MAT 0120 - Solução lista 9 - (28/05)

Exs: 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 17, 19, 22 e 23.

Exercício 4: Mostre que através de exemplos que, se tomarmos polinômios com coeficientes em $\mathbb{Z}_m$ onde m não é um inteiro primo, então as propriedades (b) e (c) do exercício anterior não são necessariamente válidas.

Dem:

Como m não é primo, então existe $a \in \mathbb{Z}_m$, tal que $mdc(a,m) \neq 1$. Logo, $\bar{a}$ é divisor de zero e, portanto, existe $\bar{b} \neq 0$ tal que $\bar{a}\bar{b} = 0$. Daí, tomando

$$f = \bar{a}x \quad e \quad g(x) = bx$$

Segue que $f \cdot g = \bar{a}\bar{b}x = \bar{0}x$.

Este exemplo resolve tanto (b) quanto (c) pois $f \cdot g = 0$, mas $f, g \neq 0$. ∎

Exercício 5:

Determinar o número de polinômios de $\mathbb{Z}_5$ de grau menor ou igual a 4.

Dem:

Em geral, polinômios de grau menor ou igual a 4 tem a forma

$$f = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0, \quad a_i \in \mathbb{Z}_5$$

Como os polinômios devem ter grau menor ou igual a 4, então a_4 pode ser zero. Logo, para cada a_i tem 5 possibilidades, a saber, $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ e $\bar{4}$.

Portanto, temos exatamente $4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^6$ polinômios de grau menor ou igual a 6.

(b) Para vocês.

■

(6) Um polinômio $f \in \mathbb{K}[x]$ diz-se inversível se existe $g \in \mathbb{K}[x]$ tal que $f \cdot g = 1$. Determinar o conjunto de todos os elementos inversíveis de $\mathbb{K}[x]$.

Dem:

Considere $f = a_0 + \dots + a_m x^m$, $a_m \neq 0$. Suponha que existe $g \in \mathbb{K}[x]$ tal que $f \cdot g = 1$. Então

$$0 = gr(1) = gr(fg) = gr(f) + gr(g).$$ Portanto,

$m = 0$ e $n = 0$. logo,

$$U(\mathbb{K}[x]) = \mathbb{K}^*$$

$\blacksquare$

(7) Achar um polinômio não constante em $\mathbb{Z}_4[x]$ que é inversível.

Dem:

Inicialmente, observe que estamos trabalhando com o anel $\mathbb{Z}_4$, então não podemos esperar um resultado análogo.

Veja que $\bar{3}$ é inversível em $\mathbb{Z}_4$, $mdc(3,4) = 1$, com

$$\bar{3} \cdot \bar{3} = \bar{1}$$

e, $\bar{2}$ é um divisor de zero, pois, $mdc(2,4) \neq 1$,

$$\bar{2} \cdot \bar{2} = \bar{0}.$$

Tome então,

$$f = 2x + 3.$$ Assim, $f \cdot f = f^2$

$$(2x+3)(2x+3) = 4x^2 + 12x + 9 = 1.$$

$\blacksquare$

Exercício 10: Determinar o quociente e o resto de dividir $f = 5x^4 + 3x^2 + 1$ por $g = 3x^2 + 2x + 1$ em $\mathbb{Z}_7[x]$

Demonstração:

Temos que

$$
\begin{array}{l|l}
\cancel{5x^4} + 3x^3 + 0x^2 + 0x + 1 & 3x^2 + 2x + 1 \\
\hline
-\cancel{12x^4} - 8x^3 - 4x^2 & 4x^2 + 3x - 1 \equiv \\
\quad \cancel{2x^3} - 4x^2 + 0x + 1 & 4x^2 + 3x + 6 \\
\quad -\cancel{9x^3} - 6x^2 - 3x & \\
\qquad -\cancel{3x^2} - 3x + 1 & \\
\qquad +\cancel{3x^2} + 2x + 1 & \\
\qquad\qquad -x + 2 \equiv 6x + 2 &
\end{array}
$$

obs:

1) $12 \equiv 5 \pmod 7$ $\qquad -8 \equiv -1 \pmod 7$

$-8 \equiv 6 \pmod 7$

$-1 \equiv 6 \pmod 7$

$-9 \equiv -2 \pmod 7$

Assim, temos que $q = 4x^2 + 2x + 3$ é o quociente e $r = -x - 2$ é o resto.

Exercício 11: Dados os polinômios $f = 3m^2X^4 - 11mX^3 - (m^2-10)X^2 + (6m^2+5m)X$ e $g = 3mX^3 - 5X^2 - mX + 6m + 3$, de $\mathbb{R}[x]$ determinar m para que f seja divisível por g.

Demonstração:

Queremos que $f = g \cdot q$, $q \in \mathbb{R}[x]$. Veja que $gr(f) = gr(g) + gr(q) \Rightarrow gr(q) = 1$ ou 0, dependendo de m. Veja que $m \neq 0$ (porque?). Logo, $gr(q) = 1$.

Assim,

$$
\begin{array}{l|l}
\cancel{3m^2X^4} - 11mX^3 - (m^2-10)X^2 + (6m^2+5m)X + 0 & 3mX^3 - 5X^2 - mX + (6m+3) \\
\cancel{-3m^2X^4} + 5mX^3 + m^2X^2 - (6m^2+3m)X & mX - 2 \\
\hline
\quad \cancel{-6mX^3} + \cancel{10X^2} + \cancel{2mX} & \\
\quad \cancel{+6mX^3} \cancel{- 10X^2} \cancel{- 2mX} + 2(6m+3) &
\end{array}
$$

Logo, devemos ter $12m + 6 = 0 \Rightarrow m = -\frac{1}{2}$.

Exercício 12: Seja n um inteiro positivo. Achar o resto de dividir $(x-2)^{10n} + (x-1)^n + 2$ por $(x-1)(x+2)$ em $\mathbb{Q}[x]$.

Demonstração:

Queremos encontrar r tal que

$$(x-2)^{10n} + (x-1)^n + 2 = (x-1)(x-2)\, q(x) + r(x)$$

$0 \leq gr(r) < 2$. Logo $r(x) = ax + b$, $a, b \in \mathbb{Q}$. Veja que $r(1) = 3$ e $r(2) = 3$. Portanto $a = 0$ e $b = 3$.

Exercício 13: Sejam $f, g \in \mathbb{K}[x]$ e seja r o resto da divisão de f por g. Provar que todo divisor comum de f e g também é um divisor comum a g e r.

Demonstração:

Seja $d \in \mathbb{K}[x]$ um divisor comum de f e g. Assim,

$$f = d \cdot p_1, \quad g = d \cdot p_2, \quad p_1, p_2 \in \mathbb{K}[x].$$

Lembre que $f = g \cdot q + r$, $0 \leq gr(r) < gr(g)$ ou $r = 0$. Com isso,

$$d p_1 = d p_2 \cdot q + r \Rightarrow d p_1 + d p_2 \cdot q = r \Rightarrow r = d(p_1 + p_2\, q)$$

Portanto $d | g$ e $d | r$.

■

Exercício 14: Seja $f, g \in \mathbb{K}[x]$. Um polinômio $d \in \mathbb{K}[x]$ diz-se máximo divisor comum se.

(i) $d | f$ e $d | g$;

(ii) Se $d' | f$ e $d' | g$ então $d' | d$.

Provar que:

(a) Mostre que se d_1 e d_2 são ambos um máximo divisor comum de f e g, então d_1 é associado a d_2

Dem:

obs: lembre-se de que d_1 e d_2 são associados se existe $a \in \mathbb{K}$, $a \neq 0$ tal que $d_1 = a \cdot d_2$.

Como $d_1 = mdc(f, g)$ então $d_1 | f$ e $d_1 | g$. Analogamente, $d_2 | f$ e $d_2 | g$. Por (ii), vemos que $d_1 | d_2$ e $d_2 | d_1$.

Logo, $d_1 = d_2 \cdot r$ e $d_2 = d_1 q$, $r, q \in \mathbb{K}[x]$. Com efeito, $d_1 = d_1 q r \Rightarrow d_1(1 - qr) = 0$. Usando que $\mathbb{K}[x]$ é um domínio de integridade (leiam Lacy Monteiro) temos que $1 - qr = 0 \Rightarrow qr = 1$.

Relembre que $U(\mathbb{K}[x]) = \mathbb{K}$. Portanto, $q, r \in \mathbb{K}$. Com isso, d_1 e d_2 são associados.

∎

(b) Prove que existe um único máximo divisor comum de f e g que é mônico. Este polinômio será denotado como $mdc(f, g)$.

Demonstração:

Já vimos por (a) que se d_1 e d_2 são ambos máximo divisor comum de f e g então

$$d_1 = \alpha d_2, \quad \alpha \in \mathbb{K}.$$

Considere $d_1 = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ e $d_2 = b_n x^n + \dots + b_0$. Como queremos provar que há um único máximo divisor comum mônico, consideramos $a_n = b_n = 1$. Pela igualdade dos polinômios temos que

$$a_n = \alpha b_n \Rightarrow 1 = \alpha.$$

Logo $d_1 = d_2$.

∎

(15) Mostre que o máximo divisor comum de dois polinômios pode ser calculado da forma análoga ao máximo divisor comum de dois números inteiros utilizando o Algoritmo de Euclides.

Demonstração: (vamos considerar mdc mônico)

Inicialmente, observe que pelo Algoritmo da Divisão, existem $q, r \in \mathbb{K}[x]$ tal que

$$f = g \cdot q + r, \quad 0 \leq gr(r) < gr(g).$$

Já vimos (ex 13) todo divisor comum de f e g também é um divisor comum de g e r. Com isso, temos que $mdc(f,g) \mid g$ e $mdc(f,g) \mid r$. Seja $d = mdc(g,r)$ então $d \mid g$ e $d \mid r \Rightarrow d \mid f$. logo, $d \mid mdc(f,g)$ Portanto,

$$mdc(f,g) = mdc(g,r) \text{ (Por que?)}$$

Assim, observe que

$$f = g \cdot q_1 + r_1, \quad 0 \leq gr(r_1) < gr(g)$$

$$g = r_1 q_2 + r_2, \quad 0 \leq gr(r_2) < gr(r_1)$$

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq gr(r_3) < gr(r_2)$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \leq gr(r_n) < gr(r_{n-1})$$

$$r_{n-1} = r_n q_{n+1}$$

Como o grau dos restos de cada divisão diminui a cada passo esse processo é finito. Vejo que no máximo temos $gr(r_n) = 0$, ou seja, $r_n \in \mathbb{K}^*$. Assim $r_{n-1} = r_n q_{n+1}$ é uma divisão exata. Assim, como vimos

$$mdc(f,g) = mdc(g, r_1) = mdc(r_1, r_2) = \dots = mdc(r_{n-1}, r_n)$$

Observe que $r_n | r_{n-1}$ então considerando a_m o coeficiente dominante de r_n, $mdc(f,g) = a_m^{-1} r_n$, pois $mdc(r_{n-1}, r_n) = a_m^{-1} r_n$.

■

Exercício 17: Achar o máximo divisor comum dos polinômios f e g nos seguintes casos.

(a) $f = X^4 + X^3 + 2X^2 - X - 3$, $g = X^3 + X^2 - 4X + 2$

(b) $f = X^4 + 2X^3 - 3X^2 + 5$, $g = X^2 - 3X + 2$

Dem: Basta aplicar o algoritmo de Euclides para polinômios.

■

Exercício 19: Sejam $f, g \in \mathbb{K}[x]$. Provar que o conjunto

$$I = \{\alpha f + \beta g : \alpha, \beta \in \mathbb{K}[x]\}$$

Tem as propriedades (i) e (ii) do exercício anterior. Utilizar este fato para provar que existem $r, s \in \mathbb{K}[x]$ tais que

$$mdc(f,g) = rf + sg$$

Demonstração:

Seja $\alpha_1 f + \beta_1 g \in I$ e $\alpha_2 f + \beta_2 g \in I$, então

$$(\alpha_1 f + \beta_1 g) + (\alpha_2 f + \beta_2 g) = (\alpha_1 + \alpha_2) f + (\beta_1 + \beta_2) g \in I$$

Agora tome $\alpha f + \beta g \in I$. Então, para $h \in \mathbb{K}[x]$,

$$h(\alpha_1 f + \beta_1 g) = (h\alpha_1) f + (h\beta_1) g \in I.$$

Pelo ex. 18, veja que, existe $f_0 \in \mathbb{K}[x]$ tal que

$$I = f_0 \mathbb{K}[x]$$

Vamos mostrar se $f_0 = a_n x^n + \dots + a_0$, $a_n \neq 0$ então

$a_n^{-1} f_0 = mdc(f,g)$. Note que $f, g \in I$, pois

$$f = 1 \cdot f + 0g \quad e \quad g = 0f + 1g.$$

Daí, $f_0 \mid f$ e $f_0 \mid g$.

Além disso, como $f_0 \in f_0 \mathbb{K}[x] \Rightarrow f_0 = \alpha f + \beta g$. Logo, se $d' \mid f$ e $d' \mid g \Rightarrow d' \mid \alpha f + \beta g = f_0$

Portanto, $f_0 = mdc(f, g)$

Exercício 22: Um polinômio $f \in K[x]$ que não é um polinômio constante, diz-se irredutível se não tem divisores próprios. Em caso contrário, ele se diz redutível.

(a) Provar que um polinômio f não constante é irredutível se e somente se toda vez que f se escreve como um produto $f = g \cdot h$ tem-se que $gr(g) = 0$ ou $gr(h) = 0$

Dem:

($\Rightarrow$) Considere que $f = g \cdot h$ tal que $gr(g) \neq 0$ e $gr(h) \neq 0$. Como g e h não podem ser ambos associados a f (veja o porquê). Devemos ter que ambos são divisores próprios de f, contradizendo o fato de f ser irredutível.

($\Leftarrow$) Veja que se $f = g \cdot h \Rightarrow gr(f) = gr(g) + gr(h)$. Logo, como $gr(f) = 0$ ou $gr(g) = 0$, vamos supor que $gr(f) = 0$, temos que $gr(g) = gr(f)$. Assim g é um polinômio constante e h é associado. logo,

f é irredutível

(b) Provar que todo polinômio f não constante tem pelo menos um divisor irredutível.

Demonstração:

Vamos proceder por indução no grau de f. Se $n=1$, $f = ax+b$. logo f é irredutível e é ele próprio seu divisor.

Supomhamos que se $gr(f) \leq n$ então f possui um divisor irredutível. Vamos provar para $gr(f) = n+1$. Se f é irredutível não há o que fazer. Se f é redutível então $f = g \cdot h$, com $gr(g) < gr(f)$ e $gr(h) < gr(f)$. logo, g e h tem divisores irredutível e, portanto f tem divisor irredutível.

(c) Provar que todo polinômio f não constante pode se escrever como um produto da forma:

$$f = \alpha f_1 \cdots f_t$$

onde $\alpha \in \mathbb{K}$ e cada f_i, $1 \leq i \leq t$ é um polinômio irredutível.

Demonstração:

Vamos proceder por indução no grau de f. $(gr(f))$

Se $n=1$, f é irredutível.

Suponha que para $gr(f) < n$,

$$f = \alpha f_1 \cdots f_t,$$

com f_i irredutíveis. Se $gr(f) = n$, então se f é irredutível, não há o que fazer. Se f é redutível então f possui divisores próprios. logo,

$$f = g \cdot h, \quad gr(g), gr(h) < n$$

Pela hipótese de indução $g = \alpha_1 f_1 \cdots f_t$ e $h = \alpha_2 h_1 \cdots h_s$, com f_i, h_j irredutíveis. Daí,

$$f = (\alpha_1 \alpha_2) f_1 \cdots f_t h_1 \cdots h_s$$

(d) Utilizar o exercício anterior para que a expressão obtida acima para f é única

Demonstração:

Considere $f = \alpha_1 f_1 \cdots f_t$ e $f = \alpha_2 g_1 \cdots g_s$. Veja que

$f \mid \alpha_2 g_1 \cdots g_s$ e, portanto, $f_1 \mid \alpha_2 g_1 \cdots g_s$. Daí,

pelo ex 21 (tentem fazê-lo) $f_1 \mid g_j$. Vamos supor que

$j = 1$ (S.P.G). Como g_1 é irredutível $g_1 = c_1 f_1$. Então

$$\alpha_1 f_1 \cdots f_t = \alpha_2 g_1 \cdots g_s \Rightarrow$$

$$\alpha_1 f_1 \cdots f_t = \alpha_2 c_1 f_1 g_2 \cdots g_s \Rightarrow$$

$$\alpha_1 f_2 \cdots f_t = \alpha_2 c_1 g_2 \cdots g_s$$

Analogamente $f_2 \mid g_l$, $2 \leq l \leq s$. Daí, supomos que

$f_2 \mid g_2$ e concluímos que $c_2 f_2 = g_2$. Assim

$$\alpha_1 f_3 \cdots f_t = \alpha_2 c_1 c_2 g_3 \cdots g_s.$$

Podemos considerar que $t < s$. Daí, continuando o

processo acima temos que

$$1 = \alpha_1^{-1} \alpha_2 c_1 c_2 \cdots c_t \, g_{t+1} \cdots g_s \Rightarrow$$

$g_{t+1}, \ldots, g_s$ são constantes, contradição. Logo, devemos

ter $s = t$. Assim, a menos da constante α, a decomposição

é única.

Exercício 23: Provar que o conjunto dos polinômios irredutíveis $\mathbb{K}[x]$ é infinito.

Demonstração:

Considere que o conjunto dos polinômios irredutíveis em $\mathbb{K}[x]$ é finito, seja ele

$$I = \{p_1, \dots, p_k\} \subseteq \mathbb{K}[x].$$

Tome o polinômio

$$f = p_1 \cdots p_k + 1$$

Note que como f é divisível por algum p_i. Assim, como $p_i \mid p_1 \cdots p_k$, devemos ter que $p_i \mid 1$, contradição.

$\square$