Algoritmo de la división

Teorema 1. *Algoritmo de la División*
Sean $f(x)$ y $g(x)$ polinomios en $K[x]$ tales que $g(x) \neq 0$. Entonces existen polinomios $q(x)$ y $r(x)$ en $K[x]$ únicos tales que

$$f(x) = g(x) \cdot q(x) + r(x) \quad \textit{donde } r(x) = 0 \ \textit{ o } \ \partial r(x) < \partial g(x)$$

Demostración. Si $g(x)\big|f(x)$ entonces $f(x) = q(x) \cdot g(x)$ para alguna $q(x) \in K[x]$ y basta tomar $r(x) = 0$. Supongamos que $g(x) \nmid f(x)$. Sea

$$\mathcal{U} = \{f(x) - g(x)s(x) \mid s(x) \in K[x]\}$$

$0 \notin \mathcal{U}$ puesto que $g(x) \nmid f(x)$. Para demostrar el teorema mostraremos que podemos encontar un polinomio $r(x)$ en $K[x]$ con las propiedades requeridas. Sea

$$\mathcal{A} = \{n \in \mathbb{N} \mid n = \partial h(x) \textit{ para algún } h(x) \in \mathcal{U}\}$$

Como $\mathcal{U} \neq \emptyset$ ($f(x) \in \mathcal{U}$) se tiene que $\mathcal{A} \neq \emptyset$. Siendo $\emptyset \neq \mathcal{A} \subseteq \mathbb{N}$, podemos considerar la mínima $n \in \mathbb{N}$ tal que $n \in \mathcal{A}$ (Axioma del buen orden).
Sean $r(x) \in \mathcal{A}$ y $q(x)$ tales que

$$r(x) = f(x) - g(x)q(x) \quad y \quad \partial r(x) = n$$

Entonces

$$f(x) = g(x)q(x) + r(x)$$

falta probar que $\partial r(x) < \partial g(x)$.
Supongamos que $\partial r(x) \geq \partial g(x)$

$$r(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

y sean a_n y b_m los coeficientes principales de $r(x)$ y $g(x)$ respectivamente. Tenemos entonces que

$$\begin{aligned}
g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0 &\Rightarrow g(x)x^{n-m} = (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)x^{n-m} \\
&\Rightarrow g(x)x^{n-m} = b_m x^n + b_{m-1}x^{n-1} + \cdots \\
&\Rightarrow b_m^{-1}g(x)x^{n-m} = b_m^{-1}(b_m x^n + b_{m-1}x^{n-1} + \cdots) \\
&\Rightarrow b_m^{-1}g(x)x^{n-m} = x^n + b_m^{-1}b_{m-1}x^{n-1} + \cdots \\
&\Rightarrow a_n b_m^{-1}g(x)x^{n-m} = a_n(x^n + b_m^{-1}b_{m-1}x^{n-1} + \cdots) \\
&\Rightarrow a_n b_m^{-1}g(x)x^{n-m} = a_n x^n + a_n b_m^{-1}b_{m-1}x^{n-1} + \cdots
\end{aligned}$$

Si hacemos

$$r_1 = r(x) - a_n b_m^{-1}g(x)x^{n-m}$$

entonces

$$r(x) = g(x)(a_n b_m^{-1}x^{n-m}) + r_1(x)$$

por lo tanto
$$f(x)=g(x)q(x)+r(x) \ \Rightarrow \ f(x)=g(x)\left(q(x)+a_nb_m^{-1}x^{n-m}\right)+r_1(x)$$
en consecuencia
$$r_1(x)=f(x)-g(x)\left(q(x)+a_nb_m^{-1}x^{n-m}\right)\in\mathcal{U}$$
Dado que $0\notin\mathcal{U}$ entonces $r_1\neq 0$ y $\partial r_1(x)<\partial r(x)$. Esto es una contradicción pues $\partial r(x)=n$ es el mínimo $n\in\mathcal{A}$, por lo que debe ser $\partial r(x)<\partial g(x)$.
Falta probar que $q(x)$ y $r(x)$ son únicos. Supongamos que $q_1(x)$ y $r_1(x)$ también satisfacen
$$f(x)=g(x)q_1(x)+r_1(x) \quad donde\ r_1(x)=0 \quad o \quad \partial r_1(x)<\partial g(x)$$
Entonces
$$\begin{pmatrix} f(x)=g(x)q(x)+r(x)\\ f(x)=g(x)q_1(x)+r_1(x)\end{pmatrix} \ \Rightarrow\ g(x)q(x)+r(x)=g(x)q_1(x)+r_1(x)$$
$$\Rightarrow\ g(x)(q(x)-q_1(x))=r_1(x)-r(x)$$
Si $r_1(x)-r(x)\neq 0$ entonces
$$\partial(r_1(x)-r(x))\leq \text{máx}\{\partial r_1(x),\partial r(x)\}<\partial g(x)$$
y por otro lado
$$\partial(r_1(x)-r(x))=\partial g(x)+\partial(q(x)-q_1(x))\geq\partial g(x)$$
Por lo tanto debe de ser $r(x)=r_1(x)$ y por ser $K[x]$ un dominio entero y $g(x)\neq 0$ se obtiene que $q_1(x)=q(x)$ □

El teorema anterior asegura la existencia de $q(x)$ y $r(x)$ con las propiedades requeridas, pero no nos dice cómo obtenerlos. Sin embargo se puede dar un algoritmo para encontrar esta pareja de polinomios como sigue:
Sean
$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0 \quad b_m\neq 0$$
Tenemos entonces
$$f(x)=g(x)\underbrace{b_m^{-1}a_nx^{n-m}}_{q_1(x)}+\underbrace{f(x)-g(x)b_m^{-1}a_nx^{n-m}}_{f_1(x)}$$
donde
$$f(x)-g(x)b_m^{-1}a_nx^{n-m}=\left(a_{n-1}-b_{m-1}b_m^{-1}a_n\right)x^{n-1}+\cdots+\left(a_{n-m}-b_0b_m^{-1}a_n\right)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_1x+a_0$$
Esto es, para
$$q_1=b_m^{-1}a_nx^{n-m}$$
$$f_1=f(x)-g(x)b_m^{-1}a_nx^{n-m}$$
se tiene
$$f(x)=g(x)q_1(x)+f_1(x) \quad donde\ \ \partial f_1(x)<\partial f(x)$$

Si $f_1(x) = 0 \quad o \quad \partial f_1(x) < \partial g(x)$ habremos terminado, siendo q_1 y f_1 los polinomios buscados. En caso contrario, es decir, si $f_1(x) \neq 0$ y $\partial f_1(x) \geq \partial g(x)$ repetimos el proceso anterior con $g(x)$ y $f_1(x)$, que es, $\partial f_1(x) = r$ y c_r es el coeficiente principal de $f_1(x)$, entonces

$$f_1(x) = g(x)\underbrace{b_m^{-1}c_r x^{r-m}}_{q_2(x)} + \underbrace{f_1(x) - g(x)b_m^{-1}c_r x^{r-m}}_{f_2(x)}$$

donde $f_2(x) = f_1(x) - g(x)b_m^{-1}c_r x^{r-m}$ es tal que

$$\partial f_2(x) < \partial f_1(x) \quad y \quad f(x) = g(x)(q_1(x) + q_2(x)) + f_2$$

Si $f_2(x) = 0 \quad o \quad \partial f_2(x) < \partial g(x)$ entonces

$$q(x) = q_1(x) + q_2(x) \quad y \quad r(x) = f_2(x)$$

satisface. En caso contrario $f_2(x) \neq 0$ y $\partial f_2(x) \geq \partial g(x)$ continuaremos de la misma forma. Así pues, mediante este proceso obtenemos una sucesión de parejas

$$(q_1(x), f_1(x)), (q_2(x), f_2(x)), ..., (q_s(x), f_s(x))$$

tales que $f_i \neq 0$ para $i = 1, ..., s$

$$f(x) = g(x)q_1(x) + f_1(x) \quad y \quad f_{i-1}(x) = g(x)q_i(x) + f_i(x) \quad para\ i = 2, ..., s$$

con

$$\partial f_s < \cdots < \partial f_1(x) < \partial f(x)$$

Debido a que ésta sucesión es decreciente, en algún momento para alguna t, debera ser

$$f_t(x) = 0 \quad o \quad \partial f_t(x) < \partial g(x)$$

y entonces los polinomios buscados serán

$$q(x) = q_1(x) + \cdots + q_t(x) \quad y \quad r(x) = f_t(x)$$

Ejemplo Sean

$$f(x) = 3x^6 + x^4 - x^3 - x^2 + x + 2 \quad y \quad g(x) = 2x^2 + 1$$

En este caso

$$b_m = 2 \Rightarrow b_m^{-1} = \frac{1}{2}, \quad a_n = 3, \quad x^{n-m} = x^{6-2} = x^4, \quad g(x)b_m^{-1}a_n x^{n-m} = (2x^2+1)\left(\frac{1}{2}\right)(3)x^4 = 3x^6 + \frac{3}{2}x^4$$

Entonces

$$\begin{aligned} f(x) &= \underbrace{(2x^2+1)}_{g(x)}\left(\underbrace{\frac{1}{2}}_{b_m^{-1}} \cdot \underbrace{3}_{a_n} \cdot \underbrace{x^4}_{x^{n-m}}\right) + \underbrace{(3x^6 + x^4 - x^3 - x^2 + x + 2)}_{f(x)} - \underbrace{\left(3x^6 + \frac{3}{2}x^4\right)}_{g(x)b_m^{-1}a_n x^{n-m}} \\ &= \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2} \cdot 3 \cdot x^4\right)}_{q_1(x)} + \underbrace{\left(-\frac{1}{2}x^4 - x^3 - x^2 + x + 2\right)}_{f_1(x)} \end{aligned}$$

Como $\partial f_1(x) \geq \partial g(x)$ continuamos el proceso, con

$$f_1(x) = -\frac{1}{2}x^4 - x^3 - x^2 + x + 2 \quad y \quad g(x) = 2x^2 + 1$$

en este caso

$$b_m = 2 \Rightarrow b_m^{-1} = \frac{1}{2}, \quad a_n = -\frac{1}{2}, \quad x^{n-m} = x^{4-2} = x^2, \quad g(x)b_m^{-1}a_n x^{n-m} = (2x^2+1)\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)x^2 = -\frac{x^4}{2} - \frac{x^2}{4}$$

Entonces

$$\begin{aligned} f_1(x) &= \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}\left(\frac{-1}{2}\right)x^2\right)}_{q_2(x)} + \underbrace{\left(-\frac{1}{2}x^4 - x^3 - x^2 + x + 2 + \frac{x^4}{2} + \frac{x^2}{4}\right)}_{f_1(x)-g(x)b_m^{-1}a_n x^{n-m}=f_2(x)} \\ &= \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}\left(\frac{-1}{2}\right)x^2\right)}_{q_2(x)} + \underbrace{\left(-x^3 - \frac{3}{4}x^2 + x + 2\right)}_{f_2(x)} \end{aligned}$$

Nuevamente, como $\partial f_2(x) \geq \partial g(x)$ continuamos el proceso con

$$f_2(x) = -x^3 - \frac{3}{4}x^2 + x + 2 \quad y \quad g(x) = 2x^2 + 1$$

en este caso

$$b_m = 2 \Rightarrow b_m^{-1} = \frac{1}{2}, \quad a_n = -1, \quad x^{n-m} = x^{3-2} = x, \quad g(x)b_m^{-1}a_n x^{n-m} = (2x^2+1)\left(\frac{1}{2}\right)(-1)\,x = -x^3 - \frac{x}{2}$$

Entonces

$$\begin{aligned} f_2(x) &= \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}(-1)x\right)}_{q_3(x)} + \underbrace{-x^3 - \frac{3}{4}x^2 + x + 2 - \left(-x^3 - \frac{x}{2}\right)}_{f_2-g(x)b_m^{-1}a_n x^{n-m}=f_3(x)} \\ &= \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}(-1)x\right)}_{q_3(x)} + \underbrace{\left(-\frac{3}{4}x^2 + \frac{3}{2}x + 2\right)}_{f_3(x)} \end{aligned}$$

Nuevamente, como $\partial f_3(x) \geq \partial g(x)$ continuamos el proceso con

$$f_3(x) = -\frac{3}{4}x^2 + \frac{3}{2}x + 2 \quad y \quad g(x) = 2x^2 + 1$$

en este caso

$$b_m = 2 \Rightarrow b_m^{-1} = \frac{1}{2}, \quad a_n = \frac{-3}{4}, \quad x^{2-2} = x^0 = 1, \quad g(x)b_m^{-1}a_n x^{n-m} = (2x^2+1)\left(-\frac{3}{4}\right)(-1)\,x = -\frac{3x^2}{4} - \frac{3}{4}$$

Entonces

$$f_3(x) = \underbrace{(2x^2+1)}_{g(x)}\underbrace{\left(\frac{1}{2}\left(\frac{-3}{4}\right)\right)}_{q_4(x)} + \underbrace{\left(\frac{3}{2}x + \frac{18}{8}\right)}_{f_4(x)}$$

Puesto que $\partial f_4(x) < \partial g(x)$, hemos terminado y por lo tanto para

$$q(x) = \frac{3}{2}x^4 - \frac{1}{4}x^2 - \frac{1}{2}x - \frac{3}{8}$$

$$r(x) = \frac{3}{2}x + \frac{19}{8}$$

se tiene

$$f(x) = g(x)q(x) + r(x)$$

donde $\partial r(x) < \partial g(x)$