Departamento de Matemática da Universidade de Coimbra 2004/05

Duração: 2h30m **Exame modelo de Álgebra II**

Justifique convenientemente as suas respostas e indique os principais cálculos

---

1. Determine:

   (a) A característica do anel $\mathcal{M}_{20}(\mathbb{Z}_5)$ das matrizes quadradas de ordem 20 com elementos no corpo $\mathbb{Z}_5$.

   (b) O máximo divisor comum de x^2+x+1 e x^4+x^3+1 em $\mathbb{Z}_3[x]$.

   (c) As raízes racionais do polinómio $x^{50}-x^{20}+x^{10}-1$.

   (d) Os subcorpos do corpo $\mathbb{F}_{64}$.

2. Seja D um domínio de integridade e $p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in D[x]$. Chama-se *derivada* de $p(x)$ ao polinómio $p(x)'=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1$. Prove que, para quaisquer $p(x),q(x)\in D[x]$ e para qualquer $\alpha\in D$:

   (a) $(p(x)+q(x))'=p(x)'+q(x)'$ e $(p(x)q(x))'=p(x)'q(x)+p(x)q(x)'$.

   (b) α é raiz de $p(x)$ de multiplicidade >1 se e só se é simultaneamente raiz de $p(x)$ e $p(x)'$.

3. Para as afirmações seguintes, escreva uma prova se a afirmação é verdadeira, caso contrário apresente uma justificação sucinta da sua falsidade:

   (a) Para qualquer corpo C, um ideal principal $I=(p(x))$ de $C[x]$ é maximal se e só se $p(x)$ é irredutível.

   (b) $\mathbb{Z}_2[x]/_{(x^3+x^2+x+1)}$ é um corpo.

   (c) É possível, usando régua (não graduada) e compasso, construir o ponto

   $$\left(\sqrt{5\sqrt{2}-3}+\sqrt{2-\sqrt[3]{2}},0\right)$$

   a partir dos pontos $(0,0)$ e $(1,0)$.

   (d) O polinómio $2x^5-10x+5$ é resolúvel por radicais.

   (e) Se p é um número primo e r divide n então p^r-1 divide p^n-1.

4. Considere a extensão $L=\mathbb{Q}(\sqrt{3},\sqrt[3]{2})\subseteq\mathbb{R}$ de $\mathbb{Q}$.

   (a) Como se define o grupo de Galois de L (sobre $\mathbb{Q}$)? Determine-o.

   (b) Indique todas as extensões intermédias de $\mathbb{Q}$ em L.

   (c) L é uma extensão de Galois de $\mathbb{Q}$? Justifique.

(v.s.f.f.)

5. Seja $\mathcal{C}$ o código $(7,3)$-linear binário definido pela matriz

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

   (a) Quantas mensagens permite $\mathcal{C}$ codificar?

   (b) Calcule a distância mínima $\delta(\mathcal{C})$. Poderá $\mathcal{C}$ detectar e/ou corrigir erros singulares?

   (c) Corrija, caso tal seja possível, os erros nas seguintes mensagens: 0001000, 1011110.