Duração: 2h30m **Exame (época normal)** 11/06/08

Justifique convenientemente as suas respostas e indique os principais cálculos.

---

1. Em cada uma das alíneas seguintes indique o valor lógico das afirmações.
   Cada resposta errada vale $-1/2\,c$, sendo c a cotação da alínea.

	V	**F**
(a) Se $a, b, u, v \in \mathbb{Z}$ são tais que $1 = ua + vb$, então a e b são primos entre si.		
(b) $\mathbb{Z}[x]$ tem um número infinito de unidades.		
(c) Se $p(x) \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Q}$, então é irredutível sobre $\mathbb{Z}$.		
(d) Em $\mathbb{Q}[x]$, o resto da divisão de $x^{100} + 3x + 1$ por $x + 1$ é -1.		

2. Seja $p(x) = x^5 - 2x^4 + 11x^3 - 9x^2 + 24x + 15 \in \mathbb{Q}[x]$.

   (a) Sabendo que $1 + 2i$ é raiz de $p(x)$, decomponha $p(x)$ em factores irredutíveis em $\mathbb{Q}[x]$.

   (b) Mostre que $p(x)$ não tem raízes racionais.

3. (a) Determine o polinómio mínimo de $\sqrt{3} + \sqrt{7}$ sobre $\mathbb{Q}$.

   (b) Mostre que $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$.

4. Seja A um anel comutativo com identidade e seja I um ideal de A.

   (a) Quando é que se diz que I é um ideal primo? Prove que se A/I é um domínio de integridade então I é um ideal primo de A.

   (b) Quando é que se diz que I é um ideal maximal? Prove que se A/I é um corpo então I é um ideal maximal de A.

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) Qual é o número de palavras de $\mathcal{C}$?

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

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

6. Seja L uma extensão de um corpo K.

   (a) Mostre que os elementos de L algébricos sobre K formam um subcorpo de L.

   (b) Como se define o *grupo de Galois* de L sobre K, $Gal(L, K)$?

   (c) Prove que se $\theta \in L$ é algébrico sobre K, de grau n, então $\mid Gal(K(\theta), K) \mid \leq n$.
