Máximo común divisor

Definición 1. *Sean $f(x)$ y $g(x)$ polinomios no ambos cero en $K[x]$. Un polinomio $d(x)$ en $K[x]$ del máximo común divisor de $f(x)$ y $g(x)$ si satisface*

a) $d(x)$ es mónico,

b) $d(x) \mid f(x)$ y $d(x) \mid g(x)$,

c) Si $h(x) \mid f(x)$ y $h(x) \mid g(x)$, entonces $h(x) \mid d(x)$

Para probar la existencia en $K[x]$ del máximo común divisor para cada pareja de polinomios no ambos cero, veremos que a lo más hay un único polinomio con esta propiedad.

Proposición 1. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero. Si $d_1(x)$ y $d_2(x)$ son polinomios que satisfacen la definición de máximo común divisor, entonces $d_1(x) = d_2(x)$.*

Demostración. Por la condición (c) y como tanto $d_1(x)$ como $d_2(x)$ son divisores comunes de $f(x)$ y $g(x)$, se tiene que $d_1(x) \big| d_2(x)$ y $d_2(x) \big| d_1(x)$, y según resultados anteriores

$$d_1(x) = a d_2(x), \quad para \quad alguna \; a \; \in \; K[x]$$

Por ser $d_1(x)$ y $d_2(x)$ ambos mónicos, entonces $a = 1$ y así $d_1(x) = d_2(x)$ □

Esta última proposición nos dice entonces que en caso de existir un polinomio $d(x)$ que satisfaga la definición, éste debe ser único.
Nota: Consideremos dos poinomios $f(x)$ y $g(x)$, no ambos cero. Sea

$$\mathcal{U} = \{ \; h(x) \; \big| \; h(x) = f(x) \; a(x) + g(x) \; b(x), \; con \; a(x), \; b(x) \; \in \; K[x] \; y \; h(x) \neq 0\}$$

y sea m el mínimo de

$$\mathcal{A} = \{\partial \; h(x) \mid h(x) \in \; \mathcal{U}\}$$

cuya existencia está garantizada por el axioma del buen orden ($\emptyset \neq \mathcal{A} \subseteq \mathbb{N}$). Si $h(x) \in \mathcal{U}$ tal que $\partial h(x) = m$, entonces $a \; h(x) \in \mathcal{U}$ para toda $a \in K - \{0\}$ y $\partial(a \; h(x)) = m$. En particular, si a es el coeficiente principal de $h(x)$, entonces $a^{-1}h(x) \in \mathcal{U}$ y es mónico. Vamos a probar que este polinomio es precisamente el máximo común divisor de $f(x)$ y $g(x)$.

Definición 2. *Un polinomio $h(x)$ es combinación lineal de $f(x)$ y $g(x)$ si existen polinomios $a(x)$ y $b(x)$ tales que*

$$h(x) = f(x) \; a(x) + g(x) \; b(x)$$

Teorema 1. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero y sea $d(x)$ un polinomio de grado mínimo en el conjunto de combinaciones lineales distintas de cero de $f(x)$ y $g(x)$, el cual es mónico. Entonces $d(x)$ es el máximo común divisor de $f(x)$ y $g(x)$.*

Demostración. La existencia de $d(x)$ está justificada en la nota. Consideremos este polinomio $d(x)$ y sea

$$d(x) = f(x) \; a(x) + g(x) \; b(x)$$

y $h(x)$ un polinomio tal que

$$h(x) \mid f(x) \quad y \quad h(x) \mid g(x)$$

Según resultados anteriores

$$h(x) \big| f(x)\ a(x) + g(x)\ b(x) = d(x)$$

con lo que queda demostrado (c) de la definición de m.c.d., así que sólo falta demostrar que $d(x) \mid f(x)$ y $d(x) \mid g(x)$.
Aplicando el algoritmo de la división a $f(x)$ y $d(x)$ obtenemos

$$f(x) = d(x)\ q(x) + r(x) \quad donde \quad r(x) = 0 \quad o \quad \partial r(x) < \partial d(x)$$

Veamos que no puede ser $r(x) \neq 0$ y entonces se tendrá $d(x) \big| f(x)$.

$$\begin{aligned} f(x) &= d(x)\ q(x) + r(x) \\ &= (f(x)\ a(x) + g(x)\ b(x))\ q(x) + r(x) \end{aligned}$$

Y de aquí obtenemos

$$r(x) = f(x)(1 - a(x)q(x)) - g(x)b(x)q(x)$$

y por lo tanto $r(x)$ es una combinación lineal de $f(x)$ y $g(x)$, luego no puede ser $r(x) \neq 0$ ya que $\partial r(x) < \partial d(x)$ y $d(x)$ es un polinomio distinto de cero de grado mínimo en el conjunto de combinaciones lineales distintas de cero de $f(x)$ y $g(x)$.
Concluimos entonces que $d(x) \mid f(x)$. Análogamente se muestra que $d(x) \mid g(x)$. Por lo tanto es el máximo común divisor de $f(x)$ y $g(x)$ □

Corolario 1. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero. Entonces existe el máximo común divisor de $f(x)$ y $g(x)$ y es combinación lineal en $K[x]$ de $f(x)$ y $g(x)$.*

Denotaremos por $(f(x), g(x))$ al m.c.d. de los polinomios $f(x)$ y $g(x)$ (no ambos cero).

Teorema 2. *Si $f(x) \mid g(x)h(x)$ y $(f(x), g(x)) = 1$, entonces $f(x) \mid h(x)$*

Demostración. Tenemos que 1 es m.c.d. de $f(x)$ y $g(x)$ por lo que existen polinomios $r(x)$ y $s(x)$ en $K[x]$ tal que

$$1 = f(x)r(x) + g(x)s(x) \ \Rightarrow\ h(x) = f(x)r(x)h(x) + g(x)s(x)h(x)$$

Por otro lado

$$f(x) \mid f(x) \quad y \quad f(x) \big| g(x)h(x) \quad implica \quad f(x) \mid f(x)r(x)h(x) + g(x)s(x)h(x) = h(x)$$

por lo tanto

$$f(x) \mid h(x)$$

□

Si $(f(x), g(x)) = 1$ diremos que $f(x)$ y $g(x)$ son primos entre sí o primos relativos.
Los divisores positivos de un número entero $a \neq 0$ son menores o iguales a el y por lo tanto hay un número finito de ellos, así que para encontrarlos basta ver cuáles de estos dividen a a.
Sin embargo, en el caso de los polinomios no resulta nada sencillo puesto que por cada grado n, existen una infinidad de polinomios de ese grado (cuandoel campo es finito). Entonces ¿cómo encontrar el m.c.d. de dos polinomios?

Algoritmo de Euclides

Dados dos polinomios $f(x)$ y $g(x)$, no ambos cero, se tiene una sucesión de igualdades, cada una de ellas obtenida a partir del algoritmo de la división, como sigue

$$\begin{aligned}
f(x) &= g(x)\cdot q_0(x) + r_0(x) \quad \partial\, r_0(x) < \partial\, g(x)\\
g(x) &= r_0(x)\cdot q_1(x) + r_1(x) \quad \partial\, r_1(x) < \partial\, r_0(x)\\
r_0(x) &= r_1(x)\cdot q_2(x) + r_2(x) \quad \partial\, r_2(x) < \partial\, r_1(x)\\
&\vdots = \vdots \quad \vdots\\
r_{n-3}(x) &= r_{n-2}(x)\cdot q_{n-1}(x) + r_{n-1}(x) \quad \partial\, r_{n-1}(x) < \partial\, r_{n-2}(x)\\
r_{n-2}(x) &= r_{n-1}(x)\cdot q_n(x) + 0 \quad r_n(x) = 0
\end{aligned}$$

Debido a que los grados de los residuos van disminuyendo, es decir,

$$\partial\, r_0(x) > \partial\, r_1(x) > \partial\, r_2(x) > \cdots$$

forzosamente $r_n(x) = 0$ para algún n. Entonces $a^{-1}r_{n-1}(x)$ será el m.c.d. de $f(x)$ y $g(x)$ donde a es el coeficiente principal de $r_{n-1}(x)$.
Si $r_0 = 0$, el m.c.d. de $f(x)$ y $g(x)$ será $f(x)$ si $g(x) = 0$ o $b^{-1}g(x)$ si $g(x) \neq 0$, donde b es el coeficiente principal de $g(x)$.

Ejemplo Consideremos

$$f(x) = 2x^6 + 4x^5 - 10x^4 - 13x^3 - 2x^2 + 5x + 6 \quad y \quad g(x) = x^4 + x^3 - 5x^2 + x - 6$$

En este caso aplicando el algoritmo de la división se tiene

$$f(x) = g(x)(2x^2 + 2x - 2) + \underbrace{(-3x^3 - 2x^2 + 19x - 6)}_{r_0(x)}$$

$$g(x) = \underbrace{(-3x^3 - 2x^2 + 19x - 6)}_{r_0(x)}\left(-\frac{1}{3}x - \frac{1}{9}\right) + \underbrace{\left(\frac{10}{9}x^2 + \frac{10}{9}x - \frac{20}{3}\right)}_{r_1(x)}$$

$$\underbrace{(-3x^3 - 2x^2 + 19x - 6)}_{r_0(x)} = \underbrace{\left(\frac{10}{9}x^2 + \frac{10}{9}x - \frac{20}{3}\right)}_{r_1(x)}\left(-\frac{27}{10}x + \frac{9}{10}\right) + 0$$

El último residuo distinto de cero es $\frac{10}{9}x^2 + \frac{10}{9}x - \frac{20}{3}$ y por lo tanto el m.c.d. de $f(x)$ y $g(x)$ es

$$(f(x), g(x)) = \frac{9}{10}\left(\frac{10}{9}x^2 + \frac{10}{9}x - \frac{20}{3}\right) = x^2 + x - 6$$