Anillos de polinomios

A = anillo

$A[x]$

$p(x) = a_n x^n + \cdots + a_1 x + a_0 \quad / \; a_i \in A$

↓ Coeficiente líder ↓ Término independiente

grado $(p(x)) = n$ (mayor exponente que aparece)

Dos polinomios son iguales si todos sus coeficientes son iguales.

Sea $A[x]$ con $p(x) = a_n x^n + \cdots + a_1 x + a_0$ y

$q(x) = b_m x^m + \cdots + b_1 x + b_0$, se define:

$p(x) + q(x) = \sum^{\max(n,m)} (a_i + b_i) x^i$, con $b_i = 0$ si $i > m$ $n \geq m$

$p(x) q(x) = \sum_{i=1}^{n+m} c_i x^i$ con $c_i = \sum_{r+s=i} a_r + b_s$.

$gr(p(x) + q(x)) \leq \max(gr(p(x)), gr(q(x)))$

$gr(p(x)\, q(x)) \leq gr(p(x)) + gr(q(x))$

→ La igualdad se dá en $A = DI$

$p(x) \in A[x]$

$a \in A \qquad ev._a : A[x] \xrightarrow{\text{morfismo}} A$

$p(x) \longmapsto p(a)$

$a \in A$ / a es raíz de $p(x) \iff p(a) = 0$

Dividir polinomios

$\mathbb{Z}_5[x]$

Podemos cojer como elementos $0, 1, 2, 3, 4$ o $0, 1, -1, 2$ y -2.

$$3x^4 + 2x + 2 \;\big|\; 2x^2 + x + 2$$

$$3 \cdot (2)^{-1} x^2 + 2^{-1} x + 2$$

$$(2)^{-1} \downarrow 3$$

$\Downarrow$ Luego

$$
\begin{array}{l|l}
\cancel{3x^4} + 2x + 2 & 2x^2 + x + 2 \\
\cancel{2x^4} + x^3 + 2x^2 & \hline 4x^2 + 3x + 2 \\
\hline
\cancel{x^3} + 2x^2 + 2x + 2 & \\
\cancel{-x^3} + 2x^2 + 4x + 2 & \\
\hline
\cancel{4x^2} + x + 2 & \\
\cancel{x^2} + 3x + 1 & \\
\hline
4x + 3 &
\end{array}
$$

Teorema:

$$
\begin{array}{l|l}
p(x) & x - a \\
\hline
p(a) & q(x)
\end{array}
$$

a es raíz de $p(x) \iff x - a \mid p(x)$

$p(x) = (x-a)(q(x)) + r$

$p(a) = 0 + r \Rightarrow \boxed{p(a) = r}$

¿Cuántas raíces tiene un polinomio?

A = Cuerpo o DI $\Rightarrow$ nº de raíces de $p \leq gr(p)$

K = cuerpo $\Rightarrow$ $K[x]$ = DE

A = DFU $\Rightarrow$ $A[x]$ = DFU

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

$A \subseteq \mathbb{Q}_A \longrightarrow$ Cuerpo de fracciones de A

$\mathbb{Z} \times \mathbb{Z}^*$

$(a,b) \sim (c,d) \overset{def}{\Leftrightarrow} ad = bc$

$[(a,b)] \underset{\text{se nota}}{=} \frac{a}{b}$

$A \times A^* / \sim \; = \mathbb{Q}$

Un polinomio es mónico si tiene coeficiente líder 1

Proceso de factorización (El esquema con los pasos está al final)

1) Sacamos el contenido (cf)

$cf = mcd(a_n \cdots a_1)$

Un polinomio es primitivo $\Leftrightarrow cf = 1$

Teorema

A = DFU

$f \in A[x]$

$f = cf \cdot f'$ $\quad f' =$ primitivo

Esta descomposición es única salvo asociados.

Teorema

$c(fg) = c(f)c$

Lema de Gauss

El producto de dos polinomios primitivos es primitivo.

Teorema

$A = DFU$

$f \in A[x]$

f = primitivo

/ f es irreducible en $A[x] \Leftrightarrow f$ es irreducible en $\mathbb{Q}[x]$

Luego:

$f(x) \in A[x]$ es irreducible
- $f(x)$ es irreducible en $\mathbb{Q}[x]$

ó
- Las constantes de $f(x)$ son irreducibles en A

$\boxed{\mathcal{U}(A[x]) = \mathcal{U}(A)}$

Para factorizar polinomios en $\mathbb{Q}_A[x]$:

$$f = \frac{1}{mcm} f' = \frac{c}{m} f' \to \text{primitivo}$$

Es unidad

Proposición

Todo polinomio de grado 1 es irreducible.

Polinomio irreducible en $A[x]$

- constantes irreducibles en A
- Polinomio irreducible en $\mathbb{Q}[x]$.

Teorema fundamental del álgebra

Todo polinomio no constante con coeficiente en $\mathbb{C}$ tiene una raíz compleja.

$$\left.\begin{array}{l} f \in \mathbb{C}[x] \\ gr(f) \geq 1 \end{array}\right\} \Rightarrow \alpha \in \mathbb{C} \,/\, f(\alpha) = 0$$

En la factorización de un polinomio se busca:

- constantes ⇒ unidades
- grado 1 ⇒ irreducible
- grado > 1 ⇒ posiblemente reducible

Si un polinomio de grado n primitivo es irreducible si no tiene factores hasta $\frac{n}{2}$

Lista polinomios irreducibles

$A = \mathbb{Z}_2$

- x
- $x+1$
- x^2+x+1
- x^3+x^2+1
- x^3+x+1

$A = \mathbb{Z}_3$

- x
- $x+1$
- $x-1$
- x^2+2x+1
- x^2+2x-1
- x^2+1

Factorizar en $\mathbb{Z}[x]$ ($\mathbb{Q}[x]$)

$A \xrightarrow{\varphi} B$ puedo encontrar $A[x] \xrightarrow[\varphi]{\text{morfismo}} B[x]$

$A, B = DFU$

$a_n x^n + \cdots + a_1 x + a_0$

$\varphi(f) = \varphi(a_n)x^n + \cdots + \varphi(a_1)x + \varphi(a_0)$

Proposición

$f \in A[x]$

$gr(f) = gr(\varphi(f))$

f se descompone como $f = gh$ entonces $\varphi(f) = \varphi(g)\varphi(a)$

factorización propia

No son unidades

Proposición

f factoriza con $(n, m) \Rightarrow \varphi(f)$ factoriza (n, m)

¡No puede perder grado!

Se suele usar el contrarecíproco:

$\boxed{\text{si } \varphi(f) \text{ no tiene factor de grado } n \Rightarrow f \text{ no tiene factor de grado } n}$

Corolario

$\varphi(f)$ irreducible $\Rightarrow f$ irreducible

A = DE (DIP)

$\frac{A}{nA} = \frac{A}{\langle n \rangle}$

$[b] \in \frac{A}{\langle n \rangle}$ es unidad $\Leftrightarrow \mathrm{mcd}(b, n) = 1$

$\frac{A}{\langle n \rangle}$ = cuerpo $\Leftrightarrow n$ = primo

Teorema

Un cuerpo tiene siempre una potencia de un primo de elementos.

La característica de un anillo se define como el menor entero positivo tal que $n \cdot 1 = 0$ o 0 si no hay ninguno:

- $\mathbb{Z}$ tiene característica 0
- $\mathbb{Z}_n$ tiene característica n.

Todo cuerpo tiene característica un primo o 0.

Criterios de primalidad

$$A \xrightarrow{\varphi\ \text{morfismo}} B$$

$$A[x] \xrightarrow[\varphi\ \text{morfismo}]{} B[x]$$

(No son el mismo φ)

(Si el primer φ es morfismo $\Rightarrow$ el segundo es morfismo)

$$\varphi(a_n x^n + \dots + a_0) := \varphi(a_n)x^n + \dots + \varphi(a_0)$$

- Reducción módulo primo:

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$$

$$6x^6 + 5x^2 + 82x + 7 \longmapsto x^2 + 1 \qquad gr(\varphi(p)) \leq gr(p)$$

Teorema

A y B = DFU

$\varphi: A \to B$ morfismo

$\varphi: A[x] \to B[x]$ morfismo

$p(x) \in A[x]$ primitivo

$gr(p) = gr(\varphi(p))$ ¡OJO! ¡NO PUEDE PERDER GRADO!

p = reducible $\Rightarrow$ $\varphi(p)$ = reducible

suele usarse el contrarrecíproco:

$\varphi(p)$ = irreducible $\Rightarrow$ p = irreducible.

Ver si $p(x) = x^4+3x^2+1$ es irreducible:

$P_2(x) = p(x) \bmod 2 = x^4+3x^3+1$

$$\left.\begin{array}{l} p_2(0) = 1 \\ P_2(1) = 1 \end{array}\right\} \Rightarrow \text{No tiene factores grado } 1$$

$x^4+x^3+1 \quad \underline{|\, x^2+x+1}$

No lo divide

$p(x)$ irreducible en $\mathbb{Z}_2[x] \Rightarrow p(x)$ irreducible en $\mathbb{Z}[x]$

Del teorema anterior se extrae:

si p tiene factor de grado $r \Rightarrow \varphi(p)$ tiene factor grado r.

Suele usarse el contrarrecíproco.

- Criterio de Eisenstein (¡ No vale en $\mathbb{Q}[x]$!) :

A = DFU

$f(x) \in A[x]$

p = primo $\in A$ con $f(x) = a_n x^n + \dots + a_0$ primitivo

$$\left.\begin{array}{l} p \text{ no divide a } a_i \text{ para } i \neq n \\ p^2 \text{ no divide a } a_0 \\ p \text{ no divide a } a_n \end{array}\right\} \Rightarrow f \text{ irreducible}$$

Pasos:

$f(x)$ — $\mathbb{Q}[x]$, → Lo llevo a $\mathbb{Z}[x]$
— $\mathbb{Z}[x]$

1) calcular el contenido

$$c_f = \text{mcd}(a_n, \dots, a_0)$$

si no es una unidad, el polinomio es reducible y ya tienes una factorización

2) $f' =$ primitivo. Aplico Eisenstein

$$\left.\begin{array}{l} f'(x) = a_n x^n + \dots + a_0 \\ p \in \mathbb{Z}_{\langle primo \rangle} / p \mid a_i \quad i = 0, \dots, n-1 \\ p \nmid a_n \wedge p^2 \nmid a_0 \end{array}\right\} \Rightarrow f' = \text{irredu.}$$

3) Busco factores de grado 1:

$$ax + b \mid f = a_n x^n + \dots + a_0$$

$$\left.\begin{array}{l} a \mid a_n \\ b \mid b_0 \end{array}\right\} f = (ax+b)g$$

4) si no tiene factores lineales reducimos módulo primo:

2, 3 | , 5, 7 ...
→ En el examen hasta ahí

¡No puede perder grado!

si f_p = irreducible ⇒ f = irreducible

si no sale irreducible vemos si f_p no tiene factores de grado r ⇒ f no tiene factores grado r.

5) " Toy desesperao"

Intentar no darlo a no ser que tengamos alguna pista o algo.

Pensamos que el polinomio es reducible:

Busco factores de grado 2:

$gr(g)=2 \quad g|f \quad g(a)|f(a)$

$f=gh \quad f(a)=g(a)h(a)$

$$\left.\begin{array}{l} g(a_0)=b_0 \\ g(a_1)=b_1 \\ g(a_2)=b_2 \end{array}\right\} \iff \left\{\begin{array}{l} g=b_0 \bmod (x-a_0) \\ g=b_1 \bmod (x-a_1) \\ g=b_2 \bmod (x-a_2) \end{array}\right.$$

Luego:

$$g \equiv g_0 \bmod \frac{(x-a_0)(x-a_1)(x-a_2)}{3}$$

Para resolverlo más fácil utilizamos el polinomio de interpolación de Lagrange:

- Para grado 2:

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

$$+b_1\frac{(x-a_0)(x-a_2)}{(a_1-a_0)(a_1-a_2)}+$$

$$+b_2\frac{(x-a_0)(x-a_1)}{(a_2-a_0)(a_2-a_1)}$$

Elijo 3 a_i y calculo todos sus divisores, calculo todos los polinomios de Lagrange. Si tiene coeficientes en $\mathbb{Q}[x]$ descartamos. Si tiene en $\mathbb{Z}[x]$ vemos si divide al nuestro