13/12/2021

POLINOMI (in una indeterminata)

Un polinomio nell' indeterminata x a coefficienti in A (anello) è una scrittura formale del tipo

SOMMA FORMALE [la scrittura per ordinare POLINOMI]

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

dove $a_i \in A$ $\quad n \in \mathbb{N}_0$

NUMERO FINITO di ELE.

DEGREE

$$\text{GRADO}(P) = \text{MAX}\{i \in \mathbb{N}_0 : a_i \neq 0\}$$

$P \equiv 0$ $\qquad \text{DEG}(0) = -\infty$

SOMMA

$$P(x) + q(x) = \sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j$$

$$= \sum_{i=0}^{\text{MAX}\{n,m\}} (a_i + b_i) x^i$$

$$p(x) = 1 + x^3 = 1 + 0x + 0x^2 + 1x^3 \quad +$$

$$q(x) = 3x + x^2 = 0 + 3x + 1x^2 + 0x^3 \quad =$$

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

PRODOTTO

$$P(x) \cdot q(x) = (1 + x^3)(3x + x^2) = 3x + x^2 + 3x^4 + x^5$$

$$\text{DEG}(p \cdot q) = \text{DEG}(p) + \text{DEG}(q)$$

non è VERO in generale

ANELLO $\mathbb{Z}_n$

$\mathbb{Z}_6$ in $\mathbb{Z}_6$, $6 \equiv 0 \mod 6$

$(2x^3+x)(3x+1) = \cancel{6x^4} + 2x^3 + 3x^2 + x$

sono 0 divisori

ma in UN DOMINIO vale di INTEGRITÀ

$DEG(p+q) \leq MAX\{DEG(p), DEG(q)\}$

se $q = -p$

$p+q \equiv 0$ $\quad \boxed{-\infty \leq DEG(p)}$

$\mathbb{Z} \longrightarrow$ ALGORITMO divisione EUCLIDEA

$\boxed{n = qm + r}$ $\quad 0 \leq r \leq m-1$

$n, m > 0$

A DOMINIO

dati due polinomi $p(x), s(x) \neq 0$

$p(x)$ e $s(x)$ A coefficienti in A

$\partial = DEG$

$\Rightarrow \exists!\ q(x)$ e $r(x)$ t.c.

$p(x) = s(x)\, q(x) + r(x)$

con $r(x) \equiv 0$ oppure

$DEG(r) < deg(s)$ POLINOMIO DI GRADO INFERIORE

$\mathbb{Z}_3[x]$

$p(x) = x^4 + 2x^2 + x + 1 \qquad s(x) = 2x^3 + x + 1$

se $s(x)$ divido $p(x) \Rightarrow s(x) = 0 \cdot p(x) + s(x)$

se $p(x)$ divido $s(x)$

GRADO 3 MOLTIPLICO

$$
\begin{array}{lll|l}
x^4 & +2x^2 & +x+1 & 2x^3+x+1 \\
\hline
x^4 & 2x^2 & +2x & 2x \\
\hline
0 & 0 & 2x+1 &
\end{array}
$$

DIFF

GRADO 1
RESTO

$\frac{1}{2} = \alpha$

$2\alpha = 1$

4 in $\mathbb{Z}_3$ è 1

$$x^4 + 2x^2 + x + 1 = (2x^3 + x + 1) \cdot 2x + 2x + 1$$

$MCD(P(x), S(x)) = ?$

$$P(x) = q_0(x) S(x) + r_0(x)$$

$$S(x) = q_1(x) r_0(x) + r_1(x) \qquad \partial r_1 < \partial r_0$$

$$r_0(x) = q_2(x) r_1(x) + r_2(x)$$

$\vdots$

MCD

$$r_n = q_{n+2} \boxed{r_{n+1}(x)} + 0$$

ultimo resto non NULLO

è un algoritmo anche termina

$MCD(f(x), g(x)) = 2\, d(x)$

in $A[x]$ gli unici elementi INVERT sono el INV. in A

$\mathbb{Z}_3[x] \supset \{0, 1, 2, 3\}$

$\mathbb{Z}_6[X] = \{0, 1, 2, 3, 5, 6\}$

unici INV.

se

$\mathbb{Z}[x]$ è VERO $\{1$ e $-1\}$

RADICE di un POLINOMIO

somma FORMALE

$P(X) \in A[X]$ $\quad$ $p(x) = \boxed{\sum_{i=0}^{n} a_i x^i}$

$\alpha \in A$ si dice radice se

$p(\alpha) = 0 \qquad p(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in A$

$p(x) = 1 + x^3 \in \mathbb{R}[X]$ somma formale

$p(2) = 1 + 2^3 = 9 \in \mathbb{R}$

$p(-1) = 1 - 1^3 = 0$

MOLTEPLICITÀ di una RADICE

$\alpha \in A$ $\quad$ α è una radice di $p(x)$ di MOLTEPLICITÀ
$m \in \mathbb{N}_0$ se $\quad$ 0 non sono radici

$(x-\alpha)^m \mid p(X) \in (x-\alpha)^{m+1} \nmid P(X)$

TH: α è una radice di $P(X) \Leftrightarrow (x-\alpha) \mid P(X)$

$p(x) = 1 + x^3$

(-1) radice di $p(x)$

$(x \overset{-(-1)}{+1}) \mid (1 + x^3)$ $\qquad$ $x^3 + 0x^2 + 0x + 1 \;\Big|\; \dfrac{x+1}{x^2 - x + 1}$

$(x+1) \mid (1+x^3) = (x+1)(x^2-x+1)$

$(x+1)^2 \mid (x^3+1)$?

$= (x+1) \mid x^2-x+1$ $\qquad\qquad$ $x^2-x+1 \mid \underline{x+1}$

la divisione avviene

se e solo se -1 è una radice di

$(-1)-(-1)+1=3$

↳ doveva essere 0

se stiamo in $\mathbb{Z}_3$ SI!!

$\mathbb{Z}_3[x]$ $\qquad$ $x^3+1 = (x+1)^3$ la molteplicità è 3

$x^p + y^p = (x+y)^p$

in $\mathbb{Z}_p$

$(x+1)^n \mid x^3+1 = (x+1)^3$