Departamento de Matemática da Universidade de Coimbra **Exame de Álgebra II**

Soluções 10/02/06

---

1. **V** **F**

(a) O produto dos polinómios x^4 e x^6 em $\mathbb{Z}_7[x]$ é x^3. | | × |
[$x^4x^6 = x^{10}$.]

(b) Se K é um corpo, $f(x), g(x) \in K[x]$ são mónicos do mesmo grau e $f(x) \mid g(x)$ então $f(x) = g(x)$. | × | |
[Da hipótese $f(x) \mid g(x)$ segue $g(x) = q(x)f(x)$ para algum $q(x) \in K[x]$. Como $g(x)$ e $f(x)$ são mónicos, também $q(x)$ o é; como $g(x)$ e $f(x)$ têm o mesmo grau, $q(x)$ tem que ter grau 0, ou seja, é uma constante. Portanto, $q(x) = 1$, logo $g(x) = f(x)$.]

(c) Se L é uma extensão finita de K e $\theta \in L$ então o grau de θ é um divisor de $[L : K]$. | × | |
[Se L é uma extensão finita de K todos os seus elementos são algébricos sobre K. Pelo Teorema da Torre, $[L : K] = [L : K(\theta)][K(\theta) : K]$. Como $[K(\theta) : K]$ coincide com o grau de θ, então o grau de θ é um divisor de $[L : K]$.]

(d) $\sqrt{2} \in \mathbb{Q}(\sqrt{2}\,i)$. | | × |
[$(\sqrt{2}\,i)^2 = -2$ donde $\sqrt{2}\,i$ é raiz do polinómio $x^2 + 2 \in \mathbb{Q}[x]$. Este polinómio é claramente irredutível sobre $\mathbb{Q}$, pelo que $[\mathbb{Q}(\sqrt{2}\,i) : \mathbb{Q}] = 2$. Portanto, $\mathbb{Q}(\sqrt{2}\,i) = \{a + b\sqrt{2}\,i \mid a, b \in \mathbb{Q}\}$. Isto diz-nos que os complexos com parte imaginária nula que pertencem a $\mathbb{Q}(\sqrt{2}\,i)$ são precisamente os racionais, pelo que $\sqrt{2} \notin \mathbb{Q}(\sqrt{2}\,i)$.]

(e) No código (7,4)-linear binário definido pela matriz $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$
a mensagem 1010011 está errada e é corrigida automaticamente como 0110011. | | × |
[1110011 não pode ser a mensagem corrigida pois nem sequer é uma palavra do código: $S(1110011) = (100) \neq 0$.
Observe que a mensagem 1010011 está de facto errada, pois $S(1010011) = (110) \neq 0$, mas o erro que o código determina é igual a (0010000), pois esta é a palavra líder que tem síndrome igual a (110). Assim, a mensagem corrigida é igual a 1000011.]

2. (a) Uma vez que $+$ é a adição usual, o par $(\mathbb{Q}, +)$ é um grupo comutativo. Bastará então verificar que a operação $*$ é distributiva relativamente à adição, associativa, comutativa

e tem elemento neutro e que todo o elemento diferente do zero tem inverso relativamente a esta operação:

Distributividade: Como $*$ é comutativa basta verificar uma das condições de distributividade: para quaisquer $a, b, c \in \mathbb{Q}$, $a*(b+c) = \frac{a(b+c)}{3} = \frac{ab+ac}{3} = \frac{ab}{3} + \frac{ac}{3} = (a*b)+(a*c)$.

Associatividade: Para quaisquer $a, b, c \in \mathbb{Q}$, $a*(b*c) = a*\frac{bc}{3} = \frac{abc}{9}$ enquanto $(a*b)*c = \frac{ab}{3}*c = \frac{abc}{9}$, pelo que se confirma a propriedade.

Comutatividade: Para quaisquer $a, b \in \mathbb{Q}$, $a*b = \frac{ab}{3} = \frac{ba}{3} = b*a$.

Elemento neutro: 3 é elemento neutro de $*$ pois, para qualquer $a \in \mathbb{Q}$, $a*3 = a$.

Existência de inversos: Para cada $a \neq 0$ em $\mathbb{Q}$, $\frac{9}{a}$ é o inverso de a pois $a*\frac{9}{a} = 3$.

(b) Consideremos $S = 3\mathbb{Z} \subseteq \mathbb{Q}$, que é claramente um subanel de A: é não vazio e, para quaisquer $x = 3a, y = 3b \in S$, tem-se $x - y = 3a - 3b = 3(a-b) \in S$ e $x*y = \frac{xy}{3} = \frac{3a3b}{3} = 3ab \in S$. Também não é difícil ver que $(S, +, *) \cong (\mathbb{Z}, +, \cdot)$:
A função

$$\begin{array}{rccc} f: & (S,+,*) & \to & (\mathbb{Z},+,\cdot) \\ & x & \mapsto & \frac{x}{3} \end{array}$$

é um homomorfismo de anéis: para quaisquer $x, y \in S$ tem-se $f(x+y) = \frac{x+y}{3} = \frac{x}{3} + \frac{y}{3} = f(x) + f(y)$ e $f(x*y) = f(\frac{xy}{3}) = \frac{xy}{9} = f(x)f(y)$.
É injectiva: $f(x) = f(y) \Leftrightarrow \frac{x}{3} = \frac{y}{3} \Leftrightarrow x = y$.
É sobrejectiva: para cada $a \in \mathbb{Z}$ seja $x = 3a \in S$; evidentemente $f(x) = \frac{3a}{3} = a$.

3. (a) 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 $x^2 + \sqrt[3]{2}x + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})[x]$. Será este polinómio irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$? Pela fórmula resolvente das equações do segundo grau, como o seu discriminante é negativo, ambas as raízes são não reais. Logo, pelo critério das raízes, $x^2 + \sqrt[3]{2}x + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})[x]$ é irredutível sobre $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, donde $[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Em conclusão,

$$[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}] = 3 \times 2 = 6.$$

(b) O polinómio $m(x) = x^3 - 2$, como vimos na alínea anterior, é irredutível sobre $\mathbb{Q}$. Seja $f(x) = x^2 + 2x + 1$. Determinar o inverso de $f(x) + \langle m(x) \rangle$ em $\mathbb{Q}[x]/\langle m(x) \rangle$ equivale a determinar o polinómio $p(x)$ de grau inferior a 3 tal que

$$(f(x) + \langle m(x) \rangle)(p(x) + \langle m(x) \rangle) = 1 + \langle m(x) \rangle,$$

ou seja, tal que $f(x)p(x) - 1 \in \langle m(x) \rangle$. Uma vez que $m(x) = (x-2)f(x) + 3x$ e $f(x) = 3x(\frac{1}{3}x + \frac{2}{3}) + 1$ (o que confirma que $mdc(m(x), f(x)) = 1$), então

$$\begin{aligned} 1 &= f(x) - [m(x) - (x-2)f(x)]\Big(\frac{1}{3}x + \frac{2}{3}\Big) \\ &= \Big[1 + (x-2)\Big(\frac{1}{3}x + \frac{2}{3}\Big)\Big] f(x) - \Big(\frac{1}{3}x + \frac{2}{3}\Big) m(x) \\ &= \Big(\frac{1}{3}x^2 - \frac{1}{3}\Big) f(x) - \Big(\frac{1}{3}x + \frac{2}{3}\Big) m(x). \end{aligned}$$

Portanto, $f(x)(\frac{1}{3}x^2 - \frac{1}{3}) - 1 \in \langle m(x)\rangle$, donde

$$(f(x) + \langle m(x)\rangle)^{-1} = \left(\frac{1}{3}x^2 - \frac{1}{3}\right) + \langle m(x)\rangle.$$

(c) Não existe nenhum corpo com 10 elementos nem com 12 elementos porque $10 = 2 \times 5$ e $12 = 2^2 \times 3$ não são potências de primos. Como $512 = 2^9$, qualquer corpo com 512 elementos tem característica 2, donde $1 + 1 + 1 + 1 = 0$.

4. (a) Proposição 2.9(3) nos Apontamentos:

Provemos que $p(x)$ é redutível se e só se I 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 $K[x]$ 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 $K[x]$.

(b) Seja $p(x)$ um polinómio de grau 2 ou 3. Se $p(x)$ é redutível sobre K então $p(x) = q_1(x)q_2(x)$, onde nem $q_1(x)$ nem $q_2(x)$ são constantes. Assim, necessariamente um destes dois polinómios é de grau 1, da forma $ax + b$. Este polinómio tem a raiz $-a^{-1}b \in K$, que será evidentemente também raiz de $p(x)$.

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

5. (a) Por definição, $\delta(\mathcal{C}) = \min\{d(a, b) \mid a, b \in \mathcal{C}, a \neq b\}$. Mas $\mathcal{C}$ é fechado para a subtracção, pelo que $a - b \in \mathcal{C}$ e, por outro lado, $d(a, b) = d(a - b, 0) = \omega(a - b)$. É então evidente que $\min\{d(a, b) \mid a, b \in \mathcal{C}, a \neq b\} = \min\{\omega(c) : c \in \mathcal{C}, c \neq 0\}$.

(b) Suponhamos que $IJ \subseteq P$ e $I \nsubseteq P$. Então existe $a \in I$ tal que $a \notin P$. Mas, para qualquer $b \in J$, $ab \in IJ \subseteq P$, o que implica, pela primalidade de P, que $a \in P$ ou $b \in P$. Como $a \notin P$, teremos que ter forçosamente b em P, o que mostra que $J \subseteq P$.