ALGEBRA 1 - 27 NOV 2018

Note Title 11/27/2018

Massimo comune divisore negli anelli speciali.

(**Def.** Un MCD fra a e b, non entrambi nulli è un elemento d tale che
1. $d \mid a$, $d \mid b$
2. $x \mid a$, $x \mid b \Rightarrow x \mid d$.)

Esistenza:

- A euclideo $\rightarrow$ divisione euclidea $\rightarrow$ algoritmo di Euclide (divisioni successive)
  Ha un termine: il grado dei resti diminuisce sempre. (i gradi $\in \mathbb{N}$).
  Inoltre, l'MCD si può trovare con un calcolo effettivo. (Si risolve l'identità di Bézout)
  $ax + by = d$).

- A PID $\quad MCD(a,b) \quad (d) = (a,b)$
  $a \in (d) \Rightarrow d \mid a \quad b \in (d) \quad d \mid b$
  $(a,b) = \{as + bt \mid s, t \in A\}$
  $x \mid a, x \mid b \Rightarrow x \mid as + bt$
  d è della forma $as + bt$
  Attenzione: trovare s e t può essere complicato.

- A UFD si usa la fattorizzazione
  $a = \mu p_1^{a_1} \cdots p_r^{a_r} \quad b = \nu p_1^{b_1} \cdots p_r^{b_r}$
  $d = p_1^{\min(a_1, b_1)} \cdots p_r^{\min(a_r, b_r)}$

Unicità Se d_1, d_2 sono due MCD fra a e b allora $d_1 | d_2$ $d_2 | d_1$, $d_1 = \lambda d_2$ $\lambda \in A^*$ (d_1 e d_2 sono "associati").

(senza dimostrazione)

LEMMA DI ZORN X un insieme con una relazione d'ordine. **Se** ogni catena di elementi di X possiede un maggiorante, allora X possiede un elemento massimale.

(Maggiorante: C catena, m maggiorante se $m \geq x$ $\forall x \in C$).

ZORN $\Leftrightarrow$ ASSIOMA DELLA SCELTA.

Conseguenza: Ogni anello (comm. con 1) possiede un ideale massimale (considero X = famiglia degli ideali dell'anello).

Anzi, dato I ideale di A, esiste un ideale massimale contenente I.

Teorema Sia A un UFD. Allora $A[X]$ è un UFD.

Conseguenze Usando ripetutamente il teorema, si vede che, se A è un UFD, allora anche $A[X_1, X_2, \dots, X_n]$ (anello dei polinomi in n variabili) è un UFD.

$A \to A[x_1] \to (A[x_1])[x_2] = A[x_1, x_2] \to \dots \to A[x_1, \dots, x_n]$

Osservazione preliminare

Abbiamo visto che se un dominio A ha le proprietà:

① ogni catena ascendente di ideali principali è stazionaria (esistenza)

② ogni elemento irriducibile è primo (unicità)

allora A è un UFD.

In realtà, le proprietà ① e ② CARATTERIZZANO i domini che sono UFD.

UFD $\Rightarrow$ ①

$(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \dots \dots$

$x_2 | x_1$, $x_3 | x_2$ ....

$x_1 = \mu p_1^{a_1} \cdots p_k^{a_k}$ ha $a_1 + \dots + a_k$ fattori primi

$x_2 = \nu p_1^{b_1} \cdots p_k^{b_k}$ $b_1 \leq a_1, \dots, b_k \leq a_k$

ha $b_1 + \dots + b_k \leq a_1 + \dots + a_k$ fattori primi.

Il n° totale di fattori primi decresce.

A un certo punto rimane costante.

$x_n = \lambda p_1^{c_1} \cdots p_k^{c_k}$ $\quad x_{n+1} = \lambda' p_1^{c_1} \cdots p_k^{c_k}$

$(x_n) = (x_{n+1})$ catena stazionaria.

UFD $\Rightarrow$ (2)

Sia p irriducibile.

Supponiamo $p \mid ab$ $\qquad ab = pc$

$a = q_1^{a_1} \cdots q_r^{a_r}$ $\qquad b = q_1^{b_1} \cdots q_r^{b_r}$

$c = q_1^{c_1} \cdots q_r^{c_r}$ $\qquad pc = p\, q_1^{c_1} \cdots q_r^{c_r}$

$\Rightarrow$ il fattore p deve stare o fra i fattori di a o fra i fattori di b $\qquad$ ($p \mid a$ o $p \mid b$).

Caso $A[X]$ con A UFD.

$f \in A[X]$

contenuto di f $= c(f) =$ MCD (coefficienti di f).

Vale il lemma di Gauss. (prodotto di primitivi è primitivo)

<u>1° fatto</u> $\qquad c(f)=1,\ c(g)=1 \Rightarrow c(fg)=1$

Infatti, supponiamo per assurdo che $c(fg) \neq 1$.

Questo significa che l'ideale generato da fg è un ideale proprio.

$\Rightarrow$ $c(fg) \in M$ massimale (Zorn)

$\Rightarrow$ primo.

Quoziente A/M

$$\bar{f}\,\bar{g} = \overline{fg} \quad \text{in } A/M[X]$$

$\overline{fg} = \bar{0}$ $\qquad$ $A/M[X]$ dominio d'integrità.

(M è un ideale primo, $= P$)

$\bar{f}(x) = \bar{a}_n X^n + \dots$ $\qquad \bar{g}(x) = \bar{b}_m X^m + \dots$

$\bar{a}_n \neq 0 \quad \bar{b}_m \neq 0 \qquad \overline{fg}(x) = \bar{a}_n \bar{b}_m X^{m+n} + \dots$

A/p è dominio d'integrità $\Rightarrow$ $\bar{a}_n \bar{b}_m \neq 0$
$\Rightarrow \bar{f}\bar{g} \neq \bar{0}$.

Allora ho $\bar{f} = \bar{0}$ o $\bar{g} = \bar{0}$

$f \in M[x]$ o $g \in M[x]$

ASSURDO. (f, g primitivi)

<u>2° passo</u> $c(fg) = c(f)c(g)$

$f = c(f) f_1$ $\qquad g = c(g) g_1$

f_1, g_1 primitivi

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

<u>3° passo</u> A UFD, K campo dei quozienti di A

(generalizza $\mathbb{Z}$ e $\mathbb{Q}$)

Supponiamo $f, g \in A[x]$ f primitivo

$f \mid g$ in $K[x]$ $\Rightarrow$ $f \mid g$ in $A[x]$.

$g = fh \qquad h \in K[x]$

$$h = \frac{1}{d} h' = \frac{1}{d} c h_1 = \frac{c}{d} h_1$$

h_1 primitivo.

$$g = f \cdot \frac{c}{d} h_1 \qquad dg = c \underbrace{f \cdot h_1}_{\text{primitivo}}$$

contenuto $= c$

$d \mid c$

$\frac{c}{d} \in A \qquad h = \frac{c}{d} h_1 \in A[x]$.

4° passo Se $f(x)$ si scrive come prodotto di due polinomi $g(x), h(x) \in K[x]$ allora si scrive come prodotto di due polinomi $g'(x), h'(x) \in A[x]$ dello stesso grado dei precedenti:

$$f(x) = g(x)h(x) = \frac{a}{b} g_1(x) \cdot \frac{c}{d} h_1(x)$$

$$bd\, f(x) = ac\, g_1(x) h_1(x)$$

$$bd \mid ac \quad \Rightarrow \quad \frac{a}{b}\frac{c}{d} \in A$$

Quindi, per esempio,

$$f(x) = \underbrace{\left(\frac{ac}{bd} g_1(x)\right)}_{\in A[x]} \cdot \underbrace{h_1(x)}_{\in A[x]}$$

"stesso grado"

Proprietà (1) (catena ascendente di ideali principali).

$$(f^{(1)}) \subseteq (f^{(2)}) \subseteq (f^{(3)}) \subseteq \dots$$

$f^{(1)} = c_1 f_1^{(1)}$ (contenuto x polinomio primitivo)

$f^{(2)} = c_2 f_2^{(1)}$ (" " " ")

. . . .

$f^{(2)} \mid f^{(1)}$ $c_2 \mid c_1$ $f_2^{(1)} \mid f_1^{(1)}$

$\downarrow$

$(c_1) \subseteq (c_2) \subseteq$ $\leftarrow$ stazionaria (in A)

I gradi degli $f_1^{(k)}$ sono stazionari

Da un certo punto in poi

$f_1^{(n)}$ = ed invertibile · $f_1^{(n+1)}$ e cioè

$(f_1^{(n)}) = (f_1^{(n+1)})$ → catena stazionaria.

Proprietà (2) Guardiamo innanzitutto quali sono gli elementi irriducibili di $A[x]$.

(Ricordiamo che $(A[x])^* = A^*$:
se $f \in (A[x])^*$ allora $\deg f = 0$. $f = c$

$c \cdot x = 1$ $c \in A^*$

le viceversa è ovvio).

1° caso $\deg f = 0$ ($f = c$ è costante)
L'unico modo possibile per scrivere $c = gh$ è che $g = a$ $h = b$ siano costanti (per questioni di grado).
f irriducibile $\Leftrightarrow$ $c \in A$ è irriducibile

2° caso $\deg f > 0$
Dimostriamo che f è irriducibile in $A[x]$
$\Leftrightarrow$ f è primitivo (e) f è irriducibile in $K[x]$

$\Rightarrow$ $f = c(f) f_1$ $\Rightarrow$ $c(f) \in A^*$ ($c(f) = 1$)
f primitivo.

Se per assurdo f non fosse irriducibile in $K[x]$ allora avrei $f = gh$
con g e h non invertibili (in $K[x]$
g e h non costanti)

Gauss → $f = g'h'$ in $A[x]$ con polinomi dello stesso grado $\Rightarrow$ f non è irriducibile in $A[X]$.

$\Leftarrow$ Se f è primitivo, non si può spezzare in modo non banale come prodotto di una costante per un polinomio dello stesso grado di f.
L'unica possibilità sarebbe che f si spezzasse come prodotto di due polinomi di grado positivo.
Ma questo non è possibile neanche in $K[X]$ e, a maggior ragione, non è possibile in $A[X]$.

Dimostriamo che IRRIDUCIBILE $\Rightarrow$ PRIMO

<u>1° caso</u> $\deg f = 0$ $\quad f = c$ è irriducibile in $A[X]$
$\Leftrightarrow$ c è irriducibile in A $\Rightarrow$ c è primo in A.

$c \mid gh \qquad c \mid c(g)c(h)\, g_1 h_1$

$c \mid c(g) \Rightarrow c \mid g$

o $\quad c \mid c(h) \Rightarrow c \mid h$

<u>2° caso</u> $\deg f > 0$

Supponiamo $f \mid gh$
Usando il fatto che f è irriducibile (e quindi primo) in $K[X]$ ho che

$f \mid g$ o $f \mid h$ in $K[X]$

f primitivo $\quad$ Gauss $\Rightarrow$ $f \mid g$ o $f \mid h$ in $A[X]$
(3° passo)

Esempio $\quad UFD \not\Rightarrow PID$

$\mathbb{Z}[X]$ $\quad (2, x)$ non principale

UFD

$K[X, Y]$ $\quad I = (X, Y)$ non principale

UFD

Se fosse principale $\quad (f) = (X, Y)$

$f \mid X \,,\; f \mid Y$

$\Rightarrow f = 1$

Ma $\quad 1 \notin I$

(i polinomi di I hanno tutti termine costante $= 0$)