Máximo común divisor de polinomios

Objetivos. Definir el concepto de máximo común divisor de dos polinomios y demostrar su existencia y su unicidad salvo múltiplos constantes no nulos. Demostrar la unicidad del máximo común divisor mónico.

Requisitos. División de polinomios, algoritmo de Euclides.

1. Divisibilidad de polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$. Se dice que f divide a g y se escribe $f \mid g$ si existe un $h \in \mathcal{P}(\mathbb{C})$ tal que $g = fh$.

2. Proposición (algunas propiedades simples de divisibilidad). Sean $f, g, u, v, d \in \mathcal{P}(\mathbb{C})$, y sea $c \in \mathbb{C} \setminus \{0\}$.

1. Si $d \mid f$ y $d \mid g$, entonces $d \mid (fu + gv)$.
2. Si $d \mid f$ y $f \mid g$, entonces $d \mid g$.
3. Si $d \mid f$, entonces $d \mid (cf)$ y $(cd) \mid f$.

3. Divisores de un polinomio. Sea $f \in \mathcal{P}(\mathbb{C})$. Denotemos por $\mathcal{D}(f)$ al conjunto de los divisores de f:

$$\mathcal{D}(f) := \{d \in \mathcal{P}(\mathbb{C}) : \quad d \mid f\}.$$

4. Observación. Sea $f \in \mathcal{P}(\mathbb{C})$. Notemos que $f \in \mathcal{D}(f)$. Más aún, si $c \in \mathbb{C} \setminus \{0\}$, entonces $cf \in \mathcal{D}(f)$. En realidad,

$$f = \frac{1}{c}(cf).$$

5. Divisores comunes de dos polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$. Denotemos por $\mathcal{D}(f, g)$ al conjunto de los divisores comunes de f y g, esto es, al conjunto de todos los polinomios h tales que $h \mid f$ y $h \mid g$:

$$\mathcal{D}(f, g) := \{h \in \mathcal{P}(\mathbb{C}) : \quad h \mid f \quad \wedge h \mid g\}.$$

En otras palabras,

$$\mathcal{D}(f, g) = \mathcal{D}(f) \cap \mathcal{D}(g).$$

6. Definición (máximo común divisor de dos polinomios). Sean $f, g, d \in \mathcal{P}(\mathbb{C})$ no ambos cero. Se dice que d es *un máximo común divisor* de f y g si d es un divisor común de f y g y si cualquier divisor común de f y g divide a d.

7. Notación (máximos comunes divisores de dos polinomios). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Denotemos por $\operatorname{MCD}(f, g)$ al conjunto de los máximos comunes divisores de f y g. Formalmente,

$$\operatorname{MCD}(f, g) := \{d \in \mathcal{D}(f, g) : \quad \forall h \in \mathcal{D}(f, g) \quad h \mid d\}.$$

8. Observación: los máximos divisores comunes se determinan por el conjunto de los divisores comunes. Si $f_1, g_1, f_2, g_2 \in \mathcal{P}(\mathbb{C})$ y $\mathcal{D}(f_1, g_1) = \mathcal{D}(f_2, g_2)$, entonces

$$\operatorname{MCD}(f_1, g_1) = \operatorname{MCD}(f_2, g_2).$$

9. Proposición. Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero y sea $d \in \operatorname{MCD}(f, g)$. Entonces para cualquier $c \in \mathbb{C}\backslash\{0\}$ tenemos que $cd \in \operatorname{MCD}(f, g)$.

10. Proposición sobre la divisibilidad mutua de dos polinomios (repaso). Sean $f, g \in \mathcal{P}(\mathbb{C})$ tales que $f \mid g$ y $g \mid f$. Entonces existe un $c \in \mathbb{C}\backslash\{0\}$ tal que $f = cg$.

11. Lema (sobre los máximos comunes divisores de dos polinomios, uno de los cuales es cero). Sea $f \in \mathcal{P}(\mathbb{C})$, $f \neq \mathbf{0}_{\mathcal{P}}$. Entonces $\operatorname{MCD}(f, \mathbf{0}_{\mathcal{P}})$ consiste de todos los polinomios de la forma cf, donde $c \in \mathbb{C}\backslash\{0\}$:

$$\operatorname{MCD}(f, \mathbf{0}_{\mathcal{P}}) = \{d \in \mathcal{P}(\mathbb{C}): \quad \exists c \in \mathbb{C}\backslash\{0\} \quad d = cf\}.$$

Demostración. Tenemos que demostrar la igualdad de dos conjuntos. Empecemos con la contención $\subseteq$. Sea $d \in \operatorname{MCD}(f, \mathbf{0}_{\mathcal{P}})$. Entonces, por un lado, $d \in \mathcal{D}(f)$ y $d \mid f$. Por otro lado, como $f \in \mathcal{D}(f, \mathbf{0}_{\mathcal{P}})$, $f \mid d$. Por la Proposición sobre la divisibilidad mutua de dos polinomios, existe un $c \in \mathbb{C}\backslash\{0\}$ tal que $d = cf$.

Ahora demostremos la contención $\supseteq$. Sea $c \in \mathbb{C}\backslash\{0\}$ y sea $d = cf$. Entonces $d \mid f$ y $d \mid \mathbf{0}_{\mathcal{P}}$, así que $d \in \mathcal{D}(f, \mathbf{0}_{\mathcal{P}})$. Además, si $h \in \mathcal{D}(f, \mathbf{0}_{\mathcal{P}})$, entonces $h \mid f$ y por consecuencia $h \mid d$. $\square$

12. Lema (sobre la división con resto y el conjunto de comunes divisores). Sean $f, g \in \mathcal{P}(\mathbb{C})$, $g \neq \mathbf{0}_{\mathcal{P}}$. Denotemos por q y r, respectivamente, al cociente y residuo de la división de f entre g:

$$f = gq + r, \qquad \deg(r) < \deg(g).$$

Entonces $\mathcal{D}(f, g) = \mathcal{D}(g, r)$ y por consecuencia $\operatorname{MCD}(f, g) = \operatorname{MCD}(g, r)$.

Demostración. Vamos a demostrar la igualdad $\mathcal{D}(f, g) = \mathcal{D}(g, r)$. Empecemos con la contención $\subseteq$. Sea $d \in \mathcal{D}(f, g)$. Entonces de la igualdad $r = f - gq$ se sigue que $d \mid r$.

Ahora demostremos la contención $\supseteq$. Sea $d \in \mathcal{D}(g, r)$. Entonces de la igualdad $f = gq + r$ se sigue que $\mid f$. $\square$

13. Teorema (existencia de un máximo común divisor). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Entonces el conjunto $\operatorname{MCD}(f, g)$ no es vacío, esto es, existe un máximo común divisor de f y g.

Demostración. Si $g = \mathbf{0}_{\mathcal{P}}$, entonces por el Lema 11 tenemos $f \in \operatorname{MCD}(f, g)$. Consideremos el caso $g \neq \mathbf{0}_{\mathcal{P}}$. Aplicamos a los polinomios f, g el algoritmo de Euclides, esto es, encontramos polinomios $q_1, r_1, q_2, r_2, \ldots, q_s, r_s, q_{s+1} \in \mathcal{P}(\mathbb{C})$ tales que $r_1, r_2, \ldots, r_s \neq \mathbf{0}_{\mathcal{P}}$,

$$\begin{aligned}
f &= gq_1 + r_1, && \deg(r_1) < \deg(g),\\
g &= r_1 q_2 + r_2, && \deg(r_2) < \deg(r_1),\\
&\ldots\\
r_{s-2} &= r_{s-1} q_s + r_s, && \deg(r_s) < \deg(r_{s-1})\\
r_{s-1} &= r_s q_{s+1} + \mathbf{0}_{\mathcal{P}}.
\end{aligned}$$

Notamos que el proceso debe terminarse a lo máximo en $\deg(g)$ pasos porque $\deg(g) > \deg(r_1) > \deg(r_2) > \ldots$. Por el Lema 11, $r_s \in \mathrm{MCD}(r_s, \mathbf{0}_{\mathcal{P}})$. Por el Lema 12, $r_s \in \mathrm{MCD}(r_{s-1}, r_s)$. Por el Lema 12, $r_s \in \mathrm{MCD}(r_{s-2}, r_{s-1})$, etc. Finalmente obtenemos $r_s \in \mathrm{MCD}(f, g)$. □

14. Ejercicio. Demostrar el teorema anterior de otra manera, procediendo por inducción. Demostrar que para cada $n \in \mathbb{N}_0$ se cumple la siguiente afirmación $\mathcal{A}(n)$:

$$\forall f, g \in \mathcal{P}(\mathbb{C}) \qquad \big((\deg(f) \leqslant n) \quad \wedge \quad (\deg(g) \leqslant n) \quad \wedge \quad (f \neq \mathbf{0}_{\mathcal{P}} \quad \vee \quad g \neq \mathbf{0}_{\mathcal{P}})\big)$$
$$\Rightarrow \quad (\exists h \in \mathrm{MCD}(f, g)).$$

15. Proposición (unicidad de máximo común divisor salvo multiplicación por constantes no nulas). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero, y sean $d_1, d_2 \in \mathrm{MCD}(f, g)$. Entonces existe $c \in \mathbb{C} \backslash \{0\}$ tal que $d_2 = cd_1$.

Demostración. Como $d_1 \in \mathrm{MCD}(f, g)$ y $d_2 \in \mathcal{D}(f, g)$, $d_1 \mid d_2$. Por otro lado, como $d_2 \in \mathrm{MCD}(f, g)$ y $d_1 \in \mathcal{D}(f, g)$, $d_2 \mid d_1$. Por la Proposición sobre la divisibilidad mutua de dos polinomios, existe un $c \in \mathbb{C} \backslash \{0\}$ tal que $d_2 = cd_1$. □

16. Proposición (existencia y unicidad del máximo común divisor mónico de dos polinomios). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Entonces existe un único polinomio mónico d tal que $d \in \mathrm{MCD}(f, g)$.

Demostración. Existencia. Sabemos que existe un polinomio $h \in \mathrm{MCD}(f, g)$. Sea $\deg(h) = n$. Denotemos a los coeficientes de h por h_j:

$$h(x) = \sum_{j=0}^{n} h_j x^j.$$

Entonces el polinomio $d(x) := \frac{1}{h_n} h(x)$ es mónico y pertenece a $\mathrm{MCD}(f, g)$.

Unicidad. Sean u, v polinomios mónicos pertenecientes a $\mathrm{MCD}(f, g)$. Entonces existe un $c \in \mathbb{C}$ tal que $v = cu$. Sea $n = \deg(u)$. Entonces $\deg(v) = n$ y para los coeficientes de las potencias mayores de u y v obtenemos $1 = v_n = cu_n = c$, de donde $c = 1$. □