

# Soluções de exercícios

## Folha 2

**7.** Mostre que se  $1 + i$  é raiz de  $p(x) \in \mathbb{R}[x]$ , então  $p(x)$  é divisível por  $x^2 - 2x + 2$  em  $\mathbb{R}[x]$ .

Se  $1 + i$  é raiz de  $p(x)$ , então o seu conjugado  $1 - i$  também o é. Logo  $p(x)$  é divisível por  $(x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2$ .

**12.** Indique, justificando, quais dos seguintes polinómios são irredutíveis sobre  $\mathbb{Q}$ :

$$p(x) = 5x^5 - 10x^3 + 6x^2 - 2x + 6, \quad q(x) = x^4 - x^2 - 2, \quad r(x) = 4x^3 - 3x - \frac{1}{2}.$$

$p(x)$ , pelo critério de Eisenstein (com  $p = 2$ ), é irredutível sobre  $\mathbb{Q}$ .

As possíveis raízes racionais de  $q(x) = x^4 - x^2 - 2$  são  $1, -1, 2$  e  $-2$ . Nenhuma delas é raiz pelo que o polinómio não tem raízes racionais. Assim, a única hipótese dele ser redutível sobre  $\mathbb{Q}$  é factorizar-se na forma

$$q(x) = (x^2 + ax + b)(x^2 + cx + d)$$

para alguns racionais  $a, b, c, d$ . Resolvendo o sistema correspondente

$$\begin{cases} a + c = 0 \\ b + ac + d = -1 \\ ad + bc = 0 \\ bd = -2. \end{cases}$$

chega-se a uma solução:

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

Portanto,  $q(x)$  é redutível sobre  $\mathbb{Q}$ .

$r(x)$  é irredutível sobre  $\mathbb{Q}$  se e só se  $8x^3 - 6x - 1$  o for. As possíveis raízes racionais deste último polinómio 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  $\mathbb{Q}$ .

**13.** Determine a factorização do polinómio  $q(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$  em factores irredutíveis.

Sabemos já (pelo exercício anterior) que  $q(x)$  não tem raízes racionais e  $q(x) = (x^2 + 1)(x^2 - 2)$ . Portanto, esta é a factorização de  $q(x)$  em factores irredutíveis.

**18.** Para cada um dos seguintes ideais  $I$  de  $\mathbb{Z}_2[x]$

(a)  $\langle x^3 + x + 1 \rangle$

(b)  $\langle x^2 \rangle$

justifique se  $\mathbb{Z}_2[x]/I$  é um corpo. Construa as tabelas de  $\mathbb{Z}_2[x]/\langle x^2 \rangle$ .

$\mathbb{Z}_2[x]/I$  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 irredutível 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 irredutível 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.

Denotando o elemento  $p(x) + \langle x^2 \rangle$  de  $\mathbb{Z}_2[x]/\langle x^2 \rangle$  por  $\overline{p(x)}$  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

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

**19. (b)** Determine  $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$  e escreva as respectivas tabelas de anel.

Por definição,  $\mathbb{Z}_2[x]/I = \{f(x) + I \mid f(x) \in \mathbb{Z}_2[x]\}$ . Mas, dividindo  $f(x)$  por  $x^2 + x + 1$ , obtemos  $f(x) = (x^2 + x + 1)q(x) + r(x)$  onde  $gr(r(x)) \leq 1$ . É claro que então  $f(x) + I = r(x) + I$ . Portanto

$$\begin{aligned} \mathbb{Z}_2[x]/I &= \{r(x) + I \mid r(x) \in \mathbb{Z}_2[x], gr(r(x)) \leq 1\} \\ &= \{0 + I, 1 + I, x + I, 1 + x + I\} \end{aligned}$$

é constituído pelas classes definidas pelos restos da divisão dos polinómios de coeficientes em  $\mathbb{Z}_2[x]$  por  $x^2 + x + 1$ .

Denotando  $0 + I$  por  $0$ ,  $1 + I$  por  $1$ ,  $x + I$  por  $\alpha$  e  $1 + x + I$  por  $\beta$ , as tabelas das operações de  $L$  são as seguintes:

$$\begin{array}{c|cccc}
+ & 0 & 1 & \alpha & \beta \\
\hline
0 & 0 & 1 & \alpha & \beta \\
1 & 1 & 0 & \beta & \alpha \\
\alpha & \alpha & \beta & 0 & 1 \\
\beta & \beta & \alpha & 1 & 0
\end{array}
\qquad
\begin{array}{c|cccc}
\times & 0 & 1 & \alpha & \beta \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & \alpha & \beta \\
\alpha & 0 & \alpha & \beta & 1 \\
\beta & 0 & \beta & 1 & \alpha
\end{array}$$

Por exemplo,

$$\alpha + \beta = (x + I) + (1 + x + I) = 1 + I = 1$$

e

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

**20.** Considere o polinómio  $p(x) = x^3 + 2x^2 + 1 \in \mathbb{Z}_5[x]$ . Mostre que  $\mathbb{Z}_5[x]/\langle p(x) \rangle$  é um corpo e descreva os seus elementos. Qual é o cardinal deste corpo?

O polinómio  $p(x) = x^3 + 2x^2 + 1$  tem grau 3 e não tem raízes em  $\mathbb{Z}_5$  logo é irreduzível em  $\mathbb{Z}_5[x]$  (de facto,  $p(0) = 1$ ,  $p(1) = 4$ ,  $p(2) = 2$ ,  $p(3) = 1$  e  $p(4) = 2$ ). Portanto, o ideal  $\langle p(x) \rangle$  é maximal em  $\mathbb{Z}_5[x]$  e  $\mathbb{Z}_5[x]/\langle p(x) \rangle$  é um corpo. Tem-se

$$\begin{aligned}
\mathbb{Z}_5[x]/\langle p(x) \rangle &= \{a_0 + a_1x + a_2x^2 + \langle p(x) \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_5\} \\
&\cong \{a_0 + a_1\theta + a_2\theta^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_5\}
\end{aligned}$$

com  $\theta^3 = -2\theta^2 - 1 = 3\theta^2 + 4$ .

Cada elemento de  $\mathbb{Z}_5[x]/\langle p(x) \rangle$  admite uma única expressão  $a_0 + a_1\theta + a_2\theta^2$ , com  $a_0, a_1, a_2 \in \mathbb{Z}_5$ , pelo que  $|\mathbb{Z}_5[x]/\langle p(x) \rangle| = 5^3 = 125$ .

**1.\*** Seja  $K$  um corpo. Mostre que se  $\varphi : K[x] \rightarrow K[x]$  é um isomorfismo tal que  $\varphi(a) = a$  para qualquer  $a \in K$ , então  $\varphi(x) = cx + d$  para algum par  $c, d \in K$ .

Pelo algoritmo da divisão em  $K[x]$ ,  $\varphi(x) = q(x)x + d$  para algum  $q(x) \in K[x]$  e algum  $d \in K$ . Como  $\varphi$  é sobrejectiva, existem  $q_1(x)$  e  $p(x)$  em  $K[x]$  tais que  $\varphi(q_1(x)) = q(x)$  e  $\varphi(p(x)) = x$ . Portanto,

$$\varphi(x) = \varphi(q_1(x))\varphi(p(x)) + \varphi(d) = \varphi(q_1(x))p(x) + d).$$

Agora, pela injectividade de  $\varphi$ , podemos concluir que  $x = q_1(x)p(x) + d$ , o que implica que  $gr(q_1(x)p(x)) = 1$ . Consequentemente, ou  $gr(q_1(x)) = 1$  e  $gr(p(x)) = 0$ , ou  $gr(q_1(x)) = 0$  e  $gr(p(x)) = 1$ . Suponhamos que acontece o primeiro caso. Então  $p(x) = a \in K$ , o que implica  $x = \varphi(p(x)) = \varphi(a) = a$ , uma contradição. Logo, ocorre necessariamente o segundo caso:  $q_1(x) = c \in K$  e

$$\varphi(x) = \varphi(q_1(x))\varphi(p(x)) + d = \varphi(cp(x) + d) = cx + d.$$

**3.\*** *Seja  $K$  um corpo. Mostre que se  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  é irredutível em  $K[x]$ , também  $a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$  o é.*

Dado  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$ , denotemos por  $\overline{p(x)}$  o polinómio  $a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ . Basta verificar que se  $p(x) = q(x)r(x)$  então  $\overline{p(x)} = \overline{q(x)} \overline{r(x)}$ .

**4.\* (b)** *Conclua que se  $A$  é um corpo, então  $p(x)$  é irredutível em  $A[x]$  se e só se  $p(x+c)$  o é.*

Se  $p(x)$  é redutível então  $p(x) = q(x)r(x)$  (onde  $q(x)$  e  $r(x)$  têm grau  $\geq 1$ ). Pela alínea (a), isto implica  $p(x+c) = q(x+c)r(x+c)$ , o que mostra que  $p(x+c)$  é redutível (é evidente que os polinómios  $q(x+c)$  e  $r(x+c)$  continuam a ter grau  $\geq 1$ ). Reciprocamente, se  $p(x+c) = q(x)r(x)$  então (novamente pela alínea (a))  $p(x) = q(x-c)r(x-c)$ , o que mostra que  $p(x)$  é redutível.

**6.\*** *Seja  $p$  um inteiro primo. Prove que o polinómio ciclotómico*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

*é irredutível em  $\mathbb{Q}[x]$ .*

Pelo Exercício 2.24, um polinómio  $p(x)$  é irredutível se e só se  $p(x+c)$  é irredutível (onde  $c$  é uma constante). Em particular,  $\Phi_p(x)$  é irredutível se e só se

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

é irredutível. Este último polinómio é igual a

$$x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{2}x + p.$$

Quando  $p$  é primo, observámos na demonstração da Proposição 1.5 que  $p$  divide  $\binom{p}{i}$  (para  $1 \leq i \leq p-1$ ). Basta agora aplicar o critério de Eisenstein.

Nota: Se  $n$  não é primo, então  $\Phi_n(x) = x^{n-1} + x^{n-2} + \dots + x + 1$  factoriza-se em  $\mathbb{Q}[x]$ . Por exemplo,

$$x^3 + x^2 + x + 1 = (x+1)(x^2 + 1).$$