Álgebra I

Lista 7

- 1) Seja R um domínio, mostre que, se $a, b \in R$ possuem um mínimo múltiplo comum, então possuem um máximo divisor comum e que $\text{mmc}(a, b) \cdot \text{mdc}(a, b) = ab$.
- 2) Mostre que, se quaisquer dois elementos de R possuírem máximo divisor comum, então também possuem mínimo múltiplo comum.
- 3) Em que anéis de polinômios, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$, o polinômio $f(x) = x^3 - 5x^2 + 25x + 10$ é redutível? Por quê?
- 4) Efetue as divisões euclidianas dos seguintes polinômios nos seguintes anéis.
 - a) $(x^6 + 13x^5 + 5x^4 + 52x^3 + 3x^2 + 3x - 13) : (x^2 + 4)$, em $\mathbb{Z}[x]$.
 - b) $x^3 : (x^2 + \bar{4}x + \bar{3})$, em $\mathbb{Z}_7[x]$.
 - c) $(x^6 + \bar{3}x^5 + \bar{2}x^3 + \bar{3}x^2 + \bar{3}x) : (x^2 - \bar{1})$, em $\mathbb{Z}_5[x]$.
- 5) Seja I o ideal no anel de polinômios $\mathbb{Z}_3[x]$ gerado por $f(x) = x^4 + x^3 + x + \bar{2}$ e $g(x) = x^4 + \bar{2}x^3 + \bar{2}x + \bar{2}$.
 - a) Mostre que $x^4 + \bar{2} \in I$.
 - b) Mostre que $\mathbb{E} = \mathbb{Z}_3/I$ é um corpo.
 - c) Determine a fatoração em primos (indecomponíveis), de $x^4 + \bar{2}$ em $\mathbb{Z}_3[x]$ e em $\mathbb{E}[x]$
- 6) Mostre que $x^2 - \bar{1} = (x - \bar{1})(x - \bar{14}) = (x - \bar{4})(x - \bar{11})$ em $\mathbb{Z}_{15}[x]$.
- 7) Seja $p(x) = x^3 + 3x - 2 \in \mathbb{Q}[x]$ (verifique que este polinômio é irredutível). Seja $z = x + \langle p \rangle$, calcule os elementos

$$\alpha = \frac{2z^2 + z - 3}{3z^2 - 4z + 1}, \quad \text{e} \quad \beta = \frac{1}{2z^2 + 4z - 5}$$

em $\mathbb{E} = \mathbb{Q}[x]/\langle p \rangle$, na forma padrão, $az^2 + bz + c$, com $a, b, c \in \mathbb{Q}$.

- 8) Decida se $\mathbb{Z}_2[x]/\langle x^3 + x + \bar{1} \rangle$ e $\mathbb{Z}_2[x]/\langle x^3 + x^2 + \bar{1} \rangle$ são ou não são corpos isomorfos.
- 9) Encontre um elemento primitivo de $\mathbb{Z}_2[x]/\langle x^3 + x + \bar{1} \rangle$.
- 10) Seja p um primo e $q = p^n$.
 - a) Mostre que a aplicação $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ dada por $F(a) = a^p$ (conhecida como aplicação de Frobenius), é um isomorfismo.
 - b) mostre que cada elemento $a \in \mathbb{F}_q$ possui uma raiz p -ésima, isto é existe $b \in \mathbb{F}_q$ tal que $a = b^p$.
 - c) Seja $\mathbb{K}$ um corpo de característica p . Mostre que para todo inteiro positivo n o homomorfismo $F_n : \mathbb{K} \rightarrow \mathbb{K}$, dados por $F_n(a) = a^{p^n}$, é injetivo.
- 11) Considere um polinômio não constante $f \in \mathbb{K}[x]$, mostre que a soma e o produto de suas raízes pertencem ao corpo $\mathbb{K}$ (mesmo que algumas das raízes estejam em alguma extensão $\mathbb{E}$ de $\mathbb{K}$).