ALGEBRA 1 - 20 NOV 2018

Note Title 11/20/2018

ANELLI SPECIALI

Ipotesi A dominio d'integrità. (comm. con 1)

Anelli euclidei o domini euclidei, domini a ideali principali (PID), domini a fattorizzazione unica (UFD).

Gerarchia: EUCLIDEO $\Rightarrow$ PID $\Rightarrow$ UFD

(non è vero il viceversa).

Domini euclidei

Def. Un dominio d'integrità A si dice un dominio euclideo se esiste una funzione "grado" $d : A \setminus \{0\} \to \mathbb{N}$ con le seguenti proprietà:

① $d(x) \leq d(xy) \quad \forall x, y \in A \setminus \{0\}$

② $\forall a, b \in A,\ b \neq 0,\ \exists\, q, r \in A$ tali che

$a = qb + r$

dove $d(r) < d(b)$ oppure $r = 0$.

Esempi già trattati, $A = \mathbb{Z}$, $d = |\ |$ $\qquad A = K[x]$, d = grado.

Altro esempio: $A = K[[x]]$

Serie formali $\quad a \in A \quad a = \sum_{i=0}^{\infty} c_i x^i$

$c_i \in K$.

Elementi invertibili: $A^* = k[[x]]^*$

Sono tutte le serie con il termine "noto" (grado 0) $\neq 0$.

Cond. necessaria $ab = 1 \leftarrow$ costante $= 1$.

$$a = \sum a_i x^i \qquad b = \sum b_i x^i$$
$$\Rightarrow a_0 b_0 = 1$$
$$\Rightarrow a_0 \neq 0.$$

Cond. sufficiente Sia $a(x)$ con $a_0 \neq 0$ e supponiamo di aver trovato $b_0, b_1, \dots, b_{n-1}$ tali che $a(x)(b_0 + b_1 x + \dots + b_{n-1} x^{n-1})$
$$= 1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^{n-1} + \text{altri termini}$$

Cerco b_n "buono": il coeff di x^n in $a(x)(b_0 + b_1 x + \dots + b_{n-1} x^{n-1} + b_n x^n)$

è $a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0$.

Per renderlo uguale a zero, basta scegliere

$$b_n = -a_0^{-1}(a_1 b_{n-1} + \dots + a_n b_0).$$

Induttivamente costruisco la serie $b(x)$ inversa di $a(x)$

El non invertibili: $a(x)$ con $\boxed{a_0 = 0}$.

$\downarrow$

SONO UN IDEALE. $\rightarrow$ UNICO IDEALE MASSIMALE.

GRADO $a(x) \in A[[x]]$

$$a(x) = c_k x^k + c_{k+1} x^{k+1} + \dots$$
$$c_k \neq 0 \qquad (c_0 = c_1 = \dots = c_{k-1} = 0)$$

Poniamo $d(a(x)) = k$.

① $d(a(x)) \leq d(a(x)b(x))$ ovvia.

② Divisione con resto: $b \neq 0$.

$d(a(x)) = m$ $\qquad$ $d(b(x)) = n$

$a(x) = c_m x^m + \dots$ $\qquad$ $b(x) = k_n x^n + \dots$

- se $m < n$ pongo $q = 0$

$$a = 0 \cdot b + a$$

- se $m \geq n$

$$a(x) = x^m u \qquad u \in A^*$$
$$b(x) = x^n v \qquad v \in A^*$$

$$x^m u = a(x) = x^{m-n} u v^{-1} \underbrace{(x^n v)}_{= b(x)} + \underbrace{0}_{\text{"resto"}}$$

Esempio <u>IMPORTANTE</u>: Gli interi di Gauss.

$$A = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

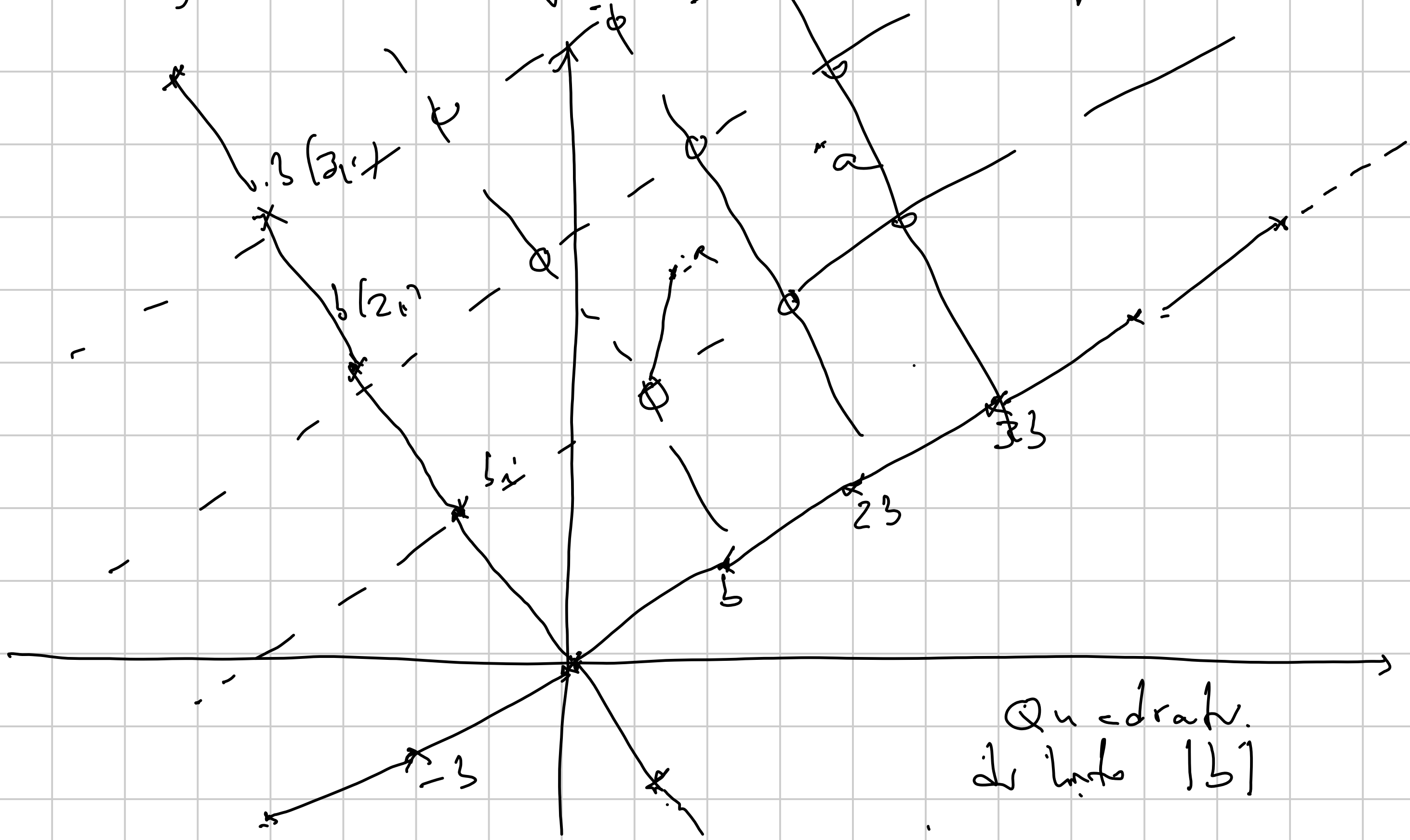
Funzione grado: $d(a+bi) = a^2 + b^2$.

(= quadrato del valore assoluto)

$d(x) \leq d(xy)$ ovvio.

Divisione euclidea. $\qquad$ ($a = qb + r$ con r "piccolo")

Disegno dei multipli di b (qb)



Sicuramente esiste $q \in A$ tale che

$$|a - qb| \le \frac{1}{\sqrt{2}} |b|$$

$$d(a - qb) \le \frac{1}{2} |b|^2 = \frac{1}{2} d(b).$$

(Lo stesso discorso vale anche per

$$\mathbb{Z}[\sqrt{-2}] = \{ a + b\sqrt{-2} \mid a, b \in \mathbb{Z} \}$$

ma <u>NON</u> per $\mathbb{Z}[\sqrt{-m}] = \{ a + b\sqrt{-m} \mid m > 2 \}$)

<u>Proprietà dei domini euclidei</u>

<u>Prop 1</u> In un dominio euclideo A tutti gli ideali sono principali $(I = (x))$.

<u>Dim.</u> Se $I = (0)$ ok.

Se $I \neq (0)$, l'insieme dei gradi degli elementi di $I \setminus (0)$ è un sottoinsieme non vuoto di $\mathbb{N}$.

Sia $x \in I \setminus \{0\}$ di grado minimo.

$x \in I \Rightarrow (x) \subseteq I$

Viceversa, sia $a \in I$, divisione euclidea:

$$\underset{I}{\underset{\cap}{a}} = q\underset{I}{\underset{\cap}{x}} + r \qquad \Rightarrow r \in I$$

$d(r) < d(x)$ IMPOSSIBILE

QUINDI $r = 0 \Rightarrow a \in (x)$.

<u>Def 2</u> Un dominio d'integrità A si dice un dominio a ideali principali (PID) se tutti i suoi ideali sono principali.

HO DIMOSTRATO: Euclideo $\Rightarrow$ PID.

<u>Proprietà 2</u> (Elementi grado minimo in $A \setminus \{0\}$)

Un elemento x di $A \setminus \{0\}$ ha grado minimo se e solo se $x \in A^\times$.

<u>Dim</u> 1 ha grado minimo

$$d(1) \leq d(1 \cdot x) = d(x) \quad \forall x \in A \setminus \{0\}$$

Se $u \in A^\times$, allora u ha grado minimo.

$\exists v$ tale che $uv = 1$

$$d(u) \leq d(uv) = d(1) \quad \text{MINIMO}$$

Supponiamo ora che $x \in A \setminus \{0\}$ abbia grado minimo.

Divido 1 per x

$$1 = qx + r$$

r non può avere grado $< d(x) \Rightarrow r = 0 \quad 1 = qx$

$\Rightarrow x \in A^*$.

Domini a ideali principali

Proprietà della catena ascendente

Ogni catena ascendente di un PID è stazionaria.

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots \subseteq \dots$$

$\Rightarrow \exists\, n_0$ tale che $I_n = I_{n_0}$ per $n \geq n_0$.

Dim. Osserviamo che $I = \bigcup_{n=1}^{\infty} I_n$ è un ideale.

$x, y \in I \Rightarrow x \in I_m \quad y \in I_n$ p.es. $m \geq n$

$x, y \in I_m$

$x + y \in I_m \subseteq I$

$I = (x)$

$\exists\, n : \quad x \in I_n$

$$(x) \subseteq I_n \subseteq I = (x)$$

$I_m \quad m \geq n$

tutti uguali

$\Rightarrow I_m = I_n \quad \forall m \geq n$.

$$(x) \subseteq (y) \iff y \mid x$$

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

$x_2 \mid x_1 \quad x_3 \mid x_2 \dots$

Prop. In un PID ogni elemento $\neq$ zero e non invertibile si può scrivere come un prodotto di elementi irriducibili. (esiste una fattorizzazione)

Dim Sia $x \in A - \{0\} - A^*$

x irriducibile $\to$ fine. Allora x non irriducibile

$x = x_1 y_1$ dove $x_1 \notin A^*$ $y_1 \notin A^*$

x_1, y_1 entrambi irriducibili $\to$ fine

Se anche avessimo che x_1 e y_1 sono prodotti di irriducibili $\to$ fine (Suppongo, per simmetria, che x_1 non sia prodotto di irriducibili)

$x_1 = x_2 y_2$ $\qquad$ x_2, y_2 non entrambi prodotti di irriducibili (e neanche invertibili)

Suppongo x_2.

$x_1 | x \qquad x_2 | x_1$

Per la catena ascendente ho a un certo punto

$$(x_k) = (x_{k+1}) = \dots (x_{k+n})$$

$$x_k = x_{k+1} u \qquad x_{k+1} = x_k v$$

$\to$ a meno di invertibili sono uguali.

Ricapitolando Se esiste $x \in A - \{0\} - A^*$ che non si può scrivere come prodotto di elementi irriducibili otterrei una catena di divisibilità infinita (ASSURDO)

Prop. 2 In un PID ogni elemento irriducibile è primo.

Dim. $(x) \subseteq A \qquad (x) \neq (0) \qquad (x) \neq A$

(x) primo $\Leftrightarrow$ x è primo
(x) massimale (all'interno degli ideali principali)
$\Leftrightarrow$ x è irriducibile
ID. MASSIMALE $\Rightarrow$ PRIMO.

Fattorizzazione unica: ogni elemento $\neq 0$ e non invertibile si può scrivere in modo unico* come prodotto di primi
* (a meno dell'ordine, e di cambiare un fattore con suo associato)
Alternativamente: ogni elemento $\neq 0$ si scrive in modo unico come prodotto di un elemento invertibile e un prodotto di primi.

$$x = \mu p_1^{a_1} \cdots p_k^{a_k}$$

PID $\Rightarrow$ UFD (Unicità della fattorizzazione)

$$x = p_1 \cdots p_k = q_1 \cdots q_h \quad \text{(anche ripetuti)}$$

p_1 divide uno dei q_j P. es. p_1 / q_1
$q_1 = p_1 u \quad u \in A^*$
Posso semplificare
$$\frac{x}{p_1} = p_2 \cdots p_k = u q_2 \cdots q_h.$$

(induzione sul n° dei fattori).