Polinomios

martes, 17 de diciembre de 2019 16:48

Grado

- Suma:

$gr(f+g) \leq \max(gr(f), gr(g))$

- Producto

$gr(f \cdot g) = gr(f) + gr(g)$ <=> estamos en un Dominio de Integridad

- Nº raíces de un polinomio f

nº raíces f $\leq gr(f)$

Teoremas

- K es un cuerpo <=> K[x] es un Dominio Euclídeo
- A es un DFU <=> A[x] es un DFU

Evaluación de un polinomio

- Si a es una raíz de f => $f(a) = 0$
- El resto de dividir f entre x-b nos da f(b)

Contenido

- El contenido es el mcd de los coeficientes
- Si $c(f) \in \mathcal{U}(A)$ => se dice que f es un polinomio primitivo

Polinomios primitivos

- Todo polinomio primitivo de grado 1 es irreducible
- Para polinomios primitivos de grado $\neq 1$, debemos comprobar si el polinomio tiene factores de grado menor o igual que la parte entera de la mitad de su grado:

Si $gr(f) = 7$, debemos comprobar si tiene factores de grado 1 (raíces), de grado 2 irreducibles ó de grado 3 irreducibles

Criterios de primalidad de polinomios

Criterio de Einsestein

Nos dice si un polinomio es irreducible. Si no prueba que sea irreducible, no prueba nada:

Un polinomio $f(x) = a_0 + \dots + a_n x^n \in A[x]$ $(A = DFU)$, será irreducible si existe un primo $p \in A$ que cumple que:

- $p \mid a_i \quad \forall i = \{0, \dots, n-1\}$. Es decir, divide a todos los coeficientes menos al líder
- $p^2 \nmid a_0$. Es decir, que el primo al cuadrado no divide al término independiente.

Ej.: $x^{25} + 49x^6 + 21x + 7$

$\exists\, p = 7$ tq

$$7 \mid a_6$$
$$7 \mid a_1 \qquad \Rightarrow \qquad 7^2 \nmid a_0$$
$$7 \mid a_0 \qquad\qquad 49 \nmid 7$$
$$7 \nmid a_{25}$$

Criterio de reducción por módulo primo

Sean A y B dos anillos, y $f : A \xrightarrow{morf} B$ un morfismo entre ellos.

Consideraremos el morfismo inducido $f: A[x] \to B[x]$ entre sus dos anillos de polinomios

En particular, usaremos el morfismo inducido:

$$f: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x] \quad \text{para } p = \text{un primo}$$

Para un polinomio $p(x) \in \mathbb{Z}[x]$ siempre se cumplirá que:

$$gr(p(x)) \geq gr(f(p(x))).$$

Teorema: Sea $f: A \to B$ un morfismo entre dos anillos y

$f: A[x] \to B[x]$ el morfismo inducido entre sus anillos de polinomios:

Si f conserva el grado para cualquier $p(x) \in A[x]$, se cumple que si $p(x)$ es reducible, $f(p(x))$ también lo es.

Si $p(x)$ es reducible, $f(p(x))$ también lo es.

Para aplicar esto como criterio de primalidad, usaremos el contrarrecíproco:
Si $f(p(x))$ es irreducible $\Rightarrow$ $p(x)$ es irreducible.

Polinomio de interpolación de Lagrange

Aplicaremos este método cuando los anteriores no hayan demostrado que el polinomio es irreducible.

Para aplicarlo, supondremos que el polinomio tiene un factor irreducible de grado 2.
Es decir $p(x) = f(x) \cdot g(x)$ con $f(x)$ ó $g(x)$ de grado 2

Para aplicar este método, tomamos a_0, a_1, a_2 para los que $p(a_i)$ tenga pocos divisores.

Los distintos b_i tendrán como posibilidades los divisores de $p(a_i)$.

Para cada combinación $a_0, a_1, a_2 - b_0, b_1, b_2$ (que cumpla los requisitos vistos con el criterio de Reducción módulo un primo), calculamos el polinomio de Lagrange.

$$L(x) = b_0 \frac{(x-a_1)(x-a_2)}{(a_0-a_1)(a_0-a_2)} + b_1 \frac{(x-a_0)(x-a_2)}{(a_1-a_0)(a_1-a_2)} + b_2 \frac{(x-a_0)(x-a_1)}{(a_2-a_0)(a_2-a_1)}$$

Para cada opción, comprobamos:

- Si $L(x) \in \mathbb{Z}[x]$
- Si $L(x) \mid p(x)$.

Si cumple ambas $\Rightarrow$ $L(x)$ es un factor irreducible de $p(x)$

Algoritmo para comprobar si un polinomio es irreducible (o factorizarlo)

$f(x) \nearrow \mathbb{Q}[x] \Rightarrow$ Saco denominador y contenido $\Rightarrow \mathbb{Z}[x]$
$\searrow \mathbb{Z}[x]$

P.1) Calculamos el contenido de f $c(f)$:

P.1) Calculamos el contenido de f $c(f)$:

- $c(f) \neq$ unidad $\Rightarrow$ es reducible $\Rightarrow f = c(f)\, f'$ $\Downarrow$ (P.2) con f' (primitivo) para factorizar
- $c(p)$ = unidad $\Rightarrow$ (P.2)

P.2) @pre: $f'(x)$ ya es primitivo

Comprobamos por Einsestein

- es reducible
- no lo es $\Rightarrow$ (P.3)

P.3) Buscamos factores de grado 1 (lineales)

$$ax+b \mid f(x) \iff f\left(\frac{-b}{a}\right) = 0$$

$$\left.\begin{array}{l} a \mid a_n \\ b \mid a_0 \end{array}\right\} \text{ Quitamos los negativos del } a$$

- Tiene factores lineales $\Rightarrow$ es reducible $\Rightarrow$ un factor es el $ax+b \mid f(x)$
- No tiene factores lineales (P.4)

P.4) @pre: f no tiene factores lineales y es primitivo

Reducimos módulo un primo: (hasta 3)

- Si mod p es irreducible $\Rightarrow$ es irreducible
- Si no es irreducible $\Rightarrow$ (P.5)

P.5) @pre: No ha servido ninguno de los criterios anteriores.

Aplicamos el método de Polinomio de interpolación de Lagrange