O facto de, no caso de A ser um corpo, o algoritmo da divisão em $A[x]$ ser sempre aplicável, tem, como em $\mathbb{Z}$, outra consequência importante:

Teorema. *Seja C um corpo. Em $C[x]$ todo o ideal é principal.*

Demonstração. Seja I um ideal de $C[x]$. Se $I = \{0\}$, então $I = (0)$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Neste caso, provaremos mais do que é exigido no enunciado do resultado, nomeadamente que existe um polinómio mónico $m(\boldsymbol{x}) \in C[x]$, único, tal que $I = (m(\boldsymbol{x}))$.

Consideremos então o conjunto

$$N = \{n \in \mathbb{N}_0 \mid \text{ existe } s(\boldsymbol{x}) \in I, gr(s(\boldsymbol{x})) = n\}.$$

É claro que, como $I \neq \{0\}$, N é não-vazio, pelo que tem um mínimo. Seja $m(\boldsymbol{x})$um polinómio em I de grau igual a esse mínimo (podemos supor que $m(\boldsymbol{x})$ é mónico; com efeito, se não fosse, isto é, se o coeficiente do termo de maior grau fosse igual a $a \neq 1$, poderíamos sempre considerar o polinómio $n(\boldsymbol{x}) = a^{-1}m(\boldsymbol{x}) \in I$).

Provemos que $I = (m(\boldsymbol{x}))$. Como $m(\boldsymbol{x}) \in I$, é óbvio que $(m(\boldsymbol{x})) \subseteq I$. Por outro lado, se $p(\boldsymbol{x}) \in I$, usando o algoritmo de divisão temos $p(\boldsymbol{x}) = q(\boldsymbol{x})m(\boldsymbol{x}) + r(\boldsymbol{x})$, onde $gr(r(\boldsymbol{x})) < gr(m(\boldsymbol{x}))$. Dado que I é um ideal, podemos concluir que $r(\boldsymbol{x}) = p(\boldsymbol{x}) - q(\boldsymbol{x})m(\boldsymbol{x}) \in I$. Mas então $r(\boldsymbol{x})$ só pode ser igual a 0 pois, com excepção do polinómio nulo, não pode haver nenhum polinómio em I de grau inferior a $gr(m(\boldsymbol{x}))$. Assim, $p(\boldsymbol{x})$ é um múltiplo de $m(\boldsymbol{x})$ pelo que pertence ao ideal $(m(\boldsymbol{x}))$.

Para provar a unicidade de $m(\boldsymbol{x})$, suponhamos $I = (n(\boldsymbol{x}))$, onde $n(\boldsymbol{x}) \in C[x]$ é mónico. Da igualdade $(m(\boldsymbol{x})) = (n(\boldsymbol{x}))$ segue

$$\begin{cases} m(\boldsymbol{x}) = p_1(\boldsymbol{x})\, n(\boldsymbol{x}) \\ n(\boldsymbol{x}) = p_2(\boldsymbol{x})\, m(\boldsymbol{x}) \end{cases} \qquad (*)$$

para alguns polinómios $p_1(\boldsymbol{x}), p_2(\boldsymbol{x})$, donde $m(\boldsymbol{x}) = p_1(\boldsymbol{x})p_2(\boldsymbol{x})m(\boldsymbol{x})$. Como $C[x]$ é um domínio de integridade, podemos cancelar $m(\boldsymbol{x}) \neq 0$ à esquerda e concluir que $p_1(\boldsymbol{x})p_2(\boldsymbol{x}) = 1$.

[Num domínio de integridade, a lei do cancelamento para o produto vale para elementos $\neq 0$: se $ba = ca$ ou $ab = ac$, com $a \neq 0$, então $b = c$ (pois $ba = ca \Leftrightarrow (b-c)a = 0 \Rightarrow b - c = 0 \Leftrightarrow b = c$)]

Então $gr(p_1(\boldsymbol{x}))+gr(p_2(\boldsymbol{x})) = 0$ e, consequentemente, $p_1(\boldsymbol{x})$ e $p_2(\boldsymbol{x})$ são polinómios constantes. Como $m(\boldsymbol{x})$ e $n(\boldsymbol{x})$ são mónicos, então de $(*)$ segue $p_1(\boldsymbol{x}) = p_2(\boldsymbol{x}) = 1$ e $n(\boldsymbol{x}) = m(\boldsymbol{x})$. ∎

[Observe mais esta analogia entre os anéis $C[x]$ e $\mathbb{Z}$:
$C[x]$ é, tal como $\mathbb{Z}$, um *domínio de ideais principais*]

Exemplos: $\mathbb{Z}[x]$ não é um domínio de ideais principais; por exemplo, o ideal $(2, \boldsymbol{x})$ não é principal.

[Verifique]

Mais geralmente, se A é um anel comutativo com identidade, a demonstração acima de que um ideal I de $A[x]$ é principal consegue fazer-se desde que o coeficiente do termo de maior grau do polinómio $m(\boldsymbol{x})$ (que agora não é necessariamente mónico) seja invertível em A. Este não é o caso do ideal $(2, \boldsymbol{x})$ em $\mathbb{Z}[x]$: qualquer polinómio $m(\boldsymbol{x}) \in (2, x)$ de grau mínimo é uma constante $\neq 1, -1$.

Corolário. *Sejam $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})$ polinómios em $C[\boldsymbol{x}]$, onde pelo menos um é não-nulo. Então existe um único polinómio mónico $d(\boldsymbol{x}) \in C[x]$ tal que:*

(1) $d(\boldsymbol{x}) \mid p_i(\boldsymbol{x})$ $(i = 1, 2, \ldots, n)$.

(2) *Se $c(\boldsymbol{x}) \in C[x]$ e $c(\boldsymbol{x}) \mid p_i(\boldsymbol{x})$ $(i = 1, 2, \ldots, n)$ então $c(\boldsymbol{x}) \mid d(\boldsymbol{x})$.*

Além disso, $d(\boldsymbol{x})$ pode ser escrito na forma

$$d(\boldsymbol{x}) = r_1(\boldsymbol{x})p_1(\boldsymbol{x}) + \cdots + r_n(\boldsymbol{x})p_n(\boldsymbol{x}) \qquad (*)$$

com $r_1(\boldsymbol{x}), \ldots, r_n(\boldsymbol{x}) \in C[x]$.

Demonstração. Consideremos o ideal $(p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x}))$, que é não-nulo. Pela demonstração do Teorema, existe um polinómio mónico $d(\boldsymbol{x})$, único, tal que

$$(p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})) = (d(\boldsymbol{x})).$$

Como cada $p_i(\boldsymbol{x}) \in (d(\boldsymbol{x}))$, a condição (1) é óbvia, enquanto $(*)$ é consequência imediata do facto de $d(\boldsymbol{x})$ pertencer a $(p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x}))$. Quanto a (2), é consequência de $(*)$. ∎

Por outras palavras, $d(\boldsymbol{x})$ é um *divisor comum* de $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})$, e é *múltiplo* de qualquer outro divisor comum destes n polinómios.

MÁXIMO DIVISOR COMUM

O polinómio $d(\boldsymbol{x})$ diz-se o *máximo divisor comum* de $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})$ e escreve-se $d(\boldsymbol{x}) = \text{mdc}\,(p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x}))$.

Analogamente, também existe um único polinómio mónico $m(\boldsymbol{x})$ tal que

$$(p_1(\boldsymbol{x})) \cap \cdots \cap (p_n(\boldsymbol{x})) = m(\boldsymbol{x}).$$

Neste caso:

(1) $p_i(\boldsymbol{x}) \mid m(\boldsymbol{x})$ $(i = 1, 2, \ldots, n)$.

(2) Se $c(\boldsymbol{x}) \in C[x]$ e $p_i(\boldsymbol{x}) \mid c(\boldsymbol{x})$ $(i = 1, 2, \ldots, n)$ então $m(\boldsymbol{x}) \mid c(\boldsymbol{x})$.

Portanto, $m(\boldsymbol{x})$ é *múltiplo comum* de $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})$, e é *divisor* de qualquer outro polinómio que seja múltiplo comum destes n polinómios.

MÍNIMO MÚLTIPLO COMUM

O polinómio $m(\boldsymbol{x})$ diz-se o *mínimo múltiplo comum* de $p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x})$ e escreve-se $m(\boldsymbol{x}) = \text{mmc}\,(p_1(\boldsymbol{x}), \ldots, p_n(\boldsymbol{x}))$.

Uma vez que, tal como nos inteiros,

$$p_1(\boldsymbol{x}) = q(\boldsymbol{x})p_2(\boldsymbol{x}) + r(\boldsymbol{x}) \Rightarrow (p_1(\boldsymbol{x}), p_2(\boldsymbol{x})) = (p_2(\boldsymbol{x}), r(\boldsymbol{x})),$$

o algoritmo de Euclides para o cálculo do máximo divisor comum mantém a sua validade em $C[x]$.

ALGORITMO DE EUCLIDES

Sejam $p_1(\boldsymbol{x}), p_2(\boldsymbol{x}) \in C[x]$, com $p_2(\boldsymbol{x}) \neq 0$.
Se $p_2(\boldsymbol{x}) \mid p_1(\boldsymbol{x})$, então $\text{mdc}\,(p_1(\boldsymbol{x}), p_2(\boldsymbol{x})) = p_1(\boldsymbol{x})$.
Se $p_2(\boldsymbol{x}) \nmid p_1(\boldsymbol{x})$, usamos o algoritmo da divisão repetidamente do seguinte modo:

$$\begin{array}{ll}
p_1(\boldsymbol{x}) = q_1(\boldsymbol{x})p_2(\boldsymbol{x}) + r_1(\boldsymbol{x}) & 0 \leq gr(r_1(\boldsymbol{x})) < gr(p_2(\boldsymbol{x})) \\
p_2(\boldsymbol{x}) = q_2(\boldsymbol{x})r_1(\boldsymbol{x}) + r_2(\boldsymbol{x}) & 0 \leq gr(r_2(\boldsymbol{x})) < gr(r_1(\boldsymbol{x})) \\
r_1(\boldsymbol{x}) = q_3(\boldsymbol{x})r_2(\boldsymbol{x}) + r_3(\boldsymbol{x}) & 0 \leq gr(r_3(\boldsymbol{x})) < gr(r_2(\boldsymbol{x})) \\
\vdots & \vdots \\
r_{t-2}(\boldsymbol{x}) = q_t(\boldsymbol{x})r_{t-1}(\boldsymbol{x}) + r_t(\boldsymbol{x}) & 0 \leq gr(r_t(\boldsymbol{x})) < gr(r_{t-1}(\boldsymbol{x})) \\
r_{t-1}(\boldsymbol{x}) = q_{t+1}(\boldsymbol{x})r_t(\boldsymbol{x}). &
\end{array}$$

Como $gr(p_2(\boldsymbol{x}))$ é finito, o processo terá que parar ao cabo de um número finito de passos. Seja a o coeficiente de maior grau do último resto não-nulo $r_t(\boldsymbol{x})$. Então $\text{mdc}\,(p_1(\boldsymbol{x}), p_2(\boldsymbol{x})) = a^{-1}r_t(\boldsymbol{x})$.

Exemplo: O algoritmo de Euclides aplicado aos polinómios

$$p_1(\boldsymbol{x}) = 2\boldsymbol{x}^6 + \boldsymbol{x}^3 + \boldsymbol{x}^2 + 2 \in \mathbb{F}_3[x], \qquad p_2(\boldsymbol{x}) = \boldsymbol{x}^4 + \boldsymbol{x}^2 + 2\boldsymbol{x} \in \mathbb{F}_3[x]$$

dá:

$$\begin{aligned} 2\boldsymbol{x}^6 + \boldsymbol{x}^3 + \boldsymbol{x}^2 + 2 &= (2\boldsymbol{x}^2 + 1)(\boldsymbol{x}^4 + \boldsymbol{x}^2 + 2\boldsymbol{x}) + \boldsymbol{x} + 2 \\ \boldsymbol{x}^4 + \boldsymbol{x}^2 + 2\boldsymbol{x} &= (\boldsymbol{x}^3 + \boldsymbol{x}^2 + 2\boldsymbol{x} + 1)(\boldsymbol{x} + 2) + 1 \\ \boldsymbol{x} + 2 &= (\boldsymbol{x} + 2)1. \end{aligned}$$

Portanto $\operatorname{mdc}(p_1(\boldsymbol{x}), p_2(\boldsymbol{x})) = 1$ e $p_1(\boldsymbol{x})$ e $p_2(\boldsymbol{x})$ são *primos entre si.*

Além disso, a partir da penúltima divisão, obtemos sucessivamente:

$$\begin{aligned} 1 &= (\boldsymbol{x}^4 + \boldsymbol{x}^2 + 2\boldsymbol{x}) - (\boldsymbol{x}^3 + \boldsymbol{x}^2 + 2\boldsymbol{x} + 1)(\boldsymbol{x} + 2) \\ &= p_2(\boldsymbol{x}) - (\boldsymbol{x}^3 + \boldsymbol{x}^2 + 2\boldsymbol{x} + 1)(p_1(\boldsymbol{x}) - (2\boldsymbol{x}^2 + 1)p_2(\boldsymbol{x})) \\ &= -(\boldsymbol{x}^3 + \boldsymbol{x}^2 + 2\boldsymbol{x} + 1)p_1(\boldsymbol{x}) + (1 + 2\boldsymbol{x}^2 + 1)p_2(\boldsymbol{x}) \\ &= (2\boldsymbol{x}^3 + 2\boldsymbol{x}^2 + \boldsymbol{x} + 2)p_1(\boldsymbol{x}) + (2\boldsymbol{x}^2 + 2)p_2(\boldsymbol{x}). \end{aligned}$$