ARITMETICA 27 NOV 2017

Note Title 11/27/2017

POLINOMI (in una variabile)

A anello. Polinomi a coefficienti in A

$A[X]$

Gli elementi di $A[X]$ sono espressioni formali

$f \in A[X]$ è del tipo

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

dove $a_i \in A$

ed è una somma finita di monomi $a_i X^i$.

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$
$$g = b_m X^m + b_{m-1} X^{m-1} + \dots + b_0$$

+ (si può supporre $n = m$, eventualmente aggiungendo dei termini $= 0$)

$$f + g = \sum_{i=0}^{n} (a_i + b_i) X^i.$$

- Si definisce in modo che valga la proprietà distributiva

$$a_i X^i \cdot b_j X^j = a_i b_j X^{i+j}.$$

$$f \cdot g = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j X^{i+j}.$$

$$= \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^k$$

I termini iniziale e finale sono semplicemente $a_n b_m X^{n+m}$ e $a_0 b_0$

In questo modo $A[X]$ diventa un anello.

I casi che considereremo sono:

$$A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}.$$

Def. Se $f \in A[X] \setminus \{0\}$,

$$f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$

si dice **grado** di f

$$\deg f = \max \{ i \in \mathbb{N} \mid a_i \neq 0 \}.$$

(Qualche volta si dice $\deg 0 = -\infty$)

Proprietà del grado:

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

$$\deg(fg) = \deg f + \deg g \quad (*)$$

(+) $\leq$ e non uguale perché

$$(X^2 + X) + (-X^2 - 1) = X - 1$$

(·) (*) In realtà l'uguaglianza vale solo se A è un dominio di integrità (non ci sono divisori di zero non banali).

Polinomi a coefficienti in un campo K.

$K[X]$ (Casi essenziali, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$)

DIVISIONE EUCLIDEA

Prop. Siano $f, g \in K[X]$, $g \neq 0$. Allora esistono e sono unici due polinomi $q, r \in K[X]$ tali che:

- $f = qg + r$
- $\deg r < \deg g$ oppure $r = 0$.

DIM. Esistenza. Sia $n = \deg g$.

Induzione su $m = \deg f$.

(Se $f = 0$ posso porre $f = 0 = 0 \cdot g + 0$ $q = r = 0$).

1° caso: $n = 0$. $g = k \in K$ $k \neq 0$.

$$f = (k^{-1}f)k + 0$$

$q = k^{-1}f$ $r = 0$.

2° caso: $n > 0$.

Casi iniziali dell'induzione: $m < n$.

$$f = 0 \cdot g + f \qquad q = 0 \quad r = f.$$

Passo induttivo: $m - 1 \Rightarrow m$ $(m \geq n)$

$$f = a_m X^m + \dots$$
$$g = b_n X^n + \dots$$

Considero: $a_m b_n^{-1} X^{m-n} g$.

Il termine di grado più alto di questo polinomio è

$$a_m b_n^{-1} X^{m-n} \cdot b_n X^n = a_m X^m$$

= termine di grado più alto di f.

Quindi $\deg \left(f - a_m b_n^{-1} X^{m-n} g \right) < m$

Per ipotesi induttiva

$$f - a_m b_n^{-1} x^{m-n} g = q' g + r'$$

$$f = (a_m b_n^{-1} x^{m-n} + q') g + r' \quad \text{OK}$$

Unicità: supponiamo $f = qg + r = q'g + r'$.

Ne segue: $(q - q')g = r' - r$

Guardiamo i gradi:

A sinistra ho $\deg((q-q')g) = \deg(q-q') + \deg g$

(se $q \neq q'$, $q - q' \neq 0$, allora questo grado è $\geq \deg g$)

A destra ho $\deg(r' - r) \leq \max(\deg r', \deg r) < \deg g$.

oppure $r' - r = 0$.

$\Rightarrow r' - r = 0 \quad r' = r$.

$(q - q')g = 0 \Rightarrow q = q'$.

ALGORITMO DI EUCLIDE PER IL MCD.

(Nota: d si dice un massimo comun divisore fra due polinomi f, g NON ENTRAMBI NULLI se:

- $d \mid f$, $d \mid g$
- $h \mid f$, $h \mid g \Rightarrow h \mid d$.)

Elementi invertibili di $K[X]$

(cioè che hanno un inverso per la moltiplicazione).

Prop. $f \in K[X]$ è invertibile $\Leftrightarrow \deg f = 0$.

Dim. Se $\deg f = 0$ $f = a_0 \neq 0$ $f^{-1} = a_0^{-1}$.

Viceversa, se f è invertibile, allora esiste $g \in K[X]$

tale che $fg = 1$

$\deg(fg) = \deg f + \deg g = \deg 1 = 0$.

$\Rightarrow \deg f = \deg g = 0$.

Prop. Siano d_1, d_2 due MCD fra f e g.
Allora esiste una costante $c \neq 0$ tale che

$$d_1 = c\, d_2.$$

Dim. $d_1 = MCD \Rightarrow d_1 \mid f,\ d_1 \mid g$

$d_2 = MCD \Rightarrow d_1 \mid d_2$ (1)

SIMMETRICAMENTE, $d_2 \mid d_1$. (2)

(1) $d_2 = h d_1$ (2) $d_1 = k d_2$

$d_2 = h k d_2$

$d_2 (1 - hk) = 0$.

$\Rightarrow 1 - hk = 0 \qquad hk = 1$

h e k sono costanti.

Conclusione: Il MCD fra f e g (f,g) è definito a meno di una costante $\neq 0$.
Un elemento privilegiato (stesso detto IL MCD) è il polinomio MONICO (= con 1° coeff = 1).

Def 1 Un polinomio $f \in K[X]$, $f \neq 0$ e f non invertibile si dice PRIMO se

$$f \mid gh \Rightarrow f \mid g \text{ o } f \mid h$$

Def 2 Un polinomio $f \in K[X]$, $f \neq 0$ e f non invertibile si dice IRRIDUCIBILE se

$$f = gh \Rightarrow g \text{ invertibile o } h \text{ invertibile}$$

(Se f non è irriducibile, allora f è il prodotto di due polinomi di grado >0).

Prop. PRIMO $\Leftrightarrow$ IRRIDUCIBILE

Dim. $\Rightarrow$ Sia f primo e supponiamo che $f = gh$. In particolare $f \mid gh$.

Quindi: $f \mid g$ o $f \mid h$

$g = fe$ $\qquad$ $h = fm$

$f = fgh$

$f = gfm$

$eh = 1$ o $gm = 1$

h invertibile $\qquad$ g invertibile

$\Leftarrow$ Sia f irriducibile e supponiamo che $f \mid gh$

Consideriamo $(f, g) = \begin{cases} 1 & \Rightarrow f \mid h \\ f & \Rightarrow f \mid g \end{cases}$.

(Se $a \mid bc$ $\quad (a, b) = 1$ allora $a \mid c$)

TEO (DI FATTORIZZAZIONE UNICA in $K[X]$)
Ogni polinomio diverso da 0 si scrive in modo unico* come prodotto di una costante $\neq 0$ e di fattori irriducibili.

* A meno dell'ordine e a meno di moltiplicazione dei fattori per una costante $\neq 0$.

DIM. Esistenza. Se f è irriducibile, ok
se no $f = gh$ $\deg g < \deg f$ e $\deg h < \deg f$.
e la dimostrazione si conclude per induzione

Unicità $f = p_1 \cdots p_r = q_1 \cdots q_s$
$p_1 \mid q_1 \cdots q_s \Rightarrow p_1 \mid q_i$ per qualche i.

Possiamo supporre che $p_1 \mid q_1$. cioè $q_1 = p_1 c$
c costante
Dimo:

$$\frac{f}{p_1} = p_2 \cdots p_r = c\, q_2 \cdots q_s$$

(Induzione sul n° dei fattori).

RADICI DI UN POLINOMIO.

POLINOMI $\xrightarrow{\phi}$ FUNZIONI POLINOMIALI
Espressioni formali

$F : K \to K$
$F(x) = f(x)$
dove $f(x)$ è un pol.

ϕ è INIETTIVA?
$F : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$

$f(x) = x^p - x \neq 0$
$F \equiv 0$ $F(x) = 0 \quad \forall x \in \mathbb{Z}/p\mathbb{Z}$.