Departamento de Matemática da Universidade de Coimbra **Corpos e Equações Algébricas**

SOLUÇÕES **Teste 2** 29/04/2011

---

1. (a) Os polinómios x^2+x+2 e x^3+x^2+3x+1 de $\mathbb{Q}[x]$ são primos entre si. [×][ ]

   (b) Se C é um corpo, $p_1(x), p_2(x) \in C[x]$ são do mesmo grau e $p_1(x) \mid p_2(x)$ então $p_1(x) = p_2(x)$. [ ][×]

   (c) $x^6 - 3x^4 + 3x^2 + 6$ é irredutível sobre $\mathbb{Q}$. [×][ ]

   (d) $x^3 - 3x^2 + 3x - 9$ é irredutível sobre $\mathbb{Q}$. [ ][×]

   `[(a) Seguindo o Algoritmo de Euclides:`

$$
\begin{aligned}
x^3+x^2+3x+1 &= x(x^2+x+2)+x+1,\\
x^2+x+2 &= x(x+1)+2.
\end{aligned}
$$

`Portanto, o máximo divisor comum de` x^2+x+2 `e` x^3+x^2+3x+1 `é o polinómio mónico associado do polinómio constante 2, isto é, 1. São assim primos entre si.`

`(b) Contra-exemplo:` $p_1(x) = x$ `e` $p_2(x) = 2x$. `De facto, o que se pode concluir das hipóteses enunciadas é que` $p_1(x)$ `e` $p_2(x)$ `são polinómios associados, não necessariamente iguais.`

`(c) Critério de Eiseinstein (`$p=3$`):` $p \mid 6, p \mid 3, p \nmid 1, p \nmid 6$.

`(d) Aqui já não é possível concluir nada pelo critério de Eiseinstein, teremos que usar o critério das raízes. As possíveis raízes racionais do polinómio dão` $\pm 1, \pm 3, \pm 9$. `Verificando obtemos a raiz 3.]`

2. Seja θ uma raiz não racional do polinómio da alínea anterior (1.d).

   (a) Determine a extensão $\mathbb{Q}(\theta)$.

   (b) Qual é o inverso de $1+\theta$ em $\mathbb{Q}(\theta)$?

   Solução:

   (a) Sabemos já que $x^3-3x^2+3x-9 = (x-3)(x^2+3)$. Então θ é raiz de x^2+3, que é claramente o polinómio mínimo de θ sobre $\mathbb{Q}$. Portanto $\mathbb{Q}(\theta) = \{a + b\theta \mid a, b \in \mathbb{Q}\}$.

   (b)

   `[Método geral]` Pelo algoritmo da divisão obtemos

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

donde $4 = x^2+3-(x-1)(x+1)$, isto é, $1 = \frac{x^2+3}{4} - \frac{(x-1)(x+1)}{4}$. Substituindo x por θ obtemos por fim $1 = -\frac{\theta-1}{4}(\theta+1)$, pelo que $(1+\theta)^{-1} = \frac{1}{4} - \frac{1}{4}\theta$.

`[Alternativa]` Queremos determinar racionais a, b tais que $(1+\theta)(a+b\theta) = 1$. Como $(1+\theta)(a+b\theta) = a + b\theta + a\theta + b\theta^2 = a + b\theta + a\theta + -3b = (a-3b) + (a+b)\theta$ e $\{1, \theta\}$

é uma base do espaço vectorial $\mathbb{Q}(\theta)$ sobre o corpo $\mathbb{Q}$, necessariamente $a - 3b = 1$ e $a + b = 0$. Resolvendo este sistema de equações em $\mathbb{Q}$ obtemos $a = \frac{1}{4}$ e $b = -\frac{1}{4}$. Portanto $(1+\theta)^{-1} = \frac{1}{4} - \frac{1}{4}\theta$.

`[Alternativa 2: Como costuma calcular o inverso de um número complexo? Repare que o processo funciona em qualquer extensão` $\mathbb{Q}(\theta)$ `de grau 2]`

$$(1+\theta)^{-1} = \frac{1}{1+\theta} = \frac{(1-\theta)}{(1+\theta)(1-\theta)} = \frac{1-\theta}{1-\theta^2} = \frac{1-\theta}{1+3} = \frac{1}{4} - \frac{1}{4}\theta.$$

3. (a) $\mathbb{R}[x]/\langle x^2 - 2x + 2\rangle$ é um corpo? Porquê?
   (b) Mostre que todo o elemento de $\mathbb{R}[x]/\langle x^2-2x+2\rangle$ é uma classe da forma $a+bx+\langle x^2-2x+2\rangle$.
   (c) Determine uma fórmula para a multiplicação
   $$\big(a + bx + \langle x^2 - 2x + 2\rangle\big) \cdot \big(c + dx + \langle x^2 - 2x + 2\rangle\big)$$
   em $\mathbb{R}[x]/\langle x^2 - 2x + 2\rangle$.

Solução:

(a) Sim, porque $x^2 - 2x + 2$ é irredutível sobre $\mathbb{R}$ (o respectivo discriminante é negativo pelo que as suas duas raízes são imaginárias).

(b) Seja $p(x) + \langle x^2 - 2x + 2\rangle \in \mathbb{R}[x]/\langle x^2 - 2x + 2\rangle$. Dividindo $p(x)$ por $x^2 - 2x + 2$ obtém-se
$$p(x) = q(x)(x^2 - 2x + 2) + r(x)$$
onde $r(x) = ax + b$ para algum par de reais a, b. Portanto
$$\begin{aligned} p(x) + \langle x^2 - 2x + 2\rangle &= (q(x)(x^2 - 2x + 2) + ax + b) + \langle x^2 - 2x + 2\rangle \\ &= ax + b + \langle x^2 - 2x + 2\rangle. \end{aligned}$$

(c)
$$\begin{aligned} &\big(a + bx + \langle x^2 - 2x + 2\rangle\big) \cdot \big(c + dx + \langle x^2 - 2x + 2\rangle\big) = \\ &\qquad = (a + bx)(c + dx) + \langle x^2 - 2x + 2\rangle \\ &\qquad = (ac + (ad + bc)x + bdx^2) + \langle x^2 - 2x + 2\rangle \\ &\qquad = (ac - 2bd) + (ad + bc + 2bd)x + \langle x^2 - 2x + 2\rangle \end{aligned}$$
pois $bdx^2 = bd(x^2 - 2x + 2) + bd(2x - 2)$.

Nota: Denotando cada classe $a+bx+\langle x^2-2x+2\rangle$ abreviadamente por $a+b+bi$, reconhecemos aqui a fórmula da multiplicação de números complexos:
$$\begin{aligned}(a + b + bi)(c + d + di) &= (ac - 2bd + ad + bc + 2bd) + (ad + bc + 2bd)i = \\ &= (ac + ad + bc) + (ad + bc + 2bd)i.\end{aligned}$$

De facto, a correspondência
$$a + bx + \langle x^2 - 2x + 2\rangle \longmapsto a + b + bi$$
define um isomorfismo entre os corpos $\mathbb{R}[x]/\langle x^2 - 2x + 2\rangle$ e $\mathbb{C}$.