - 1 = 0$ . Como  $x^3 - \frac{3}{4}x - \frac{1}{8}$  é o polinómio mínimo de  $\theta$  sobre  $\mathbb{Q}$ , então  $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$  pelo que

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

Nesta extensão já o polinómio  $8x^3 - 6x - 1$  tem uma raiz (precisamente o elemento  $\theta$ ) pelo que é redutível. Dividindo  $8x^3 - 6x - 1$  pelo factor  $x - \theta$  obtém-se:

$$8x^3 - 6x - 1 = (x - \theta)(8x^2 + 8\theta x + 8\theta^2 - 6).$$

Teremos agora que verificar se o factor  $8x^2 + 8\theta x + 8\theta^2 - 6$  é ou não redutível sobre  $\mathbb{Q}(\theta)$  para concluirmos se esta é ou não a extensão de decomposição do polinómio  $p(x)$ .

Trata-se de um polinómio de grau 2 pelo que bastará verificar se tem raízes em  $\mathbb{Q}(\theta)$ . Averiguemos então se existem racionais  $a, b, c$  tais que

$$8(a + b\theta + c\theta^2)^2 + 8\theta(a + b\theta + c\theta^2) + 8\theta^2 - 6 = 0.$$

Efectuando os cálculos obtemos

$$(8a^2 - 6) + (16ab + 8a)\theta + (8b^2 + 16ac + 8b + 8)\theta^2 + (16bc + 8c)\theta^3 + 8c^2\theta^4 = 0.$$

Mas  $8\theta^3 = 6\theta + 1$  (donde  $8\theta^4 = 6\theta^2 + \theta$ ) pelo que podemos ainda escrever

$$(8a^2 - 6 + 2bc + c) + (16ab + 8a + 12bc + 6c + c^2)\theta + (8b^2 + 16ac + 8b + 8 + 6c^2)\theta^2 = 0.$$

Então, como  $1, \theta$  e  $\theta^2$  são linearmente independentes, esta igualdade é equivalente ao sistema

$$\begin{cases} 8a^2 - 6 + 2bc + c = 0 \\ 16ab + 8a + 12bc + 6c + c^2 = 0 \\ 8b^2 + 16ac + 8b + 8 + 6c^2 = 0. \end{cases}$$

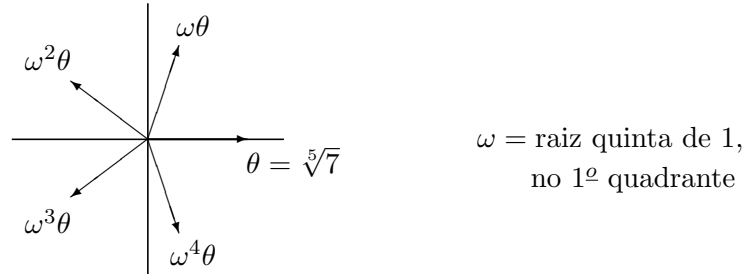
Este sistema não parece ser fácil de resolver. Tem no entanto uma solução fácil de encontrar após alguma procura e experimentação:  $a = 1, b = 0, c = -2$ . Isto mostra que o elemento  $1 - 2\theta^2$  de  $\mathbb{Q}(\theta)$  é uma raiz de  $p(x)$  pois é raiz do seu factor  $8x^2 + 8\theta x + 8\theta^2 - 6$ . Portanto este factor é divisível por  $x - (1 - 2\theta^2)$ . Efectuando a divisão obtemos  $8x^2 + 8\theta x + 8\theta^2 - 6 = (x - 1 + 2\theta^2)(8x + 8 + 8\theta - 16\theta^2)$ . Em conclusão,

$$\begin{aligned} 8x^3 - 6x - 1 &= (x - \theta)(8x^2 + 8\theta x + 8\theta^2 - 6) \\ &= 8(x - \theta)(x - 1 + 2\theta^2)(x + 1 + \theta - 2\theta^2) \\ &= 8(x - \theta)(x - (1 - 2\theta^2))(x - (-1 - \theta + 2\theta^2)) \end{aligned}$$

o que mostra que  $\theta, 1 - 2\theta^2$  e  $-1 - \theta + 2\theta^2$  são as três raízes de  $p(x)$  e que  $\mathbb{Q}(\theta)$  é de facto a sua extensão de decomposição (que tem dimensão 3).

**23.** Seja  $\theta$  a raiz real do polinómio  $x^5 - 7$ . Determine o grupo de Galois da extensão  $\mathbb{Q}(\theta)$  de  $\mathbb{Q}$ .

É claro que  $\theta = \sqrt[5]{7}$  (as outras 4 raízes não são reais):



Portanto,  $\theta$  tem polinómio mínimo  $x^5 - 7$  sobre  $\mathbb{Q}$ . Qualquer  $\mathbb{Q}$ -automorfismo de  $\mathbb{Q}(\theta)$

$$\Phi : \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta)$$

mantém fixos os números racionais e transforma  $\theta$  numa raiz do mesmo polinómio em  $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[5]{7}) \subseteq \mathbb{R}$ . Logo, necessariamente,  $\Phi(\theta) = \theta$  e só existe um  $\mathbb{Q}$ -automorfismo de  $\mathbb{Q}(\theta)$ :

$$\begin{aligned} \Phi : \mathbb{Q}(\sqrt[5]{7}) &\rightarrow \mathbb{Q}(\sqrt[5]{7}) \\ a \in \mathbb{Q} &\mapsto a \\ \sqrt[5]{7} &\mapsto \sqrt[5]{7} \end{aligned}$$

que é a identidade. Assim,  $\text{Gal}(\mathbb{Q}(\theta), \mathbb{Q})$  é o grupo trivial  $S_1 = \{id\}$ .

**24.** Seja  $L$  uma extensão de  $\mathbb{Q}$ . Determine os  $\mathbb{Q}$ -automorfismos de  $L$  para:

(a)  $L = \mathbb{Q}(\sqrt{2})$ .

(c)  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

(a) O elemento  $\sqrt{2}$  tem polinómio mínimo  $x^2 - 2$  sobre  $\mathbb{Q}$ . Pela Proposição 3.15, qualquer  $\mathbb{Q}$ -automorfismo  $\Phi : L \rightarrow L$  transforma raízes deste polinómio em raízes do mesmo polinómio. Existem, pois, precisamente dois  $\mathbb{Q}$ -automorfismos:

$$\begin{array}{ccc} \Phi_{\sqrt{2}} : \mathbb{Q}(\sqrt{2}) &\rightarrow \mathbb{Q}(\sqrt{2}) & \Phi_{-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) &\rightarrow \mathbb{Q}(\sqrt{2}) \\ a \in \mathbb{Q} &\mapsto a & a \in \mathbb{Q} &\mapsto a \\ \sqrt{2} &\mapsto \sqrt{2} & \sqrt{2} &\mapsto -\sqrt{2}. \end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento  $a + b\sqrt{2}$  de  $\mathbb{Q}(\sqrt{2})$  em  $a - b\sqrt{2}$ .



- (c) Cada  $\mathbb{Q}$ -automorfismo  $\Phi : L \rightarrow L$  é completamente determinado pela sua acção no conjunto  $\{\sqrt{2}, \sqrt{3}\}$ . A restrição  $\Phi|_{\mathbb{Q}(\sqrt{2})} : \mathbb{Q}(\sqrt{2}) \rightarrow L$  é um homomorfismo injectivo que mantém fixos os elementos de  $\mathbb{Q}$ . Então, pela Proposição 3.15, só há duas possibilidades para esta restrição, como vimos na alínea anterior: é a identidade ou aplica cada elemento  $a + b\sqrt{2}$  de  $\mathbb{Q}(\sqrt{2})$  em  $a - b\sqrt{2}$ . Portanto,  $\Phi$  prolonga o isomorfismo identidade de  $\mathbb{Q}(\sqrt{2})$  ou prolonga o isomorfismo  $\Phi_{-\sqrt{2}}$  de  $\mathbb{Q}(\sqrt{2})$ . Usando novamente a Proposição 3.15, como  $x^2 - 3$  é o polinómio mínimo de  $\sqrt{3}$  sobre  $\mathbb{Q}(\sqrt{2})$ , estes dois isomorfismos de  $\mathbb{Q}(\sqrt{2})$  só podem ser prolongados a  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  aplicando  $\sqrt{3}$  em  $\sqrt{3}$  ou  $-\sqrt{3}$ . Portanto, só existem 4 possibilidades para  $\Phi$ : a identidade e

$$\Phi(\sqrt{2}) = -\sqrt{2}, \quad \Phi(\sqrt{3}) = \sqrt{3};$$

$$\Phi(\sqrt{2}) = \sqrt{2}, \quad \Phi(\sqrt{3}) = -\sqrt{3};$$

$$\Phi(\sqrt{2}) = -\sqrt{2}, \quad \Phi(\sqrt{3}) = -\sqrt{3}.$$

O grupo de Galois tem, pois, neste caso, 4 elementos, que designamos respectivamente por  $\Phi_0, \Phi_1, \Phi_2, \Phi_3$ :

$$\Phi_0(a + b\sqrt{2} + c\sqrt{3}) = a + b\sqrt{2} + c\sqrt{3},$$

$$\Phi_1(a + b\sqrt{2} + c\sqrt{3}) = a - b\sqrt{2} + c\sqrt{3},$$

$$\Phi_2(a + b\sqrt{2} + c\sqrt{3}) = a + b\sqrt{2} - c\sqrt{3},$$

$$\Phi_3(a + b\sqrt{2} + c\sqrt{3}) = a - b\sqrt{2} - c\sqrt{3}.$$

## 25.

- (a) Para as extensões  $L$  de  $\mathbb{Q}$  do exercício anterior, calcule os respectivos grupos de Galois,  $Gal(L, \mathbb{Q})$ .
- (b) Verifique em quais desses casos a correspondência de Galois entre os subgrupos do grupo de Galois e as extensões intermédias (entre  $\mathbb{Q}$  e  $L$ ) é uma bijecção.
- (a) No primeiro caso,  $Gal(L, \mathbb{Q}) = \{id, \Phi_{-\sqrt{2}}\}$  é um grupo isomorfo a  $\mathbb{Z}_2$ .

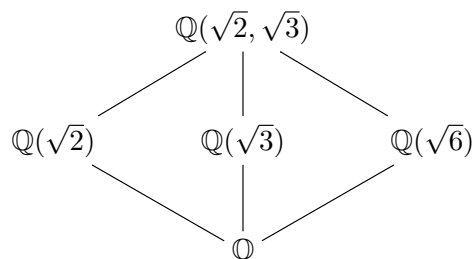
No terceiro caso, o grupo de Galois tem 4 elementos, sendo a tabela do grupo a seguinte:

$\circ$	$\Phi_0$	$\Phi_1$	$\Phi_2$	$\Phi_3$
$\Phi_0$	$\Phi_0$	$\Phi_1$	$\Phi_2$	$\Phi_3$
$\Phi_1$	$\Phi_1$	$\Phi_0$	$\Phi_3$	$\Phi_2$
$\Phi_2$	$\Phi_2$	$\Phi_3$	$\Phi_0$	$\Phi_1$
$\Phi_3$	$\Phi_3$	$\Phi_2$	$\Phi_1$	$\Phi_0$

Em conclusão, este grupo é isomorfo a  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

- (b) No primeiro caso, as extensões intermédias são só os próprios  $\mathbb{Q}$  e  $\mathbb{Q}(\sqrt{2})$ . Como  $\mathbb{Z}_2$  só tem os dois subgrupos triviais ( $\{0\}$  e o próprio  $\mathbb{Z}_2$ ), neste caso a correspondência de Galois é uma bijecção.

No segundo caso, o diagrama com as extensões intermédias é o seguinte:



A lista de subgrupos de  $\text{Gal}(L, \mathbb{Q})$  é  $\{\Phi_0\}$ ,  $\{\Phi_0, \Phi_1\}$ ,  $\{\Phi_0, \Phi_2\}$ ,  $\{\Phi_0, \Phi_3\}$ ,  $\{\Phi_0, \Phi_1, \Phi_2, \Phi_3\}$ . Neste caso, também há bijecção.

**26.** Considere a extensão  $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subseteq \mathbb{R}$  de  $\mathbb{Q}$ .

- (a) Como se define o grupo de Galois de  $L$  (sobre  $\mathbb{Q}$ )? Determine-o.  
 (b) Indique todas as extensões intermédias de  $\mathbb{Q}$  em  $L$ .  
 (c)  $L$  é uma extensão de Galois de  $\mathbb{Q}$ ? Justifique.

(a) Seja  $L = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ . Cada  $\Phi \in \text{Gal}(L, \mathbb{Q})$  é completamente determinado pela sua acção no conjunto  $\{\sqrt{3}, \sqrt[3]{2}\}$ . A restrição  $\Phi|_{\mathbb{Q}(\sqrt{3})} : \mathbb{Q}(\sqrt{3}) \rightarrow L$  é um homomorfismo injectivo que mantém fixos os elementos de  $\mathbb{Q}$ . Então, pela Proposição 3.15, só há duas possibilidades para esta restrição: é a identidade ou aplica cada elemento  $a + b\sqrt{3}$  de  $\mathbb{Q}(\sqrt{3})$  em  $a - b\sqrt{3}$ . Portanto,  $\Phi$  prolonga o isomorfismo identidade de  $\mathbb{Q}(\sqrt{3})$  ou prolonga o isomorfismo  $\Phi_{-\sqrt{3}}$  de  $\mathbb{Q}(\sqrt{3})$ . Pela Proposição 3.15, como  $x^3 - 2$  é o polinómio mínimo de  $\sqrt[3]{2}$  sobre  $\mathbb{Q}(\sqrt{3})$ , o número de prolongamentos de  $\Phi$  a  $L$  é igual ao número de raízes distintas de  $x^3 - 2$  em  $L$ , ou seja, um (que corresponde à única raiz  $\sqrt[3]{2}$ ). Assim, os dois isomorfismos de  $\mathbb{Q}(\sqrt{3})$  só podem ser prolongados a  $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$  aplicando  $\sqrt[3]{2}$  em  $\sqrt[3]{2}$ , pelo que existem exactamente duas possibilidades para  $\Phi$ : a identidade ou

$$\Phi(\sqrt{3}) = -\sqrt{3}, \quad \Phi(\sqrt[3]{2}) = \sqrt[3]{2}.$$

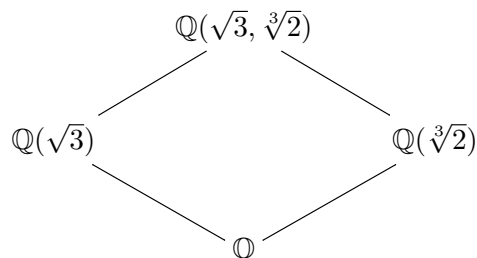
O grupo de Galois tem pois dois elementos:

$$\Phi_0(a + b\sqrt{3} + c\sqrt[3]{2}) = a + b\sqrt{3} + c\sqrt[3]{2},$$

$$\Phi_1(a + b\sqrt{3} + c\sqrt[3]{2}) = a - b\sqrt{3} + c\sqrt[3]{2}.$$

Neste caso,  $\text{Gal}(L, \mathbb{Q})$  é isomorfo a  $\mathbb{Z}_2$ .

(b) Note que  $\mathbb{Q}(\sqrt{3}\sqrt[3]{2}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ , pelo que as únicas extensões intermédias de  $\mathbb{Q}$  em  $L$  são:



(c) Não, pois  $[L : \mathbb{Q}] = 6$  mas  $|\text{Gal}(L, \mathbb{Q})| = 2$  (e pelo Teorema 3.21, se  $|\text{Gal}(L, K)|$  é diferente de  $[L : K]$ , então  $L$  não é uma extensão normal de  $K$ ).

**2\*.** Sejam  $\alpha^3 = 2$ ,  $w$  uma raiz cúbica da unidade e  $\beta = w\alpha$ . Determine a dimensão e uma base de  $\mathbb{Q}(\alpha, \beta)$  sobre  $\mathbb{Q}$ .

Pelo Teorema da Torre,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Como  $x^3 - 2$  é irreduzível sobre  $\mathbb{Q}$  (pelo critério de Eisenstein), trata-se do polinómio mínimo de  $\alpha$  sobre  $\mathbb{Q}$ . Assim,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$  e  $\{1, \alpha, \alpha^2\}$  é uma base desta extensão simples. Portanto,

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

Por outro lado,  $\beta$  é também raiz do polinómio  $f(x) = x^3 - 2$  (pois  $\beta^3 = w^3\alpha^3 = 2$ ). Será que este polinómio é irreduzível sobre  $\mathbb{Q}(\alpha)$ ? Mas agora este polinómio já é redutível sobre  $\mathbb{Q}(\alpha)$ , uma vez que  $\alpha$  é uma das suas raízes. Com efeito,  $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ . Agora dois casos podem ocorrer, ou  $\beta$  é raiz do primeiro factor, ou é raiz do segundo factor:

Caso 1:  $\beta = \alpha$ . Neste caso  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$  e o problema já está resolvido (a dimensão é 3 e a base é  $\{1, \alpha, \alpha^2\}$ ).

Caso 2:  $\beta \neq \alpha$ . Neste caso  $\beta$  é raiz de  $x^2 + \alpha x + \alpha^2$ . Agora, para indagarmos da sua irreduzibilidade sobre  $\mathbb{Q}(\alpha)$ , não podemos utilizar o Exercício 9(c), pois este polinómio não tem coeficientes racionais. Para verificarmos isso não temos outra hipótese senão investigar directamente se tem alguma raiz em  $\mathbb{Q}(\alpha)$ , ou seja, se existem racionais  $a, b$  e  $c$  tais que

$$(a + b\alpha + c\alpha^2)^2 + \alpha(a + b\alpha + c\alpha^2) + \alpha^2 = 0.$$

Efectuando os cálculos em  $\mathbb{Q}(\alpha)$ , esta equação é ainda equivalente a

$$(a^2 + 4bc + 2c) + (2ab + 2c^2 + a)\alpha + (2ac + b^2 + b + 1)\alpha^2 = 0.$$

Como  $\{1, \alpha, \alpha^2\}$  é uma base do espaço vectorial  $\mathbb{Q}(\alpha)$  (sobre  $\mathbb{Q}$ ), obtemos

$$\begin{cases} a^2 + 4bc + 2c = 0 \\ 2ab + 2c^2 + a = 0 \\ 2ac + b^2 + b + 1, \end{cases}$$

que é um sistema impossível em  $\mathbb{Q}$ :

Se  $a, c \neq 0$  então

$$\begin{cases} a^3 + 4abc + 2ac = 0 \\ 4abc + 4c^3 + 2ac = 0 \end{cases}$$

o que implica  $a^3 = 4c^3$ , ou seja,  $a/c = \sqrt[3]{4} \notin \mathbb{Q}!!!$ ; para  $a = 0$  ou  $c = 0$  temos  $b^2 + b + 1 = 0$ , o que é impossível em  $\mathbb{Q}$ .

Portanto,  $x^2 + \alpha x + \alpha^2$  é o polinómio mínimo de  $\beta$  sobre  $\mathbb{Q}(\alpha)$ . Concluindo,  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 6$  e  $\{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$  é uma base da extensão  $\mathbb{Q}(\alpha, \beta)$  de  $\mathbb{Q}$ .

Resolução alternativa, no Caso 2: Pela fórmula resolvente das equações de grau 2, as raízes de  $x^2 + \alpha x + \alpha^2$  são

$$\frac{-\alpha + \alpha i\sqrt{3}}{2} \quad \text{e} \quad \frac{-\alpha - \alpha i\sqrt{3}}{2}$$

que não pertencem a  $\mathbb{Q}(\alpha)$  pois não existem racionais  $a, b, c$  tais que  $\frac{-\alpha \pm \alpha i\sqrt{3}}{2} = a + b\alpha + c\alpha^2$ :

$$\begin{aligned} \frac{-\alpha \pm \alpha i\sqrt{3}}{2} = a + b\alpha + c\alpha^2 &\Leftrightarrow -2a + (-1 + i\sqrt{3} - 2b)\alpha + c\alpha^2 = 0 \\ &\Leftrightarrow a = 0, c = 0, i\sqrt{3}2b + 1 \in \mathbb{Q}!!! \end{aligned}$$

Portanto,  $x^2 + \alpha x + \alpha^2$  é o polinómio mínimo de  $\beta$  sobre  $\mathbb{Q}(\alpha)$ .

Outra resolução alternativa, no Caso 2: Como  $\beta$  é raiz de  $x^2 + \alpha x + \alpha^2$ , a outra raiz é  $\bar{\beta}$  e claro nenhuma pertence a  $\mathbb{Q}(\alpha)$ . Portanto,  $x^2 + \alpha x + \alpha^2$  é o polinómio mínimo de  $\beta$  sobre  $\mathbb{Q}(\alpha)$ .

**3\*.**

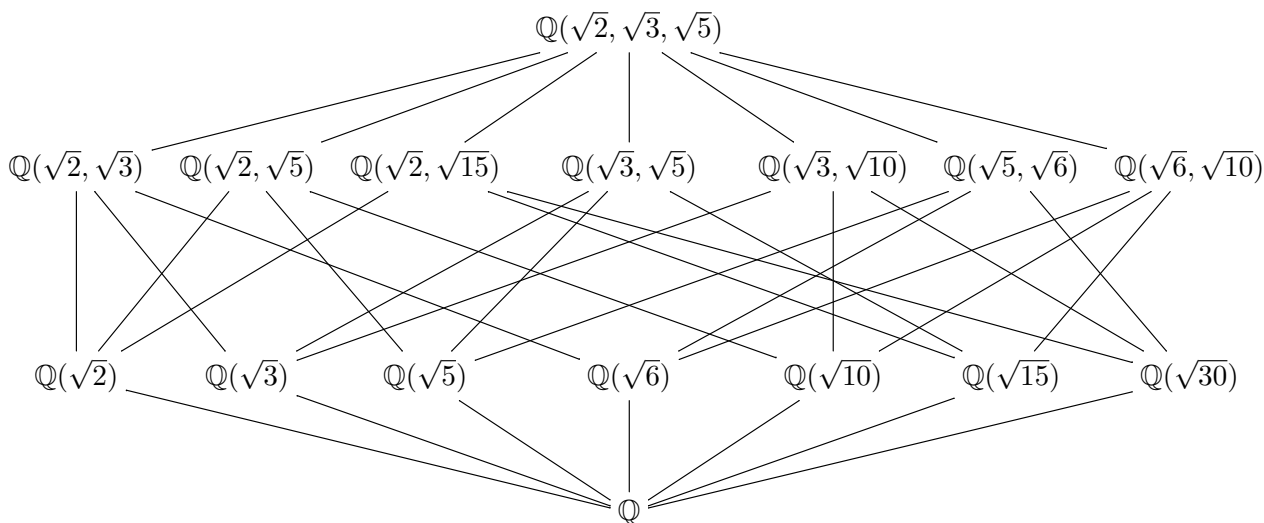
(a) *Determine os corpos intermédios entre  $\mathbb{Q}$  e  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ .*

(b) *Calcule o respectivo grupo de Galois e compare os resultados.*

(a) Como  $2 \times 3 \times 5 = 30$  tem como divisores 1, 2, 3, 5, 6, 10, 15 e 30, as extensões simples entre  $\mathbb{Q}$  e  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  são  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{3})$ ,  $\mathbb{Q}(\sqrt{5})$ ,  $\mathbb{Q}(\sqrt{6})$ ,  $\mathbb{Q}(\sqrt{10})$ ,  $\mathbb{Q}(\sqrt{15})$  e  $\mathbb{Q}(\sqrt{30})$ . Quanto às extensões duplas, temos:

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6}) \\ \mathbb{Q}(\sqrt{2}, \sqrt{5}) &= \mathbb{Q}(\sqrt{2}, \sqrt{10}) = \mathbb{Q}(\sqrt{5}, \sqrt{10}) \\ \mathbb{Q}(\sqrt{2}, \sqrt{15}) &= \mathbb{Q}(\sqrt{2}, \sqrt{30}) = \mathbb{Q}(\sqrt{15}, \sqrt{30}) \\ \mathbb{Q}(\sqrt{3}, \sqrt{5}) &= \mathbb{Q}(\sqrt{3}, \sqrt{15}) = \mathbb{Q}(\sqrt{5}, \sqrt{15}) \\ \mathbb{Q}(\sqrt{3}, \sqrt{10}) &= \mathbb{Q}(\sqrt{3}, \sqrt{30}) = \mathbb{Q}(\sqrt{10}, \sqrt{30}) \\ \mathbb{Q}(\sqrt{5}, \sqrt{6}) &= \mathbb{Q}(\sqrt{5}, \sqrt{30}) = \mathbb{Q}(\sqrt{6}, \sqrt{30}) \\ \mathbb{Q}(\sqrt{6}, \sqrt{10}) &= \mathbb{Q}(\sqrt{6}, \sqrt{15}) = \mathbb{Q}(\sqrt{10}, \sqrt{15}). \end{aligned}$$

O diagrama seguinte mostra-nos todas as extensões intermédias entre  $\mathbb{Q}$  e  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ :



(b) Neste caso,  $Gal(L, \mathbb{Q})$  é isomorfo a  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

**5\*.** Calcule o grupo de Galois do polinómio  $f(x) = x^4 - 2$  sobre o corpo  $\mathbb{Q}$ .

Uma vez que o polinómio  $f(x) = x^4 - 2$  tem raízes

$$\theta_1 = \sqrt[4]{2}, \theta_2 = -\sqrt[4]{2}, \theta_3 = \sqrt[4]{2}i, \theta_4 = -\sqrt[4]{2}i$$

então  $L = \mathbb{Q}(\sqrt[4]{2}, i)$  é a extensão de decomposição de  $f(x)$ . Portanto, o grupo pedido é o grupo  $Gal(L, \mathbb{Q}) = Gal(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q})$ . Teremos então que determinar todos os  $\mathbb{Q}$ -automorfismos de  $L$ .

Cada  $\mathbb{Q}$ -automorfismo  $\Phi : L \rightarrow L$  é completamente determinado pela sua acção no conjunto  $\{\sqrt[4]{2}, i\}$  (uma vez que todo o elemento de  $L$  é uma combinação linear

racional de potências de  $\sqrt[4]{2}$  e  $i$ ). A respectiva restrição  $\Phi|_{\mathbb{Q}(\sqrt[4]{2})} : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L$  é um homomorfismo injectivo que mantém fixos os elementos de  $\mathbb{Q}$  (ou seja, é um prolongamento do isomorfismo  $id : \mathbb{Q} \rightarrow \mathbb{Q}$ ). Estes podem ser determinados com o auxílio da Proposição 3.15:

O elemento  $\sqrt[4]{2}$  tem polinómio mínimo  $x^4 - 2$  sobre  $\mathbb{Q}$ , o que significa em particular que

$$\mathbb{Q}(\sqrt[4]{2}) = \{a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}.$$

Pela Proposição 3.15, o isomorfismo  $id : \mathbb{Q} \rightarrow \mathbb{Q}$  pode ser prolongado a um homomorfismo injectivo  $\phi : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L$  se e só se  $x^4 - 2$  tem uma raiz em  $L$ , e o número desses prolongamentos é igual ao número de raízes distintas de  $x^4 - 2$  em  $L$ , ou seja 4:

$$\begin{array}{ll} \phi_1 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L & \phi_2 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L \\ a \in \mathbb{Q} \mapsto a & a \in \mathbb{Q} \mapsto a \\ \sqrt[4]{2} \mapsto \theta_1 = \sqrt[4]{2} & \sqrt[4]{2} \mapsto \theta_2 = -\sqrt[4]{2} \end{array}$$

$$\begin{array}{ll} \phi_3 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L & \phi_4 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow L \\ a \in \mathbb{Q} \mapsto a & a \in \mathbb{Q} \mapsto a \\ \sqrt[4]{2} \mapsto \theta_3 = \sqrt[4]{2}i & \sqrt[4]{2} \mapsto \theta_4 = -\sqrt[4]{2}i. \end{array}$$

Estes são pois os únicos homomorfismos injectivos  $\mathbb{Q}(\sqrt[4]{2}) \rightarrow L$  que prolongam a  $id : \mathbb{Q} \rightarrow \mathbb{Q}$  e, conseqüentemente, os  $\Phi : L \rightarrow L$  que procuramos, quando restritos a  $\mathbb{Q}(\sqrt[4]{2})$ , coincidem necessariamente com um dos  $\phi_i$  ( $i = 1, 2, 3, 4$ ). Dito de outro modo, claramente equivalente, os  $\Phi : L \rightarrow L$  que procuramos são os prolongamentos a  $L$  de cada um dos seguintes isomorfismos de corpos:

$$\begin{array}{ll} \tilde{\phi}_1 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{Q}(\sqrt[4]{2}) & \tilde{\phi}_2 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{Q}(\sqrt[4]{2}) \\ a \in \mathbb{Q} \mapsto a & a \in \mathbb{Q} \mapsto a \\ \sqrt[4]{2} \mapsto \sqrt[4]{2} & \sqrt[4]{2} \mapsto -\sqrt[4]{2} \end{array}$$

$$\begin{array}{ll} \tilde{\phi}_3 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{Q}(\sqrt[4]{2}i) & \tilde{\phi}_4 : \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{Q}(\sqrt[4]{2}i) \\ a \in \mathbb{Q} \mapsto a & a \in \mathbb{Q} \mapsto a \\ \sqrt[4]{2} \mapsto \sqrt[4]{2}i & \sqrt[4]{2} \mapsto -\sqrt[4]{2}i. \end{array}$$

$x^2 + 1 \in \mathbb{Q}[x]$  é o polinómio mínimo de  $i$  sobre  $\mathbb{Q}(\sqrt[4]{2})$ . Usando novamente a Proposição 3.15, como cada um dos  $\tilde{\phi}_i$  mantém fixos os coeficientes de  $x^2 + 1$  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  $L \rightarrow L$ , um que transforma  $i$  em  $i$  e o outro transforma  $i$  na outra raiz  $-i$ .

Começando com  $\tilde{\phi}_1$

$$\begin{array}{ccccc}
 & & L & \overset{\Phi=?}{\dashrightarrow} & L \\
 & & \uparrow & & \uparrow \\
 \boxed{x^2 + 1} & & \mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\tilde{\phi}_1=id} & \mathbb{Q}(\sqrt[4]{2}) & \boxed{x^2 + 1}
 \end{array}$$

obtemos

$$\begin{array}{lcl}
 \Phi_1 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\
 & i & \mapsto i
 \end{array}
 \qquad
 \begin{array}{lcl}
 \Phi_2 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto \sqrt[4]{2} \\
 & i & \mapsto -i.
 \end{array}$$

$\Phi_1$  é simplesmente a identidade e  $\Phi_2$  é o isomorfismo definido por

$$\begin{array}{c}
 a_0 + a_1 \sqrt[4]{2} + a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} + a_4 i + a_5 \sqrt[4]{2} i + a_6 \sqrt[4]{4} i + a_7 \sqrt[4]{8} i \\
 \downarrow \\
 a_0 + a_1 \sqrt[4]{2} + a_2 \sqrt[4]{4} + a_3 \sqrt[4]{8} - a_4 i - a_5 \sqrt[4]{2} i - a_6 \sqrt[4]{4} i - a_7 \sqrt[4]{8} i.
 \end{array}$$

Fazendo o mesmo para  $\tilde{\phi}_2, \tilde{\phi}_3$  e  $\tilde{\phi}_4$  obtemos sucessivamente

$$\begin{array}{lcl}
 \Phi_3 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \\
 & i & \mapsto i
 \end{array}
 \qquad
 \begin{array}{lcl}
 \Phi_4 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \\
 & i & \mapsto -i
 \end{array}$$
  

$$\begin{array}{lcl}
 \Phi_5 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto \sqrt[4]{2} i \\
 & i & \mapsto i
 \end{array}
 \qquad
 \begin{array}{lcl}
 \Phi_6 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto \sqrt[4]{2} i \\
 & i & \mapsto -i
 \end{array}$$
  

$$\begin{array}{lcl}
 \Phi_7 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} i \\
 & i & \mapsto i
 \end{array}
 \qquad
 \begin{array}{lcl}
 \Phi_8 : & L & \rightarrow L \\
 & a \in \mathbb{Q} & \mapsto a \\
 & \sqrt[4]{2} & \mapsto -\sqrt[4]{2} i \\
 & i & \mapsto -i.
 \end{array}$$

Por exemplo,

$$\begin{aligned}\Phi_7(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} + a_4i + a_5\sqrt[4]{2}i + a_6\sqrt[4]{4}i + a_7\sqrt[4]{8}i) &= \\ &= a_0 - a_1\sqrt[4]{2}i - a_2\sqrt[4]{4} + a_3\sqrt[4]{8}i + a_4i + a_5\sqrt[4]{2} - a_6\sqrt[4]{4}i - a_7\sqrt[4]{8} \\ &= a_0 + a_5\sqrt[4]{2} - a_2\sqrt[4]{4} - a_7\sqrt[4]{8} + a_4i - a_1\sqrt[4]{2}i - a_6\sqrt[4]{4}i + a_3\sqrt[4]{8}i.\end{aligned}$$

Portanto,  $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}) = \{\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6, \Phi_7, \Phi_8\}$ . Observemos ainda como pode ser descrito como um subgrupo de  $\mathcal{S}_4$ :

$$\begin{aligned}\Phi_1 &= \begin{pmatrix} \theta_1 & \theta_2 & \theta_3 & \theta_4 \\ \theta_1 & \theta_2 & \theta_3 & \theta_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id \\ \Phi_2 &= \begin{pmatrix} \theta_1 & \theta_2 & \theta_3 & \theta_4 \\ \theta_1 & \theta_2 & \theta_4 & \theta_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34)\end{aligned}$$

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

$$\Phi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324), \quad \Phi_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$\Phi_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = (1423), \quad \Phi_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$

Em conclusão:

$$\boxed{\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}) = \{id, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}}$$

**6\*.** Considere um polinómio  $f(x)$  irredutível, de grau 3, escrito na sua forma reduzida  $x^3 + px + q$ , e as suas três raízes complexas distintas  $a, b, e c$ .

(a) Verifique que 
$$\begin{cases} a + b + c = 0 \\ ab + ac + bc = p \\ abc = -q. \end{cases}$$

(b) A partir da alínea anterior, mostre que  $((a-b)(a-c)(b-c))^2 = -4p^3 - 27q^2$ .

(c) Seja  $D$  o número  $-4p^3 - 27q^2$  da alínea anterior. Prove que se  $\sqrt{D} \in \mathbb{Q}$  e  $\Phi \in \text{Gal}(f(x), \mathbb{Q})$ , então  $\Phi(\sqrt{D}) = \sqrt{D}$  e, portanto,  $\text{Gal}(f(x), \mathbb{Q}) \cong A_3$ .



(d) Prove que se  $\sqrt{D} \notin \mathbb{Q}$ , então  $\mathbb{Q}(\sqrt{D})$  está na extensão de decomposição de  $f(x)$  e, portanto,  $\text{Gal}(f(x), \mathbb{Q}) \cong \mathcal{S}_3$ .

(a) Basta observar que  $x^3 + px + q = (x-a)(x-b)(x-c)$  é equivalente a  $x^3 + px + q = x^3 + (-c - a - b)x^2 + (ab + ac + bc)x - abc$ .

(b) Basta, com um pouco de paciência, desenvolver ambos os membros (substituindo, no segundo,  $p$  por  $ab + ac + bc$  e  $q$  por  $-abc$ ), até as expressões coincidirem.

(c) Pela Proposição 3.19,  $\text{Gal}(f(x), \mathbb{Q})$  é isomorfo a um subgrupo de  $\mathcal{S}_3$ . Seja  $\Phi \in \text{Gal}(f(x), \mathbb{Q}) = \text{Gal}(\mathbb{Q}(a, b, c), \mathbb{Q})$ . Por definição,  $\Phi$ , sendo um  $\mathbb{Q}$ -automorfismo, terá que preservar os racionais, logo  $\Phi(\sqrt{D}) = \sqrt{D}$ , isto é,  $\Phi((a-b)(a-c)(b-c)) = (a-b)(a-c)(b-c)$ . Consequentemente,

$$(\Phi(a) - \Phi(b))(\Phi(a) - \Phi(c))(\Phi(b) - \Phi(c)) = (a-b)(a-c)(b-c). \quad (2)$$

Mas  $\Phi$  permuta as raízes  $a$ ,  $b$  e  $c$  entre si. Para que se cumpra (2), essa permutação não pode ser ímpar (se fosse ímpar teríamos

$$(\Phi(a) - \Phi(b))(\Phi(a) - \Phi(c))(\Phi(b) - \Phi(c)) = -(a-b)(a-c)(b-c).$$

Sobram assim só as 3 permutações pares para eventual definição de  $\mathbb{Q}$ -automorfismos de  $\mathbb{Q}(a, b, c)$ . Não é difícil ver que todas elas definem de facto  $\mathbb{Q}$ -automorfismos de  $\mathbb{Q}(a, b, c)$ , pelo que  $\text{Gal}(\mathbb{Q}(a, b, c), \mathbb{Q}) \cong \mathcal{A}_3$ . Esta conclusão também se pode tirar do seguinte: como, pelo Teorema 3.21, se tem  $|\text{Gal}(\mathbb{Q}(a, b, c), \mathbb{Q})| = [\mathbb{Q}(a, b, c) : \mathbb{Q}]$ , bastará mostrar que  $[\mathbb{Q}(a, b, c) : \mathbb{Q}] \geq 3$ , o que é simples:

$$[\mathbb{Q}(a, b, c) : \mathbb{Q}] = [\mathbb{Q}(a, b, c) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] \geq 3,$$

pois  $[\mathbb{Q}(a) : \mathbb{Q}] = \text{gr}(f(x)) = 3$ .

(d) Neste caso, se  $\sqrt{D} \notin \mathbb{Q}$ , já  $\Phi(\sqrt{D})$  não precisa de ser igual a  $\sqrt{D}$ , e as permutações ímpares também definem elementos de  $\text{Gal}(\mathbb{Q}(a, b, c), \mathbb{Q})$ . Consequentemente,  $\text{Gal}(\mathbb{Q}(a, b, c), \mathbb{Q}) \cong \mathcal{S}_3$ .

**8\*(a).** Sejam  $p \geq 5$  um número primo, e  $f(x) \in \mathbb{Q}[x]$  um polinómio irredutível de grau  $p$ . Mostre que se  $f(x)$  tem exactamente duas raízes complexas não reais, então  $\text{Gal}(f(x), \mathbb{Q})$  é o grupo simétrico  $\mathcal{S}_p$  e portanto  $f(x)$  não é resolúvel por radicais.

Basta fazer o mesmo que na demonstração do Corolário 3.29 (Teorema de Abel-Ruffini).

**9\***. Mostre que os seguintes polinómios  $f(x) \in \mathbb{Q}[x]$  não são resolúveis por radicais:

(a)  $2x^5 - 10x + 5$ .

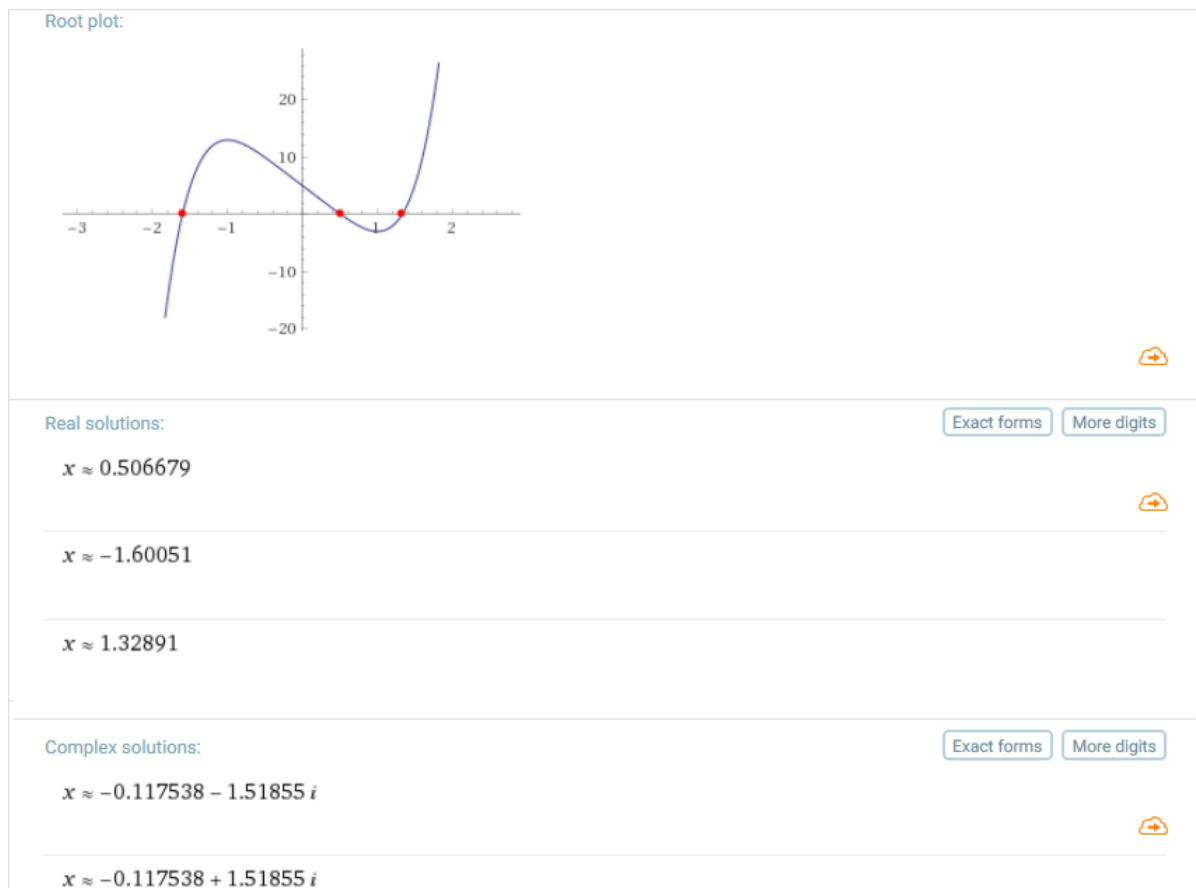
(c)  $x^5 - 6x^2 + 5$ .

(b)  $2x^5 - 5x^4 + 20$ .

(d)  $x^7 - 10x^5 + 15x + 5$ .

Fazendo o estudo e esboço das respectivas funções (ou, alternativamente, usando métodos da Matemática Numérica para localização de raízes, ou consultando o Wolfram Alpha ou algum software como o Mathematica ou Maple) não é difícil confirmar que:

(a) Este polinómio tem exactamente 2 raízes complexas não reais:



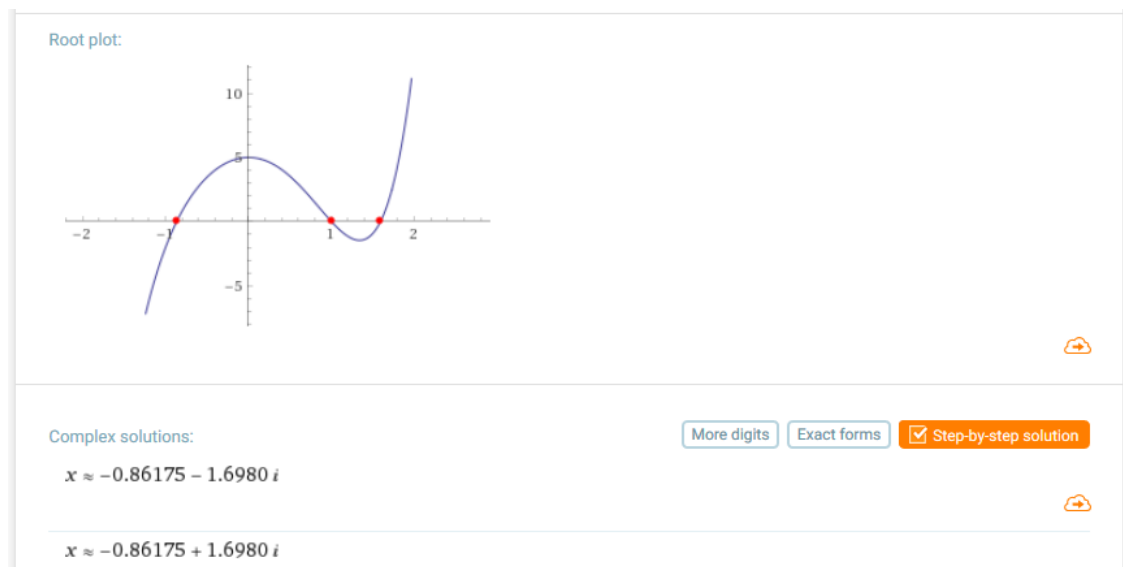
A conclusão segue do Exercício 8\*(a).

(b) Este polinómio tem exactamente 4 raízes complexas não reais:



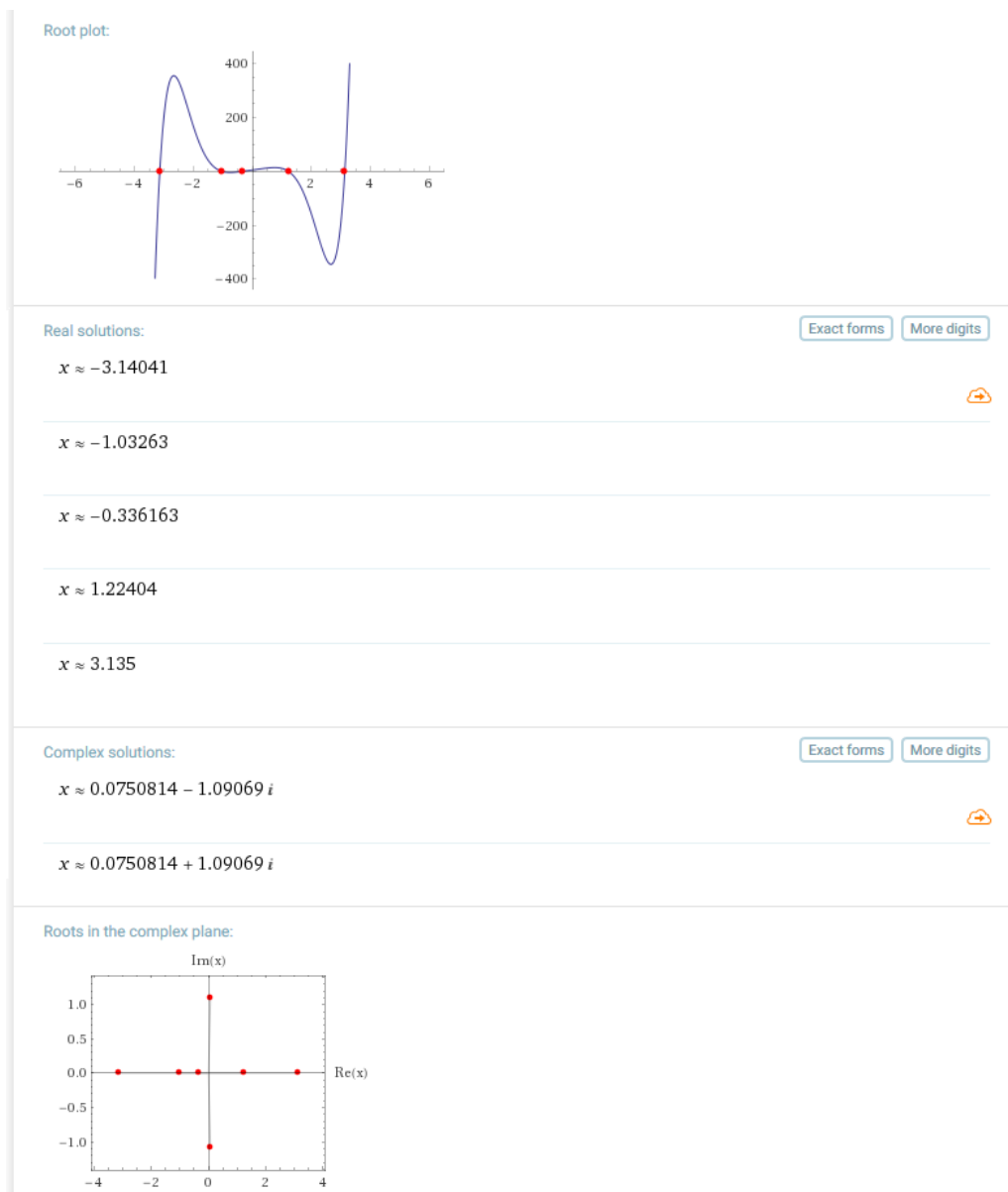
A conclusão segue do Exercício 8\*(b).

(c) Tem exactamente 2 raízes complexas não reais:



A conclusão segue do Exercício 8\*(a).

(d) Tem exactamente 2 raízes complexas não reais:



A conclusão segue do Exercício 8\*(a).