Departamento de Matemática da Universidade de Coimbra **Corpos e Equações Algébricas**

Duração: 1h15m **Exame de Recurso (parte 1)** 22/06/2020

Justifique convenientemente as suas respostas e indique os principais cálculos.

1. Considere o anel

$$M_2(\mathbb{Z}) = \{[a_{ij}] \mid a_{i,j} \in \mathbb{Z},\ i,j = 1,2\}$$

das matrizes 2×2 em $\mathbb{Z}$, com as operações usuais $+$ e $\times$ de adição e multiplicação de matrizes.

   (a) Mostre que $(M_2(\mathbb{Z}), +)$ é um grupo.

   (b) Prove que $P = \{[a_{ij}] \in M_2(\mathbb{Z}) \mid a_{ij} \text{ é par}\}$ é um ideal de $M_2(\mathbb{Z})$.

   (c) Defina ideal primo. O ideal P da alínea anterior é primo?

   (d) Quantos elementos terá o anel quociente $M_2(\mathbb{Z})/P$?

2. (a) Determine a factorização de $x^5 + 9x^4 + 18x^3 + 12x + 3$ em elementos irredutíveis em $\mathbb{Q}[x]$ e em $\mathbb{Z}_2[x]$.

   (b) No anel de polinómios $\mathbb{Z}_{16}[x]$, descreva os polinómios $d(x)$ para os quais é possível dividir qualquer polinómio $a(x)$ por $d(x)$.

3. Sejam A e B anéis e $f\colon A \to B$ uma função de A em B.

   (a) Quando é que se diz que f é um homomorfismo de anéis? Mostre que, nesse caso, $f(0_A) = 0_B$.

   (b) Suponha que A e B são domínios de integridade. Prove que necessariamente f é a aplicação nula (isto é, $\{f(a) \mid a \in A\} = \{0_B\}$) ou então $f(1_A) = 1_B$.

Departamento de Matemática da Universidade de Coimbra **Corpos e Equações Algébricas**

Duração: 1h15m **Exame de Recurso (parte 2)** 22/06/2020

Justifique convenientemente as suas respostas e indique os principais cálculos.

1. Seja θ uma raiz não nula do polinómio $x^4 - x^3 + x^2 - 2x \in \mathbb{Q}[x]$. Determine:
   (a) $\frac{\theta^2}{\theta^2+1}$ e exprima o resultado como combinação linear dos elementos duma base do espaço vectorial $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$.
   (b) O polinómio mínimo de θ^2 sobre $\mathbb{Q}$.

2. Sejam K um subcorpo de um corpo L e $\theta \in L$ um elemento algébrico sobre K. Prove que
$$K[\theta] = \{p(\theta) \mid p(x) \in K[x]\}$$
é um corpo, justificando os seguintes passos:
   (a) $K[\theta]$ é um domínio de integridade.
   (b) Sendo $p(\theta)$ um elemento não nulo de $K[\theta]$ e $m(x)$ o polinómio mínimo de θ sobre K, então
      (b1) $p(x)$ não é múltiplo de $m(x)$;
      (b2) existem $t(x), s(x) \in K[x]$ tais que $t(x)\ p(x) + s(x)\ m(x) = 1$;
      (b3) $t(\theta)\ p(\theta) = 1$.

3. Seja $\mathcal{C}$ o código binário de comprimento 7, com distância mínima 3, definido pela matriz
$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$
   (a) Qual é a eficácia de $\mathcal{C}$ na detecção de erros? E na correcção de erros?
   (b) Supondo que, no máximo, só erros singulares podem ocorrer na transmissão, corrija os erros nas mensagens $M_1 = 0101001$ e $M_2 = 0010100$.