Duração: 2h30m **Exame (época recurso)** 14/07/09

Justifique convenientemente as suas respostas e indique os principais cálculos.

---

1. Considere o anel $A = (\mathbb{Z}_6, +, \cdot)$ onde as operações $+$ e $\cdot$ são definidas por

$$a + b = a \oplus_6 b \oplus_6 1, \quad \forall a, b \in A$$

$$a \cdot b = a \oplus_6 b \oplus_6 (a \otimes_6 b), \quad \forall a, b \in A.$$

   (a) Denotando o zero de A por $\mathbb{O}$ e a identidade (caso exista) por $\mathbb{I}$, preencha (quando possível) o seguinte quadro:

$\mathbb{O}$	$\mathbb{I}$	-0	-1	-2	-3	-4	-5	0^{-1}	1^{-1}	2^{-1}	3^{-1}	4^{-1}	5^{-1}

   (b) Quais são os elementos invertíveis de A? E os divisores de zero?

   (c) Para que elementos $a \in A$ é válida a *lei do corte*

$$\forall\, b, c \in A\ (a \cdot b = a \cdot c \Rightarrow b = c)\,?$$

2. Considere o homomorfismo de anéis $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_5$ definido por $\phi(n) = n \bmod 5$.

   (a) Calcule o núcleo de ϕ.

   (b) Defina ideal maximal de um anel. Mostre que $Nuc(\phi)$ é um ideal maximal de $\mathbb{Z}_{10}$.

3. Diga, justificando sucintamente, qual o valor lógico das seguintes afirmações:

   (a) É possível, usando régua (não graduada) e compasso, duplicar um cubo.

   (b) Em $\mathbb{F}_{27}[x]$, o polinómio $x^3 + x + 1$ pode factorizar-se na forma $(x-1)q(x)$.

4. Seja $\theta \in L \supseteq K$ um elemento algébrico sobre o corpo K e $m(x)$ o respectivo polinómio mínimo. Mostre que cada elemento de $K(\theta)$ tem uma expressão única na forma $p(\theta)$, para algum polinómio $p(x) \in K[x]$ de grau inferior ao grau de $m(x)$.

5. Determine:

   (a) A dimensão e uma base da extensão $\mathbb{Q}(\sqrt{7}, \theta)$, sendo θ uma raiz não racional do polinómio $x^3 + 2x^2 + 2x + 4$.

   (b) O número de elementos do corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1\rangle$.

   (c) A factorização do polinómio $q(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ em factores irredutíveis.

6. Seja L uma extensão de um corpo K.

   (a) Recorde que o *grupo de Galois* de L sobre K, $Gal(L;K)$, é formado pelos automorfismos de L que fixam os elementos de K. Prove que se $\theta \in L$ é algébrico sobre K, de grau n, então $|Gal(K(\theta), K)| \leq n$.

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