El criterio de Eisenstein

por

Ramón Espinosa Armenta

Un polinomio con coeficientes racionales puede ser reducible en $\mathbb{R}[x]$, pero irreducible en $\mathbb{Q}[x]$. Por ejemplo, el polinomio $x^2 - 5$ es reducible en $\mathbb{R}[x]$, pues

$$x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5}),$$

pero es irreducible en $\mathbb{Q}[x]$, pues es un polinomio de grado dos que no tiene raíces racionales.

Si $a(x) \in \mathbb{Q}[x]$, entonces $Ma(x) = b(x)$, donde M es el mínimo común múltiplo de los denominadores de los coeficientes de $a(x)$ y $b(x)$ es un polinomio con coeficientes enteros. Como $a(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si $b(x)$ es irreducible en $\mathbb{Q}[x]$, al discutir el problema de irreducibilidad en $\mathbb{Q}[x]$, podemos restringir nuestra atención a polinomios con coeficientes enteros.

Si un polinomio con coeficientes enteros tiene una raíz racional entonces es reducible en $\mathbb{Q}[x]$; sin embargo el recíproco no es cierto, por ejemplo, el polinomio $x^4 - 5x^2 + 6$ no tiene raíces racionales, pero no es irreducible en $\mathbb{Q}[x]$, porque

$$x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3).$$

Veremos a continuación una condición suficiente para asegurar que un polinomio con coeficientes enteros sea irreducible en $\mathbb{Q}[x]$. Pero antes necesitamos introducir cierta terminología y probar algunos resultados preliminares.

Sea $a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, con $a_n \neq 0$. El **contenido** de $a(x)$ es el número $d = mcd(a_n, \ldots, a_1, a_0)$. Si $d = 1$ se dice que $a(x)$ es **primitivo**. El polinomio $b(x)$ obtenido al multiplicar $a(x)$ por $1/d$ es llamado el polinomio primitivo asociado con $a(x)$. Obsérvese que $a(x) = db(x)$.

Lema 1. *Si $b(x)$ y $c(x)$ son primitivos, entonces $a(x) = b(x)c(x)$ es primitivo.*

Demostración. Sea d el contenido de $a(x)$ y supongamos que $d > 1$. Por lo tanto existe p primo tal que $p|d$. Como $b(x)$ es primitivo, p no divide a algún coeficiente de $b(x)$. Sea i tal que $p \nmid b_i$ y $p \mid b_0, \ldots, p \mid b_{i-1}$. Análogamente, sea j tal que $p \nmid c_j$ y $p \mid c_0, \ldots, p \mid c_{j-1}$. Ahora bien, el coeficiente de x^{i+j} en $a(x)$ es

$$a_{i+j} = \sum_{k=0}^{i+j} b_k c_{i+j-k}.$$

Si $k = 0, 1, \ldots, i-1$ entonces $p \mid b_k c_{i+j-k}$, porque $p \mid b_k$; por otra parte, si $i+1 \leq k$ entonces $p \mid b_k c_{i+j-k}$ porque $p \mid c_{i+j-k}$. Por lo tanto p divide a

$$\sum_{\substack{k=0 \\ k \neq i}}^{i+j} b_k c_{i+j-k}.$$

Como también $p \mid a_{i+j}$ se sigue que $p \mid b_i c_j$. Como p es primo tenemos que $p \mid b_i$ o $p \mid c_j$ lo cual no es posible. Por lo tanto $a(x) = b(x)c(x)$ es primitivo. □

Lema 2 (Lema de Gauss)**.** *Si un polinomio primitivo puede factorizarse como producto de dos polinomios con coeficientes racionales, entonces puede factorizarse como producto de dos polinomios con coeficientes enteros.*

Demostración. Sea $a(x)$ un polinomio primitivo y supongamos que $a(x) = b(x)c(x)$ con $b(x), c(x) \in \mathbb{Q}[x]$. Quitando denominadores y sacando factores comunes podemos escribir

$$a(x) = \frac{p}{q}\hat{b}(x)\hat{c}(x)$$

donde $p,\ q \in \mathbb{Z}$ y $\hat{b}(x),\ \hat{c}(x) \in \mathbb{Z}[x]$ son primitivos. Por lo tanto

$$qa(x) = p\hat{b}(x)\hat{c}(x).$$

El contenido de $qa(x)$ es q, porque $a(x)$ es primitivo. Por otra parte, por el lema anterior $\hat{b}(x)\hat{c}(x)$ es primitivo, por lo tanto el contenido de $p\hat{b}(x)\hat{c}(x)$ es p. De ahí que $p = q$ y por lo tanto $a(x) = \hat{b}(x)\hat{c}(x)$. □

En 1846 el matemático alemán *Ferdinand Eisenstein* estableció una condición suficiente para que un polinomio sea irreducible en los racionales.

Teorema 1 (Criterio de Eisenstein)**.** *Sea* $a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Supongamos que existe* p *primo tal que* $p \mid a_0$, $p \mid a_1$, $\ldots$, $p \mid a_{n-1}$, $p \nmid a_n$ *y* $p^2 \nmid a_0$. *Entonces* $a(x)$ *es irreducible en* $\mathbb{Q}[x]$.

Demostración. Sin pérdida de generalidad podemos suponer que $a(x)$ es primitivo. Si $a(x)$ es reducible en $\mathbb{Q}[x]$, entonces por el lema de Gauss $a(x) = b(x)c(x)$, donde

$$b(x) = b_r x^r + \cdots + b_1 x + b_0 \quad \text{y} \quad c(x) = c_s x^s + \cdots + c_1 x + c_0$$

son polinomios con coeficientes enteros. Ahora bien, $a_0 = b_0 c_0$. Por hipótesis $p \mid a_0$, por lo tanto $p \mid b_0$ o $p \mid c_0$, pero no a ambos, porque $p^2 \nmid a_0$. Supongamos, sin pérdida de generalidad, que $p \mid b_0$ y $p \nmid c_0$. Por otra parte, como $a_n = b_r c_s$ y $p \nmid a_n$, entonces $p \nmid b_r$. Por lo tanto existe $k \leq r < n$ tal que $p \mid b_0$, $p \mid b_1$, $\ldots$, $p \mid b_{k-1}$ y $p \nmid b_k$. Como $a_k = \sum_{i=0}^{k} b_i c_{k-i}$ y $p \mid a_k$, se sigue que $p \mid b_k c_0$. Por lo tanto $p \mid b_k$ o $p \mid c_0$ lo cual es una contradicción. Con lo cual concluimos que $a(x)$ es irreducible en $\mathbb{Q}[x]$. □

Ejemplo 1. El polinomio

$$a(x) = 17x^4 - 10x^3 + 5x^2 + 25x - 35$$

es irreducible en $\mathbb{Q}[x]$, porque 5 es primo y

$$5 \mid (-10), \quad 5 \mid 5, \quad 5 \mid 25, \quad 5 \mid (-35), \quad 5 \nmid 17 \quad \text{y} \quad 25 \nmid (-35),$$

por lo que, por el criterio de Eisenstein $a(x)$ es ireducible en $\mathbb{Q}[x]$. △

Teorema 2. *Sea* p *un número primo, entonces el polinomio*

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

es irreducible en $\mathbb{Q}[x]$.

Demostración. Consideremos el polinomio

$$\hat{a}(x) = 1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1}.$$

Por lo tanto

$$\hat{a}(x) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \binom{p}{1} + \binom{p}{2} x + \binom{p}{3} x^2 + \cdots + \binom{p}{p} x^{p-1}.$$

Observemos que

$$p \mid \binom{p}{k} \qquad \text{para toda } k = 1, \ldots, p-1.$$

Además,

$$p \nmid \binom{p}{p} \quad \text{y} \quad p^2 \nmid \binom{p}{1}.$$

Por lo tanto, por el criterio de Eisenstein, $\hat{a}(x)$ es irreducible en $\mathbb{Q}[x]$. Supongamos ahora que $a(x)$ es reducible en $\mathbb{Q}[x]$. Por lo tanto existen $b(x), c(x) \in \mathbb{Q}[x]$ tales que $a(x) = b(x)c(x)$, donde grado $b(x) > 0$ y grado $c(x) > 0$. De ahí que

$$a(x+1) = b(x+1)c(x+1),$$

lo cual no es posible, porque $\hat{a}(x) = a(x+1)$ es irreducible en $\mathbb{Q}[x]$. □

Ejercicios

1. Determina si el polinomio $x^5 + 10x^4 - 25x^3 + 15x^2 - 10$ es irreducible en $\mathbb{Q}[x]$.

2. Determina si el polinomio $2x^4 + 8x^3 + 6x^2 - 10x + 2$ es irreducible en $\mathbb{Q}[x]$.

3. Determina si el polinomio $6x^7 + 14x^5 - 21x^2 + 28x - 7$ es irreducible en $\mathbb{Q}[x]$.

4. Determina si el polinomio $2x^6 + 12x^4 + 6x^3 - 18x - 9$ es irreducible en $\mathbb{Q}[x]$.