DMUC **Frequência de Corpos e Equações Algébricas**

Duração: 2h30m 1/06/2011

Soluções

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

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

   (a) A divisão de polinómios é sempre possível em $\mathbb{Z}_4[x]$. | | × |

   [Por exemplo, é impossível fazer a divisão pelo polinómio constante 2, uma vez que 2, sendo um divisor de zero de $\mathbb{Z}_4$, não é invertível.]

   (b) $p(x) \in A[x]$ pode ter mais do que $gr(p(x))$ raízes. | × | |

   [Basta que A tenha divisores de zero: em $\mathbb{Z}_4$, $2x$ tem duas raízes, 0 e 2.]

   (c) O número real $\sqrt{2-\sqrt[3]{2}}$ é algébrico sobre $\mathbb{Q}$. | × | |

   [Basta observar que $\sqrt{2-\sqrt[3]{2}}$ é raiz do polinómio $(x^2-2)^3 = -2$, que tem coeficientes racionais.]

   (d) O número real $\sqrt{2-\sqrt[3]{2}}$ é construtível, por régua e compasso, a partir de $\mathbb{Q}$. | | × |

   [A dimensão $[\mathbb{Q}(\sqrt{2-\sqrt[3]{2}}) : \mathbb{Q}]$, sendo igual a 6, não é uma potência de 2, pelo que o número não poderá ser construtível.]

   (e) $\sqrt{3} \in \mathbb{Q}(\sqrt{3}\,i)$. | | × |

   [$(\sqrt{3}\,i)^2 = -3$ donde $\sqrt{3}\,i$ é raiz do polinómio $x^2+3 \in \mathbb{Q}[x]$.
   Este polinómio é claramente irredutível sobre $\mathbb{Q}$, pelo que $[\mathbb{Q}(\sqrt{3}\,i) : \mathbb{Q}] = 2$. Portanto, $\mathbb{Q}(\sqrt{3}\,i) = \{a + b\sqrt{3}\,i \mid a, b \in \mathbb{Q}\}$. Isto diz-nos que os complexos com parte imaginária nula que pertencem a $\mathbb{Q}(\sqrt{3}\,i)$ são precisamente os racionais, pelo que $\sqrt{3} \notin \mathbb{Q}(\sqrt{3}\,i)$.]

2. (a) Basta observar que $I \neq \emptyset$ e para quaisquer $\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} 0 & b' \\ 0 & c' \end{bmatrix} \in I$ e $\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \in T_2(\mathbb{Z})$,

$$\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} - \begin{bmatrix} 0 & b' \\ 0 & c' \end{bmatrix} = \begin{bmatrix} 0 & b-b' \\ 0 & c-c' \end{bmatrix} \in I,$$

$$\begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} = \begin{bmatrix} 0 & bc' \\ 0 & cc' \end{bmatrix} \in I$$

e

$$\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \cdot \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 0 & a'b+b'c \\ 0 & c'c \end{bmatrix} \in I.$$

   (b) Uma vez que $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + I = \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} + I$ sse $\begin{bmatrix} a-a' & b-b' \\ 0 & c-c' \end{bmatrix} \in I$, isto é, $a = a'$, então

$$T_2(\mathbb{Z})/I = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + I \mid a, b, c \in \mathbb{Z} \right\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + I \mid a \in \mathbb{Z} \right\}.$$

O isomorfismo $\Phi : \mathbb{Z} \to T_2(\mathbb{Z})/I$ é agora evidente: basta definir

$$\Phi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + I,$$

pois trata-se claramente de uma bijecção que satisfaz $\Phi(a+b) = \Phi(a) + \Phi(b)$ e $\Phi(ab) = \Phi(a)\Phi(b)$.

3. (a) Seja $p(x)$ um polinómio de grau 2 ou 3. Se $p(x)$ é redutível sobre K então $p(x) = q_1(x)q_2(x)$, onde nem $q_1(x)$ nem $q_2(x)$ são constantes. Assim, necessariamente um destes dois polinómios é de grau 1, da forma $ax + b$. Este polinómio tem a raiz $-a^{-1}b \in K$, que será evidentemente também raiz de $p(x)$.

   Reciprocamente, se $p(x)$ tem uma raiz α em K então, pelo Teorema do Resto, $p(x) = (x - \alpha)q(x)$ para algum polinómio $q(x) \in K[x]$. Pela regra dos graus, $q(x)$ tem necessariamente grau ≥ 1, pelo que não é uma unidade de $K[x]$. Portanto, $(x-\alpha)q(x)$ é uma factorização não trivial de $p(x)$ em $K[x]$, o que mostra que este polinómio é redutível sobre K.

   (b) (Metade da Proposição 2.9(3) nos Apontamentos)

   Suponhamos, por absurdo, que I não é maximal, ou seja, que existe um ideal $J = \langle q(x) \rangle$ (pois $K[x]$ é um domínio de ideais principais) tal que $I \subset J \subset K[x]$. Então $p(x) = r(x)q(x)$ para algum $r(x) \in K[x]$. É claro que $gr(r(x)) \geq 1$ (pois se $r(x)$ fosse constante, $q(x)$ pertenceria a $\langle p(x) \rangle$ e teríamos $J = I$). Por outro lado, também $gr(q(x)) \geq 1$ (caso contrário, $J = K[x]$). Assim, a factorização $p(x) = r(x)q(x)$ mostra que $p(x)$ é redutível sobre K.

4. (a) Uma vez que $p(x)$ tem coeficientes inteiros, se $\frac{p}{q}$ é raiz de $p(x)$ então $p \mid -3$ e $q \mid 2$, ou seja,

$$\frac{p}{q} \in \left\{ \pm 1, \pm\frac{1}{2}, \pm 3, \pm\frac{3}{2} \right\}.$$

   Verificando uma a uma, concluímos que só $\frac{1}{2}$ é raiz de $p(x)$.

   (b) Pela alínea anterior sabemos que $p(x)$ é divisível por $(2x - 1)$. Efectuando a divisão obtemos $p(x) = (2x-1)(x^3 - 3x^2 - 6x + 3)$. Pelo critério de Eisenstein, $x^3 - 3x^2 - 6x + 3$ é irredutível sobre $\mathbb{Q}$ (basta considerar o primo 3). Portanto, $(2x-1)(x^3 - 3x^2 - 6x + 3)$ é a factorização de $p(x)$ em factores irredutíveis sobre $\mathbb{Q}$.

   (c) α é raiz do polinómio $m(x) = x^3 - 3x^2 - 6x + 3 \in \mathbb{Q}[x]$, que é irredutível sobre $\mathbb{Q}$ como vimos. Portanto, $m(x)$ é o polinómio mínimo de α sobre $\mathbb{Q}$, pelo que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $\{1, \theta, \theta^2\}$ é uma base desta extensão.

   (d) Seja $f(x) = x$. Uma vez que $m(x) = f(x)(x^2 - 3x - 6) + 3$ (o que confirma que $mdc(m(x), f(x)) = 1$), então $3 = m(x) - (x^2 - 3x - 6)f(x)$, ou seja,

$$1 = \frac{m(x)}{3} - \frac{x^2 - 3x - 6}{3} f(x).$$

   Substituindo x por α obtemos $1 = -\dfrac{\alpha^2 - 3\alpha - 6}{3}\alpha$, o que mostra que em $\mathbb{Q}(\alpha)$

$$\alpha^{-1} = -\frac{1}{3}\alpha^2 + \alpha + 2.$$

Solução alternativa: Como $\alpha^3 - 3\alpha^2 - 6\alpha + 3 = 0$ então $\alpha^3 - 3\alpha^2 - 6\alpha = -3$, isto é, $\dfrac{\alpha(\alpha^2 - 3\alpha - 6)}{-3} = 1$. Logo, em $\mathbb{Q}(\alpha)$

$$\alpha^{-1} = -\frac{1}{3}\alpha^2 + \alpha + 2.$$

5. Não existe nenhum corpo com 12 elementos porque $12 = 2^2 \times 3$ não é uma potência de um primo. Como $256 = 2^8$, $\mathbb{F}_{256}$ tem característica 2, donde $1+1+1+1 = 0$. Portanto 1 é raiz do polinómio $p(x) = x^3 + x^2 + x + 1$ e consequentemente $x - 1 = x + 1$ é divisor de $p(x)$. Fazendo a divisão obtemos $p(x) = (x + 1)(x^2 + 1)$. Claramente $x^2 + 1$ tem novamente a identidade como raiz e factoriza-se em $(x + 1)(x + 1)$. Portanto $p(x) = (x + 1)^3$ pelo que tem uma única raiz (a identidade) com multiplicidade 3.

6. (a) Seja M um ideal maximal de A e $a \in A \setminus M$. Então o ideal

$$\langle M \cup \{a\}\rangle = \{m + ax \mid m \in M, x \in A\}$$

contém M estritamente pelo que terá que coincidir com A. Em particular, $1 \in \langle M \cup \{a\}\rangle$. Logo existem $m \in M$ e $x \in A$ tais que $1 = m + ax$, isto é, $1 - ax = m \in M$.

Reciprocamente, seja M um ideal próprio satisfazendo a condição enunciada e seja J um ideal de A satisfazendo $M \subset J \subseteq A$. Existe pelo menos um elemento $a \in J \setminus M$. Por hipótese existe então $x \in A$ tal que $1 - ax \in M$. Como $1 - ax \in J$ e $ax \in J$ então $1 \in J$ o que é suficiente para concluirmos que $J = A$ (de facto, como qualquer $a \in A$ se escreve na forma $a = a \cdot 1 \in J$, então $A \subseteq J$).

(b) Seja M um ideal maximal de A. Se $ab \in M$ e $b \notin M$ então, usando (a), existe $x \in A$ tal que $1 - bx = m \in M$. Logo $a = a \cdot 1 = a(m + bx) = am + abx \in M$. Isto mostra que

$$ab \in M \Rightarrow a \in M \text{ ou } b \in M,$$

logo M é primo.