Criterios de irreducibilidad para polinomios de cualquier grado

Facultad de Ciencias UNAM

Introducción

En esta sección veremos criterios de irreducibilidad útiles para polinomios de cualquier grado, incluyendo el famoso "Criterio de Eisenstein".

Condiciones suficientes para que un polinomio sea irreducible usando un anillo cociente

Proposición 1

Supongamos que R es un dominio entero, que I es un ideal propio de R, y para toda $q(x) = b_m x^m + \cdots + b_0 \in R[x]$, denotemos $\overline{q(x)} := \overline{b_m} x^m + \cdots + \overline{b_0} \in (R/I)[x]$ donde $\overline{\alpha} := \alpha + I$.

Si $p(x) \in R[x]$ es un polinomio mónico no constante tal que $\overline{p(x)}$ no se puede factorizar en dos polinomios en $(R/I)[x]$ no constantes de grado mas chico, entonces $p(x)$ es irreducible en $R[x]$.

Demostración. Procedemos por contrapuesta. Supongamos que $p(x)$ es reducible en $R[x]$. Es decir, existen $a(x), b(x)$ no invertibles en $R[x]$ tales que $p(x) = a(x)b(x)$.

Antes de encontrar la factorización de $\overline{p(x)}$, veamos que existen $a'(x), b'(x) \in R[x]$ mónicos no invertibles tales que $p(x) = a'(x)b'(x)$.

Supongamos que

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \text{y}$$
$$b(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

Como $p(x)$ es mónico y $p(x) = a(x)b(x)$, las igualdades anteriores implican que $a_n b_m = 1$. Con esto en mente, es fácil verificar que

$$a'(x) := b_m a(x) \quad \text{y} \quad b'(x) := a_n b(x)$$

son polinomios mónicos tales que $p(x) = a'(x)b'(x)$.
Ahora si, encontremos la factorización de $\overline{p(x)}$. Obviamente $\overline{p(x)} = \overline{a(x)}\ \overline{b(x)}$ es la factorización buscada pero hay que verificar que $\overline{a'(x)}$ y $\overline{b'(x)}$ no son constantes. Afortunadamente, esto es consecuencia inmediata de la siguiente observacion.

Si $q(x) = q_r x^r + q_{r-1}x^{r-1} + \cdots + q_1 x + q_0$, entonces

$$\begin{aligned} \overline{q(x)} \in (R/I)[x] \text{ es constante } &\iff \overline{q_i} = \overline{0} \text{ para toda } i \neq 0 \\ &\iff q_i \in I \text{ para toda } i \neq 0. \end{aligned}$$

Usando esto, obtenemos que $\overline{a'(x)}, \overline{b'(x)}$ no son constantes porque sus coeficientes delanteros son 1 y el $1 \notin I$ (pues I es propio por hipótesis).

$\square$

Observación

A pesar de que no daremos una demostración de esto, es importante notar que el converso de la proposición anterior *no* es cierto. Específicamente, existen $p(x) \in \mathbb{Z}[x]$ tales que

$$\begin{gathered} p(x) \text{ es irreducible en } \mathbb{Z}[x] \textit{ pero} \\ \overline{p(x)} \text{ es reducible en cualquier } (\mathbb{Z}/n\mathbb{Z})[x] = \mathbb{Z}_n[x]. \end{gathered}$$

Un ejemplo de semejante $p(x)$ es

$$x^4 - 72x^2 - 4.$$

Una aplicación de la proposición anterior

- $x^n + x + 1$ es irreducible en $\mathbb{Z}[x]$: recordemos que ya vimos que $x^n + x + 1$ es irreducible en $\mathbb{Z}_2[x]$.
- $x^2 + 1$ es irreducible en $\mathbb{Z}[x]$: recordemos que ya vimos que $x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$.
- $x^2 + xy + 1$ es irreducible en $\mathbb{Z}[x, y]$. Primero recordemos que $\mathbb{Z}[x, y] = (\mathbb{Z}[y])[x]$. En este anillo, el polinomio

$$x^2 + xy + 1 = (1)x^2 + (y)x + 1 \in (\mathbb{Z}[y])[x]$$

  es mónico[1]. Por lo tanto, podemos aplicar la proposición anterior con $R = \mathbb{Z}[y]$ y $p(x) = (1)x^2 + (y)x + 1 \in \left(\mathbb{Z}[y]\right)[x]$. También, definimos $I = (y)$.

[1] En contraste, el polinomio $x^2 + xy + 1 = (x)y + (x^2 + 1) \in (\mathbb{Z}[x])[y]$ no es mónico pues su coeficiente delantero es $x \in \mathbb{Z}[x]$.

De esta manera, obtenemos que en $\left(\mathbb{Z}[y]/(y)\right)[x]$,

$$\overline{p(x)} = \overline{1}x^2 + \overline{y}x + \overline{1} = \overline{1}x^2 + \overline{0}x + \overline{1} = \overline{1}x^2 + \overline{1}$$

Usando (i) esta igualdad, (ii) el isomorfismo $\mathbb{Z}[y]/(y) \cong \mathbb{Z}$ y (iii) el inciso anterior, obtenemos que[2] $\overline{p(x)}$ es irreducible en $\left(\mathbb{Z}[y]/(y)\right)[x]$. Usando la proposición anterior, obtenemos lo deseado.

- Hay que tener cuidado cuando apliquemos la proposición anterior a polinomios de varias variables. Por ejemplo, considera $p(x) = xy + x + y + 1 \in \mathbb{Z}[x, y]$. Si ponemos $I = (x)$, obtenemos

$$\overline{p(x)} = \overline{1}y + \overline{1} \in \left(\mathbb{Z}[x]/(x)\right)[y]$$

y como $y + 1$ es irreducible en $\mathbb{Z}[y]$, uno podría pensar que esto implica (usando un argumento análogo al del inciso anterior) que $p(x) = xy + x + y + 1$ es irreducible en $\mathbb{Z}[x, y]$.

[2] Es fácil verificar que si $\phi : R \to S$ es un isomorfismo de anillos, entonces r es irreducible en R si y solo si $\phi(r)$ es irreducible en S. Este isomorfismo se extiende naturalmente a un isomorfismo $\Phi : R[x] \to S[x]$ y por lo tanto, también tenemos que $p(x) \in R[x]$ es irreducible en $R[x]$ si y solo si $\Phi(p(x)) \in S[x]$ es irreducible en $S[x]$.

Sin embargo,

$$p(x) = xy + x + y + 1 = (x + 1)(y + 1)$$

y por lo tanto, $p(x)$ es reducible en $\mathbb{Z}[x, y]$.

¿Cual fue el problema?

- La razón por la que la proposición anterior no funciono fue porque $xy + x + y + 1$ *no* es mónico en $\big(\mathbb{Z}[x]\big)[y]$. En efecto,

  $$xy + x + y + 1 = (x + 1)y + (x + 1)$$

  y por lo tanto, el coeficiente delantero de $p(x)$ es $x + 1 \neq 1$. En resumen, nunca verificamos las condiciones de la proposición. Cabe aclarar que por la simetría del polinomio respecto a las variables x y y, no ayuda considerar a $p(x)$ en $\big(\mathbb{Z}[y]\big)[x]$ o considerar el ideal (y).

- En un sentido mas general, el problema es que existe $q(x) \in \mathbb{Z}[x,y]$ tal que $q(x)$ no es invertible en $\mathbb{Z}[x,y]$ pero $\overline{q(x)} \in \big(\mathbb{Z}[x]/(x)\big)\,[y]$ si es invertible.

  En efecto, $x+1$ es un ejemplo de semejante $q(x)$ y por lo tanto, la factorización

  $$p(x) = xy + x + y + 1 = (x+1)(y+1)$$

  no implica la reducibilidad de $p(x) \in \big(\mathbb{Z}[x]/(x)\big)\,[y]$:

  $$\begin{aligned}\overline{p(x)} = \left(\overline{x+1}\right)\left(\overline{(1)y+1}\right) &= \left(\overline{x}+\overline{1}\right)\left(\overline{1}y+\overline{1}\right)\\ &= \left(\overline{0}+\overline{1}\right)\left(\overline{1}y+\overline{1}\right)\\ &= \overline{1}y+\overline{1}\end{aligned}$$

El criterio de Eisenstein

Proposición 2

Supongamos que R es un dominio entero y que

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x].$$

es un polinomio primitivo con $\deg p(x) = n \geq 1$.
Si existe un ideal primo P de R tal que

- $a_i \in P$ para toda $i \in \{0, 1, \ldots, n-1\}$,
- $a_n \notin P$, y
- $a_0 \notin P^2$,

entonces $p(x)$ es irreducible en $R[x]$.

Demostración. Procedemos por contrapuesta. Específicamente, supongamos que $p(x) = a_n x^n + \cdots + a_0$ es un polinomio primitivo tal que

- $a_i \in P$ para toda $i \in \{0, 1, \ldots, n-1\}$,
- $a_n \notin P$,
- $p(x)$ es reducible en $R[x]$

y veamos que $a_0 \in P^2$.

Como $p(x)$ es reducible, existen $f(x), g(x) \in R[x]$ no invertibles tales que $p(x) = f(x)g(x)$. Mas aun, como $p(x)$ es primitivo, $f(x)$ y $g(x)$ son polinomios no constantes: de lo contrario, encontraríamos un elemento no invertible que divide a todos los coeficientes de $p(x)$ (contradiciendo que $p(x)$ es primitivo).

Por otro lado, como $a_i \in P$ para toda $i \in \{0, 1, \ldots, n-1\}$, entonces

$$\begin{aligned} \overline{f(x)}\,\overline{g(x)} = \overline{p(x)} &= \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0} \\ &= \overline{a_n}x^n + \overline{0}x^{n-1} + \cdots + \overline{0}x + \overline{0} = \overline{a_n}x^n. \end{aligned} \tag{1}$$

Veamos que esto implica que los coeficientes constantes de $\overline{f(x)}$ y $\overline{g(x)}$ son $\overline{0}$. Para esto, supongamos que

$$\begin{aligned} f(x) &= f_m x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0 \quad \text{y} \\ g(x) &= g_l x^l + g_{l-1}x^{l-1} + \cdots + g_1 x + g_0 \end{aligned}$$

y para proceder por contradicción también supongamos que $\overline{g_0} \neq \overline{0}$.

Entonces (1) implica que $\overline{f_0}\,\overline{g_0} = \overline{0}$ y como R/P es un dominio entero (pues P es un ideal primo) entonces $\overline{f_0} = \overline{0}$ o $\overline{g_0} = \overline{0}$ pero supusimos $\overline{g_0} \neq \overline{0}$ entonces $\overline{f_0} = \overline{0}$.

Por otro lado, de nuevo (1) implica que $\overline{f_1}\overline{g_0} + \overline{f_0}\overline{g_1} = \overline{0}$ pero como $\overline{f_0} = 0$, entonces $\overline{f_1}\overline{g_0} = \overline{0}$. De nuevo usando que $\overline{g(x)} \neq \overline{0}$ y que R/P es un dominio entero, obtenemos que $\overline{f_1} = \overline{0}$. Procediendo de esta manera, obtenemos que

$$\overline{f_k} = \overline{0} \text{ para toda } k = 1, \ldots, m. \tag{2}$$

En efecto, en el k-esimo paso (con $k \in \{2, \ldots, m\}$) obtenemos una igualdad en $(R/P)[x]$ de la forma

$$\overline{f_k}\,\overline{g_0} + \Big(\text{sumandos de la forma } \overline{f_i}\,\overline{g_{i-k}} \text{ con } i < k\Big) = \overline{0}$$

Por lo tanto, usando inducción (fuerte) obtenemos (2). Sin embargo, (2) es imposible pues tendríamos

$$\overline{a_n}x^n = \overline{f(x)}\,\overline{g(x)} = \overline{0}\,\overline{g(x)} = \overline{0}$$

y por lo tanto, $\overline{a_n} = \overline{0}$ o equivalentemente, $a_n \in P$ (contradiciendo $a_n \notin P$).
Por lo tanto, $\overline{f_0} = \overline{0} = \overline{g_0}$ o equivalentemente, $f_0, g_0 \in P$. De donde, $a_0 =^3 f_0 g_0 \in P^2$. □

[3]Pues $p(x) = f(x)g(x)$.

El criterio de Eisenstein en $\mathbb{Z}[x]$

Proposición 3

Supongamos que

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

es un polinomio primitivo con $\deg p(x) = n \geq 1$.
Si existe $p \in \mathbb{Z}$ primo tal que

- $p | a_i$ para toda $i \in \{0, 1, \ldots, n-1\}$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

entonces $p(x)$ es irreducible en $\mathbb{Z}[x]$ y también[4] en $\mathbb{Q}[x]$.

Demostración. Es simplemente reescribir el criterio de Eisenstein en términos de divisibilidad y ocupando que los ideales primos de $\mathbb{Z}$ son los (p) con p primo. $\square$

[4]c.f. proposición 1.26.1.

Aplicaciones del criterio de Eisenstein

- $x^4 + 10x + 5 \in \mathbb{Z}[x]$ es irreducible en $\mathbb{Z}[x]$ por el criterio de Eisenstein aplicado con el primo $p = 5$.
- Supongamos que $n \in \mathbb{Z}_{\geq 1}$. Si $a \in \mathbb{Z}$ es divisible por algún primo p pero no es divisible por p^2, entonces $x^n - a$ es irreducible en $\mathbb{Z}[x]$. En particular, $x^n - p$ es irreducible en $\mathbb{Z}[x]$ para todo primo p.
- Si R es un dominio entero y $n \in \mathbb{Z}_{\geq 1}$, entonces $y^n - x$ es irreducible en $R[x, y]$: Primero recordemos que $R[x, y] = (R[x])[y]$ y por lo tanto, basta encontrar un ideal primo P de $R[x]$ tal que satisfaga las condiciones del criterio de Eisenstein. Es fácil verificar que $P = (x)$ cumple lo deseado (recordemos que (x) es primo en $R[x]$ porque $R[x]/(x) \cong R$ es un dominio entero).

Un truquito para ocupar el criterio de Eisenstein indirectamente

Lema 4

Supongamos que R es un dominio entero y que $p(x), q(x) \in R[x]$ con $\deg q(x) \geq 1$.

1. Si $p(x)$ no es invertible en $R[x]$, entonces $p(q(x))$ no es invertible en $R[x]$.
2. Si $p(q(x))$ es irreducible en $R[x]$, entonces $p(x)$ es irreducible en $R[x]$.

Demostración. Procedemos por contrapuesta en ambos incisos.

1. Si $p(q(x))$ es invertible en $R[x]$, entonces $p(q(x)) = u$ para alguna $u \in R$ invertible. Pero entonces

   $$\deg p(x) \cdot \deg q(x) = \deg p(q(x)) = \deg u = 0$$

   y como $\deg q(x) \geq 1$, entonces la ecuación anterior implica que $\deg p(x) = 0$ es decir, $p(x)$ es un polinomio constante. Finalmente, la igualdad $p(q(x)) = u$ implica $p(x) = u$ y por lo tanto, como $u \in R$ es invertible, entonces $p(x)$ también.
2. Si $p(x)$ es reducible en $R[x]$, entonces existen $a(x), b(x) \in R[x]$ no invertibles tales que $p(x) = a(x)b(x)$. Por el inciso anterior, $a(q(x)), b(q(x))$ también son polinomios no invertibles y por lo tanto, la igualdad

   $$p(q(x)) = a(q(x))b(q(x))$$

   implica que $p(q(x))$ es reducible.

$\square$

Aplicaciones (indirectas) del criterio de Eisenstein

- $x^4 + 1$ es irreducible en $\mathbb{Z}[x]$: Denotemos $p(x) = x^4 + 1$ y $q(x) = x + 1$. Por el lema anterior basta probar que $p(q(x))$ es irreducible. Pero como

$$p(q(x)) = (q(x))^4 + 1 = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2,$$

usando el criterio de Eisenstein con el primo $p = 2$, obtenemos lo deseado.

- Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo. Definimos el **polinomio p-ciclotómico** por

$$\phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

Notemos que como

$$x^p - 1 = (x-1)x^{p-1} + x^{p-2} + \cdots + x + 1,$$

entonces

$$\phi_p(x) = \frac{x^p - 1}{x - 1}.$$

Veamos que para todo primo p, $\phi_p(x)$ es irreducible en $\mathbb{Z}[x]$.

Para esto, denotemos $q(x) := x + 1$. Por el lema anterior, basta probar que $\phi_p(q(x))$ es irreducible. Pero como

$$\begin{aligned}\varphi_p(q(x)) = \varphi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p,\end{aligned}$$

entonces usando el criterio de Eisenstein con el primo p, obtenemos lo deseado.