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

Duração: 1h15m 1/06/2020

Soluções

1. (a) As possíveis raízes racionais de $q(x) = x^4 - x^2 - 2$ são 1, -1, 2 e -2. Nenhuma delas é raiz pelo que o polinómio não tem raízes racionais. Assim, a única hipótese dele ser redutível sobre $\mathbb{Q}$ é factorizar-se na forma

$$q(x) = (x^2 + ax + b)(x^2 + cx + d)$$

para alguns racionais a, b, c, d. Resolvendo o sistema correspondente

$$\begin{cases} a + c = 0 \\ b + ac + d = -1 \\ ad + bc = 0 \\ bd = -2. \end{cases}$$

chega-se a uma solução:

$$q(x) = (x^2 + 1)(x^2 - 2).$$

Finalmente, é evidente que cada um dos factores de $q(x)$ acima é irredutível (ambos de grau 2, nenhum tem raízes racionais). Temos assim encontrados os factores irredutíveis de $q(x)$.

(b) Seja θ uma raiz de $q(x)$. Pelo Teorema da Torre,

$$[\mathbb{Q}(\sqrt{2}, \theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \theta) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{2}, \theta) : \mathbb{Q}(\sqrt{2})],$$

pois $x^2 - 2$ é o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$. Qual é o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{2})$? Como θ é raiz de $q(x) = (x^2 + 1)(x^2 - 2)$ então $\theta = \pm i \notin \mathbb{Q}(\sqrt{2})$ ou $\theta = \pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. No primeiro caso, $x^2 + 1$ é o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{2})$ pelo que $[\mathbb{Q}(\sqrt{2}, \theta) : \mathbb{Q}] = 4$ e

$$\mathbb{Q}(\sqrt{2}, \theta) = \mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + c\,i + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}.$$

No segundo caso,

$$\mathbb{Q}(\sqrt{2}, \theta) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

(c) No caso $\theta = \pm i$, $\theta + 1 = 1 \pm i$, pelo que

$$(\theta + 1)^{-1} = \frac{1}{1 \pm i} = \frac{(1 \mp i)}{(1 \pm i)(1 \mp i)} = \frac{1 \mp i}{1 + 1} = \frac{1}{2} \mp \frac{1}{2}i.$$

No caso $\theta = \pm\sqrt{2}$, $\theta + 1 = 1 \pm \sqrt{2}$, pelo que

$$(\theta + 1)^{-1} = \frac{1}{1 \pm \sqrt{2}} = \frac{(1 \mp \sqrt{2})}{(1 \pm \sqrt{2})(1 \mp \sqrt{2})} = \frac{1 \mp \sqrt{2}}{1 - 2} = -1 \pm \sqrt{2}.$$

2. 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.

3. (a) A palavra $\mathbf{c} = (c_1,\, c_2,\, c_3,\, c_4,\, c_5) \in \mathbb{F}_3^5$ está em $\mathcal{C}$ sse

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

isto é, $c_1 + c_3 = 0,\ 2c_1 + c_2 + c_4 = 0$ e $2c_2 + c_5 = 0$.

Portanto, as palavras de $\mathbb{F}_3^5$ que pertencem a $\mathcal{C}$ são as palavras (nove ao todo)

$$(c_1,\ c_2,\ 2c_1,\ c_1 + 2c_2,\ c_1) \quad c_1, c_2 \in \mathbb{F}_3.$$

(b) $\mathrm{S}(\mathbf{y})$ é igual a

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

(c) Basta encontrar o líder da classe da palavra $\mathbf{y}$, ou seja, o líder da classe das palavras que têm síndrome igual a $\mathrm{S}(\mathbf{y})$. Estas úlimas palavras são solução da equação

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

isto é, são as palavras $(c_1,\ c_2,\ 2c_1 + 1,\ c_1 + 2c_2,\ c_2) \quad c_1, c_2 \in \mathbb{F}_3$. Pesquisando um pouco, torna-se evidente que a palavra neste conjunto com menor peso é a palavra $\mathbf{e} = (0,\ 0,\ 1,\ 0, 0)$. Assim, a palavra original correcta $\mathbf{c}$ é a palavra $\mathbf{c} = \mathbf{y} - \mathbf{e} = (1, 1, 2, 0, 1)$.

4. Seja $\theta \in L \setminus K$ (que existe pois $[L : K] > 1$ implica $L \neq K$). Como

$$2 = [L : K] = [L : K(\theta)]\,[K(\theta) : K]$$

e $[K(\theta) : K] > 1$ então $[L : K(\theta)] = 1$, isto é, $L = K(\theta)$.

Como $2 = [L : K] = [K(\theta) : K]$ então θ é raiz de um polinómio de grau 2 (o seu polinómio mínimo sobre K), da forma $x^2 + bx + c \in K[x]$. Por outro lado, a fórmula resolvente das equações do segundo grau vale em qualquer corpo K de característica diferente de 2 (para provar isso basta verificar que os elementos

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2} \quad (*)$$

satisfazem de facto a equação $x^2 + bx + c = 0$; é claro que a fórmula $(*)$ não faz sentido em corpos de característica 2 pois a divisão por $2 = 0$ não é possível...). Assim,

$$\theta = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{ou} \quad \theta = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Daqui decorre que $(2\theta + b)^2 = b^2 - 4c \in K$. Como $K(\theta) = K(2\theta + b)$, fica provado que $K(\theta) = K(\sqrt{\alpha})$ onde $\alpha = b^2 - 4c \in K$.