Estruturas Algébricas

Aula 3

Os Polinômios

Abramo Hefez

2025

Os Polinômios

Esta aula será dedicada ao estudo dos polinômios com coeficientes em um anel comutativo.

Polinômios são objetos matemáticos de grande interesse tanto teórico quanto prático. Eles serão aqui estudados como objetos algébricos formais e não como funções como em Cálculo, o que aumentará o espectro de suas aplicações.

Polinômios com coeficientes em anéis

Seja A um anel comutativo. Um símbolo x não pertencente ao anel A será chamado de uma **indeterminada sobre** A.

Vamos utilizar símbolos x^j, para $j = 0$ ou para j natural, e escreveremos $x^0 = 1$ e $x^1 = x$.

Até aqui, esses símbolos não representam potências de x, sendo apenas simbolos que mais adiante representarão potências de x em um determinado anel.

Um **polinômio** $f(x)$ com coeficientes em A é uma expressão formal do tipo

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n = \sum_{j=0}^{n} a_j x^j,$$

onde $n \in \mathbb{N} \cup \{0\}$ e $a_0, a_1, \ldots, a_n \in A$.

Denotamos por $A[x]$ o conjunto de todos os polinômios com coeficientes em A.

Para $0 \leqslant j \leqslant n$, os elementos a_j são chamados de **coeficientes** do polinômio $f(x)$. Quando $a_j = 1$, escrevemos x^j no lugar de $a_j x^j$

As parcelas $a_j x^j$, de **termos** e os termos $a_j x^j$ tais que $a_j \neq 0$, de **monômios de grau** j do polinômio $f(x)$.

O coeficiente a_0 é chamado de **termo constante**

Chamamos $f(x) = a_0$ de **polinômio constante**.

Quando $f(x) = 0$, chamamos $f(x)$ de **polinômio nulo**. Este polinômio poderá ser escrito na forma $f(x) = 0 + 0x + \cdots + 0x^n$, qualquer que seja $n \in \mathbb{N} \cup \{0\}$.

Costuma-se omitir o termo $a_j x^j$, sempre que $a_j = 0$.

Pode-se escrever um polinômio $f(x)$ com os seus termos $a_j x^j$ em qualquer ordem, mas dá-se preferência à ordem crescente ou à ordem decrescente em j.

Exemplos

São polinômios em $\mathbb{R}[x]$:

$$f(x) = \tfrac{1}{2} + x + \sqrt{2}x^2 + 2x^3 \quad \text{e}$$

$$g(x) = -\sqrt{3}x + 2 - \tfrac{2}{5}x^5 + \pi x^3.$$

São polinômios em $\mathbb{Z}[x]$:

$$p(x) = -x + 3x^2 - 3x^4, \quad q(x) = x^2 + 2x + 3, \quad \text{e}$$

$$r(x) = -3x^4 + 2 - x + 3x^2.$$

O polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, com as convenções que fizemos acima, pode ser escrito como

$$f(x) = a_0 + a_1x + \cdots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \cdots + 0x^m,$$

para todo número natural $m > n$. Isto será útil quando compararmos dois polinômios $f(x), g(x) \in A[x]$.

Dizemos que $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x^1 + b_2x^2 + \cdots + b_nx^n$ em $A[x]$ são **polinômios iguais** se, e somente se, $a_j = b_j$, para $0 \leq j \leqslant n$. Nesse caso, escrevemos $f(x) = g(x)$.

Por exemplo, os termos constantes dos polinômios $p(x) = -x + 3x^2 - 3x^4$ e $r(x) = 2 - x + 3x^2 - 3x^4$ são diferentes. Logo, $p(x) \neq r(x)$.

Os polinômios

$$2x^4 + x^5 + 4x^2 - 3 - x \quad \text{e}$$

$$-3 + 4x^2 - x + x^5 + 2x^4,$$

em $\mathbb{Z}[x]$ são iguais, porque os seus coeficientes a_j são: $a_0 = -3$, $a_1 = -1$, $a_2 = 4$, $a_3 = 0$, $a_4 = 2$ e $a_5 = 1$.

Note que se escrevermos os polinômios com os seus termos em ordem crescente ou decrescente, visualizamos imediatamente a igualdade ou não dos polinômios.

Em todo polinômio, não nulo, $f(x) \neq 0$, algum coeficiente deve ser diferente de zero, então há um maior índice n tal que $a_n \neq 0$. Definimos o **grau** de $f(x)$ como sendo este número n e o denotamos por $\mathrm{grau}(f(x))$.

Nesse caso, a_n é chamado de **coeficiente líder** de $f(x)$.

Os polinômios de grau n com coeficiente líder $a_n = 1$ são chamados de **polinômios mônicos**.

Atenção! Não definimos o grau do polinômio nulo: $f(x) = 0$.

Com estas definições, temos

$$\mathrm{grau}(f(x)) = 0 \text{ se, e somente se, } f(x) = a \neq 0,\ a \in A.$$

No conjunto $A[x]$, podemos definir operações de adição e multiplicação de polinômios, a partir das operações de adição e multiplicação de A.

Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ em $A[x]$. Definimos a operação de **adição** desses polinômios como segue

$$f(x) + g(x) = \sum_{j=0}^{\max(n,m)} c_j x^j, \text{ onde } c_j = a_j + b_j, \text{ para } 0 \leqslant j \leqslant \max(n, m).$$

O resultado da adição de dois polinômios é chamado de **soma**.

Exemplo

Sejam $f(x) = 3x^3 - 3x^2 + 4x + 5$ e $g(x) = 2x^2 - 6x - 1$ em $\mathbb{Z}[x]$. Então,

$$\begin{aligned} f(x) + g(x) &= (3+0)x^3 + (-3+2)x^2 + (4+(-6))x + (5+(-1)) \\ &= 3x^3 - x^2 - 2x + 4 \end{aligned}$$

Para a operação de adição de polinômios, vale a seguinte propriedade do grau: se $f(x) \neq 0$, $g(x) \neq 0$ e $f(x) + g(x) \neq 0$, então

$$\mathrm{grau}(f(x) + g(x)) \leqslant \max\{\, \mathrm{grau}(f(x)), \mathrm{grau}(g(x)) \,\},$$

valendo a igualdade sempre que $\mathrm{grau}(f(x)) \neq \mathrm{grau}(g(x))$.

Dados os polinômios $f(x) = \sum_{j=0}^{n} a_j x^j$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ em $A[x]$, definimos a **multiplicação** desses polinômios como segue:

$$f(x) \cdot g(x) = \sum_{j=0}^{n+m} c_j x^j,$$

onde

$$\begin{aligned}
c_0 &= a_0 \cdot b_0 \\
c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\
c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 \\
&\vdots \\
c_j &= a_0 \cdot b_j + a_1 \cdot b_{j-1} + \cdots + a_j \cdot b_0 = \sum_{\lambda+\mu=j} a_\lambda \cdot b_\mu \\
&\vdots \\
c_{n+m} &= a_n \cdot b_m \,.
\end{aligned}$$

O resultado da multiplicação de dois polinômios é chamado de **produto**.

Segue, imediatamente, da definição da multiplicação de polinômios, que:

1) Para quaisquer $j, k \in \mathbb{N} \cup \{0\}$, vale a identidade:

$$x^j \cdot x^k = x^{j+k}.$$

Portanto, x^j, que era apenas um símbolo para A, comporta-se como uma potência em $A[x]$;

2) Se $f(x) = a$ e $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, então

$$f(x) \cdot g(x) = a \cdot g(x) = (a \cdot b_0) + (a \cdot b_1)x + \cdots + (a \cdot b_m)x^m .$$

Como consequência das propriedades da adição e da multiplicação do anel A, a adição e a multiplicação de polinômios em $A[x]$ possuem propriedades que descreveremos a seguir.

Proposição A adição e a multiplicação em $A[x]$ têm as seguintes propriedades: Para quaisquer $f(x)$, $g(x)$ e $h(x)$ em $A[x]$,

(Associatividade) $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$ e
$$(f(x)\cdot g(x))\cdot h(x)=f(x)\cdot(g(x)\cdot h(x));$$

(Comutatividade) $f(x)+g(x)=g(x)+f(x)$ e
$$f(x)\cdot g(x)=g(x)\cdot f(x);$$

(Distributividade) $f(x)\cdot(g(x)+h(x))=f(x)\cdot g(x)+f(x)\cdot h(x)$;

(Existência de elemento neutro aditivo) O polinômio nulo é tal que $f(x)=0+f(x)$, para todo $f(x)\in A[x]$.

(Existência de simétrico) Dado $f(x)=a_0+a_1x+\cdots+a_nx^n$, o simétrico de $f(x)$ é o polinômio
$$-f(x)=(-a_0)+(-a_1)x+\cdots+(-a_n)x^n.$$

(Existência de elemento neutro multiplicativo) O polinômio constante 1 é tal que $1\cdot f(x)=f(x)$, para todo $f(x)\in A[x]$.

Prova A demonstração é uma série de verficações simples, porém tediosas. Faremos a demonstração de algumas das propriedades e deixaremos as outras como exercício.

Sejam dados $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{m} b_j x^j$ e $h(x) = \sum_{j=0}^{\ell} c_j x^j$.

Associatividade da adição: Podemos supor que $n = m = \ell$, após reescrever $f(x)$, $g(x)$ e $h(x)$ com as mesmas potências de x:

$$\begin{aligned}
(f(x) + g(x)) + h(x) &\overset{(1)}{=} \sum_{j=0}^{n} (a_j + b_j)x^j + \sum_{j=0}^{n} c_j x^j \\
&\overset{(2)}{=} \sum_{j=0}^{n} \big((a_j + b_j) + c_j\big)x^j \\
&\overset{(3)}{=} \sum_{j=0}^{n} \big(a_j + (b_j + c_j)\big)x^j \\
&\overset{(4)}{=} \sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{n} (b_j + c_j)x^j \\
&\overset{(5)}{=} f(x) + (g(x) + h(x)),
\end{aligned}$$

Comutatividade da multiplicação:

$$\begin{aligned} f(x)\cdot g(x) &= \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda \cdot b_\mu\right)x^j \\ &= \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} b_\mu \cdot a_\lambda\right)x^j \\ &= g(x)\cdot f(x), \end{aligned}$$

pois, em A, temos $a_\lambda \cdot b_\mu = b_\mu \cdot a_\lambda$, para quaisquer λ e μ.

Distributividade: Podemos supor $\ell = m$, após reescrever $g(x)$ e $h(x)$ com as mesmas potências de x:

$$
\begin{aligned}
f(x)\cdot(g(x)+h(x)) &\overset{(1)}{=} \left(\sum_{j=0}^{n} a_j x^j\right)\cdot\left(\sum_{j=0}^{m}(b_j+c_j)x^j\right)\\
&\overset{(2)}{=} \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot(b_\mu+c_\mu)\right)x^j\\
&\overset{(3)}{=} \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot b_\mu + a_\lambda\cdot c_\mu)\right)x^j\\
&\overset{(4)}{=} \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot b_\mu\right)x^j + \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot c_\mu\right)x^j\\
&\overset{(5)}{=} f(x)\cdot g(x)+f(x)\cdot h(x),
\end{aligned}
$$

onde em (1) usamos a definição da adição em $A[x]$; em (2), a definição da multiplicação em $A[x]$; em (3), a distributividade em A; em (4), a definição da adição em $A[x]$; e, em (5), novamente, a definição da multiplicação em $A[x]$.

Tendo em vista as propriedades das operações de $A[x]$, enunciadas na Proposição, temos que $A[x]$ é um anel comutativo.

A multiplicação de polinômios pode ser também efetuada utilizando a propriedades contidas na Proposição, como faremos no exemplo a seguir.

Exemplo Sejam $f(x) = 2x^3 + 3x^2 - 4x + 3$ e $g(x) = x^2 + 2x + 3$ em $\mathbb{Z}[x]$. Vamos calcular $f(x) \cdot g(x)$. Usando a propriedade distributiva da multiplicação de polinômios, temos

$$\begin{aligned} f(x) \cdot g(x) &= (2x^3 + 3x^2 - 4x + 3) \cdot (x^2 + 2x + 3) \\ &= 2x^3 \cdot (x^2 + 2x + 3) + 3x^2 \cdot (x^2 + 2x + 3) + \\ &\quad (-4x) \cdot (x^2 + 2x + 3) + 3 \cdot (x^2 + 2x + 3) \\ &= (2x^5 + 4x^4 + 6x^3) + (3x^4 + 6x^3 + 9x^2) + \\ &\quad (-4x^3 - 8x^2 - 12x) + (3x^2 + 6x + 9) \end{aligned}$$

$$\begin{aligned} &= 2x^5 + (4+3)x^4 + (6+6-4)x^3 + (9-8+3)x^2 + (-12+6)x + 9 \\ &= 2x^5 + 7x^4 + 8x^3 + 4x^2 - 6x + 9. \end{aligned}$$

No Exemplo acima, temos que

$$\mathrm{grau}(f(x)\cdot g(x)) = 5 = \mathrm{grau}(f(x)) + \mathrm{grau}(g(x)).$$

Isto não é uma mera coincidência. Temos a seguinte propriedade importante do grau em $A[x]$:

Proposição Seja A um domínio de integridade. Temos que

i) Se $P(x), Q(x) \in A[x] \setminus \{0\}$, então

$$\mathrm{gr}(P(x)\cdot Q(x)) = \mathrm{gr}(P(x)) + \mathrm{gr}(Q(x));$$

ii) $A[x]$ é um domínio de integridade;

iii) Os elementos invertíveis de $A[x]$ são os elementos invertíveis de A. Em símbolos: $A[x]^* = A^*$

Prova (i) Suponhamos que $P(x) = a_0 + \cdots + a_n x^n$ e $Q(x) = b_0 + \cdots + b_m x^m$, com $a_n \neq 0$ e $b_m \neq 0$. Logo, $P(x) \cdot Q(x) = a_0 \cdot b_0 + \cdots + (a_n \cdot b_m)x^{n+m}$. Como A é um domínio, $a_n \cdot b_m \neq 0$, logo

$$\mathrm{gr}(P(x) \cdot Q(x)) = n + m = \mathrm{gr}(P(x)) + \mathrm{gr}(Q(x)).$$

(ii) Segue imediatamente de (i).

(iii) Basta mostrar que todo elemento invertível de $A[x]$ é invertível em A, já que a recíproca é óbvia.

Seja $P(x)$ um elemento invertível em $A[x]$, então existe um elemento $Q(x) \in A[x]$ tal que $P(x) \cdot Q(x) = 1$. Logo, $P(x) \neq 0$ e $Q(x) \neq 0$ e, portanto, de (i) temos que

$$\mathrm{gr}(P(x)) + \mathrm{gr}(Q(x)) = \mathrm{gr}(P(x) \cdot Q(x)) = \mathrm{gr}(1) = 0.$$

Consequentemente, $\mathrm{gr}P(x) = \mathrm{gr}Q(x) = 0$ e, portanto, $P(x), Q(x) \in A$ com $P(x) \cdot Q(x) = 1$; logo, $P(x)$ é invertível em A.

A propriedade, acima, será chamada de **propriedade multiplicativa do grau**.

A propriedade multiplicativa dos graus não é válida em geral se A não for um domínio. Por exemplo, em $\mathbb{Z}_4[x]$, se considerarmos os polinômios $p(x) = [2]x + 1$ e $q(x) = [2]$, então $p(x)q(x) = [2]$ e, portanto,

$$0 = \text{grau}(p(x)q(x)) \neq 1 + 0 = \text{grau}(p(x)) + \text{grau}(q(x)).$$

Também se A não for um domínio, os ítens (ii) e (iii) da Proposição podem deixar de valer. Por exemplo, em $\mathbb{Z}_4[x]$ temos os seguintes fatos:

$$[2] \cdot [2]x = [0] \quad \text{e} \quad ([2]x + [1])(([2]x + [1]) = [1].$$

Uma observação importante a ser feita e que será utilizada mais adiante é que, mesmo que A não seja um domínio de integridade, se um dos coeficientes líderes de $f(x)$ ou de $g(x)$ for invertível, continua valendo a propriedade multiplicativa do grau.

A seguir apresentamos um método que permite resolver alguns problemas envolvendo polinômios, chamado método dos coeficientes a determinar de Descartes.

Exemplo Determinar dois polinômios de grau 2 com coeficientes inteiros cujo produto seja $x^4 + 4 \in \mathbb{Z}[x]$.

Escrevamos em $\mathbb{Z}[x]$:

$$\begin{aligned} x^4 + 4 &= f(x)g(x) = (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd. \end{aligned}$$

Da igualdade de polinômios, segue

(1) $a + c = 0$ (2) $d + ac + b = 0$

(3) $ad + bc = 0$ (4) $bd = 4$.

De (4), obtemos as seis possiblidades para os valores de b e d, a saber, $b = 1$ e $d = 4$, ou $b = 2$ e $d = 2$, ou $b = 4$ e $d = 1$, ou $b = -1$ e $d = -4$, ou $b = -2$ e $d = -2$, ou $b = -4$ e $d = -1$.

De (1), temos que $a = -c$. Substituindo em (2), obtemos que $d + b = c^2$. Assim, a única possibilidade é $b = 2$ e $d = 2$ e, nesse caso, $c = 2$ ou $c = -2$. Logo, $a = -2$ ou $a = 2$. A equação (3) é satisfeita. Portanto, $f(x) = x^2 - 2x + 2$ e $g(x) = x^2 + 2x + 2$.

Raízes de polinômios

Se $p(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e $\alpha \in A$, define-se

$$p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in A.$$

Diremos que α é uma **raiz** de $p(x)$ se $p(\alpha) = 0$.

Em um anel dizemos que um elemento a divide um elemento b, se existir um elemento c tal que $b = ac$.

Proposição Sejam A um anel, $p(x) \in A[x]$ e $\alpha \in A$. Temos que α é uma raiz de $p(x)$ se, e somente se, $(x - \alpha)$ divide $p(x)$.

Prova Dado $p(x) = a_nx^n + \cdots + a_1x + a_0$, escrevendo

$$p(x) = p(x-\alpha+\alpha) = a_n[(x-\alpha)+\alpha]^n + \cdots + a_1[(x-\alpha)+\alpha] + a_0$$

e expandindo as potências $[(x - \alpha) + \alpha]^i$, para $i = 1, \ldots, n$, pelo binômio de Newton, vê-se que existe um polinômio $q(x)$ tal que

$$p(x) = p(\alpha) + (x - \alpha)q(x).$$

Portanto, se $p(\alpha) = 0$, então $p(x) = (x - \alpha)q(x)$, logo $(x - \alpha)$ divide $p(x)$.

Reciprocamente, se $(x-\alpha)$ divide $p(x)$, então existe $q_1(x)$ tal que $p(x) = (x-\alpha)q_1(x)$, logo $p(\alpha) + (x-\alpha)q(x) = (x-\alpha)q_1(x)$. Avaliando esta última expressão em $x = \alpha$, temos que $p(\alpha) = 0$.

Teorema Um polinômio de grau n com coeficientes em um domínio A possui, no máximo, n raízes distintas em A.

Prova Sejam $\alpha_1, \ldots, \alpha_m$ raízes distintas em A de um polinômio $p(x)$ de grau n. Pela Proposição anterior, temos que existe um polinômio $q_1(x) \in A[x]$ tal que

$$p(x) = (x-\alpha_1)q_1(x).$$

Como α_2 é raiz de $p(x)$, temos que $0 = p(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2)$, logo, sendo $\alpha_2 \neq \alpha_1$ e sendo A um domínio, então $q_1(\alpha_2) = 0$. Pela Proposição anterior, temos que existe $q_2(x) \in A[x]$ tal que $q_1(x) = (x-\alpha_2)q_2(x)$.

Segue daí que

$$p(x) = (x-\alpha_1)(x-\alpha_2)q_2(x).$$

Esse raciocínio se repete até obtermos $q_m(x) \in A[x]$ tal que

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_m) q_m(x).$$

Segue, então, que $n = \mathrm{grau}(p(x)) = m + \mathrm{grau}(q_m(x))$, o que nos fornece a desigualdade $m \leq n$.

Se A não é um domínio, este resultado pode ser falso: o polinômio $[2]x \in \mathbb{Z}_4[x]$ de grau 1 possui as raízes [0] e [2].

Sejam A um anel e $\alpha \in A$ uma raiz de $p(x) \in A[x]$.

Diremos que α é uma raiz de $p(x)$ de **multiplicidade** $m \geq 1$ quando $(x - \alpha)^m$ é a maior potência de $(x - \alpha)$ que divide $p(x)$.

Quando $m = 1$, diremos que α é uma **raiz simples** de $p(x)$,

e quando $m > 1$, diremos que α é uma **raiz múltipla** de $p(x)$.

É claro que α é uma raiz de $p(x)$ de multiplicidade m se, e somente se, existe $q(x) \in A[x]$ tal que

$$p(x) = (x - \alpha)^m q(x), \quad \mathrm{com} \quad q(\alpha) \neq 0.$$

Corpos algebricamente fechados

Dizemos que um corpo K é algebricamente fechado, se todo polinômio em $K[x] \setminus K$ tem pelo menos uma raiz em K.

$\mathbb{R}$ não é algebricamente fechado, pois $x^2 + 1$ não tem raízes em $\mathbb{R}$.

Por outro lado, devido ao **Teorema Fundamental da Álgebra**, temos que $\mathbb{C}$ é um corpo algebricamente fechado.

Proposição Seja $p(x) \in K[x] \setminus K$, sendo K um corpo algebricamente fechado. Se $\mathrm{grau}(p(x)) = n$, com $n \geq 1$, então, existem $a, \alpha_1, \alpha_2, \ldots, \alpha_n \in K$, tais que

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Prova A prova será feita por indução sobre n. Se $n = 1$, temos que $p(x) = ax + b$ e, portanto, $p(x) = a(x - (-b/a))$, provando o resultado nesse caso, tomando $\alpha_1 = -b/a$.

Suponhamos agora que o resultado seja verdadeiro para polinômios de grau $n - 1$. Seja $p(x)$ um polinômio de grau n. Como K é algebricamente fechado, existe $\alpha_1 \in K$ tal que $p(\alpha_1) = 0$, logo, $p(x) = (x\alpha_1)q(x)$, sendo $q(x)$ um polinômio de grau $n - 1$. Aplicando a hipótese de indução a $q(x)$, o resultado segue.

Derivação de polinômios

Sejam A um anel e $p(x) = \sum_{j=0}^{n} a_j x^j$ em $A[x]$. Se $\text{grau}(p(x)) \geq 1$, então a **derivada** de $p(x)$, denotada por $p'(x)$, é o polinômio

$$p'(x) = \sum_{j=1}^{n} j a_j x^{j-1},$$

definindo $p'(x) = 0$ se $p(x) = a \in A$.

Note que essa definição de derivada é apenas formal, não envolvendo nenhum processo de limite.

Proposição Sejam $p(x), q(x) \in A[x]$ e $a \in A$. Temos que

i) $(p(x) + q(x))' = p'(x) + q'(x)$;

ii) $(ap(x))' = ap'(x)$;

iii) $(p(x) \cdot q(x))' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$;

iv) $(p(x)^r)' = rp(x)^{r-1} \cdot p'(x)$, para todo $r \geq 1$.

Prova As asserções (i) e (ii) são trivialmente verificadas.

Para provar (iii), pela linearidade da derivação (propriedades (i) e (ii)), é suficiente mostrar que vale (iii) para produtos de monômios.

Isso segue das igualdades abaixo:

$$\begin{aligned}(x^r \cdot x^s)' &= (x^{r+s})' = (r+s)x^{r+s-1} = rx^{r-1} \cdot x^s + x^r(sx^{s-1}) \\ &= (x^r)' \cdot x^s + x^r \cdot (x^s)'.\end{aligned}$$

A prova de (iv) será feita por indução sobre r. O caso $r = 1$ é óbvio.

Suponhamos que $r \geq 1$ e que a afirmação seja verdadeira para r.

Então,

$$\left(p(x)^{r+1}\right)' = \left(p(x)^r \cdot p(x)\right)' = \left(p(x)^r\right)' \cdot p(x) + p(x)^r \cdot p'(x) =$$

$$rp(x)^{r-1} \cdot p'(x) \cdot p(x) + p(x)^r \cdot p'(x) = (r+1)p(x)^r \cdot p'(x),$$

onde a segunda igualdade é consequência de (iii) e, a terceira igualdade, da hipótese de indução.

Isso mostra que a asserção é verdadeira para $r + 1$, logo, é verdadeira para todo r.

O resultado a seguir é um critério para decidir se um determinado polinômio possui raízes múltiplas.

Proposição Um polinômio $p(x) \in A[x]$, onde A é um anel comutativo, tem uma raíz múltipla α se, e somente se, $p(\alpha) = p'(\alpha) = 0$.

Prova α é raiz múltipla de $p(x)$ se, e somente se, $p(x) = (x - \alpha)q(x)$ para algum polinômio $q(x) \in A[x]$ divisível por $(x - \alpha)$, ou seja, com $q(\alpha) = 0$.

Portanto, α é raiz múltipla de $p(x)$ se, e somente se, $p(\alpha) = q(\alpha) = 0$.

Note agora que $p'(x) = q(x) + (x - \alpha)q'(x)$ e, consequentemente, $q(\alpha) = 0$ se, e somente se, $p'(\alpha) = 0$.

Finalmente, temos que α é raiz múltipla de $p(x)$ se, e somente se, $p(\alpha) = p'(\alpha) = 0$.

Polinômios $\times$ Funções Polinomiais

É importante diferenciar um polinômio de uma função polinomial, conforme veremos a seguir.

Dado um polinômio $p(x) \in A[x]$, podemos a ele associar uma função $\tilde{p}\colon A \to A$ definida por $a \mapsto p(a)$.

Se $\mathcal{F}(A, A)$ é o conjunto das funções de A em A, que sabemos ser um anel, temos definida uma função

$$\begin{array}{rccc} \phi\colon & A[x] & \to & \mathcal{F}(A, A) \\ & p(x) & \mapsto & \tilde{p} \end{array}$$

É um exercício mostrar que ϕ é um homomorfismo de anéis.

O subanel $\mathcal{FP}(A) := \phi(A[x])$ de $\mathcal{F}(A, A)$ é chamado de **anel das funções polinomiais** de A.

Em geral, o homomorfismo ϕ não é sobrejetor, ou seja, o anel $\mathcal{FP}(A)$ das funções polinomiais pode estar contido propriamente no anel $\mathcal{F}(A, A)$ de todas as funções de A.

Por exemplo, se $A = \mathbb{R}$, sabe-se do Cálculo que a função exponencial não é polinomial.

Tampouco, o homomorfismo ϕ é em geral injetor.

Por exemplo, se $A = \mathbb{Z}_2$, os polinômios $p(x) = x$ e $q(x) = x^2$ induzem a mesma função polinomial sobre $\mathbb{Z}_2$, pois $p(0) = q(0) = 0$ e $p(1) = q(1) = 1$.

No entanto, em algumas situações é possível garantir a injetividade ou a sobrejetividade de ϕ.

Proposição Se A é um domínio infinito, então ϕ é injetora.

Prova Suponha que se tenha dois polinômios $p(x)$ e $q(x)$ tais que $\phi(p(x)) = \phi(q(x))$, logo por ϕ ser um homomorfismo isso implica que $\phi(p(x) - q(x)) = 0$.

Assim o polinômio $t(x) = p(x) - q(x)$ induz a função nula, logo se anula para todo $x \in A$.

Como A é um domínio, se $t(x)$ fosse um polinômio não nulo, ele teria um número finito de raízes, mas sendo A infinito e todos os elementos e A são raízes de $t(x)$, isso implica que $t(x) = 0$ como polinômio e, portanto $p(x) = q(x)$.

Portanto, se, por exemplo, $A = \mathbb{R}$, temos que $\phi\colon \mathbb{R}[x] \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ é injetora, logo $\phi\colon \mathbb{R}[x] \to \mathcal{FP}(\mathbb{R})$ é um isomorfismo. Esta é a razão de no Cálculo não se fazer distinção entre polinômios e funções polinomiais.

Veremos mais adiante que, quando A é um domínio finito, o homomorfismo ϕ nunca é injetor, porém é sempre sobrejetor.

Polinômios em várias indeterminadas

Sejam A um anel e $A[x_1]$ o anel de polinômios com coeficientes em A na indeterminada x_1. Se x_2 é uma indeterminada sobre o anel $A[x_1]$, definimos

$$A[x_1, x_2] = \big(A[x_1]\big)[x_2].$$

Procedendo indutivamente, definimos o anel de polinômios em n indeterminadas

$$A[x_1, x_2, \ldots, x_n] = \big(A[x_1, x_2, \ldots, x_{n-1}]\big)[x_n].$$

O polinômio em n indeterminadas $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ pode ser escrito como

$$f(x_1, \ldots, x_n) = \sum_{\substack{0 \leqslant j_1 \leqslant s_1 \\ \vdots \\ 0 \leqslant j_n \leqslant s_n}} a_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n},$$

onde $s_1, \ldots s_n \in \mathbb{N} \cup \{0\}$ e $a_{j_1,\ldots,j_n} \in A$.

Cada termo do tipo $a_{j_1,\ldots,j_n}x_1^{j_1}\cdots x_n^{j_n}$ é chamado de **monômio** e seu **grau** é definido como $j_1+\cdots+j_n$, sempre que $a_{j_1,\ldots,j_n}\neq 0$.

Definimos o **grau** de um polinômio não nulo em n indeterminadas com coeficientes em A como sendo o maior dos graus dos seus monômios não nulos.

Exemplo São polinômios em $\mathbb{Q}[x_1,x_2,x_3]$

$f(x_1,x_2,x_3)=x_1x_2-\frac{1}{4}x_1x_3+x_2^2-x_1^2$,

$g(x_1,x_2,x_3)=\frac{1}{3}+x_1-2x_3+x_1x_2-\frac{2}{5}x_1^2+3x_1x_2x_3^2-2x_2^4x_3+x_3^5$ e

$h(x_1,x_2,x_3)=2+x_1x_3-\frac{3}{4}x_1x_2x_3+4x_2^3-3x_1x_3x_2^3+x_2^5+\frac{1}{2}x_2^3x_3^3$.

Temos que

$$\mathrm{grau}(f(x_1,x_2,x_3))=2,\mathrm{grau}(g(x_1,x_2,x_3))=5 \text{ e } \mathrm{grau}(h(x_1,x_2,x_3))=6.$$

Um polinômio não nulo é chamado **homogêneo** de grau m se todos os seus monômios não nulos têm grau m.

Em um polinômio não nulo em n indeterminadas, a soma dos seus monômios não nulos de grau m é um polinômio homogêneo, chamado de **componente homogênea** de grau m. Todo polinômio não nulo é a soma das suas componentes homogêneas. No exemplo anterior, $f(x_1, x_2, x_3)$ é um polinômio homogêneo de grau 2 e as componentes homogêneas de $h(x_1, x_2, x_3)$ são:

componente homogênea de grau 0: 2;

componente homogênea de grau 2: x_1x_3;

componente homogênea de grau 3: $-\frac{3}{4}x_1x_2x_3 + 4x_2^3$;

componente homogênea de grau 5: $-3x_1x_3x_2^3 + x_2^5$;

componente homogênea de grau 6: $\frac{1}{2}x_2^3x_3^3$.

Se A for um domínio de integridade, sabemos que $A[x_1]$ é um domíno de integridade. Logo, por um argumento de indução, segue-se que $A[x_1, \ldots, x_n]$ é um domínio de integridade.

FIM DA AULA 3