Duração: 2h30m 10/02/06

O primeiro grupo de questões é de escolha múltipla; uma resposta certa terá a cotação máxima que lhe for atribuída e uma resposta errada perderá metade dessa cotação (desde que a nota do exame permaneça não negativa).
Nas outras questões justifique convenientemente as suas respostas e indique os principais cálculos.

1. Em cada uma das alíneas seguintes indique o valor lógico das afirmações:

   (**V**: verdadeira; **F**: falsa) **V F**

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

   (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 $f(x) = g(x)$.

   (c) Se L é uma extensão finita de K e $\theta \in L$ então o grau de θ é um divisor de $[L : K]$.

   (d) $\sqrt{2} \in \mathbb{Q}(\sqrt{2}\, i)$.

   (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 1110011.

2. Seja $A = (\mathbb{Q}, +, *)$, onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = ab/3$.

   (a) Mostre que A é um corpo.

   (b) Determine um subanel de A que seja isomorfo ao anel usual $(\mathbb{Z}, +, \cdot)$ dos inteiros, descrevendo o isomorfismo.

3. (a) Determine $[\mathbb{Q}(\sqrt[3]{2}, \theta) : \mathbb{Q}]$, onde $\theta^2 + \sqrt[3]{2}\theta + \sqrt[3]{4} = 0$.

   (b) Calcule o inverso do elemento $x^2 + 2x + 1 + \langle x^3 - 2 \rangle$ no corpo $\mathbb{Q}[x]/\langle x^3 - 2 \rangle$.

   (c) Existe algum corpo com 10 elementos? E com 12 elementos? Num corpo com 512 elementos, a identidade 1 é raiz do polinómio $x^3 + x^2 + x + 1$?

4. Sejam K um corpo e $p(x) \in K[x]$. Prove que:

   (a) O ideal $I = \langle p(x) \rangle$ é maximal se e só se $p(x)$ é irredutível sobre K.

   (b) Se $p(x)$ é de grau 2 ou 3, então $p(x)$ é redutível sobre K se e só se existe $\alpha \in K$ tal que $p(\alpha) = 0$.

5. Prove que:

   (a) Se um código $\mathcal{C}$ de comprimento n em $\mathbb{F}_q$ é fechado para a subtracção, então $\delta(\mathcal{C})$ é igual a $\min\{\omega(c) \mid c \in \mathcal{C},\, c \neq 0\}$ (onde $\omega(c)$ denota o peso da palavra c).

   (b) Se A é um anel, I e J são ideais de A e P é um ideal primo de A, então

   $$IJ \subseteq P \;\Rightarrow\; I \subseteq P \text{ ou } J \subseteq P.$$

   (Observação: IJ denota o conjunto $\{ab \mid a \in I, b \in J\}$.)