Algebra Superior 2 13·05·20

Def. Un polinomio de grado positivo, $p(x) \in \mathbb{R}[x]$, es irreducible si no puede ser expresado como el producto de dos polinomios de grado menor. En caso contrario será reducible.

Ejemplo. x^3+2x^2+4x+8 es reducible porque puede expresarse como el producto $(x^2+4)(x+2)$.

x^2+1 es irreducible en $\mathbb{R}[x]$ porque no puede ser expresado como un producto de 2 polinomios de grado menor.

Obs. Como cualquier polinomio es divisible por constantes y múltiplos de sí mismo, el hecho de que un polinomio sea irreducible implica que no tiene otros divisores además de los triviales.

Prop. Sean $p(x) \in \mathbb{R}[x]$ irreducible y $f(x) \in \mathbb{R}[x]$. Entonces $p(x) \mid f(x)$ o el máximo común divisor mónico de $p(x)$ y $f(x)$ es 1.

Dem. Al igual que en $\mathbb{Z}$ denotemos por $(p(x), f(x))$ al máximo común divisor y reservemos esta notación para el máximo común divisor mónico.

Sea $d(x) = (p(x), f(x))$.

Entonces $d(x) \mid p(x)$ y como $p(x)$ es irreducible eso implica que $d(x)$ es constante o múltiplo de $p(x)$.

Si $d(x)$ es constante se tiene que $d(x) = 1$ ✓

Si $d(x) \cdot k = p(x)$ con $k \neq 0$, entonces $d(x) \mid f(x)$ ✓
Así $p(x) \mid f(x)$ como se quería ∎

Prop. Sea $p(x) \in \mathbb{R}[x]$ un polinomio irreducible.
Si $p(x) \mid a(x)b(x)$ con $a(x), b(x) \in \mathbb{R}[x]$,
entonces $p(x) \mid a(x)$ o $p(x) \mid b(x)$.

Dem. Supongamos que $p(x) \nmid a(x)$ y
demostremos entonces que $p(x) \mid b(x)$.

Si $p(x) \nmid (a(x))$, entonces $(p(x), a(x)) = 1$,
y sabemos que existen $c(x), d(x) \in \mathbb{R}[x]$
tales que

$$1 = c(x)a(x) + d(x)p(x)$$

así $b(x) = b(x)c(x)a(x) + b(x)d(x)p(x)$.

Se cumple que $p(x) \mid p(x)$ y que $p(x) \mid a(x)b(x)$

por tanto $p(x) \mid b(x)c(x)a(x) + b(x)d(x)p(x)$

ie, $p(x) \mid b(x)$ ∎

Teorema de Factorización Unica.

Cualquier polinomio, $p(x) \in \mathbb{R}[x]$, de grado positivo se puede escribir de manera única como producto de un número real no cero y polinomios irreducibles mónicos.

Dem. Supongamos que $Grad(p(x)) = 1$, entonces $p(x) = bx + c$ con $b, c \in \mathbb{R}$ y $b \neq 0$.

El polinomio $x + \frac{c}{b}$ es mónico e irreducible

y podemos escribir a $p(x)$ como $b\left(x + \frac{c}{b}\right)$ ✓.

Si $Grad(p(x)) = n > 1$, supongamos que todo polinomio de grado m con $1 \leq m < n$ se puede expesar como producto de un real no cero y polinomios irreducibles mónicos, es decir, de la forma

$$c p_1(x) p_2(x) \cdots p_k(x)$$

con $c \neq 0$ y $p_i(x)$ mónicos irreducibles en $\mathbb{R}[x]$.

Si $p(x) = \sum_{i=0}^{n} a_i x^i$ es irreducible, entonces

$$a_n \left(x^n + \frac{1}{a_n} a_{n-1} x^{n-1} + \cdots + \frac{1}{a_n} a_1 x + \frac{1}{a_n} a_0 \right) \text{ es}$$

el producto buscado.

Si $p(x)$ no es irreducible, entonces

$$p(x) = b(x) c(x) \quad \text{con} \quad Grad(b(x)) < Grad(p(x))$$
$$\text{y} \quad Grad(c(x)) < Grad(p(x)).$$

Por hipótesis de inducción

$$b(x) = c_1 p_1(x)\, p_2(x) \cdots p_r(x)$$
$$c(x) = c_2\, q_1(x)\, q_2(x) \cdots q_s(x).$$

Por tanto, $p(x) = c_1 c_2\, p_1(x) \cdots p_r(x)\, q_1(x) \cdots q_s(x)$, y esto es lo que se quería.

Falta ver que la expresión es única: lo haremos por inducción nuevamente.

Si $Grad(p(x)) = 1$ supongamos que

$$p(x) = a_1(x+b_1) \quad y \quad p(x) = a_2(x+b_2),$$

entonces $a_1(x+b_1) = a_2(x+b_2)$ y
por tanto $a_1 = a_2$ y $b_1 = b_2$ ✓.

Si $Grad(p(x)) = n > 1$ supongamos que la expresión es única para todos los polinomios de grado m con $1 \leq m < n$.

Tenemos entonces que si

$$p(x) = c_1\, p_1(x)\, p_2(x) \cdots p_{m'}(x)$$
$$= c_2\, q_1(x) \cdots q_{n'}(x)$$

entonces $c_1 = c_2$ y que $p_1 \mid q_1 \cdots q_{n'}$.

Entonces $p_1 = q_j$ para alguna j.
luego $p_2 = q_k$ para alguna k y así sucesivamente....

■

El siguiente teorema es un resultado muy útil, omitiremos su demostración (si quieren sería un bonito ejercicio para ustedes, la pueden hacer por inducción sobre el grado del polinomio.

Teo. Sea $c \in \mathbb{R}$. Todo polinomio $p(x) \in \mathbb{R}[x]$ distinto de cero puede expresarse de forma única de la forma

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

en donde $n = \text{Grad}(p(x))$ y $a_0, a_1, \ldots, a_n \in \mathbb{R}$.