Departamento de Matemática da Universidade de Coimbra

Corpos e Equações Algébricas

SOLUÇÕES **Exame (Época normal)** 19/06/09

---

1. (a) Seja $S = \langle 6, 8\rangle$ o subanel que pretendemos determinar. Então $S = \langle 2\rangle = 2\mathbb{Z}$. De facto:

   $6, 8 \in S \Rightarrow 2 = 8 - 6 \in S \Rightarrow 2\mathbb{Z} \subseteq S$.

   Por outro lado, $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$ que contém 6 e 8, logo $S \subseteq 2\mathbb{Z}$.

   (b) Como

$$x^5 - 7x^3 + 2x^2 - 14 = (x^3 - x^2 - 7x + 7)(x^2 + x + 1) + 3x^2 - 21$$

   e

$$x^3 - x^2 - 7x + 7 = (3x^2 - 21)\Big(\frac{1}{3}x - \frac{1}{3}\Big) + 0$$

   então, pelo Algoritmo de Euclides

$$\mathrm{mdc}(x^5 - 7x^3 + 2x^2 - 14, x^3 - x^2 - 7x + 7)$$

   é o polinómio mónico associado de $3x^2 - 21$, isto é, $x^2 - 7$.

   (c) $p(x)$, pelo critério de Eisenstein (com $p = 2$), é irredutível sobre $\mathbb{Q}$.

   As possíveis raízes racionais de $q(x) = x^4 - x^2 - 2$ são 1, -1, 2 e -2. Nenhuma delas é raiz pelo que o polinómio não tem raízes racionais. Assim, a única hipótese dele ser redutível sobre $\mathbb{Q}$ é factorizar-se na forma

$$q(x) = (x^2 + ax + b)(x^2 + cx + d)$$

   para alguns racionais a, b, c, d. Resolvendo o sistema correspondente

$$\begin{cases} a + c = 0 \\ b + ac + d = -1 \\ ad + bc = 0 \\ bd = -2. \end{cases}$$

   chega-se a uma solução:

$$q(x) = (x^2 + 1)(x^2 - 2).$$

   Portanto, $q(x)$ é redutível sobre $\mathbb{Q}$.

   $r(x)$ é irredutível sobre $\mathbb{Q}$ se e só se $8x^3 - 6x - 1$ o for. As possíveis raízes racionais deste último polinómio são: $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. Nenhuma delas é de facto uma raiz pelo que o polinómio, não tendo raízes em $\mathbb{Q}$ e sendo de grau 3, é irredutível sobre $\mathbb{Q}$.

2. (a) Não. Por exemplo, em $\mathbb{Z}_6$, 2 e 3 são divisores de zero (pois $2 \times 3 = 0$) mas $2+3=5$ não é (pois é invertível: $5 \times 5 = 1$).

   (b) Não. Novamente em $\mathbb{Z}_6$, 5 é invertível mas $5+5=4$ não é (pois é um divisor de zero: $4 \times 3 = 0$). Outro exemplo: em $\mathbb{Z}$, $1+1=2$ não é invertível.

   (c) Não: seja I um ideal próprio de um anel A com identidade 1; se $1 \in I$ então,para qualquer $a \in A$, $a = a \times 1 \in I$, um absurdo.

3. (a) Como $(x-a)$ é mónico, podemos realizar a divisão de $f(x)$ por $(x-a)$, obtendo $f(x) = (x-a)q(x)+r(x)$ com $gr(r(x)) < 1$ (ou seja, $r(x)$ é um polinómio constante $r(x) = b$). Portanto:

$$a \text{ é raiz de } f(x) \Leftrightarrow f(a) = 0 \Leftrightarrow b = r(a) = 0 \Leftrightarrow (x-a) \mid f(x).$$

   (b) Faremos uma demonstração por indução sobre n. O caso $n = 0$ é óbvio: $f(x)$ será um polinómio constante não nulo pelo que não terá raízes em D.

   Suponhamos agora, por hipótese de indução, que o resultado vale para qualquer polinómio de grau n. Nessas condições, seja $f(x)$ um polinómio de grau $n+1$. Se $f(x)$ não tiver raízes em D, não há nada a provar. Caso contrário, se tem uma raiz $a \in D$ então, pela alínea anterior, $f(x) = (x-a)q(x)$. Como D é um domínio de integridade, $gr(q(x)) = n$. Logo, pela hipótese de indução, $q(x)$ tem no máximo n raízes. Isto implica que $f(x)$ tem no máximo $n+1$ raízes (porque se $b \neq a$ é raiz de $f(x)$ então é raiz de $q(x)$ pois $0 = f(b) = q(b)(b-a)$ implica $q(b) = 0$).

   (c) Por exemplo, em $\mathbb{Z}_4[x]$, o polinómio $2x^2 + 2x$ é de grau 2 mas tem 4 raízes: 0, 1, 2 e 3.

4. (a) Do Exercício 1(b) decorre imediatamente que $I = \langle x^2 - 7 \rangle$.

   (b) O ideal $I = \langle x^2 - 7 \rangle$ é maximal se e só se $x^2 - 7$ é irredutível sobre $\mathbb{Q}$, o que é verdade pelo critério de Eisenstein.

   (c) Sim, pois I sendo maximal, então $\mathbb{Q}[x]/I$ é um corpo. Determinemos o inverso de $x + I$, isto é, $a + bx + I \in \mathbb{Q}[x]/I$ tal que $(x+I)(a+bx+I) = 1 + I$. Para isso teremos que determinar $a + bx \in \mathbb{Q}[x]$ tal que $ax + bx^2 - 1 \in I = \langle x^2 - 7 \rangle$.

   Basta tomar $a = 0$ e $b = \frac{1}{7}$ pois $\frac{1}{7}x^2 - 1 = \frac{1}{7}(x^2 - 7)$. Portanto,

$$(x+I)^{-1} = \frac{1}{7}x + I.$$

5. (a) Como $x^2 - 6$ é o polinómio mínimo de $\sqrt{6}$ sobre $\mathbb{Q}$, então $[\mathbb{Q}(\sqrt{6}), \mathbb{Q}] = 2$ e $\{1, \sqrt{6}\}$ é uma base do espaço vectorial $\mathbb{Q}(\sqrt{6})$ sobre $\mathbb{Q}$. Portanto

$$\mathbb{Q}(\sqrt{6}) = \{a + b\sqrt{6} \mid a, b \in \mathbb{Q}\}.$$

   (b) Seja $L = \mathbb{Q}(\sqrt{6})$. O elemento $\sqrt{6}$ tem polinómio mínimo $x^2 - 6$. Como qualquer $\mathbb{Q}$-automorfismo $\Phi : L \to L$ transforma raízes deste polinómio em raízes, existem precisamente dois $\mathbb{Q}$-automorfismos:

$$\begin{array}{rccc} \Phi_{\sqrt{6}}: & \mathbb{Q}(\sqrt{6}) & \to & \mathbb{Q}(\sqrt{6}) \\ & a\in\mathbb{Q} & \mapsto & a \\ & \sqrt{6} & \mapsto & \sqrt{6} \end{array} \qquad \text{e} \qquad \begin{array}{rccc} \Phi_{-\sqrt{6}}: & \mathbb{Q}(\sqrt{6}) & \to & \mathbb{Q}(\sqrt{6}) \\ & a\in\mathbb{Q} & \mapsto & a \\ & \sqrt{6} & \mapsto & -\sqrt{6}. \end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento $a+b\sqrt{6}$ de $\mathbb{Q}(\sqrt{6})$ em $a-b\sqrt{6}$. Portanto, $Gal(L,\mathbb{Q}) = \{id, \Phi_{-\sqrt{6}}\}$, que é um grupo isomorfo a $\mathcal{S}_2$.

(c) Pelo Teorema da Torre,

$$\begin{aligned} [\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}(\sqrt{6},\sqrt{10})]\,[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}(\sqrt{6},\sqrt{10})]\,[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}(\sqrt{6})]\,[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]. \end{aligned}$$

Como vimos em (a), $[\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2$. Qual é o polinómio mínimo de $\sqrt{10}$ sobre $\mathbb{Q}(\sqrt{6}) = \{a+b\sqrt{6} : a,b\in\mathbb{Q}\}$? $\sqrt{10}$ é raiz de $x^2-10\in\mathbb{Q}[x]\subseteq\mathbb{Q}(\sqrt{6})[x]$. Será que este polinómio é irredutível sobre $\mathbb{Q}(\sqrt{6})$? Sim, pois as suas duas raízes $\pm\sqrt{10} = \pm\sqrt{2}\,\sqrt{5}$ não pertencem a $\mathbb{Q}(\sqrt{6})$:
Com efeito, $\pm\sqrt{10} = a+b\sqrt{6}$ para algum par a,b de racionais implicaria $10 = a^2+6b^2+2ab\sqrt{6}$, ou seja,

$$\sqrt{6} = \frac{10-a^2-6b^2}{2ab} \in \mathbb{Q} \quad (\text{no caso } a,b\neq 0)$$

ou $10 = 6b^2$ (no caso $a=0$) ou $10=a^2$ (no caso $b=0$), uma contradição, em qualquer um dos três casos.
Portanto, x^2-10 é o polinómio mínimo de $\sqrt{10}$ sobre $\mathbb{Q}(\sqrt{6})$, pelo que

$$[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}(\sqrt{6})] = 2,$$

sendo $\{1,\sqrt{10}\}$ uma base de $\mathbb{Q}(\sqrt{6},\sqrt{10})$ sobre $\mathbb{Q}(\sqrt{6})$. Consequentemente,

$$[\mathbb{Q}(\sqrt{6},\sqrt{10}):\mathbb{Q}] = 4$$

e, pela demonstração do Teorema da Torre,

$$\{1,\sqrt{6},\sqrt{10},\sqrt{60}\} = \{1,\sqrt{2}\sqrt{3},\sqrt{2}\sqrt{5},2\sqrt{3}\sqrt{5}\}$$

constitui uma base de $\mathbb{Q}(\sqrt{6},\sqrt{10})$ sobre $\mathbb{Q}$. Assim,

$$\mathbb{Q}(\sqrt{6},\sqrt{10}) = \{a+b\sqrt{2}\sqrt{3}+c\sqrt{2}\sqrt{5}+d\sqrt{3}\sqrt{5} \mid a,b,c,d\in\mathbb{Q}\}.$$

Finalmente, como $\sqrt{15} = \sqrt{3}\sqrt{5}\in\mathbb{Q}(\sqrt{6},\sqrt{10})$ então $x-\sqrt{15}$ é o polinómio mínimo de $\sqrt{15}$ sobre $\mathbb{Q}(\sqrt{6},\sqrt{10})$ pelo que $[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}(\sqrt{6},\sqrt{10})] = 1$.
Em conclusão, $[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}):\mathbb{Q}] = 4$ e

$$\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) = \mathbb{Q}(\sqrt{6},\sqrt{10}) = \{a+b\sqrt{2}\sqrt{3}+c\sqrt{2}\sqrt{5}+d\sqrt{3}\sqrt{5} \mid a,b,c,d\in\mathbb{Q}\}.$$

6. (a) Provar que $-a = a$ para qualquer $a \in A$ equivale a provar que $a + a = 0$ para qualquer $a \in A$. Como, por hipótese, $(a+a)^2 = a + a$, e

$$\begin{aligned} (a+a)^2 = a+a &\Leftrightarrow a^2 + a^2 + a^2 + a^2 = a + a \\ &\Leftrightarrow a + a + a + a = a + a \\ &\Leftrightarrow a + a = 0, \end{aligned}$$

está provado.

Solução alternativa: Por hipótese, $(-a)^2 = -a$. Por outro lado, $(-a)(-a) = -(-a) = a$. Logo $-a = a$.

(b) Sejam $a, b \in A$. Por hipótese, $(a+b)^2 = a + b$. Além disso,

$$\begin{aligned} (a+b)^2 = a+b &\Leftrightarrow a^2 + ab + ba + b^2 = a + b \\ &\Leftrightarrow a + ab + ba + b = a + b \\ &\Leftrightarrow ab + ba = 0. \end{aligned}$$

Portanto, $ab = -ba$. Logo, pela alínea anterior, $ab = ba$, o que mostra que A é comutativo.

(c) (i)$\Rightarrow$(ii): $A/I = \{a + I \mid a \in A\}$. Como I é primo, então $I \neq A$ pelo que $1 \notin I$ (Exercício 2(c)) e, consequentemente, $1 + I \neq 0 + I$. Portanto A/I possui pelo menos as classes $0 + I$ e $1 + I$ e, se queremos mostrar que $A/I \cong \mathbb{Z}_2$, teremos então que mostrar que A/I não possui mais nenhum elemento. Se $a \in I$ então $a + I = 0 + I$. Se $a \notin I$ então $a + I \neq 0 + I$, pelo que teremos de mostrar neste caso que $a + I = 1 + I$. Pela alínea (a), $a + a = 0$, isto é, $a(a+1) = 0 \in I$. Logo, como I é primo, $a \in I$ ou $a + 1 \in I$. A primeira condição é falsa pelo que necessariamente $a + 1 \in I$, ou seja, $a + I = 1 + I$ (note que $a - 1 = a + 1$, pela alínea (a)).

(ii)$\Rightarrow$(iii): A condição (ii) diz-nos, em particular, que A/I é um corpo, pelo que I é imediatamente maximal (resultado teórico das aulas).

(iii)$\Rightarrow$ (i): Resultado provado nas aulas que assegura que todo o ideal maximal é primo.
