DMat-FCTUC **1ª Frequência de Corpos e Equações Algébricas**

Duração: 1h30m 4/04/2018

Soluções

---

1. aAa é claramente não vazio (contém, por exemplo, os elementos $a0a = 0$ e $a1a = a$). Sejam axa e aya dois elementos arbitrários de aAa. Então

$$axa - aya = a(xa - ya) = a(x - y)a \in aAa \quad \text{e} \quad (axa)(aya) = a(xay)a \in aAa.$$

Isto mostra que aAa é um subanel de A. Além disso,

$$(a1a)(axa) = aaxa = axa \quad \text{e} \quad (axa)(a1a) = axaa = axa.$$

2. (a) Nesse caso $I = A$. De facto, por definição de ideal, se $1 \in I$ então $a = a \cdot 1 \in I$ para qualquer $a \in A$.

   (b) Nesse caso $I = \{0\}$ ou $I = A$ (isto é, um corpo só admite os ideais triviais). De facto, se $I \neq \{0\}$, seja $a \neq 0$ um elemento de I. Como A é um corpo, a tem inverso a' em A. Mas então, por definição de ideal, $1 = a' \cdot a \in I$ e, pela alínea anterior, $I = A$.

3. (a) Se $\sqrt{2}\,i$ é raiz de $p(x)$, então o seu conjugado $-\sqrt{2}\,i$ também o é, logo $p(x)$ é divisível por $(x - \sqrt{2}\,i)(x + \sqrt{2}\,i)$, isto é, por $x^2 + 2$. Efectuando a divisão de $p(x)$ por $x^2 + 2$ obtemos $p(x) = (x^2 + 2)(x^2 - 2x + 2)$. Esta é a decomposição de $p(x)$ em factores irredutíveis em $\mathbb{Q}[x]$. De facto, $x^2 + 2$ é irredutível em $\mathbb{Q}[x]$ uma vez que é de grau 2 e, como vimos, não tem raízes racionais, enquanto $x^2 - 2x + 2$ é irredutível pelo critério de Eisenstein ($p = 2$), por exemplo (ou, em alternativa, porque também não tem raízes racionais, as suas duas raízes são complexas: $x = \frac{2\pm\sqrt{4-8}}{2} = \frac{2\pm 2i}{2} = 1 \pm i$.).

   (b) As únicas possíveis raízes racionais de q_m são 1 e -1. Como $q_m(1) = m - m^2 = m(1-m)$ e $q_m(-1) = m^2 + m - 2$ então para $m = 0$, $m = 1$ e $m = -2$, q_m tem raízes racionais (1 nos dois primeiros casos e -1 nos últimos dois).

4. (a) Por um teorema estudado nas aulas, $\langle a(x), b(x)\rangle = \langle \mathrm{mdc}(a(x), b(x))\rangle$. Calculemos então $m(x) = \mathrm{mdc}(a(x), b(x))$:

   Como
$$a(x) = b(x)(x^2 + x + 1) + 3x^2 - 21$$
   e
$$b(x) = (3x^2 - 21)\Big(\frac{1}{3}x - \frac{1}{3}\Big) + 0$$
   então, pelo Algoritmo de Euclides, $\mathrm{mdc}(a(x), b(x))$ é o polinómio mónico associado de $3x^2 - 21$, isto é, $x^2 - 7$. Portanto, confirma-se que $m(x) = x^2 - 7$.

   (b) Por outro teorema estudado nas aulas sabemos que um ideal principal $I = \langle m(x)\rangle$ de $\mathbb{Q}[x]$ é maximal se e só se $m(x)$ é irredutível em $\mathbb{Q}[x]$. No caso presente, $m(x) = x^2 - 7$ é claramente irredutível (por exemplo, pelo critério de Esisenstein, $p = 7$) pelo que a resposta é afirmativa: I é maximal.

(c) Sim, pois I sendo maximal, implica, como sabemos, que $\mathbb{Q}[x]/I$ seja um corpo. Determinemos o inverso de $1 + x + I$ em $\mathbb{Q}[x]/I$. Como

$$\begin{aligned}\mathbb{Q}[x]/I &= \{p(x) + I \mid p(x) \in \mathbb{Q}[x]\} \\ &= \{r(x) + I \mid r(x) \in \mathbb{Q}[x], \mathrm{gr}(r(x)) \leq 1\} \\ &= \{a + bx + I \mid a, b \in \mathbb{Q}\} \qquad (*)\end{aligned}$$

(onde em $(*)$ já não temos classes repetidas) bastará determinar $a + bx + I \in \mathbb{Q}[x]/I$ tal que $(1 + x + I)(a + bx + I) = 1 + I$. Para isso teremos que determinar $a, b \in \mathbb{Q}$ tais que $a + (a + b)x + bx^2 + I = 1 + I$. Como $x^2 + I = 7 + I$, então $bx^2 + I = 7b + I$, pelo que o problema resume-se à determinação de racionais a, b tais que $(a+7b)+(a+b)x+I = 1+I$, ou seja, $a + 7b = 1$ e $a + b = 0$ (porque já vimos que as classes de polinómios de grau ≤ 1 são todas diferentes). Daqui sai imediatamente $a = -\frac{1}{6}$ e $b = \frac{1}{6}$. Portanto,

$$(1 + x + I)^{-1} = -\frac{1}{6} + \frac{1}{6}x + I.$$

<u>Solução alternativa</u>: Fazendo a alínea (d) primeiro, podemos usá-la aqui. O que se pretende é determinar o inverso do par $(1, 1)$ no corpo $\mathbb{Q} \times \mathbb{Q}$:

$$(1, 1) \cdot (a, b) = (1, 0) \Leftrightarrow (a + 7b, a + b) = (1, 0) \Leftrightarrow a = -\frac{1}{6} \ \wedge \ b = \frac{1}{6}.$$

(d) De $(*)$ decorre imediatamente que

$$\begin{array}{rccc}\varphi\colon & \mathbb{Q}[x]/I & \to & \mathbb{Q} \times \mathbb{Q} \\ & a + bx + I & \mapsto & (a, b)\end{array}$$

é uma função bijectiva. É também evidente, da definição da soma no anel $\mathbb{Q}[x]/I$ que

$$\varphi((a + bx + I) + (c + dx + I)) = (a + c, b + d) = \varphi(a + bx + I) + \varphi(c + dx + I).$$

Finalmente, $\varphi((a + bx + I) \cdot (c + dx + I)) = \varphi(ac + (ad + bc)x + bdx^2 + I)$. Repetindo os cálculos feitos na alínea anterior, obtemos então: $\varphi((a + bx + I) \cdot (c + dx + I)) = \varphi((ac+7bd)+(ad+bc)x+I) = (ac+7bd, ad+bc) = (a, b)\cdot(c, d) = \varphi(a+bx+I)\cdot\varphi(c+dx+I)$.

<u>Observação</u>: Como $\mathbb{Q}[x]/I$ é um corpo, ficamos a saber que $\mathbb{Q} \times \mathbb{Q}$ com as operações indicadas também é um corpo.