DMUC **Exame de Corpos e Equações Algébricas**

Duração: 2h30m 29/06/2011

Soluções

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

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

	V	**F**
(a) Seja A um anel. Então $(a+b)(a-b) = a^2 - b^2$ para quaisquer $a, b \in A$. [Como $(a+b)(a-b) = a^2 - ab + ba - b^2$, a afirmação é falsa em anéis não comutativos.]		×
(b) Em $\mathbb{Z}_{16}[x]$, $4x^2 + 2x + 4$ é um divisor de zero. [$8 \cdot (4x^2 + 2x + 4) = 0$.]	×	
(c) $\mathbb{Q}[x]/\langle 2x^{50} - x^{49} + 18x^5 - 9x^4 + 6x - 3\rangle$ é um corpo. [Basta observar que $2x^{50} - x^{49} + 18x^5 - 9x^4 + 6x - 3$ é redutível sobre $\mathbb{Q}$ pois é de grau ≥ 2 e tem uma raiz racional: $1/2$.]		×
(d) Sejam K,K_1 e K_2 corpos com $K \subseteq K_i$ $(i = 1, 2)$. Se K_1 e K_2 são extensões finitas de K e $\text{mdc}([K_1 : K], [K_2 : K]) = 1$ então $K \subsetneq K_1 \cap K_2$. [Contra-exemplo: $K = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$ e $K_2 = \mathbb{Q}(\sqrt[3]{2})$.]		×

2. (a) $(x^2 + 1)(x^2 + 1)$.

   (b) As únicas possíveis raízes racionais de p_m são 1 e -1. Como $p_m(1) = m - m^2 = m(1-m)$ e $p_m(-1) = m^2 + m - 2$ então para $m = 0$, $m = 1$ e $m = -2$, p_m tem raízes racionais (1 nos dois primeiros casos e -1 nos últimos dois).

3. (Teorema 2.7 nos Apontamentos) Seja I um ideal de $K[x]$. Se $I = \{0\}$, então $I = \langle 0\rangle$, que é um ideal principal. Podemos pois admitir que $I \neq \{0\}$.

   Consideremos então o conjunto $N = \{n \in \mathbb{N}_0 \mid \text{ existe } s(x) \in I, gr(s(x)) = n\}$. 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 (podemos supor que $m(x)$ é mónico; com efeito, se não fosse, isto é, se o coeficiente do termo de maior grau fosse igual a $a \neq 1$, poderíamos sempre considerar o polinómio $n(x) = a^{-1}m(x) \in I$).

   Provemos que I é principal mostrando 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 temos $p(x) = q(x)m(x) + r(x)$, onde $gr(r(x)) < gr(m(x))$. 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 $gr(m(x))$. Assim, $p(x)$ é um múltiplo de $m(x)$ pelo que pertence ao ideal $\langle m(x)\rangle$.

   Se K não é um corpo, o anel de polinómios $K[x]$ não é necessariamente de ideais principais. Por exemplo, para $K = \mathbb{Z}$, o ideal $\langle 2, x\rangle$ de $K[x]$ não é principal.

4. $p(4) = 2 \cdot 4^{100} + 60 = 2^{201} + 60$. Assim, em $\mathbb{F}_3$, $p(4) = (2^{201} + 60) \mod 3 = 2^{201} \mod 3$. Mas $2 \mod 3 = 2$, $2^2 \mod 3 = 1$, $2^3 \mod 3 = 2$, etc., isto é, $2^n \mod 3$ é igual a 1 se n é par e igual a 2 se n é ímpar logo $p(4) = 2$.

   Por outro lado, em $\mathbb{F}_7$, $p(4) = (2^{201} + 60) \mod 7 = (2^{201} + 4) \mod 7$. Neste caso, $2 \mod 7 = 2, 2^2 \mod 7 = 4, 2^3 \mod 7 = 1, 2^4 \mod 7 = 2, 2^5 \mod 7 = 4$, etc.. Como 201 é divisível por 3 então $2^{201} \mod 7 = 1$ e consequentemente $p(4) = 5$.

5. (a) O polinómio $x^3 - 6x^2 + 9x + 3$, do qual θ é raiz, é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$), logo é o polinómio mínimo $m(x)$ de θ sobre $\mathbb{Q}$. Seja $f(x) = x^2 - 6x + 8$. Uma vez que $m(x) = xf(x) + x + 3$ e $f(x) = (x - 9)(x + 3) + 35$ (o que confirma que $mdc(m(x), f(x)) = 1$), então

$$35 = f(x) - (x - 9)(m(x) - xf(x)) = (x^2 - 9x + 1)f(x) - (x - 9)m(x),$$

   ou seja,

$$1 = \frac{1}{35}[(x^2 - 9x + 1)f(x) - (x - 9)m(x)].$$

   Substituindo x por θ obtemos $1 = \frac{1}{35}(\theta^2 - 9\theta + 1)f(\theta)$, o que mostra que

$$(\theta^2 - 6\theta + 8)^{-1} = f(\theta)^{-1} = \frac{1}{35}(\theta^2 - 9\theta + 1).$$

   (b) Pelo Teorema da Torre,

$$[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

   Como $x^2 - 3$ é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$), trata-se do polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$, donde $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Por outro lado, θ é raiz do polinómio $x^2 + \sqrt{3}x + 3 \in \mathbb{Q}(\sqrt{3})[x]$. Será este polinómio irredutível sobre $\mathbb{Q}(\sqrt{3})$? Pela fórmula resolvente das equações do segundo grau, as suas duas raízes são

$$\frac{-\sqrt{3} \pm \sqrt{3 - 12}}{2},$$

   ambas não reais. Logo, pelo critério das raízes, $x^2 + \sqrt{3}x + 3$ é irredutível sobre $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, donde $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})] = 2$. Em conclusão, $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = 2 \times 2 = 4$.

   (c) Pelo Teorema da Torre,

$$[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

   Como $x^3 - 2$ é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 2$), trata-se do polinómio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, donde $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Por outro lado, θ é raiz do polinómio $p(x) = x^2 + \frac{3}{2}x + \frac{3}{2} \in \mathbb{Q}[x]$. Será este polinómio irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$? Sim. Podemos provar isso de modo análogo à alínea anterior ou alternativamente do seguinte modo: $p(x) \in \mathbb{Q}[x]$, é irredutível sobre $\mathbb{Q}$ (se fosse redutível então $2p(x) = 2x^2 + 3x + 3$ também seria, o que não é possível pelo critério de Eisenstein) e o seu grau, maior do que 1, é um número primo com $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Logo $p(x)$ não tem raízes em $\mathbb{Q}(\sqrt[3]{2})$. Assim, pelo critério das raízes, $p(x)$ é irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$, donde $[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Em conclusão, $[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}] = 2 \times 3 = 6$.

6. Seja $\theta \in L \setminus K$ (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 $\alpha = b^2 - 4c \in K$.