ARITMETICA 4 DIC 2017

Note Title 12/4/2017

$f \in \mathbb{Q}[X] \Rightarrow f = \frac{1}{d} g \qquad g \in \mathbb{Z}[X]$

(d = m.c.m. dei denominatori dei coeff. di f).

Def. Sia $f \in \mathbb{Z}[X]$. Si dice CONTENUTO di f, $c(f)$ il MCD dei coefficienti di f.

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

$c(f) = MCD(a_n, a_{n-1}, \dots, a_0)$.

Lemma 1 Se $f, g \in \mathbb{Z}[X]$, allora

$$c(fg) = c(f)\,c(g).$$

Dim. Primo caso: supponiamo $c(f) = c(g) = 1$ e dimostriamo che $c(fg) = 1$

Per assurdo: se $c(fg) \neq 1$, allora esiste un numero primo p tale che $p \mid c(fg)$.

Consideriamo i polinomi modulo p

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

$\bar{f} = \bar{a}_n X^n + \bar{a}_{n-1} X^{n-1} + \dots + \bar{a}_0$

dove $\bar{a}_i$ è la classe di a_i modulo p.

Esempio: $f = 5X^2 + 4X - 2$

$p = 3 \qquad \bar{f} = \bar{5} X^2 + \bar{4} X - \bar{2} = \bar{2} X^2 + \bar{X} + \bar{1}$

Si ha ovviamente che $\overline{fg} = \bar{f} \cdot \bar{g}$

Nella nostra ipotesi assurda $\overline{fg} = \bar{0}$

Ma $\bar f \neq \bar 0$, $\bar g \neq \bar 0$

$\bar f \neq \bar 0$, $\bar g \neq \bar 0$ $\quad \bar f \bar g = \bar 0$

CONTRADDIZIONE

$\bar f, \bar g, \bar{fg} \in \mathbb{Z}/p\mathbb{Z}[x]$

↓

CAMPO

Caso generale

Ogni polinomio $f \in \mathbb{Z}[x]$ si può scrivere nella forma

$$f = c(f) f_1$$

dove f_1 è PRIMITIVO (cioè $c(f_1) = 1$).

$f = c(f) f_1 \qquad g = c(g) f_1$

$$fg = c(f)c(g) \underbrace{f_1 g_1}_{1}$$

PRIMITIVO

$$\Rightarrow \quad c(fg) = c(f)\, c(g).$$

Lemma 2 Siano $f, h \in \mathbb{Z}[x]$ tali che:

1. $h \mid f$ in $\mathbb{Q}[x]$
2. h è primitivo.

Allora $h \mid f$ in $\mathbb{Z}[x]$.

($h \mid f$ in $\mathbb{Q}[x]$: $\exists\, g \in \mathbb{Q}[x]$ t.c. $f = hg$)

($h \mid f$ in $\mathbb{Z}[x]$: $\exists\, g \in \mathbb{Z}[x]$ t.c. $f = hg$)

Dim. Sia $g \in \mathbb{Q}[x]$ t.c. $f = hg$

$$g = \frac{1}{d} g' \qquad g' \in \mathbb{Z}[x] \qquad g' = \underbrace{c(g')}_{a} g_1 = a g_1$$

con $g_1 \in \mathbb{Z}[x]$ PRIMITIVO.

$$g = \frac{a}{d} g_1$$

$f = h\left(\frac{a}{d} g_1\right)$ $\qquad df = a \underbrace{h g_1}_{\text{PRIMITIVO}}$

Il contenuto del polinomio a destra è $\boxed{a}$.

" " " a sinistra è un multiplo di d.

Quindi dica, osserva $\frac{a}{d} \in \mathbb{Z}$.

$g = \frac{a}{d} g_1 \Rightarrow g \in \mathbb{Z}[x]$.

LEMMA DI GAUSS Se $f \in \mathbb{Z}[x]$ si scrive come prodotto $f = gh$ con $g, h \in \mathbb{Q}[x]$ allora si scrive anche come $f = g'h'$ con $g', h' \in \mathbb{Z}[x]$ con $\deg g' = \deg g$ e $\deg h' = \deg h$.

$$\left[x^2 - 1 = (3x-3)\left(\frac{1}{3}x + \frac{1}{3}\right) = (x-1)(x+1) \right]$$

Dim. $f = gh$ $\qquad g, h \in \mathbb{Q}[x]$

$g = \frac{a}{b} g_1$ $\qquad h = \frac{c}{d} h_1$

g_1, h_1 PRIMITIVI

$f = \frac{a}{b}\frac{c}{d} g_1 h_1$ $\qquad bd f = ac \underbrace{g_1 h_1}_{\text{PRIMITIVO}}$

$bd \mid ac$

Quindi $\frac{a}{b}\frac{c}{d} \in \mathbb{Z}$. $\qquad f = \left(\frac{a}{b}\frac{c}{d}\right) g_1 \cdot h_1$

(coeff interi).

$\deg g = \deg g_1$
$\deg h = \deg h_1$

Riassunto: LA FATTORIZZAZIONE di polinomi $f \in \mathbb{Q}[X]$ si riconduce alla fattorizzazione di polinomi $f' \in \mathbb{Z}[X]$.

Esempi di "trucchi" che possono aiutare per cercare la fattorizzazione di un pol. $f \in \mathbb{Z}[X]$.

Esempio 1 $\quad f = gh$ | primo

$$\bar{f} = \bar{g}\bar{h}$$

Se $f = a_n X^n + \dots$ e $p \nmid a_n$ allora $\bar{f}$ ha lo stesso grado di f.

SUPPONIAMO VERA QUESTA CONDIZIONE

Se f è RIDUCIBILE, allora anche $\bar{f}$ è RIDUCIBILE
Altrimenti: $\bar{f}$ IRRID. $\Rightarrow$ f IRRID.

$$f = 2017X^3 + 1402X^2 + 1961X + 10001$$

$p = 2 \quad \bar{f} = X^3 + X + 1$

modulo 2 non ci sono radici (basta guardare $\bar{0}, \bar{1}$)

$\bar{f}$ IRR. $\Rightarrow$ f IRR.

Esempio 2 (CRITERIO DI EISENSTEIN)

$f \in \mathbb{Z}[X]$ $\quad f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$

Supponiamo che esista un primo p tale che:

(1) $p \nmid a_n$

(2) $p \mid a_{n-1}, p \mid a_{n-2}, \dots, p \mid a_0$

MA $p^2 \nmid a_0$.

Allora f è irriducibile.

Dim. Supponiamo, per assurdo f RIDUCIBILE, quindi $f = gh$ con $\deg g < n$, $\deg h < n$.

$\deg g \geq 0$ e $\deg h \geq 0$

Riducendo modulo p ottengo $\bar{f} = \bar{g}\bar{h}$

$$\bar{f} = \bar{a}_n X^n = \bar{g}\bar{h}$$

$$\bar{g} = \bar{b}_r X^r \qquad \bar{h} = \bar{c}_s X^s \qquad r+s=n, \quad r,s>0$$

Il termine noto di $\bar{g}$ e di $\bar{h}$ è uguale a $\bar{0}$,

" " " di g e di h è divisibile per p.

" " " di $g \cdot h$ (= f) è divisibile per p^2.

CONTRO L'IPOTESI.

GLI IDEALI DI $K[X]$ (K campo).

(Analogo degli ideali di $\mathbb{Z}$).

Oss. 1 Se $f \in K[X]$ allora $I = \{ gf \mid g \in K[X] \}$ è un ideale

Dim. sgr: $0 \in I$ $\quad 0 = 0 \cdot f \in I$

+ $\quad gf, hf \in I \Rightarrow gf + hf = (g+h)f \in I$

$gf \in I \Rightarrow -gf = (-g)f \in I.$

moltiplicazione:

$gf \in I \quad h \in K[X] \Rightarrow hgf \in I$

$\uparrow$

$(hg)f$

Prop. Gli ideali di $K[X]$ sono tutti e soli della forma

$$(f) = \{gf \mid g \in K[X]\}$$

(= MULTIPLI di qualche polinomio f).

Dim. Se $I = \{0\}$ è ovvio (multipli di 0).

Se $I \neq \{0\}$ I possiede un el $\neq 0$ di grado minimo (fra i gradi dei pol. $\in I$).

Chiamo $f \in I$ un pol. di grado minimo.

Tesi: $I = (f)$

$I \supseteq (f)$: se $f \in I$ (proprietà di ass.) allora $fg \in I$.

$I \subseteq (f)$ Sia $g \in I$ e considero la divisione euclidea:

$$g = qf + r$$

dove $\deg r < \deg f$ oppure $r = 0$.

Voglio dimostrare che $r = 0$.

In effetti, se fosse $r \neq 0$, avrei

$r = g - qf \in I$

Però $\deg r < \deg f$ CONTRADDIZIONE.

Quindi ora degli anelli quozienti del tipo.

$$A = K[X]/(f)$$

Gli elementi di A sono rappresentati dai resti della divisione per f., cioè, se $\deg f = n$, i polinomi del tipo

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

Oss Se $f = \text{cost} \neq 0$, allora $(f) = K[X]$
f ha un inverso g $fg = 1 \in (f)$
$1 \in (f)$ $1 \cdot h = h \in (f)$ $\forall h \in K[X]$.

$$A = \left\{ \overline{a_0 + a_1 X + \dots + a_{n-1} X^{n-1}} \;\middle|\; a_i \in K \right\}$$

$$a_0 + a_1 X + \dots + a_{n-1} X^{n-1} = \bar{a}_0 + \bar{a}_1 \bar{X} + \dots + \bar{a}_{n-1} \bar{X}^{n-1}$$

Se $n > 0$ $a_i \mapsto \bar{a}_i$ è INIETTIVA.
In questo caso stesso si omette la sbarra in $\bar{a}_i$ e si scrive semplicemente a_i.

Prop. A è uno SPAZIO VETTORIALE su K con base $\bar{1}, \bar{X}, \dots, \bar{X}^{n-1}$. ($\dim = n$).

Dim. Che A sia uno S.V. è Facile.

Generatori: ogni elemento è della forma

$$a_0 \bar{1} + a_2 \bar{X} + \dots + a_{n-1} \bar{X}^{n-1}$$

Lin indip.: Supponiamo di avere

$$c_0 \bar{1} + c_1 \bar{X} + \dots + c_{n-1} \bar{X}^{n-1} = \bar{0}$$

$$c_0 + c_1 X + \dots + c_{n-1} X^{n-1} \to \bar{0}$$

$= 1 \in (f)$

$\deg \leq n-1$ (o $g=0$) ← VIETATO → grado $\geq n$, ogni el. $= 0$

$g = 0$ cioè

$$c_0 = c_1 = \dots = c_{n-1} = 0 .$$