DMat-FCTUC **Exame (época de recurso) de Corpos e Equações Algébricas**

Duração: 2h30m 21/06/2018

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 $(\mathbb{Z}, +, \cdot)$.		×
(b) O resto da divisão de $x^{100} + 3x + 1$ por $x + 1$ é igual a -1.	×	
(c) A raiz real de $p(x) = x^5 - 2x^3 + 4x + 2$ é construtível a partir dos racionais.		×

   [Por exemplo, $1 \in \mathbb{N}$ mas $-1 \notin \mathbb{N}$.]

   [Como $x + 1 = x - (-1)$, o resto da divisão de $q(x) = x^{100} + 3x + 1$ por $x + 1$ é, pelo Teorema do Resto, igual a $p(-1) = (-1)^{100} + 3(-1) + 1 = -1$.]

   [Seja α a raiz real de $p(x) = x^5 - 2x^3 + 4x + 2$ (que existe porque o grau de $p(x)$ é ímpar). O polinómio $p(x)$ é irredutível sobre $\mathbb{Q}[x]$ (pelo critério de Eisenstein). Como é mónico, então é o polinómio mínimo de α sobre $\mathbb{Q}$. Assim $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Como este número não é uma potência de 2, pelo critério algébrico estudado sobre a construtibilidade (por régua e compasso) de números, podemos concluir que α não é construtível.]

2. (a) $p(x) = x^{10} + 3x^5 - \frac{9}{5}x^3 + 27x^2 + 3 = \frac{1}{5}(5x^{10} + 15x^5 - 9x^3 + 27x^2 + 3)$. Como o último polinómio é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$) e é associado de $p(x)$, então $p(x)$ também é irredutível sobre $\mathbb{Q}$ pelo que coincide com a sua factorização em irredutíveis.

   (b) Como, pelo Algoritmo de Euclides,

   $$x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 2) + (x + 2)$$
   $$x^2 + x + 1 = (x + 2)(x + 2)$$

   então $\text{mdc}(x^4 + x^3 + 1, x^2 + x + 1) = x + 2$.

3. (a) A diz-se um *domínio de integridade* quando tiver uma identidade (isto é, um elemento neutro para a segunda operação) e não tiver divisores de zero. Será um *corpo* quando, além disso, todo o elemento $\neq 0$ possuir inverso (para a segunda operação).

   (b) Claramente $I : J \neq \emptyset$ pois o zero do anel A pertence sempre a $I : J$. Além disso:

   - Para quaisquer $x, y \in I : J$, $x - y \in I : J$: de facto, se $xJ, yJ \subseteq I$, então $(x - y)J \subseteq I$ pois, para qualquer $j \in J$, $(x - y)j = xj - yj \in I$ (uma vez que, I sendo um ideal, é fechado para a subtracção).
   - Para quaisquer $a \in A$ e $x \in I : J$, $ax \in I : J$: se $xJ \subseteq I$, então $(ax)J \subseteq I$ pois, para qualquer $j \in J$, $(ax)j = a(xj) \in I$ (uma vez que $xj \in I$, por hipótese, e I é um ideal).

(c) Por um lado,

$$2\mathbb{Z}\colon 4\mathbb{Z} = \{x \in \mathbb{Z} \mid x(4\mathbb{Z}) \subseteq 2\mathbb{Z}\} = \mathbb{Z}$$

(pois qualquer elemento de $x(4\mathbb{Z})$ será sempre um múltiplo de 4 logo, em particular, múltiplo de 2), enquanto

$$4\mathbb{Z}\colon 2\mathbb{Z} = \{x \in \mathbb{Z} \mid x(2\mathbb{Z}) \subseteq 4\mathbb{Z}\} = 2\mathbb{Z}$$

(se x for um múltiplo de 2, então multiplicado por qualquer múltiplo de 2 será sempre um múltiplo de 4; reciprocamente, se x não for múltiplo de 2 será ímpar pelo que multiplicado pelos múltiplos de 2 que não são múltiplos de 4, nunca dará um múltiplo de 4).

4. (a) Seja $\theta = \sqrt{1+3i}$. Então

$$\theta^2 = 1 + 3i \Leftrightarrow \theta^2 - 1 = 3i \Rightarrow (\theta^2-1)^2 = -9 \Leftrightarrow \theta^4 - 2\theta^2 + 10 = 0.$$

Portanto θ é raiz do polinómio mónico $x^4 - 2x^2 + 10 \in \mathbb{Q}[x]$. Como este polinómio é mónico (pelo critério de Eisenstein, $p = 2$), trata-se do polinómio mínimo de θ sobre $\mathbb{Q}$.

(b) As possíveis raízes racionais de $p(x)$ são $\pm 1, \pm 3$. É evidente que 1 e -1 são raízes, donde $p(x) = (x-1)(x+1)(x^2-3)$ e as outras duas raízes são irracionais, $\sqrt{3}$ e $-\sqrt{3}$. Claramente, o corpo de decomposição de $p(x)$ é a extensão $\mathbb{Q}(\sqrt{3})$. Como x^2-3 é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$, esta extensão é o corpo $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.

(c) Uma vez que $\sqrt{8} = 2\sqrt{2}$, então $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$. Logo $[\mathbb{Q}(\sqrt{8}) : \mathbb{Q}(\sqrt{2})] = 1$ e a base é simplesmente $\{1\}$.

Alternativa: Como $\sqrt{8} = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, então $x - \sqrt{8} \in \mathbb{Q}(\sqrt{2})[x]$ pelo que será este o polimónio mínimo de $\sqrt{8}$ sobre $\mathbb{Q}(\sqrt{2})$, donde $[\mathbb{Q}(\sqrt{8}) : \mathbb{Q}(\sqrt{2})] = 1$.

(d) É óbvio que $\mathbb{Q}(\sqrt{2}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{5})$ pois evidentemente $\sqrt{2}+\sqrt{5} \in \mathbb{Q}(\sqrt{2},\sqrt{5})$. Por outro lado, se dizem que $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ é uma extensão de $\mathbb{Q}(\sqrt{5})$ é porque $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$ (e, claro, por simetria também $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$). Portanto $\mathbb{Q}(\sqrt{2},\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$ e temos a igualdade $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2},\sqrt{5})$

Nota: Não é difícil observar directamente que $\mathbb{Q}(\sqrt{2},\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$. Com efeito, como $(\sqrt{2}+\sqrt{5})^2 = 7 + 2\sqrt{10}$, então $\sqrt{10} \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$, e como $\sqrt{10}(\sqrt{2}+\sqrt{5}) = 2\sqrt{5} + 5\sqrt{2}$, também $2\sqrt{5}+5\sqrt{2}$ pertence a $\mathbb{Q}(\sqrt{2}+\sqrt{5})$. Então

$$\sqrt{2} = \frac{1}{3}[(2\sqrt{5}+5\sqrt{2}) - (2\sqrt{2}+2\sqrt{5})] \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$$

e

$$\sqrt{5} = -\frac{1}{3}[(2\sqrt{5}+5\sqrt{2}) - (5\sqrt{2}+5\sqrt{5})] \in \mathbb{Q}(\sqrt{2}+\sqrt{5}).$$

Assim $[\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}(\sqrt{5})] = [\mathbb{Q}(\sqrt{5},\sqrt{2}) : \mathbb{Q}(\sqrt{5})] = 2$ pois x^2-2 é o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}(\sqrt{5})$, uma vez que é irredutível sobre $\mathbb{Q}(\sqrt{5})$ pois as suas duas raízes irracionais, $\pm\sqrt{2}$, não pertencem a $\mathbb{Q}(\sqrt{5})$: $a + b\sqrt{5} = \pm\sqrt{2}$ implica $b \neq 0$ (senão $\sqrt{2}$ seria racional!) e $a \neq 0$ (senão $\sqrt{2/5}$ seria racional!). Portanto

$$a + b\sqrt{5} = \pm\sqrt{2} \Rightarrow a, b \neq 0, (a+b\sqrt{5})^2 = 2 \Leftrightarrow a, b \neq 0, 2ab\sqrt{5} = 2 - a^2 - 5b$$
$$\Leftrightarrow \sqrt{5} = \frac{2-a^2-5b}{2ab} \in \mathbb{Q} \text{ !!!}$$

5. (a) Um ideal I do anel A diz-se *maximal* se $I \neq A$ e, para qualquer ideal J de A, a propriedade $I \subseteq J$ implica $J = I$ ou $J = A$.

   (b) Provemos que $p(x)$ é redutível se e só se $I = \langle p(x) \rangle$ não é maximal.

   Suponhamos que $p(x)$ é redutível. Então ou é invertível ou tem um factor próprio. No primeiro caso tem-se $1 = (p(x))^{-1}p(x) \in I$, donde $I = K[x]$ não é maximal. No segundo caso tem-se $p(x) = q_1(x)q_2(x)$ com $gr(q_1(x)) \geq 1$ e $gr(q_2(x)) \geq 1$. Então $1 \leq gr(q_1(x)) < gr(p(x))$, pelo que

   $$\langle p(x) \rangle \subset \langle q_1(x) \rangle \subset K[x],$$

   o que mostra que, também neste caso, I não é maximal.

   Reciprocamente, suponhamos que I não é maximal, ou seja, que existe um ideal $J = \langle q(x) \rangle$ (pois, como sabemos, $K[x]$ 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 em $K[x]$.

   (c) Temos $K \subseteq K(\theta^2) \subseteq K(\theta) \subseteq L$ e $[L : K] = 5$. Como θ é raiz de $x^2 - \theta^2 \in K(\theta^2)[x]$ então $[K(\theta) : K(\theta^2)] \leq 2$. Por outro lado, pelo Teorema da Torre, $[K(\theta) : K(\theta^2)]$ divide $[L : K]$. Logo $[K(\theta) : K(\theta^2)] = 1$ e, consequentemente, $K(\theta) = K(\theta^2)$.
