Polinomios

Sea $\mathbb{K}$ un cuerpo $(\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z})$

p = Primo

$\mathbb{K}$) $\mathbb{K}[x]$ el anillo de polinomios con coeficientes en $\mathbb{K}$

$$\mathbb{K}[x] = \sum_{i=0}^{n} a_i x^i \quad : a_i \in \mathbb{K}$$

En $\mathbb{K}[x]$ hay suma y Producto de Polinomios

+) $F = \sum_{i=0}^{n} a_i x^i \qquad g = \sum_{j=0}^{m} b_j x^j$

$$F + g = \sum_{i=0}^{\max(n;m)} (a_i + b_i) x^i$$

·) $$F \cdot g = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j \cdot b_{i-j} \right) x^i \qquad \text{(distributiva)}$$

Prop: $(\mathbb{K}[x], +, \cdot)$ es un anillo conmutativo con unidad $(F = 1)$

Propiedad fundamental: El grado del polinomio. (La máx potencia de x)

Si $F \in \mathbb{K}[x]$ y $F \neq 0$ El grado de F es el máx $i \in \mathbb{N}_0 \,/\, a_i \neq 0$

obs: el polinomio $F = 0$ no tiene grado

Prop del grado:
- $gr(F+g) \leq \max(gr(F); gr(g))$
- Si $gr(F) \neq gr(g) \Rightarrow gr(F+g) = \max(gr(F); gr(g))$
- $gr(F \cdot g) = gr(F) + gr(g)$

Coeficiente principal

Sea $F \in \mathbb{K}[x]$, $gr(F) = n \Rightarrow a_n$ es el coef Principal $(a_n \neq 0)$

Notacion: al coeficiente principal de f lo llamamos $c(f)$

Ej: si $f = \sqrt{2}\,x^3 + 3x - 4i$ $\quad F \in \mathbb{C}[x]$, $gr(f) = 3$

$\Longrightarrow c(f) = \sqrt{2}$

obs: $F = 0$ no tiene coef Principal

Prop: Sean $f, g \in \mathbb{K}[x]$ $\quad f, g \neq 0 \Longrightarrow c(f \cdot g) = c(f) \cdot c(g) \neq 0$

Def: Polinomio mónico $\Leftrightarrow$ Coef Principal $= 1$

Ej: $x^n + 1 \in \mathbb{K}[x]$ para cualquier cuerpo $\mathbb{K}$

obs: si $F \in \mathbb{K}[x]$ $\quad F \neq 0$

entonces $\dfrac{1}{c(F)} \cdot F$ es un polinomio mónico con el mismo grado de F

eg: $F = \sqrt{2}\,x^3 + 3x - 4i$

$\dfrac{F}{c(F)} = x^3 + \dfrac{3}{\sqrt{2}}x - \dfrac{4i}{\sqrt{2}}$ (Pol mónico)

Prop: $(\mathbb{K}, \cdot, +)$ anillo conmut con unidad

los unidades del anillo son los elementos inversibles $\left(F \in \mathbb{K}[x] \,/\, \exists\, g \in \mathbb{K}[x] : F \cdot g = 1\right)$

$\downarrow$

Polinomios constantes $(gr = 0)$

Dem: si $F \cdot g = 1 \Rightarrow gr(F \cdot g) = gr(1) = 0 \Longrightarrow gr(F) + gr(g) = 0$ si:

si: $gr(F) = gr(g) = 0$ (ambos constantes)

Teorema: $\mathcal{U}(\mathbb{K}[x]) = \mathcal{U}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$

HOJA Nº

FECHA

Divisibilidad de polinomios

Dados $f, g \in \mathbb{K}[x]$ g divide a f si:

$$\exists\, p \in \mathbb{K}[x] \;/\; f = g \cdot p \qquad \text{Notación } g \mid f$$

* aplican las mismas prop que estudiamos en $\mathbb{Z}$ (alg. div, mcd, etc)

Prop) • $g \mid 0$

• $g \mid f \Rightarrow c \cdot g \mid f \quad \forall c \in \mathbb{K} \setminus \{0\}$

y

$g \mid cf \quad \forall c \in \mathbb{K}$

• $g \mid f \Rightarrow gr(g) \leq gr(f)$

• $g \mid f$ y $f \mid g \Rightarrow f = c \cdot g \quad c \in \mathbb{K} \setminus \{0\}$

• $g \mid f \wedge gr(f) = gr(g) \Rightarrow f = c \cdot g \quad c \in \mathbb{K} \setminus \{0\}$

Polinomios irreducibles

$f \in \mathbb{K}[x]$ es irreducible si: $\nexists\, g \in \mathbb{K}[x] \quad gr(g) > 0 \;/\; g \mid f$

(f no tiene divisores propios)

f es reducible si $f = g \cdot p$ con $gr(g) \neq 0 \neq gr(p)$

Ej: • los polinomios de grado 1 son irreducibles

• $x^2 + 1$ es irreducible en $\mathbb{R}[x]$ xq no tiene raices reales
es reducible en $\mathbb{C}[x]$

NOTA $x^2 + 1 = (x+i)(x-i)$

- $x^2 - 2$ es irreducible en $\mathbb{Q}[x]$
  es reducible en $\mathbb{R}[x]$

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

- obs: i) en $\mathbb{Q}[x]$ hay polinomios de todos los grados
  ii) en $\mathbb{R}[x]$ los irreducibles son de gr 1 y algunos de gr 2
  iii) TF Algebra $\Rightarrow$ en $\mathbb{C}[x]$ los irreducibles solo son de gr 1

- ej $x^2 - 3$ es irreducible en $\mathbb{Z}/7\mathbb{Z}$

Algoritmo de la división

$F, g \in \mathbb{K}[x]$ no nulos $\exists!\ q, r \in \mathbb{K}[x] \ /\ F = g \cdot q + r$

$r = 0$ ó $gr(r) < gr(g)$

Dem: Sea $A = \{F - g \cdot q : q \in \mathbb{K}[x]\}$

$F \in A$ (tomando $q = 0$) $\Rightarrow A \neq \emptyset$

Si $0 \in A \Rightarrow 0 = F - g \cdot q \Rightarrow F = g \cdot q$ y tomamos $r = 0$

si $0 \notin A$ tomamos $r \in A$ un polinomio de grado mínimo

Veamos que $gr(r) < gr(g)$

Supongamos que no: entonces tomamos $\tilde{r} = r - x^{(gr\,r - gr\,g)} \cdot g \cdot \frac{c(r)}{c(g)}$

$\Rightarrow gr(\tilde{r}) < gr(r)$ además $\tilde{r} \in A \Rightarrow \tilde{r} \neq 0$

ABSURDO pq r es de grado mín en A

Hemos concluido que $\exists r \in A \ /\ F = g \cdot q + r$ y

$r = 0$ ó $gr(r) < gr(g)$

ej: $r = 5x^4 - 3x - 2$

$g = 2x^3 - 1$

$\tilde{r} = r - \frac{5}{2} \cdot x \cdot g$

NOTA

HOJA Nº

FECHA

Veamos ahora que r y q son únicos.

Supongamos que: $F = g \cdot q + r \quad r = 0 \text{ ó } gr(r) < gr(g)$

$F = g \cdot \tilde{q} + \tilde{r} \quad \tilde{r} = 0 \text{ ó } gr(\tilde{r}) < gr(g)$

Entonces $g(q - \tilde{q}) = -r + \tilde{r} \implies g \mid r - \tilde{r}$

esto $\implies r - \tilde{r} = 0 \implies r = \tilde{r}$

Entonces $g(q - \tilde{q}) = 0 \implies q - \tilde{q} = 0 \implies q = \tilde{q}$

MCD

Dados $F, g \in \mathbb{K}[x]$ no ambos nulos, el mcd entre ellos es el único polinomio mónico $(F:g) \in \mathbb{K}[x]$ / a) $(F:g) \mid F$

b) $(F:g) \mid g$

c) $(F:g)$ es mónico

d) $(F:g)$ es el polinomio de mayor grado que verifica (a) (b) y (c)

$(F:g) \in Div_{món}(F) \cap Div_{món}(g)$

de grado máx

obs: no es obvio que $(F:g)$ es único

Teorema: $(F:g)$ es combinación lineal de F y g, es decir,

$\exists\, h, f \in \mathbb{K}[x]$ / $(F:g) = F \cdot h + g \cdot f$

además si $d \mid F$ y $d \mid g \implies d \mid (F:g)$

además $\forall\, l, h \in \mathbb{K}[x] \quad (F:g) \mid F \cdot l + g \cdot h$

además es único.

NOTA