O argumento de prova da existência, no teorema anterior (Algoritmo de Divisão), pode ser facilmente transformado num algoritmo de cálculo do quociente e do resto (onde, dado um polinómio $p(\boldsymbol{x}) = p_n\boldsymbol{x}^n + p_{n-1}\boldsymbol{x}^{n-1} + \cdots + p_0$, de grau n, designamos por $p^{\text{top}}(\boldsymbol{x}) = p_n\boldsymbol{x}^n$ o termo de grau máximo):

ALGORITMO DA DIVISÃO

Dados: $p(\boldsymbol{x}) = p_n\boldsymbol{x}^n + p_{n-1}\boldsymbol{x}^{n-1} + \cdots + p_0$, $d(\boldsymbol{x}) = d_m\boldsymbol{x}^m + d_{m-1}\boldsymbol{x}^{m-1} + \cdots + d_0$ tal que d_m é invertível.

Para dividir $p(\boldsymbol{x})$ por $d(\boldsymbol{x})$ procede-se por iteração, do seguinte modo:

Começando com $q_0(\boldsymbol{x}) = 0$ e $r_0(\boldsymbol{x}) = p(\boldsymbol{x})$, faz-se em cada passo

$$q_i(\boldsymbol{x}) = q_{i-1}(\boldsymbol{x}) + d_m^{-1}\frac{r_{i-1}^{\text{top}}(\boldsymbol{x})}{\boldsymbol{x}^m}, \quad r_i(\boldsymbol{x}) = r_{i-1}(\boldsymbol{x}) - d_m^{-1}\frac{r_{i-1}^{\text{top}}(\boldsymbol{x})}{\boldsymbol{x}^m}d(\boldsymbol{x}) :$$

$$\begin{array}{rl|l}
 & p_n\boldsymbol{x}^n + p_{n-1}\boldsymbol{x}^{n-1} + \cdots + p_1\boldsymbol{x} + p_0 & d_m\boldsymbol{x}^m + d_{m-1}\boldsymbol{x}^{m-1} + \cdots + d_1\boldsymbol{x} + d_0 \\
 & -p_n\boldsymbol{x}^n - d_m^{-1}p_nd_{m-1}\boldsymbol{x}^{n-1} - \cdots & \underbrace{d_m^{-1}p_n\boldsymbol{x}^{n-m}}_{q_1(\boldsymbol{x})} + d_m^{-1}(p_{n-1} - d_m^{-1}p_nd_{m-1})x^{n-m-1} + \cdots \\
\hline
r_1(\boldsymbol{x}): & (p_{n-1} - d_m^{-1}p_nd_{m-1})\boldsymbol{x}^{n-1} + \cdots & \underbrace{\qquad\qquad\qquad\qquad}_{q_2(\boldsymbol{x})} \\
 & -(p_{n-1} - d_m^{-1}p_nd_{m-1})\boldsymbol{x}^{n-1} + \cdots & \vdots \\
\hline
r_2(\boldsymbol{x}): & \cdots & \underbrace{\qquad\qquad\qquad\qquad}_{q_i(\boldsymbol{x})} \\
\vdots & \vdots & \\
r_i(\boldsymbol{x}): & \cdots &
\end{array}$$

A iteração termina quando $gr(r_i(\boldsymbol{x})) < m$.

Então faz-se $r(\boldsymbol{x}) = r_i(\boldsymbol{x})$ e $q(\boldsymbol{x}) = q_i(\boldsymbol{x})$.

`[Observe: a analogia entre o algoritmo da divisão nos anéis` $A[x]$
`e o algoritmo da divisão em` $\mathbb{Z}$`]`

O resultado seguinte é um corolário imediato do Algoritmo de Divisão:

Corolário 1. *Seja C um corpo. Para quaisquer $p(\boldsymbol{x})$ e $d(\boldsymbol{x}) \neq 0$ em $C[x]$, existem polinómios únicos $q(\boldsymbol{x})$ e $r(\boldsymbol{x})$ tais que $p(\boldsymbol{x}) = q(\boldsymbol{x})d(\boldsymbol{x}) + r(\boldsymbol{x})$, com $gr(r(\boldsymbol{x})) < gr(d(\boldsymbol{x}))$.* ∎

Observámos na Aula 5 que não é de todo conveniente definir os polinómios com coeficientes em A como *funções* de determinado tipo, com domínio e valores em A. No entanto, nada nos impede de definir funções de A em A a partir de polinómios em $A[x]$.

FUNÇÃO POLINOMIAL

Se $p(\boldsymbol{x}) = \sum_{i=0}^{n} p_i \boldsymbol{x}^i$ é um polinómio em $A[x]$, a função $p : A \to A$ definida por $p(a) = \sum_{i=0}^{n} p_i a^i$ diz-se *função polinomial associada a* $p(\boldsymbol{x})$.

Exemplo: Seja $A = \mathbb{Z}_2$ e $p(\boldsymbol{x}) = 1 + \boldsymbol{x} + \boldsymbol{x}^2$. A função polinomial associada ao polinómio $p(\boldsymbol{x})$ é $p : \mathbb{Z}_2 \to \mathbb{Z}_2$ dada por $p(a) = 1 + a + a^2$, para qualquer $a \in \mathbb{Z}_2$. Neste caso, temos $p(0) = p(1) = 1$, e portanto p é uma função constante, apesar de $p(\boldsymbol{x})$ não ser um polinómio constante. Em particular, se $q(\boldsymbol{x}) = 1$, temos $p(\boldsymbol{x}) \neq q(\boldsymbol{x})$ e $p = q$.

O resultado seguinte é outro corolário do Algoritmo de Divisão.

Corolário 2. [Teorema do resto]
Se $p(\boldsymbol{x}) \in A[x]$ e $a \in A$, o resto da divisão de $p(\boldsymbol{x})$ por $(\boldsymbol{x} - a)$ é o polinómio constante $r(\boldsymbol{x}) = p(a)$. Portanto, $p(\boldsymbol{x})$ é um múltiplo de $(\boldsymbol{x} - a)$ se e só se $p(a) = 0$.

Demonstração. Como $(\boldsymbol{x} - a)$ é mónico, podemos realizar a divisão de $p(\boldsymbol{x})$ por $(\boldsymbol{x} - a)$, obtendo $p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x} - a) + r(\boldsymbol{x})$ com $gr(r(\boldsymbol{x})) < 1$ (ou seja, $r(\boldsymbol{x})$ é um polinómio constante $r(\boldsymbol{x}) = b$). Então a identidade de polinómios $p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x} - a) + b$ implica $p(a) = b$, donde $r(\boldsymbol{x}) = p(a)$. ∎

RAIZ DE UM POLINÓMIO

Um elemento $a \in A$ diz-se *raiz* de um polinómio $p(\boldsymbol{x}) = \sum_{i=0}^{n} p_i \boldsymbol{x}^i$ de $A[x]$ caso $p(a) = 0$. Portanto, $p(\boldsymbol{x})$ é um múltiplo de $(\boldsymbol{x} - a)$ se e só se a é uma raiz de $p(\boldsymbol{x})$.

Outra das consequências do Algoritmo de Divisão (ou mais directamente do Corolário 2) é o resultado clássico sobre o número máximo de raízes de um polinómio não-nulo, que é válido quando A é um domínio de integridade.

Proposição. *Seja D um domínio de integridade. Se $p(\boldsymbol{x}) \in D[x]$ e $gr(p(\boldsymbol{x})) = n \geq 0$ então $p(\boldsymbol{x})$ tem no máximo n raízes em D.*

Demonstração. Faremos uma demonstração por indução sobre n. O caso $n = 0$ é óbvio: $p(\boldsymbol{x})$ será um polinómio constante não-nulo pelo que não terá raízes em D.

Suponhamos agora, por hipótese de indução, que o resultado vale para qualquer polinómio de grau n. Nessas condições, seja $p(\boldsymbol{x})$ um polinómio de grau $n+1$. Se $p(\boldsymbol{x})$ não tiver raízes em D, não há nada a provar. Caso contrário, se tem uma raiz $a \in D$ então, pelo Corolário 2, $p(\boldsymbol{x}) = q(\boldsymbol{x})(\boldsymbol{x} - a)$. Como D é um domínio de integridade, $gr(q(\boldsymbol{x})) = n$. Logo, pela hipótese de indução, $q(\boldsymbol{x})$ tem no máximo n raízes. Isto implica que $p(\boldsymbol{x})$ tem no máximo $n+1$ raízes (porque se $b \neq a$ é raiz de $p(\boldsymbol{x})$ então é raiz de $q(\boldsymbol{x})$ pois $0 = p(b) = q(b)(b-a)$ implica $q(b) = 0$). ∎

Mas cuidado: no caso geral em que A não é um domínio de integridade, não há relação nenhuma entre o número de raízes e o grau do polinómio. Por exemplo, em $\mathbb{Z}_4[x]$, o polinómio $2\boldsymbol{x} + 2\boldsymbol{x}^2$ é de grau 2 mas tem 4 raízes: 0, 1, 2 e 3. Por outro lado, $1 + \boldsymbol{x}^2$ é de grau 3 mas só tem uma raiz: 3.

MULTIPLICIDADE DA RAIZ

Seja D um domínio de integridade. Se $a \in D$ é raiz de um polinómio $p(\boldsymbol{x}) \neq 0$ de $D[x]$, o maior natural m tal que $p(\boldsymbol{x})$ é múltiplo de $(x-a)^m$ diz-se a *multiplicidade* da raiz a.

[Exercício: Prove que a soma das multiplicidades das raízes de $p(\boldsymbol{x})$ é $\leq gr(p(\boldsymbol{x}))$]

Exemplos: $1 + \boldsymbol{x}^2$ é de grau 2 e não tem raízes em $\mathbb{R}$ (e, por maioria de razão, em $\mathbb{Q}$ e $\mathbb{Z}$). Em $\mathbb{C}$ tem exactamente 2 raízes, i e $-i$, de multiplicidade 1.
$1 - 2\boldsymbol{x} + 2\boldsymbol{x}^2 - 2\boldsymbol{x}^3 + \boldsymbol{x}^4$ é de grau 4 e tem exactamente uma raiz em $\mathbb{R}$, 1, de multiplicidade 2. Por outro lado, em $\mathbb{C}$ tem exactamente 3 raízes (1, i e $-i$), sendo a primeira de multiplicidade 2 e as outras de multiplicidade 1 (portanto, neste caso a soma das multiplicidades iguala o grau do polinómio).

[No próximo capítulo analisaremos melhor esta diferença entre os corpos $\mathbb{C}$ e $\mathbb{R}$: em $\mathbb{C}[x]$ a soma das multiplicidades das raízes de qualquer polinómio de grau n é exactamente n; em $\mathbb{R}[x]$ a soma das multiplicidades das raízes de qualquer polinómio de grau n não excede n, podendo ser menor que n]

[Dir-se-à que $\mathbb{C}$ é, ao contrário de $\mathbb{R}$, um corpo *algebricamente fechado*]