Justifique convenientemente as suas respostas e indique os principais cálculos

Duração: 2h30m 14/02/05

---

1. Dado um anel $(A, +, \cdot)$, seja $\mathcal{F} = (A^A, +, \cdot)$ o anel das aplicações de A em A com a adição e multiplicação definidas do seguinte modo:

$$\forall\, f, g \in \mathcal{F} \;\; \forall\, x \in A \quad (f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Para cada $(a, b) \in A \times A$ considere o conjunto $\mathcal{F}_{(a,b)} = \{f \in \mathcal{F} \mid f(a) = b\}$.

(a) Prove que $\mathcal{F}_{(a,b)}$ é um subanel de $\mathcal{F}$ se e só se $b = 0$.

(b) Mostre que $\mathcal{F}_{(a,0)}$ é um ideal de $\mathcal{F}$.

(c) Prove que o anel quociente $\mathcal{F}/\mathcal{F}_{(a,0)}$ é isomorfo a A.

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

(a) $6x^2 + 3x + 6$ é um divisor de zero de $\mathbb{Z}_9[x]$.

(b) Os polinómios $2x$ e $x + 2$ de $\mathbb{F}_3[x]$ são primos entre si.

(c) Existe $n \geq 2$ tal que $\sqrt[n]{2}$ é racional.

(d) Se $\alpha, \beta \in \mathbb{C}$ são algébricos sobre $\mathbb{Q}$ então $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$.

(e) Todo o subcorpo de $\mathbb{F}_{p^n}$ tem ordem p^d, para algum divisor positivo d de n.

3. Responda a <u>quatro</u> das seguintes questões:

(a) Dados $a, b \in \mathbb{F}_5$, resolva em $\mathbb{F}_5$ o sistema

$$\begin{cases} x + 2y = a \\ -3x + 3y = b. \end{cases}$$

(b) Determine todos os primos ímpares p para os quais $x - 2$ divide $x^4 + x^3 + x^2 + x$ em $\mathbb{F}_p[x]$.

(c) Determine a dimensão e uma base da extensão $\mathbb{Q}(\sqrt{3 + \sqrt{3}})$ de $\mathbb{Q}$.

(d) Mostre que o polinómio $2x^5 - 10x + 5$ não é resolúvel por radicais.

(e) Seja P um corpo primo. Prove que existe um e um só automorfismo de P.

(f) Quando é que um código $\mathcal{C}$ se diz t-corrector de erros? Mostre que se $t \leq (\delta(\mathcal{C}) - 1)/2$, então $\mathcal{C}$ é t-corrector de erros.

4. Sejam K um corpo e L uma extensão de K. 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 $\left|Gal\big(K(\theta), K\big)\right| \leq n$.
