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

*Duração: 1h30m* 20/04/2022

# Soluções

1. (a) Se $a/b$ é raiz de $p(x)$ então $a|1$ e $b|2$. Portanto, as únicas possíveis raízes racionais de $p(x)$ são $\pm 1$ e $\pm\frac{1}{2}$. Verificando, observamos que só $\frac{1}{2}$ é de facto uma raiz.

   (b) Pela alínea anterior, $p(x)$ é divisível por $x - \frac{1}{2}$, isto é, por $2x - 1$. Dividindo $p(x)$ por $2x - 1$ obtemos
   $$p(x) = (2x - 1)(x^3 - 3x^2 - 6x + 1).$$
   Ainda pela alínea anterior, o factor $x^3 - 3x^2 - 6x + 1$ terá quando muito uma raiz racional, $\frac{1}{2}$ (caso esta seja uma raiz múltipla de $p(x)$), mas é evidente que este não é o caso (verificando, por substituição de $x$ por $\frac{1}{2}$, ou então observando que como $x^3 - 3x^2 - 6x + 1$ é mónico, todas as suas raízes racionais são necessariamente inteiras). Em conclusão, $x^3 - 3x^2 - 6x + 1$ é de grau 3 e não tem raízes racionais pelo que é irredutível em $\mathbb{Q}$. Assim,
   $$p(x) = (2x - 1)(x^3 - 3x^2 - 6x + 1) = 2(x - \tfrac{1}{2})(x^3 - 3x^2 - 6x + 1)$$
   é a factorização de $p(x)$ em factores irredutíveis em $\mathbb{Q}$.

   (c) Em $\mathbb{Q}[x]$ é muito simples: $q(x)$ é irredutível em $\mathbb{Q}$, pelo critério de Eisenstein (tomando $p = 5$), pelo que a factorização de $q(x)$ é ele próprio.
   Em $\mathbb{Z}_2[x]$, $q(x) = x^5 + x^4 + 1$. É evidente que não tem raízes em $\mathbb{Z}_2$ pelo que a única hipótese de ser redutível é admitir uma factorização do tipo
   $$x^5 + x^4 + 1 = (x^3 + ax^2 + bx + 1)(x^2 + cx + 1).$$
   Esta identidade implica
   $$\begin{cases} 1 = c + a \\ 0 = 1 + ac + b \\ 0 = a + bc + 1 \\ 0 = b + c \end{cases} \Leftrightarrow \begin{cases} c = a + 1 \\ a + ac = 0 \\ c + bc = 0 \\ b = c \end{cases} \Leftrightarrow \begin{cases} c = a + 1 \\ a(c + 1) = 0 \Leftrightarrow aa = 0 \Leftrightarrow a = 0 \\ c(b + 1) = 0 \\ b = c \end{cases}$$
   Portanto, $a = 0, b = c = 1$ e
   $$x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1)$$
   é a factorização de $q(x)$ em irredutíveis em $\mathbb{Z}_2[x]$ (os dois factores são irredutíveis porque não têm raízes em $\mathbb{Z}_2$).

   (d) Pelo algoritmo deduzido nas aulas, denotando $\langle x^2 + 1\rangle$ por $I$ e a classe lateral $r(x) + I$ por $\overline{r(x)}$, temos
   $$\mathbb{Z}_7[x]/\langle x^2 + 1\rangle = \{r(x) + I \mid r(x) \in \mathbb{Z}_7[x],\ \mathrm{gr}(r(x)) < 2\} = \{\overline{a + bx} \mid a, b \in \mathbb{Z}_7\}.$$
   Portanto, este corpo tem $7 \times 7 = 49$ elementos.

2. (a) Sim, pois $x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$, uma vez que é de grau 2 e 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) Em primeiro lugar, tal como em 1(d),

$$A = \mathbb{Z}_2[x]/I = \{\overline{r(x)} \mid r(x) \in \mathbb{Z}_2[x], \mathrm{gr}(r(x)) < 2\} = \{\overline{0}, \overline{1}, \overline{x}, \overline{1+x}\}.$$

   Usando a definição da multiplicação entre classes laterais obtemos imediatamente a tabela da multiplicação de $A$:

| $\cdot$ | $0$ | $1$ | $\overline{x}$ | $\overline{1+x}$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\overline{x}$ | $\overline{1+x}$ |
| $\overline{x}$ | $0$ | $\overline{x}$ | $\overline{1+x}$ | $1$ |
| $\overline{1+x}$ | $0$ | $\overline{1+x}$ | $1$ | $\overline{x}$ |

   Por exemplo,

$$\overline{x}\,\overline{1+x} = x(1+x) + I = x + x^2 + I = 1 + I = \overline{1}.$$

3. (a) Afirmação **falsa**. Por exemplo, o polinómio $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ é redutível em $\mathbb{R}[x]$ mas não tem raízes em $\mathbb{R}$.

   (b) Afirmação **verdadeira**. Prova:

   Seja $I$ um ideal de $\mathbb{Q}[x]$. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Provemos que existe um polinómio $m(x) \in \mathbb{Q}[x]$ tal que $I = \langle m(x) \rangle$:

   Consideremos o conjunto

$$N = \{n \in \mathbb{N}_0 \mid \text{ existe } s(x) \in I, \mathrm{gr}(s(x)) = n\}.$$

   É claro que, como $I \neq \{0\}$, $N$ é não vazio, pelo que tem um mínimo. Seja $m(x)$ um polinómio em $I$ de grau igual a esse mínimo. Finalmente, provemos que $I = \langle m(x) \rangle$.

   Como $m(x) \in I$, é óbvio que $\langle m(x) \rangle \subseteq I$. Por outro lado, se $p(x) \in I$, usando o algoritmo de divisão em $\mathbb{Q}[x]$ obtemos $p(x) = q(x)m(x) + r(x)$, onde $\mathrm{gr}(r(x)) < \mathrm{gr}(m(x))$. Dado que $I$ é um ideal, podemos concluir que $r(x) = p(x) - q(x)m(x) \in I$. Mas então $r(x)$ só pode ser igual a 0 pois, com excepção do polinómio nulo, não pode haver nenhum polinómio em $I$ de grau inferior a $\mathrm{gr}(m(x))$. Assim, $p(x)$ é um múltiplo de $m(x)$ pelo que pertence ao ideal $\langle m(x) \rangle$.

   (c) Afirmação **falsa**. Se existisse $n \geq 2$ tal que $\theta = \sqrt[n]{\frac{2}{5}}$ fosse racional então, como $\theta$ é raiz do polinómio $5x^n - 2 \in \mathbb{Q}[x]$, este polinómio seria redutível em $\mathbb{Q}$, o que é impossível pelo critério de Eisenstein (tomando $p = 2$).