Departamento de Matemática da Universidade de Coimbra

Corpos e Equações Algébricas

SOLUÇÕES **Frequência** 27/05/08

---

1. (a) $\mathbb{Z}$ é todo o anel logo não é maximal.

   $4\mathbb{Z}$ não é maximal pois $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.

   $3\mathbb{Z}$ é maximal pois sendo $\mathbb{Z}$ um domínio de ideais principais, um ideal $I =< n >= n\mathbb{Z}$ é maximal sse n é primo.

   (b) $6x + 6$ é de grau 1 logo é irredutível em $\mathbb{R}[x]$ (pois $\mathbb{R}$ é um corpo).

   $x^2 + 4$ tem grau 2 e não tem raízes reais, logo é irredutível em $\mathbb{R}[x]$.

   $x^3 + 1$ tem grau 3 logo é redutível em $\mathbb{R}[x]$ (tem-se $x^3 + 1 = (x + 1)(x^2 - x + 1)$ em $\mathbb{R}[x]$.

   (c) $2x^2 + 2 = 2(x^2 + 1)$ em $\mathbb{Z}[x]$ e nem 2 nem $x^2 + 1$ são unidades de $\mathbb{Z}[x]$, pelo que $2x^2 + 2$ é redutível em $\mathbb{Z}[x]$.

   x^3+3x^2+6x+3 é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein e como é mónico então é irredutível em $\mathbb{Z}[x]$.

   $x^2 - 1 = (x - 1)(x + 1)$ e nem $x - 1$ nem $x + 1$ são unidades de $\mathbb{Z}[x]$, logo $x^2 - 1$ é redutível em $\mathbb{Z}[x]$.

2. (a) Um polinómio $p(x) \in K[x]$ diz-se o *polinómio mínimo* de $\theta \in L$ sobre K se é mónico, irredutível sobre $K[x]$ e admite θ como raiz.

   (b) (i) 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 $\mathbb{Q}$.

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

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

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

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

   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 $\mathbb{Q}(\sqrt{3})$.

(iii) $[\mathbb{Q}(\theta):\mathbb{Q}]$ 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,

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

3. (a) Se $d \in D - \{0\}$, então para quaisquer $x, y \in D$,

$$dx = dy \Leftrightarrow dx - dy = 0 \Leftrightarrow d(x-y) = 0 \Rightarrow x - y = 0 \Leftrightarrow x = y,$$

o que mostra que ϕ_d é injectiva.

(b) Se D é finito então, para cada $d \in D - \{0\}$, sendo injectiva, ϕ_d é imediatamente bijectiva. Portanto, existe $c \in D$ tal que $\phi_d(c) = 1$, isto é, $dc = 1$. Isto significa que qualquer $d \in D - \{0\}$ é invertível e D é um corpo.

4. (a) O polinómio $p(x) = x^3 + 2x^2 + 1$ tem grau 3 e não tem raízes em $\mathbb{Z}_5$ logo é irredutível em $\mathbb{Z}_5[x]$ (de facto, $p(0) = 1$, $p(1) = 4$, $p(2) = 2$, $p(3) = 1$ e $p(4) = 2$). Portanto, o ideal $\langle p(x) \rangle$ é maximal em $\mathbb{Z}_5[x]$ e $K = \mathbb{Z}_5[x]/\langle p(x) \rangle$ é um corpo. Tem-se

$$\begin{aligned} K &= \{a_0 + a_1x + a_2x^2 + \langle p(x) \rangle \mid a_0, a_1, a_2 \in \mathbb{Z}_5\} \\ &\cong \{a_0 + a_1\theta + a_2\theta^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_5\} \end{aligned}$$

com $\theta^3 = -2\theta^2 - 1 = 3\theta^2 + 4$.

(b) Cada elemento de K admite uma única expressão $a_0 + a_1\theta + a_2\theta^2$, com $a_0, a_1, a_2 \in \mathbb{Z}_5$, pelo que $|K| = 5^3 = 125$. Como $\mathbb{Z}_5 \subseteq K$ e a característica de $\mathbb{Z}_5$ é 5, obtemos $car(K) = 5$. Por outro lado, $[K : \mathbb{Z}_5] = 3$ já que $(1, \theta, \theta^2)$ constitui uma base do espaço vectorial K sobre $\mathbb{Z}_5$.

5. (a) Seja $p(x) = x^4 - 3x^3 + 2x^2 + 2x - 4$. Se $p(1+i) = 0$ então $p(1-i) = 0$ (pois em geral, se $a + bi$ é raiz de $p(x)$ também $a - bi$ é raiz de $p(x)$). Portanto, $(x - (1+i))(x - (1-i)) = x^2 - 2x + 2$ divide $p(x)$ em $\mathbb{Q}[x]$. De facto,

$$x^4 - 3x^3 + 2x^2 + 2x - 4 = (x^2 - 2x + 2)(x^2 - x - 2).$$

Vejamos agora se $x^2 - x - 2$ tem raízes em $\mathbb{Q}$:

$$x^2 - x - 2 = 0 \Leftrightarrow x = \frac{1 \pm \sqrt{1+8}}{2} = \frac{1 \pm 3}{2} \Leftrightarrow x = 2 \vee x = -1.$$

Em conclusão, $p(x) = (x^2 - 2x + 2)(x - 2)(x + 1)$ é a decomposição de $p(x)$ em factores irredutíveis em $\mathbb{Q}[x]$ ($x^2 - 2x + 2$ é irredutível em $\mathbb{Q}[x]$ porque tem grau 2 e não tem raízes racionais).

(b) Seja agora $p(x) = x^5 - 2x^3 + 4x + 2$.

(i) Em $\mathbb{C}[x]$, $p(x)$ decompõe-se em 5 factores lineares (pois $\mathbb{C}$ é um corpo algebricamente fechado) correspondentes às suas 5 raízes em $\mathbb{C}$. Além disso, as raízes complexas não reais aparecem aos pares. Como 5 é ímpar, uma dessas raízes é necessariamente real.

(ii) 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.

6. Temos $K \subseteq K(\theta^2) \subseteq K(\theta) \subseteq L$ e $[L : K] = 7$. 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, $K(\theta) = K(\theta^2)$.
