Designemos por $\boldsymbol{x}$ (a que chamaremos a *indeterminada* $\boldsymbol{x}$) o polinómio

$$(0, 1, 0, 0, \ldots).$$

É evidente que $\boldsymbol{x}^2 = (0, 0, 1, 0, \ldots)$, $\boldsymbol{x}^3 = (0, 0, 0, 1, 0, \ldots)$, etc. Alargamos esta observação ao caso $n = 0$, convencionando $\boldsymbol{x}^0 = (1, 0, 0, \ldots) = \mathbf{1}$.

Mais geralmente, se $\boldsymbol{p} = (p_0, p_1, \ldots, p_n, 0, 0, \ldots)$ é um polinómio arbitrário de grau n, o produto $\boldsymbol{px}$ é o polinómio de grau $n+1$ que se obtém de $\boldsymbol{p}$ por translação de todos os seus coeficientes para a direita, ou seja

$$\boldsymbol{px} = (0, p_0, p_1, \ldots, p_n, 0, 0, \ldots),$$

porque

$$(\boldsymbol{px})_0 = p_0 x_0 = 0,$$
$$(\boldsymbol{px})_{i+1} = \sum_{j=0}^{i+1} p_j x_{i+1-j} = p_i.$$

Então, identificando (como na aula anterior) cada polinómio constante $\boldsymbol{a}$ pelo correspondente elemento a de A, podemos finalmente obter a forma a que estávamos habituados para representar um polinómio:

$$\begin{aligned}
\boldsymbol{p} &= (p_0, p_1, \ldots, p_n, 0, 0, \ldots) \\
&= (p_0, 0, 0, \ldots) + (0, p_1, 0, 0, \ldots) + (0, 0, p_2, 0, 0, \ldots) + \cdots + (0, \ldots, 0, p_n, 0, 0, \ldots) \\
&= p_0 + p_1\boldsymbol{x} + p_2\boldsymbol{x}^2 + \cdots + p_n\boldsymbol{x}^n \\
&= \sum_{i=0}^{n} p_i \boldsymbol{x}^i.
\end{aligned}$$

A soma à direita é a *forma canónica* do polinómio $\boldsymbol{p}$. Como é habitual, um coeficiente é omitido se for igual a 1.

Temos assim duas formas perfeitamente equivalentes de representar os elementos de $A[x]$: como sucessões

$$\boldsymbol{p} = (p_0, p_1, \ldots, p_n, 0, 0, \ldots)$$

ou como somas formais

$$\boldsymbol{p} = p_0 + p_1\boldsymbol{x} + p_2\boldsymbol{x}^2 + \cdots + p_n\boldsymbol{x}^n = \sum_{i=0}^{n} p_i \boldsymbol{x}^i. \qquad (*)$$

Chama-se a $(*)$ a *forma canónica* do polinómio $\boldsymbol{p}$.

[Confirme: em termos da forma canónica, as operações $+$ e $\star$ do anel $A[x]$ correspondem exactamente às operações de polinómios a que estávamos habituados]

Portanto, para somar e multiplicar estes polinómios, procedemos exactamente como estamos habituados com os polinómios com coeficientes reais.

Exemplo: Em $\mathbb{Z}_4[x]$, para $\boldsymbol{p} = 1 + \boldsymbol{x} + 2\boldsymbol{x}^2$ e $\boldsymbol{q} = 1 + 2\boldsymbol{x}^2$, temos:

$$\begin{aligned} \boldsymbol{p} + \boldsymbol{q} &= (1 + \boldsymbol{x} + 2\boldsymbol{x}^2) + (1 + 2\boldsymbol{x}^2) \\ &= (1 + 1) + (1 + 0)\boldsymbol{x} + (2 + 2)\boldsymbol{x}^2 \\ &= 2 + \boldsymbol{x}, \end{aligned}$$

$$\begin{aligned} \boldsymbol{pq} &= (1 + \boldsymbol{x} + 2\boldsymbol{x}^2)(1 + 2\boldsymbol{x}^2) \\ &= (1 + \boldsymbol{x} + 2\boldsymbol{x}^2)1 + (1 + \boldsymbol{x} + 2\boldsymbol{x}^2)2\boldsymbol{x}^2 \\ &= (1 + \boldsymbol{x} + 2\boldsymbol{x}^2) + (2\boldsymbol{x}^2 + 2\boldsymbol{x}^3 + 0\boldsymbol{x}^4) \\ &= 1 + \boldsymbol{x} + 2\boldsymbol{x}^3. \end{aligned}$$

GRAU

Se $\boldsymbol{p} \neq 0$ é um polinómio, o *grau* de $\boldsymbol{p}$ é o inteiro $gr(\boldsymbol{p})$ definido por

$$gr(\boldsymbol{p}) = \max\{n \in \mathbb{N}_0 \mid p_n \neq 0\}.$$

Se $\boldsymbol{p} = 0$, convencionamos que $gr(\boldsymbol{p}) = -\infty$.

Um polinómio $\boldsymbol{p}$ de grau $n \geq 0$ diz-se *mónico* se o coeficiente p_n do termo de maior grau for igual a 1.

Assim, os polinómios constantes têm grau ≤ 0. O exemplo acima de produto de polinómios em $\mathbb{Z}_4[x]$ mostra que, por causa da possível existência de divisores de zero, nem sempre o grau do produto de dois polinómios é a soma dos graus dos polinómios factores. O próximo resultado esclarece completamente as propriedades do grau relativamente à soma e ao produto de polinómios. Para evitar frequentes excepções envolvendo o polinómio nulo, convencionamos que $gr(\boldsymbol{p}) + gr(\boldsymbol{q}) = -\infty$ sempre que $\boldsymbol{p} = 0$ ou $\boldsymbol{q} = 0$.

Proposição. *Sejam* $\boldsymbol{p}, \boldsymbol{q} \in A[x]$. *Então:*

(a) $gr(\boldsymbol{p}+\boldsymbol{q}) \leq \max\{gr(\boldsymbol{p}), gr(\boldsymbol{q})\}$.

(b) $gr(\boldsymbol{pq}) \leq gr(\boldsymbol{p}) + gr(\boldsymbol{q})$.

(c) *Se A é um domínio de integridade,* $gr(\boldsymbol{pq}) = gr(\boldsymbol{p}) + gr(\boldsymbol{q})$.

Demonstração. A prova de (a) é muito simples e deixa-se como exercício. Quanto a (b) e (c) basta observar o seguinte: se $\boldsymbol{p}$ é de grau n e $\boldsymbol{q}$ é de grau m, então $\boldsymbol{pq} = p_0q_0 + (p_0q_1 + p_1q_0)\boldsymbol{x} + \cdots + p_nq_m\boldsymbol{x}^{n+m}$, pelo que $gr(\boldsymbol{pq}) \leq n+m = gr(\boldsymbol{p}) + gr(\boldsymbol{q})$; não existindo divisores de zero em A, tem-se necessariamente $p_nq_m \neq 0$, donde, neste caso, $gr(\boldsymbol{pq}) = n + m = gr(\boldsymbol{p}) + gr(\boldsymbol{q})$. ∎

Quais são as unidades de $A[x]$? Se A possui divisores de zero, $A[x]$ contém polinómios invertíveis de grau maior que zero — por exemplo, em $\mathbb{Z}_4[x]$,

$$(1 + 2\boldsymbol{x})(1 + 2\boldsymbol{x}) = 1;$$

no entanto, se A é um domínio de integridade, as unidades de $A[x]$ são precisamente os polinómios de grau zero, $\boldsymbol{p} = a$, onde a é uma unidade de A; então, se A é um corpo, as unidades de $A[x]$ são os polinómios de grau zero.

`[Verifique: se` A `é um domínio de integridade, as unidades de` $A[x]$ `coincidem com as unidades de` A`]`

Vamos agora estudar em pormenor o anel dos polinómios $A[x]$. Na base deste estudo está o algoritmo usual da divisão de polinómios de coeficientes reais. Será que podemos continuar a aplicá-lo num anel A arbitrário? Daqui em diante passamos a adoptar a seguinte convenção: o polinómio $\boldsymbol{p}$ é representado pelo símbolo $p(\boldsymbol{x})$, e o valor do polinómio $\boldsymbol{p}$ no ponto a é representado por $p(a)$. Continuamos a supor que A é um anel comutativo unitário.

Seja $A = \mathbb{Z}_6$. A divisão de $p(\boldsymbol{x}) = \boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 4$ por $d(\boldsymbol{x}) = \boldsymbol{x}^2 + 2\boldsymbol{x} + 2$ é possível, resultando no quociente $q(\boldsymbol{x}) = \boldsymbol{x}^2 + 1$, com resto $r(\boldsymbol{x}) = 5\boldsymbol{x} + 2$:

$$\begin{array}{rl|l}
\boldsymbol{x}^4 + 2\boldsymbol{x}^3 + 3\boldsymbol{x}^2 + \boldsymbol{x} + 4 & & \boldsymbol{x}^2 + 2\boldsymbol{x} + 2 \\
\cline{3-3}
-\boldsymbol{x}^4 - 2\boldsymbol{x}^3 - 2\boldsymbol{x}^2 & & \boldsymbol{x}^2 + 1 \\
\cline{1-1}
\boldsymbol{x}^2 + \boldsymbol{x} + 4 & & \\
-\boldsymbol{x}^2 - 2\boldsymbol{x} - 2 & & \\
\cline{1-1}
5\boldsymbol{x} + 2 & &
\end{array}$$

É claro que se o coeficiente d_2 de $d(\boldsymbol{x})$ fosse 2 a divisão já não seria possível: não existe nenhum elemento q_2 em $\mathbb{Z}_6$ tal que $2q_2 = 1$ para podermos prosseguir com o algoritmo! (Tudo porque 2, sendo um divisor de zero, não é invertível.) Quando o polinómio divisor é mónico ou A é um domínio de integridade, a divisão é sempre possível. Mais geralmente:

Teorema. [Algoritmo de Divisão]
Sejam $p(\boldsymbol{x})$ e $d(\boldsymbol{x}) \neq 0$ elementos de $A[x]$, de graus n e m, respectivamente. Se d_m é uma unidade de A então existem polinómios únicos $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$, com $gr(r(\boldsymbol{x})) < gr(d(\boldsymbol{x}))$, tais que $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$.

Demonstração.
Existência: O caso $n < m$ é evidente: podemos tomar $q(\boldsymbol{x}) = 0$ e $r(\boldsymbol{x}) = p(\boldsymbol{x})$.

Suponhamos então $n \geq m$. Demonstramos a existência de $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ por indução sobre n:

- Se $n = 0$ então $m = 0$. Portanto $d(\boldsymbol{x}) = d_0$ e d_0 é invertível pelo que bastará tomar $q(\boldsymbol{x}) = d_0^{-1}p(\boldsymbol{x})$ e $r(\boldsymbol{x}) = 0$.

- Vamos agora supor que o resultado é verdadeiro para qualquer polinómio de grau inferior a n. Precisamos de provar que ele também é válido para polinómios de grau n. Seja então $p(\boldsymbol{x}) = p_n\boldsymbol{x}^n + p_{n-1}\boldsymbol{x}^{n-1} + \cdots + p_1\boldsymbol{x} + p_0$, onde $p_n \neq 0$ e comecemos a fazer a divisão de $p(\boldsymbol{x})$ por $d(\boldsymbol{x})$:

$$\begin{array}{l|l} p_n\boldsymbol{x}^n + p_{n-1}\boldsymbol{x}^{n-1} + \cdots + p_1\boldsymbol{x} + p_0 & d_m\boldsymbol{x}^m + d_{m-1}\boldsymbol{x}^{m-1} + \cdots + d_1\boldsymbol{x} + d_0 \\ -p_n\boldsymbol{x}^n - p_n d_m^{-1} d_{m-1}\boldsymbol{x}^{n-1} - \cdots & \\ \hline \underbrace{(p_{n-1} - p_n d_m^{-1} d_{m-1})\boldsymbol{x}^{n-1} + \cdots}_{\tilde{p}(\boldsymbol{x})} & p_n d_m^{-1}\boldsymbol{x}^{n-m} \end{array}$$

  Considerando agora o polinómio $\tilde{p}(\boldsymbol{x}) = p(\boldsymbol{x}) - p_n d_m^{-1}\boldsymbol{x}^{n-m}d(\boldsymbol{x})$, é claro que $gr(\tilde{p}(\boldsymbol{x})) < n$, logo, pela hipótese de indução, existem polinómios $\tilde{q}(\boldsymbol{x})$ e $\tilde{r}(\boldsymbol{x})$ satisfazendo $\tilde{p}(\boldsymbol{x}) = \tilde{q}(\boldsymbol{x})d(\boldsymbol{x}) + \tilde{r}(\boldsymbol{x})$, onde $gr(\tilde{r}(\boldsymbol{x})) < gr(d(\boldsymbol{x}))$. Então

$$p(\boldsymbol{x}) = p_n d_m^{-1} x^{n-m} d(\boldsymbol{x}) + \tilde{p}(\boldsymbol{x}) = (\underbrace{p_n d_m^{-1} x^{n-m} + \tilde{q}(\boldsymbol{x})}_{q(\boldsymbol{x})})d(\boldsymbol{x}) + \underbrace{\tilde{r}(\boldsymbol{x})}_{r(\boldsymbol{x})}.$$

Unicidade: Se $p(\boldsymbol{x}) = q_1(\boldsymbol{x})d(\boldsymbol{x}) + r_1(\boldsymbol{x}) = p(\boldsymbol{x}) = q_2(\boldsymbol{x})d(\boldsymbol{x}) + r_2(\boldsymbol{x})$, então $(q_1(\boldsymbol{x}) - q_2(\boldsymbol{x}))d(\boldsymbol{x}) = r_2(\boldsymbol{x}) - r_1(\boldsymbol{x})$. Se $q_2(\boldsymbol{x})$ é diferente de $q_1(\boldsymbol{x})$ obtém-se uma

contradição analisando os graus dos polinómios: por um lado,

$$gr(r_2(\boldsymbol{x}) - r_1(\boldsymbol{x})) \leq \max\{gr(r_1(\boldsymbol{x})), gr(r_2(\boldsymbol{x}))\} < gr(d(\boldsymbol{x})),$$

mas, por outro lado,

$$\begin{aligned} gr(r_2(\boldsymbol{x}) - r_1(\boldsymbol{x})) &= gr((q_1(\boldsymbol{x}) - q_2(\boldsymbol{x}))d(\boldsymbol{x})) \\ &= gr(q_1(\boldsymbol{x}) - q_2(\boldsymbol{x})) + gr(d(\boldsymbol{x})) \quad \text{(pois } d_m \text{ não é div. de zero)} \\ &\geq gr(d(\boldsymbol{x})). \end{aligned}$$

Assim $q_1(\boldsymbol{x}) = q_2(\boldsymbol{x})$, o que implica imediatamente $r_1(\boldsymbol{x}) = r_2(\boldsymbol{x})$. ∎

Tal como no caso dos inteiros, os polinómios $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ dizem-se respectivamente *quociente* e *resto* da divisão de $p(\boldsymbol{x})$ por $d(\boldsymbol{x})$. O caso em que $r(\boldsymbol{x}) = 0$ corresponde, claro está, ao caso em que $d(\boldsymbol{x})$ é *divisor* (ou *factor*) de $p(\boldsymbol{x})$. Neste caso escrevemos $d(\boldsymbol{x})|p(\boldsymbol{x})$.