# MAT0231 - Álgebra II para Licenciatura

## Prova P2

1.- Explique brevemente a verdade ou falsidade das seguintes afirmações **(2.8 pontos)**

(a) Sejam $I$ e $J$ ideais de $\mathbb{R}[x]$. Existe um polinômio $p(x) \in \mathbb{R}[x]$ tal que $I + J = \mathbb{R}[x]p(x)$.

(b) Um polinômio $f(x) \in \mathbb{Z}[x]$ pode fatorar como $f(x) = a(x)b(x)$ onde $a(x), b(x) \in \mathbb{Z}[x]$ com $1 \leq \partial a(x), \partial b(x) < \partial f(x)$ se, e somente se, $f(x)$ for redutível em $\mathbb{Q}[x]$.

(c) O polinômio $2x^6 + 28x^4 + 12x^2 + 20x + 4$ é irredutível em $\mathbb{Q}[x]$.

(d) O polinômio $x^3 - 323x^2 + 1155$ é irredutível em $\mathbb{Q}[x]$.

**Resposta:**

(a) Verdadeiro.
Se $K$ é um corpo, todo ideal $P$ de $K[x]$ é da forma $L = K[x]f(x)$ para algum $f(x) \in K[x]$.
Em geral, se $I$ e $J$ são ideais de um anel $S$, $I + J$ é também ideal de $S$.
Assim como $\mathbb{R}$ é corpo e $I + J$ é ideal de $\mathbb{R}[x]$, temos que existe $p(x) \in \mathbb{R}[x]$ tal que $I + J = \mathbb{R}[x]p(x)$.

(b) Verdadeiro
É o enunciado do Lema de Gauss.

(c) Verdadeiro
$2x^6 + 28x^4 + 12x^2 + 20x + 4 = 2(x^6 + 14x^4 + 6x^2 + 10x + 2)$ e 2 é inversível em $\mathbb{Q}[x]$ Assim $2x^6 + 28x^4 + 12x^2 + 20x + 4$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $x^6 + 14x^4 + 6x^2 + 10x + 2$ é irredutível em $\mathbb{Q}[x]$. Aplicando Eisenstein com $p = 2$ obtemos que $x^6 + 14x^4 + 6x^2 + 10x + 2$ é irredutível em $\mathbb{Q}[x]$ e portanto, $2x^6 + 28x^4 + 12x^2 + 20x + 4$ é irredutível em $\mathbb{Q}[x]$.

(d) Verdadeiro.
Consideremos o homomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_2[x]$, $a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$.
Sabemos que quando $\overline{a_n} \neq 0$ em $\mathbb{Z}_2$ e $\overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$ é irredutível em $\mathbb{Z}_2[x]$, então podemos afirmar que $a_0 + a_1x + \cdots + a_nx^n$ é irredutível em $\mathbb{Q}[x]$.
A imagem de $x^3 - 323x^2 + 1155$ é $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ que é de grau 3. Assim $x^3 + x^2 + 1$ é irredutível em $\mathbb{Z}_2[x]$ se, e somente se, não possui raízes em $\mathbb{Z}_2$. É fácil comprovar que a avaliação desse polinômio em $\bar{0}$ e $\bar{1}$ não da $\bar{0}$.

2.- Faça uma lista (sem repetições) com todos os elementos do anel

$$\frac{\mathbb{Z}_2[x]}{\mathbb{Z}_2[x](x^3 + x^2 + x + 1)}.$$

Nessa lista, identifique o elemento que seja igual a $\overline{x^5 + x^4}$. **(2 pontos)**

**Resposta:**
Se $K$ é um corpo e $f(x) \in K[x]\backslash$, então sabemos que elementos de $\frac{K[x]}{K[x]f(x)}$ estão representados pelos possíveis restos de dividir por $f(x)$, ou seja, pelo zero e os polinômios de grau $\leq \partial f(x) - 1$. Assim uma lista sem repetições de $\frac{\mathbb{Z}_2[x]}{\mathbb{Z}_2[x](x^3+x^2+x+1)}$ vem dada por

$$\bar{0},\ \bar{1},\ \bar{x},\ \overline{1 + x},\ \overline{x^2},\ \overline{1 + x^2},\ \overline{1 + x + x^2},\ \overline{x + x^2}.$$

Assim quando $g(x) \in K[x]$ e queremos saber qual é o polinômio $u(x)$ de grau menor que $\partial f(x)$ tal que $\overline{g(x)} = \overline{u(x)}$, o que fazemos é dividir $f(x)$ entre $g(x)$ e o resto é o polinômio desejado.

Como $x^5 + x^4 = (x^2 + 1)(x^3 + x^2 + x + 1) + x + 1$ em $\mathbb{Z}_2[x]$, obtemos que $\overline{x^5 + x^4} = \overline{x + 1}$.

3.- Sejam $K$ um corpo e $f(x), g(x) \in K[x] \setminus \{0\}$ com máximo divisor comum $d(x) \in K[x]$. Dado $h(x) \in K[x]$, mostre que existem polinômios $a(x), b(x) \in K[x]$ satisfazendo a equação

$$a(x)f(x) + b(x)g(x) = h(x)$$

se, e somente se, $h(x)$ é divisível por $d(x)$. **(2 pontos)**

**Resposta:**
Sabemos que como $d(x)$ é o $\mathrm{mdc}(f(x), g(x))$, então

$$K[x]f(x) + K[x]g(x) = K[x]d(x).$$

Logo existem polinômios $a(x), b(x) \in K[x]$ tais que $a(x)f(x) + b(x)g(x) = h(x)$ se, e somente se, $h(x) \in K[x]d(x)$. Ou seja, se, e somente se, $d(x) \mid h(x)$.

4.- Explique por que os seguintes anéis são ou não são corpos **(2.8 pontos)**

(a) $\frac{\mathbb{Q}[x]}{\mathbb{Q}[x](x^6+30x^5-15x^3+6x-120)}$,

(b) $\frac{\mathbb{Q}[x]}{\mathbb{Q}[x](x^3+4x^2+2x)}$,

(c) $\mathbb{Z}_2[x]$,

(d) $\frac{\mathbb{Z}_5[x]}{\mathbb{Z}_5[x](x^4+1)}$

**Resposta:** Se $K$ é um corpo e $f(x) \in K[x]$ de grau $\geq 1$, temos que $\frac{K[x]}{K[x]f(x)}$ é um corpo se, e somente se, $f(x)$ é irredutível em $K[x]$. Isso será usado em (a), (b) e (d).

(a) Aplicando Eisenstein com $p = 3$ obtemos que $x^6 + 30x^5 - 15x^3 + 6x - 120$ é irredutível em $\mathbb{Q}[x]$. Logo $\frac{\mathbb{Q}[x]}{\mathbb{Q}[x](x^6+30x^5-15x^3+6x-120)}$ é um corpo

(b) $\frac{\mathbb{Q}[x]}{\mathbb{Q}[x](x^3+4x^2+2x)}$ não é um corpo pois $x^3 + 4x^2 + 2x = x(x^2 2x + 2)$ não é irredutível em $\mathbb{Q}[x]$.

(c) Como $\mathbb{Z}_2$ é um corpo, sabemos que $\mathbb{Z}_2[x]$ não é um corpo pois os únicos elementos inversíveis de $\mathbb{Z}_2$ são os polinômios constantes não nulos.

(d) $\frac{\mathbb{Z}_5[x]}{\mathbb{Z}_5[x](x^4+1)}$ não é um corpo porque $x^4 + 1$ é redutível em $\mathbb{Z}_5[x]$:
é fácil ver que $x^4 + 1$ não possui raízes em $\mathbb{Z}_5$. Assim se $x^4 + 1$ é redut'ivel, ele seria produto de dois polinômios de grau 2. Escrevendo $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$, obtemos que

$$a + c = 0, \ d + ac + b = 0, \ ad + bc = 0, \ bc = 1.$$

Isso implica que $c = -a$, $(d - b)a = 0$ e portanto $a = c = 0$, $b = 2$, $c = 3$ é solução. Portanto $x^4 + 1 = (x^2 + 2)(x^2 + 3)$ em $\mathbb{Z}_5[x]$.

5.- Encontre um polinômio $p(x) \in \mathbb{Z}_3[x]$ de grau $\leq 2$ tal que $\overline{p(x)}$ seja o inverso de $\overline{x^2+x+1}$ no corpo

$$\frac{\mathbb{Z}_3[x]}{\mathbb{Z}_3[x](x^3+x^2+2x+1)}.$$

**(2 pontos)**

**Resposta:**
Como $\frac{\mathbb{Z}_3[x]}{\mathbb{Z}_3[x](x^3+x^2+2x+1)}$ é um corpo, temos que $x^3+x^2+2x+1$ é irredutível em $\mathbb{Z}_3[x]$ (é fácil provar $x^3+x^2+2x+1$ é irredutível em $\mathbb{Z}_3[x]$ , pois como o grau é três é suficiente verificar que não possui raízes em $\mathbb{Z}_3$).

Assim $\mathrm{mdc}(x^2+x+1, x^3+x^2+2x+1) = 1$, pois o mdc tem que dividir $x^2+x+1$ e $x^3+x^2+2x+1$. Logo existem $a(x), b(x) \in \mathbb{Z}_3[x]$ tais que $a(x)(x^2+x+1)+b(x)(x^3+x^2+2x+1) = 1$ e portanto, tomando classes temos que

$$\overline{a(x)(x^2+x+1)} + \overline{b(x)(x^3+x^2+2x+1)} = \overline{a(x)} \cdot \overline{(x^2+x+1)} = \overline{1}$$

em $\frac{\mathbb{Z}_3[x]}{\mathbb{Z}_3[x](x^3+x^2+2x+1)}$. Para encontrar esses $a(x), b(x) \in \mathbb{Z}_3[x]$ usamos o procedimento estudado em sala de aula:

- $x^3+x^2+2x+1 = x(x^2+x+1)+x+1$
- $x^2+x+1 = x(x+1)+1$

Da segunda igualdade obtemos

$$1 = x^2+x+1-x(x+1)$$

. Da primeira obtemos $x+1 = x^3+x^2+2x+1-x(x^2+x+1)$ que substituindo na igualdade anterior obtemos

$$\begin{aligned} 1 &= x^2+x+1-x(x+1) \\ &= x^2+x+1-x(x^3+x^2+2x+1-x(x^2+x+1)) \\ &= (x^2+1)(x^2+x+1)-x(x^3+x^2+2x+1) \end{aligned}$$

Portanto o inverso de $\overline{x^2+x+1}$ no corpo $\frac{\mathbb{Z}_3[x]}{\mathbb{Z}_3[x](x^3+x^2+2x+1)}$ é $\overline{x^2+1}$.