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

Duração: 1h30m 14/04/2023

SOLUÇÕES

---

1. (a) Se a/b é raiz de $p(x)$ então $a|2$ e $b|1$. Portanto, as únicas possíveis raízes racionais de $p(x)$ são ± 1 e ± 2. Verificando, observamos que só 2 é de facto uma raiz.
   Dividindo $p(x)$ por $x-2$ obtemos

   $$p(x) = -(x-2)(x^3 - 6x^2 - 3x + 1).$$

   Por sua vez, o factor $x^3 - 6x^2 - 3x + 1$ terá quando muito a raiz racional 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 2, ou então observando que como $x^3 - 3x^2 - 6x + 1$ é mónico e o seu termo independente é igual a 1, as únicas raízes possíveis seriam ± 1). Assim, $x^3 - 6x^2 - 3x + 1$, sendo de grau 3 e não tendo raízes racionais, é irredutível em $\mathbb{Q}$ e a factorização acima de $p(x)$ é a sua factorização em factores irredutíveis em $\mathbb{Q}$.

   (b) Usando o algoritmo de Euclides, obtemos

   $$x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 2) + x + 2$$
   $$x^2 + x + 1 = (x + 2)(x + 2) + \mathbf{0}$$

   pelo que $\operatorname{mdc}(x^4 + x^3 + 1, x^2 + x + 1) = x + 2$.

   (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 $\mathbb{Z}_2$).

2. (a) Pelo algoritmo deduzido nas aulas, denotando a classe lateral $r(x) + I$ por $\overline{r(x)}$, temos

$$A/I = \mathbb{Z}_7[x]/\langle x^2+1\rangle = \{r(x) + I \mid r(x) \in \mathbb{Z}_7[x],\ \mathrm{gr}(r(x)) < 2\} = \{\overline{a+bx} \mid a, b \in \mathbb{Z}_7\}.$$

Portanto, este corpo tem $7 \times 7 = 49$ elementos, sendo as suas operações dadas pelas fórmulas

$$\overline{a+bx} + \overline{c+dx} = \overline{a+bx+c+dx} = \overline{a+c+(b+d)x}$$

e

$$\overline{a+bx} \cdot \overline{c+dx} = \overline{(a+bx)\cdot(c+dx)} = \overline{ac+(ad+bc)x+bdx^2} = \overline{(ac+6bd)+(ad+bc)x}$$

uma vez que em A/I, $\overline{1+x^2} = \overline{0}$, isto é, $\overline{x^2} = \overline{-1} = \overline{6}$.

(Claro que as operações nos coeficientes dos polinómios em cada classe são feitas no corpo $\mathbb{Z}_7$).

(b) Sim, pois $x^2 + 1$ é irredutível em $\mathbb{Z}_7[x]$, uma vez que é de grau 2 e não tem raízes em $\mathbb{Z}_7$.

(c) Pela fórmula para a multiplicação de (a), temos

$$\overline{a+bx} \cdot \overline{0+1x} = \overline{1} \Leftrightarrow \overline{6b+ax} = \overline{1} \Leftrightarrow 6b = 1, a = 0 \Leftrightarrow a = 0, b = 6^{-1} = 6.$$

Portanto, o inverso de $\overline{x}$ em A/I é o elemento $\overline{6x}$.

Resolução alternativa: Uma vez que $\overline{x^2} = \overline{6}$, então $\overline{1} = \overline{36} = \overline{6\cdot 6} = \overline{6x^2} = \overline{6x} \cdot \overline{x}$.

3. (a) Afirmação **verdadeira**. Prova:

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

(b) Afirmação **falsa**. O algoritmo da divisão não é possível em $\mathbb{Z}_6[x]$ para polinómios divisores cujo coeficiente de maior grau seja igual a 2, 3 ou 4 (porque estes elementos são divisores de zero em $\mathbb{Z}_6$, logo não são invertíveis). Por exemplo, não é possível dividir x por $2x$, uma vez que não existe nenhum $p(x) \in \mathbb{Z}_6[x]$ e nenhum $r \in \mathbb{Z}_6$ tais que $x = 2x \cdot p(x) + r$.

(c) Afirmação **verdadeira**. Prova:

$\Rightarrow$: Seja $p(x) \in C[x]$ um polinómio de grau ≥ 2. Por hipótese é redutível pelo que se pode escrever como um produto de um par de polinómios de grau ≥ 1. Repetindo este raciocínio, para cada um desses factores, chegaremos, ao cabo de um número finito de passos, a uma factorização de $p(x)$ como um produto de polinómios irredutíveis (podíamos argumentar, alternativamente, com o Teorema da factorização única em $C[x]$ para chegar a esta mesma conclusão). Cada um destes factores é de **grau 1**, por hipótese; é claro que cada um deles nos dá uma raiz de $p(x)$ em C.

(Provamos assim mais do que o requerido: todo o polinómio de grau n em $C[x]$ terá exactamente n raízes em C.)

$\Leftarrow$: Todos os polinómios de grau 1 são irredutíveis, por definição. Não há mais irredutíveis em $C[x]$ pois qualquer polinómio de grau ≥ 2 terá, por hipótese, pelo menos uma raiz $\theta \in C$, pelo que será divisível pelo polinómio $x - \theta \in C[x]$, logo redutível em $C[x]$.

(d) Afirmação **verdadeira**. Se existisse $n \geq 2$ tal que $\theta = \sqrt[n]{\frac{3}{4}}$ fosse racional então, como θ é raiz do polinómio $4x^n - 3 \in \mathbb{Q}[x]$, este polinómio seria redutível em $\mathbb{Q}$, o que é impossível pelo critério de Eisenstein (tomando $p = 3$).
