

Os dois primeiros grupos de questões são de escolha múltipla; uma resposta certa terá a cotação máxima que lhe for atribuída e uma resposta errada perderá metade dessa cotação (desde que a nota do teste permaneça não negativa).

1. Em cada uma das alíneas seguintes indique o valor lógico das afirmações:

(**V**: verdadeira; **F**: falsa)

V **F**

- (a) Seja A um anel. Então um polinómio $p(x) \in A[x]$ de grau n não pode ter mais do que n raízes.
- (b) Em $\mathbb{Z}_5[x]$, $\text{mdc}(x^4 + x^3 + 2x^2 + x + 1, x^3 + 3x^2 + x + 3) = x^2 + 1$.
- (c) Se $p(x) \in \mathbb{Z}[x]$ é um polinómio mónico, então qualquer raiz racional de $p(x)$ é inteira.
- (d) Se D é um domínio de integridade, um polinómio redutível de $D[x]$ tem necessariamente raízes em D .

2. Indique quais dos seguintes polinómios são irredutíveis sobre o anel indicado colocando, em cada alínea, uma cruz na coluna correcta:

(**S**: é irredutível; **N**: não é irredutível)

S **N**

- (a) $p(x) = 2x^{50} - x^{49} + 18x^5 - 9x^4 + 6x - 3$, $A = \mathbb{Q}$.
- (b) $p(x) = 3x + 6$, $A = \mathbb{Z}$.

3. Sendo $I = \langle x^2 + x + 1 \rangle$, considere o anel quociente $A = \mathbb{Z}_2[x]/I$.

- (a) A é um corpo?
- (b) Qual é o inverso de $x^3 + I$?
- (c) Determine os elementos de A e as respectivas tabelas da adição e multiplicação.

Os dois primeiros grupos de questões são de escolha múltipla; uma resposta certa terá a cotação máxima que lhe for atribuída e uma resposta errada perderá metade dessa cotação (desde que a nota do teste permaneça não negativa).

1. Em cada uma das alíneas seguintes indique o valor lógico das afirmações:

(**V**: verdadeira; **F**: falsa)

V **F**

(a) Seja A um anel. Então um polinómio $p(x) \in A[x]$ de grau n não pode ter mais do que n raízes.

	×
--	---

[Por exemplo, em $\mathbb{Z}_6[x]$, o polinómio $x^2 + x$, de grau 2, tem quatro raízes: 0,2,3,5.]

(b) Em $\mathbb{Z}_5[x]$, $\text{mdc}(x^4 + x^3 + 2x^2 + x + 1, x^3 + 3x^2 + x + 3) = x^2 + 1$.

×	
---	--

[Seguindo o Algoritmo de Euclides:

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

$$x^3 + 3x^2 + x + 3 = (2x^2 + 2)(3x + 4).$$

Portanto, $\langle x^4 + x^3 + 2x^2 + x + 1, x^3 + 3x^2 + x + 3 \rangle = \langle 2x^2 + 2 \rangle = \langle x^2 + 1 \rangle$.]

(c) Se $p(x) \in \mathbb{Z}[x]$ é um polinómio mónico, então qualquer raiz racional de $p(x)$ é inteira.

×	
---	--

[Se $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ e c/d (escrito na forma reduzida) é raiz de $p(x)$, então $c^n + a_{n-1}c^{n-1}d + \dots + a_1cd^{n-1} + a_0d^n = 0$, isto é, $c^n = -(a_{n-1}c^{n-1}d + \dots + a_1cd^{n-1} + a_0d^n)$. Como d divide o segundo membro, terá que dividir o primeiro membro, ou seja c^n . Mas $\text{mdc}(c, d) = 1$, logo necessariamente $d = 1$ e c/d é inteiro.]

(d) Se D é um domínio de integridade, um polinómio redutível de $D[x]$ tem necessariamente raízes em D .

	×
--	---

[Por exemplo, em $\mathbb{R}[x]$, $(x^2 + 1)^2$ é redutível mas não tem raízes reais.]

2. Indique quais dos seguintes polinómios são irredutíveis sobre o anel indicado colocando, em cada alínea, uma cruz na coluna correcta:

(**S**: é irredutível; **N**: não é irredutível)

S **N**

(a) $p(x) = 2x^{50} - x^{49} + 18x^5 - 9x^4 + 6x - 3$, $A = \mathbb{Q}$.

	×
--	---

[Porque $p(x)$ é de grau ≥ 2 e tem uma raiz racional: $1/2$.]

(b) $p(x) = 3x + 6$, $A = \mathbb{Z}$.

	×
--	---

[Porque $p(x) = 3(x + 2)$, e 3 e $x + 2$ não são invertíveis em $\mathbb{Z}[x]$.]

3. (a) Sim, uma vez que $x^2 + x + 1$ é um polinómio irreduzível sobre \mathbb{Z}_2 (pois não tem raízes em \mathbb{Z}_2).

(b) Como $x^3 = (x^2 + x + 1)(x + 1) + 1$, então $x^3 + I = 1 + I$. Portanto

$$(x^3 + I)^{-1} = (1 + I)^{-1} = 1 + I.$$

(c) 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 α e $1 + x + I$ por β , as tabelas das operações de L são as seguintes:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

\cdot	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Por exemplo,

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

e

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