Criterios de irreducibilidad para polinomios de grado menor o igual a 3

Facultad de Ciencias UNAM

Introducción

En esta sección presentamos criterios de irreducibilidad en $R[x]$ donde R es un dominio entero. Nuestro interés en estos criterios nace de 2 cosas:

1. El problema clásico de encontrar $y \in \mathbb{Z}$ tal que

$$ay^3 + by^2 + cy + d = 0$$

   con $a, b, c, d \in \mathbb{Z}$.

2. El siguiente hecho que pronto veremos (c.f. corolario 3): Dadas $a, b, c, d \in \mathbb{Z}$,

$$\exists y \in \mathbb{Z} \left(ay^3 + by^2 + cy + d = 0 \right) \iff$$
$$p(x) = ax^2 + bx^2 + cx + d \text{ es reducible en } \mathbb{Z}[x]$$

En esta sección nos limitamos a ver criterios que son útiles para polinomios de grado ≤ 3.

Raíces de polinomios

Definición

Supongamos que R es un anillo y $p(x) \in R[x]$. Si

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

entonces, decimos que $\alpha \in R$ es una **raíz de** $p(x)$ **en** R si

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0$$

Naturalmente, si consideramos a $p(x)$ como una función de R en R, α es una raíz si $p(\alpha) = 0$.

$p(x)$ tiene una raíz en $F \iff p(x) \in F[x]$ tiene un divisor de grado 1

Proposición 1

Supongamos que F es un campo y que $p(x) \in F[x]$. Entonces $p(x)$ tiene una raíz en F si y solo si $a(x)|p(x)$ para alguna $a(x) \in F[x]$ con $\deg a(x) = 1$.

Demostración.
$\Longleftarrow$) Si $a(x)|p(x)$ para alguna $a(x) \in F[x]$ con $\deg a(x) = 1$, entonces $a(x) = a_1x + a_0$ con $a_1 \neq 0$ y existe $b(x) \in F[x]$ tal que $p(x) = a(x)b(x)$. Como F es campo, podemos definir $\alpha := -\frac{a_0}{a_1} \in F$ y usando la igualdad

$$p(x) = (a_1x + a_0)b(x)$$

es fácil verificar que α es raíz de $p(x)$ en F.

$\Longrightarrow$) Supongamos que $\alpha \in F$ es una raíz de $p(x)$ en F y definamos $a(x) := x - \alpha$. Como F es campo, entonces $F[x]$ es un dominio euclidiano y por lo tanto existen $q(x), r(x) \in F[x]$ tales que

$$\begin{aligned} p(x) &= q(x)a(x) + r(x) \\ &= q(x)(x-\alpha) + r(x) \text{ con } \deg r(x) < \deg(x-\alpha) = 1 \text{ o } r(x) = 0 \end{aligned} \tag{1}$$

Como $\deg r(x) < 1$, entonces $r(x)$ es un polinomio constante y por lo tanto, podemos escribir $r(x) = r \in R$. De esta manera, (1) se convierte en

$$p(x) = q(x)(x-\alpha) + r$$

y evaluando en α obtenemos

$$0 = p(\alpha) = q(\alpha)(\alpha - \alpha) + r = r$$

Por lo tanto, $r(x) = r = 0$ y claramente $a(x) = (x-\alpha) | p(x)$.

$\square$

La importancia de la existencia de raíces

Proposición 2

Supongamos que F es un campo y que $p(x) \in F[x]$. Si $\alpha_1, \ldots, \alpha_k \in F$ son raíces de $p(x)$, entonces

$$(x - \alpha_1) \cdots (x - \alpha_k) | p(x)$$

En particular, $p(x)$ tiene a lo mas $\deg p(x)$ raíces.

Demostración. Procedamos por inducción sobre el numero de raíces.

El paso base es consecuencia de la implicación "$\Longrightarrow$" de la proposición anterior.

Para el paso inductivo, supongamos que $\alpha_1, \ldots, \alpha_n \in F$ son raíces de $p(x)$. Por hipótesis de inducción,

$$(x - \alpha_1) \cdots (x - \alpha_{n-1}) | p(x).$$

En particular, el polinomio

$$\frac{p(x)}{(x-\alpha_1)\cdots(x-\alpha_{n-1})}$$

esta bien definido y claramente tiene a α_n como raíz (pues α_n es raíz de $p(x)$, es decir, $p(\alpha_n)=0$). Por la proposición anterior, esto implica que

$$(x-\alpha_n)\,\Big|\,\frac{p(x)}{(x-\alpha_1)\cdots(x-\alpha_{n-1})}$$

y por lo tanto (por la proposición 1.15.8),

$$(x-\alpha_1)\cdots(x-\alpha_n)\,\big|\,p(x)\ .$$

□

Irreducibilidad en polinomios de grados = 2,3

Corolario 3

Supongamos que F es un campo y que $p(x) \in F[x]$. Si $\deg p(x) \in \{2, 3\}$, entonces $p(x)$ es reducible en $F[x]$ si y solo si $p(x)$ tiene una raíz en F.

Demostración. Como $\deg p(x) \in \{2, 3\}$, entonces

$$p(x) \text{ es reducible en } F[x] \iff p(x) \text{ tiene un factor de grado 1} \tag{2}$$

En efecto, la implicación "$\Longleftarrow$" es obvia y para ver la implicación "$\Longrightarrow$", supongamos que $p(x) = a(x)b(x)$ con $a(x), b(x) \in F[x]$ no invertibles. En particular, $a(x), b(x)$ no son constantes y por lo tanto, $\deg a(x), \deg b(x) \geq 1$. Usando (i) esto, (ii) la hipótesis $\deg p(x) \in \{2, 3\}$ y (iii) la igualdad $\deg p(x) = \deg a(x) + \deg b(x)$ es fácil obtener lo deseado.

Para concluir, usa (2) y la proposición 1. □

Una aplicación del corolario anterior

Sea $F = \mathbb{Z}_2$ (es campo porque 2 es primo) y denotemos $[0]_2 = 0$ y $[1]_2 = 1$. Entonces

- $x^2 + 1$ es reducible en $\mathbb{Z}_2[x]$: El $1 \in \mathbb{Z}_2$ es raíz porque recordemos que en $\mathbb{Z}_2$, $(1)^2 + 1 = 1 + 1 = 0$.
- $x^2 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$: No tiene raíces: $(0)^2 + (0) + 1 = 1$ y $(1)^2 + 1 + 1 = 1 + 1 + 1 = 1$.
- $x^n + x + 1$ es irreducible en $\mathbb{Z}_2[x]$: Tampoco tiene raíces: $(0)^n + (0) + 1 = 1$ y $(1)^n + 1 + 1 = 1 + 1 + 1 = 1$.

Sea $F = \mathbb{Z}_3$ (es campo porque 3 es primo) y denotemos $[0]_3 = 0$, $[1]_3 = 1$, y $[2]_3 = 2$.

- $x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$: No tiene raíces: $(0)^2 + 1 = 1$, $(1)^2 + 1 = 2$, y $(2)^2 + 1 = 4 + 1 = 5 = 1$.

Una propiedad importante de las raíces racionales

Proposición 4

Supongamos que R es un DIP, que F es su campo de fracciones, y que $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, con $a_n \neq 0$. Si $\frac{r}{s} \in F$ es raíz de $p(x)$ en F y r, s son primos relativos, entonces $r|a_0$ y $s|a_n$.

Demostración. Por hipótesis

$$0 = p\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0$$

Multiplicando por s^n obtenemos

$$0 = a_n r^n + a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \cdots + a_2 r^2 s^{n-2} + a_1 r s^{n-1} + a_0 s^n$$

Manipulando un poquito la igualdad anterior, obtenemos que

$$a_n r^n = s\left(-a_{n-1}r^{n-1}s - \cdots a_1 r s^{n-1} - a_0 s^n\right)$$

En particular, $s|a_n r^n$. Mas aun, como r, s son primos relativos y R es un DIP, entonces la relación $s|a_n r^n$ implica que $s|a_n$ (c.f. proposición 1.19.3). Análogamente, $r|a_0$. $\square$

Aplicaciones de la proposición anterior

- $x^3 - 3x - 1$ es irreducible en $\mathbb{Z}[x]$. Como tiene grado 3, basta probar que no tiene raíces en $F = \mathbb{Q}$. Supongamos lo contrario, y sea $\frac{r}{s} \in \mathbb{Q}$ una raíz. Sin perdida de generalidad, podemos suponer que $\frac{r}{s}$ ya esta en su forma reducida, es decir, que r, s son primos relativos. Por la proposición anterior, $r|1$ y $s|1$. Como $r, s \in \mathbb{Z}$, esto implica que $\frac{r}{s} = \pm 1$. Sin embargo, evaluando directamente, vemos que

$$(1)^3 - 3(1) - (1) = -3 \neq 0 \quad \text{y} \quad (-1)^3 - (3)(-1) - (-1) = 4 \neq 0$$

- Si $p \in \mathbb{Z}_{\geq 0}$ es primo, entonces $x^2 - p$ y $x^3 - p$ son irreducibles en $\mathbb{Q}[x]$. De nuevo, como tienen grados = 2,3, entonces basta probar que no tienen raíces en $\mathbb{Q}$. De nuevo, supongamos lo contrario y sea $\frac{r}{s} \in \mathbb{Q}$ una raíz tal que r, s son primos relativos. Por la proposición anterior, $r|p$ y $s|1$. Como $r, s \in \mathbb{Z}$, esto implica que $\frac{r}{s} \in \{\pm 1, \pm p\}$. Sin embargo, evaluando directamente vemos que ninguno de estos dos enteros son raíz.

Comentario

Las técnicas presentadas hasta el momento están limitadas a polinomios con grados = 2,3, pues dependen de que la factorización en irreducibles tenga un factor de grado 1. Obviamente, este no es necesariamente el caso para polinomios de grado 4 porque puede ser (por ejemplo) el producto de dos polinomios irreducibles de grado 2.

En la siguiente sección veremos criterios de irreducibilidad útiles para polinomios de cualquier grado, incluyendo el famoso “Criterio de Eisenstein”.