DMUC **Exame de Corpos e Equações Algébricas**

Duração: 2h30m 9/06/2011

Soluções

---

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

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

	V	**F**
(a) $\mathbb{N}$ é um subanel de $(\mathbb{Z}, +, \cdot)$. [Por exemplo, $1 \in \mathbb{N}$ mas $-1 \notin \mathbb{N}$.]		×
(b) Os polinómios $2x$ e $x+2$ de $\mathbb{Z}_3[x]$ são primos entre si. [$2x = 2(x+2)+2$ pelo que $\mathrm{mdc}(2x, x+2)$ é o polinómio mónico de $\mathbb{Z}_3[x]$ associado de 2, ou seja, 1.]	×	
(c) $2x^{50} + x^{49} - x^{48} + 18x^6 + 18x^5 - 2x - 2$ é irredutível sobre $\mathbb{Q}$. [Porque é de grau ≥ 2 e tem uma raiz racional: -1.]		×
(d) Se L é uma extensão finita de K e $\theta \in L$ então $\mathrm{grau}(\theta) \mid [L : K]$. [$\mathrm{grau}(\theta) = [K(\theta) : K]$ e pelo Teorema da Torre $[L : K] = [L : K(\theta)]\,[K(\theta) : K]$.]	×	
(e) Os corpos $\mathbb{F}_{11}[x]/\langle x^2 + x + 4\rangle$ e $\mathbb{F}_{11}[x]/\langle x^2 + 1\rangle$ são isomorfos. [Têm o mesmo cardinal (11^2) logo são ambos isomorfos a $\mathbb{F}_{11^2}$.]	×	

2. (a) A operação é comutativa em G:

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b+a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \quad (*)$$

   Assim, para provar que $(G, \cdot)$ é um grupo abeliano basta verificar que é um subgrupo do grupo multiplicativo das matrizes quadradas de ordem 2 com coeficientes inteiros, o que é óbvio:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G,$$

   o produto de quaisquer dois elementos de G pertence a G (evidente de $(*)$) e, também por $(*)$,

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in G$$

   (b) A comutatividade e associatividade da multiplicação em $\mathbb{Z}$ implicam imediatamente que $\odot$ é uma operação comutativa e associativa em G. O elemento neutro de $\odot$ é a matriz

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Finalmente, a distributividade é consequência do facto da multiplicação em $\mathbb{Z}$ ser distributiva relativamente à adição:

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \odot \left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & b+c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a(b+c) \\ 0 & 1 \end{bmatrix}$$

$$\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right) \cdot \left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & ac \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & ab+ac \\ 0 & 1 \end{bmatrix}$$

(c) I_n será primo se $I_n \neq G$ (portanto, se $n \neq 1$) e

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in I_n \quad \Rightarrow \quad \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in I_n \text{ ou } \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix} \in I_n$$

ou seja,

$$ab \in n\mathbb{Z} \Rightarrow a \in n\mathbb{Z} \text{ ou } b \in n\mathbb{Z}$$

isto é,

$$n \mid ab \Rightarrow n \mid a \text{ ou } n \mid b.$$

Portanto I_n é primo se e só se n é primo.

3. Como o polinómio é mónico, todas as raízes racionais são inteiras e divisoras de 1. Portanto as únicas possbilidades são 1 e -1. Claro que 1 nunca pode ser raiz e -1 é-o no caso de n ser ímpar. Em conclusão, se n é par $f(x)$ não tem raízes racionais e se n é ímpar tem uma única raiz racional, -1.

4. (a) Seja $\theta = \sqrt{1+\sqrt{3}} \in \mathbb{R}$. Como $\theta^2 = 1+\sqrt{3}$ então $\theta^2 - 1 = \sqrt{3}$ e, portanto, $(\theta^2-1)^2 = 3$. Assim $\theta^4 - 2\theta^2 - 2 = 0$ pelo que θ é raiz de $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. Este polinómio é irredutivel em $\mathbb{Q}[x]$, pelo critério de Eisenstein (tomando $p = 2$), e é assim o polinómio mínimo de θ sobre $\mathbb{Q}$.

(b) $[\mathbb{Q}(\theta) : \mathbb{Q}]$ é igual ao grau do polinómio mínimo de θ sobre $\mathbb{Q}$, isto é, 4. Uma base desta extensão sobre $\mathbb{Q}$ é então $(1, \theta, \theta^2, \theta^3)$ isto é,

$$\left(1, \sqrt{1+\sqrt{3}}, 1+\sqrt{3}, (1+\sqrt{3})\sqrt{1+\sqrt{3}}\right).$$

(c) Os elementos de $\mathbb{Q}(\sqrt{3})$ são da forma $a + b\sqrt{3}$, com $a, b \in \mathbb{Q}$. Comecemos por observar que $\theta \notin \mathbb{Q}(\sqrt{3})$:

$\theta \in \mathbb{Q}(\sqrt{3}) \Rightarrow \exists\, a, b \in \mathbb{Q} : \sqrt{1+\sqrt{3}} = a + b\sqrt{3} \Rightarrow 1 + \sqrt{3} = a^2 + 2ab\sqrt{3} + 3b^2$

$\Leftrightarrow 1 = a^2 + 3b^2, 1 = 2ab \Leftrightarrow a, b \neq 0, a = \frac{1}{2b}, 1 = \frac{1}{4b^2} + 3b^2 \Rightarrow 4b^2 = 1 + 12b^4$

$\Leftrightarrow 12b^4 - 4b^2 + 1 = 0 \Leftrightarrow b^2 = \frac{4 \pm \sqrt{-32}}{24} \notin \mathbb{Q}$, um absurdo!

Então o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{3})$ tem grau ≥ 2. Por outro lado, θ é raiz de $x^2 - (1+\sqrt{3}) \in \mathbb{Q}(\sqrt{3})[x]$, pelo que é este o polinómio mínimo de θ sobre $\mathbb{Q}(\sqrt{3})$.

5. Observemos antes de mais que as unidades de $D[x]$ são os polinómios constantes $u(x) = d$, com $d \in D \setminus \{0\}$ invertível. Denotemos este conjunto de polinómios por $\mathcal{U}_{D[x]}$.

   Seja $p(x) \in D[x]$ um polinómio mónico de grau 2 ou 3. Se $p(x)$ é redutível sobre D então $p(x) = q_1(x)q_2(x)$ com $q_1(x), q_2(x) \notin \mathcal{U}_{D[x]}$. Como $p(x)$ é mónico então os coeficientes dos termos de maior grau de $q_1(x)$ e $q_2(x)$ são invertíveis, o que garante que $q_1(x)$ e $q_2(x)$ não são constantes. Assim, necessariamente um destes dois polinómios é de grau 1, da forma $ax + b$, com a invertível. Este polinómio tem a raiz $-a^{-1}b \in D$, que será evidentemente também raiz de $p(x)$.

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

6. (a) É claro que α e β são simultaneamente raízes do polinómio nulo 0, donde $0 \in A$. Se $f(x), g(x) \in A$ e $t(x) \in K[x]$, então

   $$(f - g)(\alpha) = f(\alpha) - g(\alpha) = 0 - 0 = 0 = f(\beta) - g(\beta) = (f - g)(\beta)$$

   e

   $$(f\,t)(\alpha) = f(\alpha)\,t(\alpha) = 0\,t(\alpha) = 0 = f(\beta)\,t(\beta) = (f\,t)(\beta)$$

   pelo que $(f - g)(x) = f(x) - g(x) \in A$ e $(f\,t)(x) = f(x)\,t(x) \in A$, o que mostra que A é um ideal de $K[x]$.

   (b) Se $\alpha, \beta \in K$ então $h(x) = (x - \alpha)(x - \beta) \in K[x]$ e $h(\alpha) = h(\beta) = 0$, donde $h(x) \in A$. Portanto $\langle h(x)\rangle \subseteq A$, tendo-se $\langle h(x)\rangle = h(x)K[x]$ pois $K[x]$ é um anel comutativo com identidade. Admitamos que $p(x) \in A$. Como $p(\alpha) = 0$ então, pelo Teorema do Resto, $x - \alpha$ divide $p(x)$ em $K[x]$, pelo que existe $r(x) \in K[x]$ tal que $p(x) = (x - \alpha)r(x)$. Por outro lado, $0 = p(\beta) = (\beta - \alpha)r(\beta)$ em K, com $\beta - \alpha \neq 0$, o que implica imediatamente $r(\beta) = 0$. Isto significa que $x - \beta$ divide $r(x)$. Portanto $(x - \alpha)(x - \beta)$ divide $p(x)$, ou seja, $h(x)$ divide $p(x)$. Assim, $p(x) \in h(x)K[x] = \langle h(x)\rangle$.

   (c) Como $\alpha, \beta \in \overline{K}$ então α e β são algébricos sobre K e podemos falar nos polinómios mínimos $p_\alpha(x)$ e $p_\beta(x)$ de α e β respectivamente, sobre K.

   Admitamos que A é um ideal primo. Como $p_\alpha(\alpha) = 0 = p_\beta(\beta)$, então $p_\alpha(x)p_\beta(x) \in A$. Como A é primo, podemos então concluir que $p_\alpha(x) \in A$ ou $p_\beta(x) \in A$. Sem perda de generalidade, suponhamos que $p_\alpha(x) \in A$. Então $p_\alpha(\beta) = 0$. Por ser polinómio mínimo de α, $p_\alpha(x)$ é irredutível e mónico e sendo anulador de β tem de ser o seu polinómio mínimo. Assim, $p_\alpha(x) = p_\beta(x)$.

   Reciprocamente, admitamos que $p_\alpha(x) = p_\beta(x)$. Sejam $f_1(x), f_2(x) \in K[x]$ tais que $f_1(x)f_2(x) \in A$. Então $f_1(\alpha)f_2(\alpha) = 0 = f_1(\beta)f_2(\beta)$. Logo $f_1(\alpha) = 0$ ou $f_2(\alpha) = 0$. No primeiro caso $p_\alpha(x)$ divide $f_1(x)$. Logo existe $r(x) \in K[x]$ tal que $f_1(x) = p_\alpha(x)\,r(x) = p_\beta(x)\,r(x)$. Portanto $f_1(\beta) = p_\beta(\beta)\,r(\beta) = 0\,r(\beta) = 0$, o que mostra que $f_1(x) \in A$. No segundo caso, podemos mostrar de modo análogo que $f_2(x) \in A$.