Departamento de Matemática da Universidade de Coimbra

Corpos e Equações Algébricas

SOLUÇÕES **Exame de recurso** 7/07/08

---

1. (a) É verdadeira:

   Pelo Teorema do Resto, $p(x)$ é da forma $(x-2)q(x)$. Derivando vem $p'(x) = q(x) + (x-2)q'(x)$. Mas $x-2$ também divide $p'(x)$ pois 2 também é raiz de $p'(x)$. Logo $x-2$ divide $q(x)$, o que mostra que $(x-2)^2$ divide $p(x)$.

   (b) É verdadeira:

   Todo o ideal maximal é, em particular, primo. Portanto, se um ideal não é primo, nunca pode ser maximal.

   (c) É verdadeira:

   Se $1+i$ é raiz de $p(x)$, então o seu conjugado $1-i$ também o é. Logo $p(x)$ é divisível por $(x-(1+i))(x-(1-i)) = x^2-2x+2$.

   (d) É falsa:

   A duplicação de um cubo de lado unitário é equivalente à construção, a partir de $\mathbb{Q}$, de um segmento de comprimento $\sqrt[3]{2}$. Se tal fosse possível, então $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ seria uma potência de 2. Ora $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, pois x^3-2 é o polinómio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$.

2. (a) Se $\sqrt{2}\,i$ é raiz de $p(x)$, então o seu conjugado $-\sqrt{2}\,i$ também o é, logo $p(x)$ é divisível por $(x-\sqrt{2}\,i)(x+\sqrt{2}\,i)$, isto é, por x^2+2. Efectuando a divisão de $p(x)$ por x^2+2 obtemos $p(x) = (x^2+2)(x^2-2x+2)$. Determinemos as duas raízes complexas de x^2-2x+2:

$$x = \frac{2 \pm \sqrt{4-8}}{2} = \frac{2 \pm 2i}{2} = 1 \pm i.$$

   Em conclusão, as raízes de $p(x)$ são $\pm\sqrt{2}\,i$, $1 \pm i$. Logo, o corpo de decomposição de $p(x)$ é a extensão

$$\begin{aligned} F &= \mathbb{Q}(\sqrt{2}\,i, -\sqrt{2}\,i, 1+i, 1-i) \\ &= \mathbb{Q}(\sqrt{2}\,i, 1+i, 1-i) && \text{(pois } -\sqrt{2}\,i \text{ é simétrico de } \sqrt{2}\,i) \\ &= \mathbb{Q}(\sqrt{2}\,i, i, -i) && \text{(pois } 1 \in \mathbb{Q}) \\ &= \mathbb{Q}(\sqrt{2}\,i, i) && \text{(pois } -i \text{ é simétrico de } i) \\ &= \mathbb{Q}(\sqrt{2}, i) && \text{(pois } \sqrt{2} = -(\sqrt{2}\,i)i). \end{aligned}$$

   (b) Pelo Teorema da Torre,

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

   O segundo factor é igual a 2 pois x^2-2 é claramente o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$. Quanto ao primeiro factor, também é igual a 2 pois x^2+1 é o polinómio mínimo de i sobre $\mathbb{Q}(\sqrt{2})$ (a irredutibilidade é também óbvia neste caso pois $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ e as raízes de x^2+1 são imaginárias). Em conclusão, $[F : \mathbb{Q}] = 4$ e $\{1, \sqrt{2}, i, \sqrt{2}\,i\}$ constitui uma base de F sobre $\mathbb{Q}$.

(c) $(1+\sqrt{2})(1+\sqrt{2}\,i) = 1+\sqrt{2}\,i+\sqrt{2}+2i = 1+\sqrt{2}+2i+\sqrt{2}\,i$ tem coordenadas $(1,1,2,1)$ na base de (b).

3. (a) Pelo critério de Eisenstein ($p=2$), o polinómio x^3-4x+2 é irredutível sobre $\mathbb{Q}$ pelo que se trata do polinómio mínimo de θ sobre $\mathbb{Q}$. Portanto, $[\mathbb{Q}(\theta):\mathbb{Q}]=3$.

(b) Calculemos primeiro o inverso de $\theta+1$ em $\mathbb{Q}(\theta)$, ou seja, o elemento $a\theta^2+b\theta+c$ de $\mathbb{Q}(\theta)$ que satisfaz $(\theta+1)(a\theta^2+b\theta+c)=1$. Esta última igualdade é equivalente a

$$\begin{aligned} a\theta^3+(b+a)\theta^2+(c+b)\theta+c=1 &\Leftrightarrow a(4\theta-2)+(b+a)\theta^2+(c+b)\theta+c-1=0 \\ &\Leftrightarrow (a+b)\theta^2+(4a+b+c)\theta+(-2a+c-1)=0. \end{aligned}$$

Como $1,\theta,\theta^2$ são linearmente independentes, obtemos então o sistema

$$\begin{cases} a+b=0 \\ 4a+b+c=0 \\ -2a+c-1=0 \end{cases}$$

que tem solução $a=-1/5$, $b=1/5$ e $c=3/5$. Portanto[1],

$$(\theta+1)^{-1}=\frac{-\theta^2+\theta+3}{5}.$$

Finalmente,

$$\begin{aligned} \frac{5\theta^2-10}{\theta+1} &= (5\theta^2-10)\left(\frac{-\theta^2+\theta+3}{5}\right) \\ &= (\theta^2-2)(-\theta^2+\theta+3) \\ &= -\theta^4+\theta^3+5\theta^2-2\theta-6 \\ &= -(4\theta^2-2\theta)+(4\theta-2)+5\theta^2-2\theta-6 \\ &= \theta^2+4\theta-8. \end{aligned}$$

4. (a) $\mathcal{N}(\mathbb{Z})=\{a\in\mathbb{Z}\mid \exists n\in\mathbb{N}, a^n=0\}=\{0\}$.

$$\begin{aligned} \mathcal{N}(\mathbb{Z}_{32}) &= \{a\in\mathbb{Z}_{32}\mid \exists n\in\mathbb{N}, a^n=0\} \\ &= \{a\in\mathbb{Z}_{32}\mid \exists n\in\mathbb{N}, 32 \text{ divide } a^n\}. \end{aligned}$$

Ora $32|a^n \Rightarrow a^n$ é par $\Rightarrow a$ é par $\Rightarrow a$ é par;
Reciprocamente, a é par $\Rightarrow 2|a \Rightarrow 2^5|a^5 \Rightarrow 32|a^5$. Portanto,

$$\begin{aligned} \mathcal{N}(\mathbb{Z}_{32}) &= \{a\in\mathbb{Z}_{32}\mid a \text{ é par }\} \\ &= \{0,2,4,6,\ldots,30\}. \end{aligned}$$

(b) (i) $0^1=0$ pelo que $0\in\mathcal{N}(A)$.
Sejam $a\in\mathcal{N}(A)$ e $x\in A$. Então $a^n=0$ para algum $n\in\mathbb{N}$ e, consequentemente, $(ax)^n=a^nx^n=0$, o que mostra que $ax\in\mathcal{N}(A)$.
Finalmente, sejam $a,b\in\mathcal{N}(A)$. Então $a^n=0=b^m$ para alguns naturais n e m. Pretendemos provar que $a-b\in\mathcal{N}(A)$. O caso $a=0$ ou $b=0$ é óbvio.

[1] Alternativamente, podia-se também determinar o inverso de $\theta+1$ usando o algoritmo de Euclides no cálculo de $\text{mdc}(x+1,x^3-4x+2)=1$.

Suponhamos então $a, b \neq 0$ (donde $n, m > 1$). Pela fórmula do binómio de Newton (que provámos ser verdadeira num anel comutativo qualquer),

$$\begin{aligned}(a-b)^{nm} &= \sum_{k=0}^{nm} \binom{nm}{k} a^k (-b)^{nm-k} \\ &= a^0 b^{nm} + \binom{nm}{1} a b^{nm-1} + \binom{nm}{2} a^2 b^{nm-2} + \ldots + \binom{nm}{n-1} a^{n-1} b^{nm-n+1} + \\ &\quad + \binom{nm}{n} a^n b^{nm-n} + \ldots + \binom{nm}{nm-1} a^{nm-1} b + a^{nm} b^0.\end{aligned}$$

Neste último somatório, as parcelas da linha de cima são todas nulas porque o expoente em b é sempre $\geq m$ (note que $nm - n + 1 = n(m-1) + 1$ é $\geq m$ pois $n(m-1) \geq m - 1$ uma vez que $m - 1 > 0$ e $n > 1$); na linha de baixo são também todas nulas porque o expoente em a é sempre $\geq n$.
Portanto, $(a-b)^{nm} = 0$, o que mostra que $a - b \in \mathcal{N}(A)$.

(ii) Seja I um ideal primo de A. Para cada $a \in \mathcal{N}(A)$, existe $n \in \mathbb{N}$ tal que $a^n = 0 \in I$. Como I é primo, então $a \in I$.

(iii) $A/\mathcal{N}(A) = \{a + \mathcal{N}(A) \mid a \in A\}$ pelo que

$$\begin{aligned}a + \mathcal{N}(A) \in \mathcal{N}(A/\mathcal{N}(A)) &\Leftrightarrow \exists n \in \mathbb{N} : (a + \mathcal{N}(A))^n = \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N} : a^n + \mathcal{N}(A) = \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N} : a^n \in \mathcal{N}(A) \\ &\Leftrightarrow \exists n \in \mathbb{N}, \exists m \in \mathbb{N} : (a^n)^m = 0 \\ &\Leftrightarrow \exists n, m \in \mathbb{N} : a^{nm} = 0 \\ &\Leftrightarrow a \in \mathcal{N}(A) \\ &\Leftrightarrow a + \mathcal{N}(A) = \mathcal{N}(A).\end{aligned}$$

Portanto $\mathcal{N}(A/\mathcal{N}(A)) = \{\mathcal{N}(A)\}$.

5. (a) $V(\alpha) = \frac{1}{3}$ Área$_{\text{base}} \times$ altura $= \frac{1}{3}(2\alpha)^2\alpha = \frac{4}{3}\alpha^3$.

   (b) Se $\frac{4}{3}\alpha^3 = \alpha^2 + 1$ então α é raiz de $4x^3 - 3x^2 - 3 \in \mathbb{Q}[x]$, sendo este polinómio irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein). Assim, o polinómio mínimo de α sobre $\mathbb{Q}$ é de grau 3 pelo que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \neq 2^t$, $(t \in \mathbb{N}_0)$. Logo α não é um real construtível.

6. $\Rightarrow$: Seja L uma extensão algébrica de K e seja $\theta \in L$. Como $[K(\theta) : K]$ é dada pelo grau de um polinómio irredutível, então $[K(\theta) : K] = 1$. Logo $K(\theta) = K$, ou seja, $\theta \in K$, o que mostra que $L = K$. Portanto, a única extensão algébrica de K é o próprio K.

   $\Leftarrow$: Se não existem extensões algébricas próprias de K então K é um corpo algebricamente fechado. Seja $p(x) \in K[x]$ um polinómio irredutível sobre K de grau ≥ 1. Por hipótese, $p(x)$ tem uma raiz θ em K, isto é, $p(x) = (x - \theta)q(x)$ para algum $q(x) \in K[x]$. Como $p(x)$ é irredutível sobre K, $q(x)$ só pode ser uma constante, o que garante que $p(x)$ tem grau 1.