# ALGEBRA 1 — 13 NOV 2018

Note Title 11/13/2018

Anelli $\longrightarrow$ anelli commutativi con identità.
(salvo avviso esplicito)

<u>Divisione fra ideali</u> $\quad A$ anello, $I, J$ ideali.

$$I : J = \{ x \in A \mid xJ \subseteq I \}$$

E' un ideale: $\quad$ sgr $+ \qquad 0 \cdot J = 0 \subseteq I$.

$$xJ \subseteq I \qquad yJ \subseteq I$$

$a \in (x+y)J \qquad a = (x+y)j \qquad j \in J$

$$a = xj + yj \in I + I = I$$

<u>opposto</u> $\qquad xJ \subseteq I \Longrightarrow (-x)J \subseteq I$

$$xj \in I \qquad -xj \in I.$$

<u>Assorbimento</u> $\qquad xJ \subseteq I \quad a \in A \Longrightarrow axJ \subseteq I$

$$axJ = x\underbrace{aJ} \subseteq xJ \subseteq I.$$

$a = -1 \quad$ molt. per $-1$ = opposto.

Caso $\quad A = \mathbb{Z} \qquad I = (m) \qquad J = (n)$

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

$x \in I : J \qquad x = p_1^{\xi_1} p_2^{\xi_2} \cdots p_k^{\xi_k}$. (altri fattori)

Ci vuole che $p_i^{\xi_i + b_i}$ sia multiplo di $p_i^{a_i}$

$\xi_i + b_i \geq a_i \qquad \xi_i \geq a_i - b_i$

$$\xi_i \geq \max(a_i - b_i, 0) = c_i$$

$$I : J = (p_1^{c_1} \cdots p_k^{c_k}).$$

---

<u>Radicale di un ideale</u> $A$ anello, $I$ ideale

$$\sqrt{I} = \{ x \in A \mid \exists n \in \mathbb{N} \; x^n \in I \}$$

$\sqrt{I}$ <u>ideale</u>: $\qquad 0 \in \sqrt{I}$ ok.

Somma: $\quad x \in \sqrt{I} \quad y \in \sqrt{I} \qquad x^m \in I \quad y^n \in I$

$$(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}$$

Tutti gli addendi $\in I$ se si ha sempre
$i \geq m$ oppure $k - i \geq n$

Quindi basta prendere $k = m + n - 1$
( $i < m \quad k - i < n \implies$
$i \leq m-1 \quad k-i \leq n-1 \implies k \leq m+n-2$ )

Assorbimento : $\quad x^n \in I \quad (ax)^n = a^n x^n \in I$

$\sqrt{(0)}$ = nilpotenti di $A$.

In $\mathbb{Z}$ : $\quad m = p_1^{a_1} \cdots p_k^{a_k} \implies$

$\sqrt{(m)} = (p_1 \dots p_k)$

$\sqrt{I} \supseteq I$ banalmente.

---

Ideali principali : $I = (x) = \{ax : a \in A\}$
(cioè generati da un solo elemento)

Per quali $x$ si ha $I = A$?

- $x = 1$ $\quad a \cdot 1 = a \quad \forall a \in A \quad a \in I$
- $x \in A^*$ $\quad \left( \begin{aligned} A^* &= \{x \in A \mid x \text{ invertibile}\} \\ &= \{x \in A \mid \exists y \in A \ xy = 1\} \end{aligned} \right)$

In $I = (x)$ c'è $xy = 1$
se c'è 1 ci sono tutti gli elementi.

Invece, se $x \notin A^*$, allora $(x) \neq A$
Infatti $1 \notin (x)$

Quando si ha $(x) = (y)$?

$\boxed{(x) \subseteq (y)} \iff \exists\, a \in A$ t.c. $x = ay$
$\Updownarrow$ $\qquad \boxed{\iff y \mid x}$
$x \in (y)$

$(x) = (y) \iff x \mid y$ e $y \mid x$

Certamente questo succede se $y = ax$
con $a \in A^*$. Infatti, se $ab = 1$

$y = ax \Rightarrow by = bax = x$

Supponiamo invece $x | y$ $y | x$

$y = ax$ $x = by$

$y = aby$

$y(ab-1) = 0$.

$y \neq 0$ DOM. D'INTEGRITÀ $\Rightarrow$

$ab = 1$ $a \in A^*$

CONCLUSIONE: In un dominio d'integrità

$(x) = (y) \Leftrightarrow x = ay$ con $a \in A^*$.

($x$ e $y$ si dicono ASSOCIATI).

<u>Oss.</u> Un anello $A$ è un campo $\Leftrightarrow$ gli unici ideali di $A$ sono $\{0\}$, $A$.

<u>Dim</u> $\Rightarrow$ Sia $A$ un campo. Allora ogni $x \in A$ $x \neq 0$ è invertibile.

Se $I$ è un ideale $\neq 0$, allora contiene un elemento invertibile $\rightarrow$ è tutto l'anello.

Viceversa, se $A$ non è un campo, contiene un elemento $x \neq 0$ non invertibile

$I = (x) \rightarrow I \neq (0), I \neq A$.

<u>Oss. 2</u> Un dominio d'integrità $A$ <u>finito</u> è un campo.

<u>Dim.</u> Sia $x \in A$, $x \neq 0$.

Considero le potenze di $x$

$$x, x^2, x^3, \dots$$

Esistono $m > n$ tali che $x^m = x^n$

$$x^m - x^n = 0$$

$$x^n(x^{m-n} - 1) = 0$$

$\neq 0$ (dominio)

$$x^{m-n} - 1 = 0$$

$$x^{m-n} = 1$$

$$x \cdot \underbrace{x^{m-n-1}}_{y \text{ inverso di } x} = 1$$

---

## Teorema cinese per anelli

Sia $A$ un anello e siano $I, J$ ideali tali che $I + J = A$ (coprimi: $I + J = (1)$)

Allora

$$\underbrace{A/_{I \cdot J} = A/_{I \cap J}}_{\text{(visto come esercizi.)}} \cong A/_I \times A/_J$$

Dim. Si considera l'omomorfismo

$$\varphi : A \to A/_I \times A/_J$$

dato dalle proiezioni: $\varphi(x) = (x + I, x + J)$

$$\ker \varphi = \{x \in A \mid x + I = I \quad x + J = J\}$$

$$= \{x \in A \mid x \in I, x \in J\} = I \cap J$$

Surgettività: Basta vedere che $(\bar{1},\bar{0})$, $(\bar{0},\bar{1})$ sono nell'immagine

$$\left( (\bar{1},\bar{0}) \in \operatorname{Im}\varphi \quad (\bar{1},\bar{0}) = \varphi(x) \Rightarrow (\bar{a},\bar{0}) = \varphi(ax) \in \operatorname{Im}\varphi \right.$$

$$(\bar{0},\bar{1}) \in \operatorname{Im}\varphi \Rightarrow (\bar{0},\bar{b}) \in \operatorname{Im}\varphi$$

e quindi $\left. (\bar{a},\bar{b}) = (\bar{a},\bar{0}) + (\bar{0},\bar{b}) \in \operatorname{Im}\varphi \right)$

$$(\bar{1},\bar{0}) \in \operatorname{Im}\varphi \iff \exists x \in A \text{ t.c. } (x+I,\ x+J) = (1+I,\ J)$$

$$I+J = A \Rightarrow \exists x \in I, y \in J \text{ t.c. } x+y = 1$$

$$y = 1-x \in 1+I \qquad \varphi(y) = (\bar{1},\bar{0})$$
$$\in J$$

Analogamente per $(\bar{0},\bar{1})$.

## Caratteristica di un anello

$A$ anello. Consideriamo

$$I = \{ k \in \mathbb{Z} \mid kx = 0 \quad \forall x \in A \}$$

$I$ è un ideale di $\mathbb{Z}$ (banalmente)

$$I = (m) \qquad (m \geq 0)$$

$$m \overset{\text{def}}{=} \operatorname{char} A.$$

Oss. Questa definizione generale si usa per anelli non commutativi con identità. ECCEZIONE

Infatti se $A$ è comm. con $1$

$$k \cdot 1 = 0 \Rightarrow k \cdot x = 0 \quad \forall x \in A$$

$$kx = k \cdot 1 \cdot x = 0 \cdot x = 0.$$

Quindi

$$\operatorname{char} A = \begin{cases} \operatorname{ord}_+ 1 & \text{se finito} \\ 0 & \text{se } \operatorname{ord}_+ 1 \text{ è infinito} \end{cases}$$

<u>Esempio</u> $\mathbb{Z}/_{p\mathbb{Z}}[x]$ ha caratteristica $p$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ hanno caratteristica $0$.

<u>Sottoanello fondamentale di $A$</u>

Considero la funzione

$$f : \mathbb{Z} \to A$$

definita da

$$f(1) = 1 \qquad f(k) = k \cdot 1$$

$f$ è omomorfismo $\quad f(a+b) = f(a) + f(b)$

$$f(ab) \underset{\text{proprietà distributiva}}{=} f(a) f(b)$$

Teo. di omomorfismo:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[dr, "\pi"'] & A \\ & \mathbb{Z}/(\ker f) \arrow[u, dotted, "\varphi"'] \end{tikzcd}$$

$\varphi$ iniettiva

Questo dice che $A$ contiene un sottoanello isomorfo a $\mathbb{Z}/(\ker f)$.

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & \operatorname{char} = m \\ \mathbb{Z} & \operatorname{char} = 0 \end{cases}$$

Questo è quello che si dice SOTTOANELLO FONDAMENTALE ed individua char $A$.

<u>Oss.</u> Se $A$ è un dominio d'integrità, allora char $A = 0$ oppure un numero primo.

( $A \supseteq A_0$ sottoanello fondamentale che anch'esso è un dominio d'integrità )

## IDEALI PRIMI E IDEALI MASSIMALI

<u>Def 1</u> Un ideale $P$ di un anello $A$ con $P \neq A$ ($P$ proprio) si dice primo se
$$xy \in P \implies x \in P \text{ oppure } y \in P.$$

<u>Def. 2</u> Un ideale proprio $M$ di $A$ si dice massimale se dato $I$ ideale di $A$ con $M \subseteq I \subseteq A$, si ha
$$I = M \text{ oppure } I = A$$

<u>Oss. 1</u> $P$ è un ideale primo di $A$ $\iff$ $A/P$ è un dominio d'integrità.

<u>Dim</u> ($\Rightarrow$) $xy \in P \implies x \in P$ oppure $y \in P$

Proiettando in $A/P$ $\quad \pi(x) = \bar{x}$

$$\overline{xy} = \bar{x} \cdot \bar{y} = \bar{0} \implies \bar{x} = 0 \text{ oppure } \bar{y} = 0.$$

La freccia $\Leftarrow$ è identica (si rovesciano le implicazioni)

**Oss 2** Un ideale $M$ di $A$ è massimale
$\iff$ $A/M$ è un campo.

**Dim.** $M$ massimale $\iff$ gli unici ideali che contengono $M$ sono $M$ ed $A$
$\iff$ Gli unici ideali di $A/M$ sono $\{\bar{0}\}$ e $A/M$.
(tramite la corrispondenza biunivoca fra ideali, vedi dopo).

**Conseguenza** massimale $\Rightarrow$ primo.

**Oss $\alpha$** $A$ dom. d'integrità $\iff$ $(0)$ è primo.

---

ELEMENTI PRIMI E ELEMENTI IRRIDUCIBILI.
(IPOTESI: $A$ è un dominio d'integrità)

**Def 3** Un elemento $p \in A$, $p \neq 0$, $p \notin A^*$ si dice primo se
$$p \mid xy \Rightarrow p \mid x \text{ oppure } p \mid y .$$

**Def 4** Un elemento $x \in A$ $x \neq 0$, $x \notin A^*$ si dice irriducibile se
$$x = ab \Rightarrow a \in A^* \text{ oppure } b \in A^*$$

**Prop.** PRIMO $\Rightarrow$ IRRIDUCIBILE

**Dim.** Sia $p$ primo e sia $p = ab$

In particolare $p \mid ab$. Quindi $p \mid a$ oppure $p \mid b$

Se $p \mid a$ $\qquad a = pc$

$$p = pc \cdot b \qquad p(cb-1) = 0.$$

$$p \neq 0 \quad \Rightarrow cb - 1 = 0$$

$$cb = 1 \Rightarrow b \in A^*$$

Se $p \mid b$ ... $a \in A^*$.

--

$P = (p)$ principale primo $\neq (0)$

Questo avviene $\Leftrightarrow$ $p$ è un elemento primo.

$$\underset{\substack{\shortparallel \\ (p)}}{xy \in P} \Rightarrow x \in P \text{ o } y \in P$$

$$\Updownarrow$$

$$p \mid xy \Rightarrow p \mid x \text{ o } p \mid y$$

...

$M = (x)$ principale è massimale fra gli ideali principali.

Questo è vero $\Leftrightarrow$ $x$ è irriducibile

$$M \subseteq I \subseteq A \qquad \Leftrightarrow a \mid x$$

$$(x) \subseteq (a) \subseteq A$$

$$\Leftrightarrow x = ab \qquad \Leftrightarrow a \in A^* \text{ o } b \in A^*$$

$$(a) = A \qquad b \in A^*$$

$$x = ab \qquad b^* \in A$$

$$(x) = (a)$$