Seja $q(\boldsymbol{x})$ um factor de $p(\boldsymbol{x})$. Se $p(\boldsymbol{x}) = a(\boldsymbol{x})q(\boldsymbol{x})$ onde nem $a(\boldsymbol{x})$ nem $q(\boldsymbol{x})$ são invertíveis, $q(\boldsymbol{x})$ diz-se um *factor próprio* de $p(\boldsymbol{x})$.

POLINÓMIO IRREDUTÍVEL

Um polinómio $p(\boldsymbol{x})$ de $A[x]$ diz-se *irredutível* em $A[x]$ quando não tem factores próprios (em $A[x]$) e não é invertível (em $A[x]$). Caso contrário, $p(\boldsymbol{x})$ diz-se *redutível*.

Portanto, $p(\boldsymbol{x})$ é irredutível quando não é invertível e $p(\boldsymbol{x}) = q_1(\boldsymbol{x})q_2(\boldsymbol{x})$ implica que um dos polinómios $q_1(\boldsymbol{x})$ ou $q_2(\boldsymbol{x})$ seja invertível. Assim, quando C é um corpo, um polinómio $p(\boldsymbol{x}) \neq 0$ em $C[x]$ é irredutível se e só se $gr(p(\boldsymbol{x}) \geq 1$ e $p(\boldsymbol{x}) = q_1(\boldsymbol{x})q_2(\boldsymbol{x})$ implica $gr(q_1(\boldsymbol{x})) = 0$ ou $gr(q_2(\boldsymbol{x})) = 0$. Em particular, todo o polinómio de grau 1 é irredutível.

Exemplos: (1) Para qualquer anel A, $p(\boldsymbol{x}) = \boldsymbol{x}$ é irredutível.

(2) Se $A = \mathbb{Z}$, $p(\boldsymbol{x}) = 2\boldsymbol{x} - 3$ é irredutível mas $q(\boldsymbol{x}) = 2\boldsymbol{x} + 6$ é redutível (porque $2\boldsymbol{x} + 6 = 2(\boldsymbol{x} + 3)$ e 2 e $\boldsymbol{x} + 3$ não são invertíveis em $\mathbb{Z}[x]$).

(3) A redutibilidade ou irredutibilidade de um dado polinómio depende fortemente do anel em consideração. Por exemplo, o polinómio $\boldsymbol{x}^2 - 2 \in \mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$, mas $\boldsymbol{x}^2 - 2 = (\boldsymbol{x} + \sqrt{2})(\boldsymbol{x} - \sqrt{2})$ é redutível em $\mathbb{R}[x] \supset \mathbb{Q}[x]$; por outro lado, $\boldsymbol{x}^2 + 1$ é irredutível em $\mathbb{Q}[x]$ ou $\mathbb{R}[x]$ mas é redutível em $\mathbb{C}[x] \supset \mathbb{R}[x] \supset \mathbb{Q}[x]$.

(4) Seja D um domínio de integridade. Um polinómio redutível em $D[x]$ não tem necessariamente raízes. É o caso de $\boldsymbol{x}^4 + 2\boldsymbol{x}^2 + 1$, que é redutível em $\mathbb{Z}[x]$, porque $\boldsymbol{x}^4 + 2\boldsymbol{x}^2 + 1 = (\boldsymbol{x}^2 + 1)^2$, e que não tem raízes em $\mathbb{Z}$.

(5) Se $gr(p(\boldsymbol{x})) \geq 2$ e $p(\boldsymbol{x})$ tem pelo menos uma raiz em D, então, pelo Teorema do Resto, $p(\boldsymbol{x})$ é redutível em $D[x]$.

(6) Se $p(\boldsymbol{x})$ é mónico e tem grau 2 ou 3, então $p(\boldsymbol{x})$ é redutível em $D[x]$ se e só se tem pelo menos uma raiz em D.

`[Porquê?]`

(7) Em $\mathbb{R}[x]$ os únicos polinómios irredutíveis são os polinómios de grau 1 e os polinómios $p(\boldsymbol{x}) = a\boldsymbol{x}^2 + b\boldsymbol{x} + c$ de grau 2 com *discriminante* $\Delta = b^2 - 4ac$ negativo.

[É consequência do seguinte facto: se $c \in \mathbb{C}$ é raiz de $p(\boldsymbol{x}) \in C[x]$, o complexo conjugado de c é também raiz de $p(\boldsymbol{x})$]

É possível em certos casos descrever todos os polinómios irredutíveis em $D[x]$, como em $\mathbb{R}[x]$. Noutros casos, este problema torna-se muito complexo e é praticamente impossível fazê-lo, conhecendo-se somente resultados parciais (alguns critérios que permitem em alguns casos concluir da redutibilidade ou irredutibilidade de um dado polinómio). É o caso de $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$.

[Alguns desses critérios serão dados na aula prática]

Proposição 1. *Sejam $I = (p(\boldsymbol{x}))$ e $J = (q(\boldsymbol{x}))$ ideais de $C[x]$. Então:*

(1) *$I \subseteq J$ se e só se $q(\boldsymbol{x}) \mid p(\boldsymbol{x})$.*

(2) *Se $I = J$ e $p(\boldsymbol{x})$ e $q(\boldsymbol{x})$ são mónicos ou nulos então $p(\boldsymbol{x}) = q(\boldsymbol{x})$.*

(3) *I é maximal se e só se $p(\boldsymbol{x})$ é irredutível.*

Demonstração. (1) $I \subseteq J \Leftrightarrow p(\boldsymbol{x}) \in (q(\boldsymbol{x})) \Leftrightarrow q(\boldsymbol{x}) \mid p(\boldsymbol{x})$.

(2) O caso em que um dos polinómios é nulo é óbvio. Suponhamos então que são ambos mónicos. Por (1), $I = J$ se e só se $p(\boldsymbol{x}) \mid q(\boldsymbol{x})$ e $q(\boldsymbol{x}) \mid p(\boldsymbol{x})$. Então

$$\begin{cases} q(\boldsymbol{x}) = a(\boldsymbol{x})\, p(\boldsymbol{x}) \\ p(\boldsymbol{x}) = b(\boldsymbol{x})\, q(\boldsymbol{x}) \end{cases}$$

para alguns polinómios $a(\boldsymbol{x}), b(\boldsymbol{x}) \in C[x]$. Daqui segue (como observámos já na demonstração do Teorema da aula anterior) que $p(\boldsymbol{x}) = q(\boldsymbol{x})$.

(3) Provaremos que $p(\boldsymbol{x})$ é redutível se e só se I não é maximal. Suponhamos que $p(\boldsymbol{x})$ é redutível. Então ou é invertível ou tem um factor próprio. No primeiro caso tem-se $1 = (p(\boldsymbol{x}))^{-1} p(\boldsymbol{x}) \in I$, donde $I = C[x]$ não é maximal. No segundo caso tem-se $p(\boldsymbol{x}) = q_1(\boldsymbol{x}) q_2(\boldsymbol{x})$ com $gr(q_1(\boldsymbol{x})) \geq 1$ e $gr(q_2(\boldsymbol{x})) \geq 1$. Então $1 \leq gr(q_1(\boldsymbol{x})) < gr(p(\boldsymbol{x}))$, pelo que

$$(p(\boldsymbol{x})) \subset (q_1(\boldsymbol{x})) \subset C[x],$$

o que mostra que, também neste caso, I não é maximal.

Reciprocamente, suponhamos que I não é maximal, ou seja, que existe um ideal $J = (q(\boldsymbol{x}))$ (recorde que $C[x]$ é um domínio de ideais principais) tal que $I \subset J \subset C[x]$. Então $p(\boldsymbol{x}) = r(\boldsymbol{x}) q(\boldsymbol{x})$ para algum $r(\boldsymbol{x}) \in C[x]$. É claro que

$gr(r(\boldsymbol{x})) \geq 1$ (pois se $r(\boldsymbol{x})$ fosse constante, $q(\boldsymbol{x})$ pertenceria a $(p(\boldsymbol{x}))$ e teríamos $J = I$). Por outro lado, também $gr(q(\boldsymbol{x})) \geq 1$ (caso contrário, $J = C[x]$). Assim, a factorização $p(\boldsymbol{x}) = r(\boldsymbol{x})q(\boldsymbol{x})$ mostra que $p(\boldsymbol{x})$ é redutível em $C[x]$. ∎

Proposição 2. *Se um polinómio irredutível $p(\boldsymbol{x}) \in C[x]$ divide um produto $r_1(\boldsymbol{x})r_2(\boldsymbol{x}) \cdots r_m(\boldsymbol{x})$ de polinómios em $C[x]$, então pelo menos um dos factores $r_i(\boldsymbol{x})$ é divisível por $p(\boldsymbol{x})$.*

Demonstração. Consideremos o ideal principal $I = (p(\boldsymbol{x}))$. Pelo Teorema da Aula 3, $C[x]/I$ é um corpo (logo não tem divisores de zero). Mas

$$(r_1(\boldsymbol{x}) + I) \cdot (r_2(\boldsymbol{x}) + I) \cdot \cdots \cdot (r_m(\boldsymbol{x}) + I) = r_1(\boldsymbol{x})r_2(\boldsymbol{x}) \cdots r_m(\boldsymbol{x}) + I = I,$$

uma vez que, por hipótese, $r_1(\boldsymbol{x})r_2(\boldsymbol{x}) \cdots r_m(\boldsymbol{x}) \in I$. Então, necessariamente um dos factores é nulo, isto é, $r_i(\boldsymbol{x}) + I = I$ para algum $i \in \{1, 2, \ldots, m\}$. Isto significa precisamente que $r_i(\boldsymbol{x}) \in I$, ou seja, $p(\boldsymbol{x}) \mid r_i(\boldsymbol{x})$. ∎

O teorema seguinte mostra a importância dos polinómios irredutíveis no anel $C[x]$.

Teorema. [Factorização única em $C[x]$]

Todo o polinómio $r(\boldsymbol{x}) \in C[x]$ de grau positivo pode ser escrito na forma

$$r(\boldsymbol{x}) = cp_1(\boldsymbol{x})^{n_1}p_2(\boldsymbol{x})^{n_2} \cdots p_t(\boldsymbol{x})^{n_t} \qquad (*)$$

onde $c \in C$, $p_1(\boldsymbol{x}), p_2(\boldsymbol{x}), \ldots, p_t(\boldsymbol{x})$ são polimónios mónicos irredutíveis em $C[x]$, todos distintos, e $n_1, n_2, \ldots, n_t \in \mathbb{N}$.

E mais: esta factorização é única a menos da ordem pela qual se escrevem os factores.

`[Observe mais uma vez o paralelismo com` $\mathbb{Z}$`:`
`os polinómios irredutíveis correspondem aos inteiros primos;`
`este teorema corresponde ao Teorema Fundamental da Aritmética]`

Referir-nos-emos a $(*)$ como a *factorização canónica* de $p(\boldsymbol{x})$ em $C[x]$.