

1. (a)  $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ .

Elementos invertíveis: 1, 3, 5 e 7 ( $a^{-1} = a$  para  $a = 1, 3, 5, 7$ ).

Divisores de zero: 2, 4, 6 ( $2 \times_8 4 = 6 \times_8 4 = 0$ ).

- (b)  $x^4 - 1 = (x^2)^2 - 1^2 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$  dá-nos a factorização de  $x^4 - 1$  em polinómios irreduzíveis de  $\mathbb{R}[x]$ . Portanto, os divisores de  $x^4 - 1$  são os polinómios

1,  $(x - 1)$ ,  $(x + 1)$ ,  $(x^2 + 1)$ ,  $(x - 1)(x + 1) = x^2 - 1$ ,  $(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$ ,

$$(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1, x^4 - 1$$

e os respectivos polinómios associados.

- (c) Pelo Teorema do Resto (válido em qualquer anel comutativo com identidade),  $x - 2$  divide  $x^4 + x^3 + x^2 + x$  em  $\mathbb{Z}_n[x]$  precisamente quando 2 é raiz de  $x^4 + x^3 + x^2 + x$  em  $\mathbb{Z}_n[x]$ , ou seja, quando  $2^4 + 2^3 + 2^2 + 2 = 30 \equiv_n 0$ , isto é,  $n \mid 30 = 2 \times 3 \times 5$ . Portanto, como  $n > 2$ ,  $x - 2$  divide  $x^4 + x^3 + x^2 + x$  em  $\mathbb{Z}_n[x]$  se e só se  $n = 3, 5, 6, 10, 15$ , ou 30.

2.  $\mathbb{Z}_2[x]/I$  é um corpo se e só se o ideal  $I = \langle p(x) \rangle$  é maximal, isto é, se e só se  $p(x)$  é irreduzível sobre  $\mathbb{Z}_2$ .

- (a) O polinómio  $p(x) = x^3 + x + 1$  tem grau 3 e não tem raízes em  $\mathbb{Z}_2$  logo é irreduzível em  $\mathbb{Z}_2[x]$  (de facto,  $p(0) = p(1) = 1$ ). Portanto, o ideal  $\langle x^3 + x + 1 \rangle$  é maximal em  $\mathbb{Z}_2[x]$  e  $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$  é um corpo.

- (b) O polinómio  $p(x) = x^2$  tem uma raiz em  $\mathbb{Z}_2$  ( $p(0) = 0$ ) logo é redutível em  $\mathbb{Z}_2[x]$ . Portanto, o ideal  $\langle x^2 \rangle$  não é maximal em  $\mathbb{Z}_2[x]$  pelo que  $\mathbb{Z}_2[x]/\langle x^2 \rangle$  não é um corpo.

Tem-se

$$\begin{aligned} \mathbb{Z}_2[x]/\langle x^2 \rangle &= \{\overline{p(x)} : p(x) \in \mathbb{Z}_2[x]\} \\ &= \{\overline{a_0 + a_1x} : a_0, a_1 \in \mathbb{Z}_2\} \end{aligned}$$

pois para cada  $p(x) = x^2q(x) + r(x)$ ,  $\overline{p(x)} = \overline{r(x)}$  (onde  $gr(r(x)) \leq 2$ ). Portanto  $\mathbb{Z}_2[x]/\langle x^2 \rangle = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$ , com tabelas

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

×	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{0}$	$\bar{x}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$

3. (a) Um polinómio  $m(x) \in K[x]$  diz-se *polinómio mínimo* de  $\theta \in L$  sobre  $K$  se é mónico, irreduzível sobre  $K$  e admite  $\theta$  como raiz.

O conjunto  $I = \{p(x) \in K[x] : p(\theta) = 0\}$ , é um ideal de  $K[x]$ . Portanto, como  $K[x]$  é um domínio de ideais principais, podemos concluir que existe um polinómio mónico  $m_\theta(x) \in K[x]$ , único, tal que  $I = \langle m_\theta(x) \rangle$ . Só resta justificar que  $m_\theta(x)$  é irreduzível sobre  $K$ :

Como  $m_\theta(x)$  tem uma raiz, tem de ser de grau  $\geq 1$  necessariamente. Suponhamos que  $m_\theta(x)$  era reduzível, isto é, que  $m_\theta(x) = p_1(x)p_2(x)$ , com

$$1 \leq \text{gr}(p_1(x)), \text{gr}(p_2(x)) < \text{gr}(m_\theta(x)). \quad (1)$$

Então  $0 = m_\theta(\theta) = p_1(\theta)p_2(\theta)$ , donde  $p_1(\theta) = 0$  ou  $p_2(\theta) = 0$ . Qualquer uma destas possibilidades contradiz (1): se  $p_i(\theta) = 0$  ( $i = 1$  ou  $i = 2$ ), então  $p_i(x) \in I$ , ou seja,  $m_\theta(x) \mid p_i(x)$ , donde  $\text{gr}(p_i(x)) \geq \text{gr}(m_\theta(x))$ .

- (b) 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 reduzível 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

$$\begin{cases} a' = -a \\ \text{-----} \\ a(b' - b) = 0 \Leftrightarrow a = 0 \vee b' = b \\ \text{-----} \end{cases}$$

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  $-a^2 + 4 = -16 \Leftrightarrow a^2 = 20$  ou  $-a^2 - 4 = -16 \Leftrightarrow a^2 = 12$ , ambas impossíveis em  $\mathbb{Q}$ .

Em conclusão, o sistema é impossível.

(c) A inclusão  $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$  é óbvia pois  $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ . Por outro lado, da alínea anterior,  $[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] = 4$ . Bastará assim mostrar que também  $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}]$  é igual a 4. Pelo Teorema da Torre,  $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$  pois  $x^2 - 3$  é o polinómio mínimo de  $\sqrt{3}$  sobre  $\mathbb{Q}$  e  $x^2 - 5$  é o polinómio mínimo de  $\sqrt{5}$  sobre  $\mathbb{Q}(\sqrt{3})$  (pois é um polinómio de grau 2 que não tem raízes em  $\mathbb{Q}(\sqrt{3})$ ).

(d) Da alínea anterior sabemos que

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}.$$

Portanto, queremos determinar  $a, b, c, d \in \mathbb{Q}$  tais que

$$(5\sqrt{3} - 3\sqrt{5})(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = 1.$$

Fazendo os cálculos, isto é equivalente a

$$(15b - 15c - 1) + (5a - 15d)\sqrt{3} + (15d - 3a)\sqrt{5} + (5c - 3b)\sqrt{15} = 0,$$

ou seja (uma vez que  $1, \sqrt{3}, \sqrt{5}$  e  $\sqrt{15}$  são linearmente independentes):

$$\begin{cases} 15b - 15c - 1 = 0 \\ 5a - 15d = 0 \\ 15d - 3a = 0 \\ 5c - 3b = 0 \end{cases} \Leftrightarrow \begin{cases} b - c = \frac{1}{15} \\ a = 3d \\ a = 5d \\ 5c = 3b \end{cases} \Leftrightarrow \begin{cases} d = 0 \\ a = 0 \\ c = \frac{1}{10} \\ b = \frac{1}{6} \end{cases}.$$

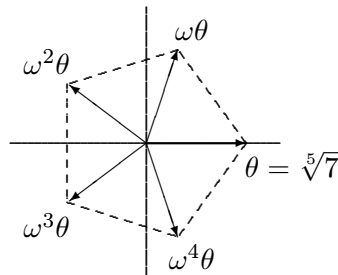
Solução alternativa:

$$\begin{aligned} (5\sqrt{3} - 3\sqrt{5})^{-1} &= \frac{1}{5\sqrt{3} - 3\sqrt{5}} = \frac{5\sqrt{3} + 3\sqrt{5}}{(5\sqrt{3} - 3\sqrt{5})(5\sqrt{3} + 3\sqrt{5})} \\ &= \frac{5\sqrt{3} + 3\sqrt{5}}{5 \times 5 \times 3 - 3 \times 3 \times 5} \\ &= \frac{5\sqrt{3} + 3\sqrt{5}}{5 \times 6} \\ &= \frac{1}{6}\sqrt{3} + \frac{1}{10}\sqrt{5}. \end{aligned}$$

4. (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 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 construtível a partir dos racionais.

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



$\omega =$  raiz quinta de 1,  
no 1<sup>o</sup> quadrante

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,  $Gal(\mathbb{Q}(\theta), \mathbb{Q})$  é o grupo trivial  $S_1 = \{id\}$ .

6. Seja  $\{a_i\}_{i \in I}$  uma base do espaço vectorial  $L$  sobre  $K$  e seja  $\{b_j\}_{j \in J}$  uma base do espaço vectorial  $M$  sobre  $L$ . Bastará provar que  $\{a_i b_j\}_{i \in I, j \in J}$  é uma base do espaço vectorial  $M$  sobre  $K$ .

É claro que cada elemento  $a_i b_j$  pertence a  $M$ , pois cada  $a_i \in L \subseteq M$  e cada  $b_j \in M$ . Provemos que se trata de um conjunto de vectores linearmente independente sobre  $K$ :

Se  $\sum_{i \in I, j \in J} \kappa_{ij} a_i b_j = 0$ , com  $\kappa_{ij} \in K$ , isto significa que  $\sum_{j \in J} \left( \sum_{i \in I} \kappa_{ij} a_i \right) b_j = 0$ . Como cada  $\sum_{i \in I} \kappa_{ij} a_i$  pertence a  $L$  e os  $b_j$  são linearmente independentes sobre  $L$ , então  $\sum_{i \in I} \kappa_{ij} a_i = 0$  para qualquer  $j \in J$ . Mas os  $a_i$  são linearmente independentes sobre  $K$  e, portanto,  $\kappa_{ij} = 0$  para quaisquer  $i \in I$  e  $j \in J$ .

Finalmente, vejamos que se trata de um conjunto de geradores de  $M$  sobre  $K$ :

Seja  $c \in M$ . Então podemos escrever  $c = \sum_{j \in J} l_j b_j$ , onde  $l_j \in L$ , porque  $\{b_j\}_{j \in J}$  é uma base de  $M$  sobre  $L$ . Mas, por sua vez, cada  $l_j$  é uma combinação linear  $l_j = \sum_{i \in I} \kappa_{ij} a_i$ , porque  $\{a_i\}_{i \in I}$  é uma base de  $L$  sobre  $K$ . Consequentemente,

$$c = \sum_{j \in J} \left( \sum_{i \in I} \kappa_{ij} a_i \right) b_j = \sum_{i \in I, j \in J} \kappa_{ij} a_i b_j.$$