ALGEBRA 1 – 8 NOV 2018

Note Title 11/8/2018

ANELLI

- gruppi commutativi rispetto a $+$
- moltiplicazione associativa
- proprietà distributiva della moltiplicazione rispetto alla somma ($a(b+c)=ab+ac$ $(a+b)c=ac+bc$)

Esempi.

- Esempi numerici : $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ...
- Polinomi : $K[x]$, $\mathbb{Z}[x,y] = \{\sum a_{ij} x^i y^j\}$.
- Matrici quadrate ($\leftrightarrow$ funzioni lineari da $\mathbb{K}^n$ in $\mathbb{K}^n$)
  Moltiplicazione NON COMMUTATIVA.
- Funzioni $f: X \to \mathbb{R}$
  $(f+g)(x) = f(x)+g(x)$ $\qquad fg(x)=f(x)g(x)$
  $f:\mathbb{R}\to\mathbb{R}$, f continue, f derivabili, ...
- Serie : $\sum_{i=0}^{\infty} a_i x^i$ $\quad a_i \in \mathbb{R}$ (p. es.)
- G gruppo abeliano $(+)$ $A = \mathrm{End}(G)$
  $= \{f: G \to G \mid f \text{ omomorfismo}\}$
  $(f+g)(x) = f(x)+g(x)$
  $f\cdot g$ = composizione $f\circ g$.

Sottoanelli, ideali.

$\updownarrow \qquad \updownarrow$

sottogruppi, sottogruppi normali

Def Un sottoinsieme I di un anello A si dice un IDEALE di A se:
- I è un sottogruppo rispetto a $+$
- valgono le proprietà di "assorbimento", cioè

$$xI \subseteq I \quad Ix \subseteq I \quad \forall x \in A$$

$$\forall x \in A \ \forall y \in I \quad xy \in I \quad yx \in I.$$

Ideali di $\mathbb{Z}$ = sottogruppi di $\mathbb{Z}$

$$m\mathbb{Z} \qquad m \geq 0.$$

Ass. $a \in \mathbb{Z}$ $\quad x \in m\mathbb{Z}$ $\quad x = my$ $\quad ax = may \in m\mathbb{Z}$.

Quozienti $\quad A$ anello, I ideale

$$A/I = \{x+I \mid x \in A\}$$

Operazioni: $\quad (x+I)+(y+I) = x+y+I$ ok per gruppi

$$(x+I)(y+I) = xy+I.$$

Buona definizione del prodotto: cioè
se $x'+I = x+I$ e $y'+I = y+I$ allora $x'y'+I = xy+I$

$x'+I = x+I \iff x' \in x+I \quad x' = x+i \quad i \in I$

$y' = y+i' \quad i' \in I$

$$x'y' = (x+i)(y+i') = xy + \underset{I}{\underset{\cap}{iy}} + \underset{I}{\underset{\cap}{xi'}} + \underset{I}{\underset{\cap}{ii'}}$$

Nelle congruenze modulo un polinomio, l'ideale è costituito dai multipli del polinomio

Omomorfismi fra anelli: $f: A \to B$ $\quad f(x+y) = f(x)+f(y)$
$f(xy) = f(x)f(y)$

Esempi

$f: \mathbb{Z} \to \mathbb{Z}$ Certamente se $f(1) = k$

$$f(x) = kx.$$

Prodotto: $f(xy) \overset{?}{=} f(x)f(y)$

$$kxy \overset{?}{=} kx \cdot ky$$

Vale solo se $k = 0, 1$.

$f: K[x] \to K$ "omomorfismo di valutazione"

$$p(x) \mapsto p(a) \qquad a \in K$$

$$(p+q)(a) = p(a) + q(a)$$

$$(pq)(a) = p(a) \cdot q(a).$$

Nucleo di un omomorfismo

Def. Se $f: A \to B$ è un omomorfismo si dice nucleo di f, $\ker f$ l'insieme

$$\{x \in A \mid f(x) = 0\}$$

Oss. $\ker f$ è un ideale di A.

Dim. Sappiamo già che è un sottogruppo per $+$.

Assorbimento: siano $a \in A$ $x \in \ker f$ $(f(x)=0)$

Allora $f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$.

$(\forall y \in A$ si ha $y \cdot 0 = 0$: infatti

$$y \cdot 0 = y(0+0) = y \cdot 0 + y \cdot 0$$

eliminando, $y \cdot 0 = 0)$

Analogamente $f(xa) = 0$

Teo. di omomorfismo per anelli.

Sia $f: A \to B$ un omomorfismo di anelli. $\operatorname{Ker} f = I$. Allora esiste uno e un solo omomorfismo $\varphi: A/I \to B$ tale che il diagramma

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B \\
& A/I \arrow[ur, dashed, "\varphi"'] &
\end{tikzcd}$$

commuta (π è la proiezione canonica: $\pi(x) = x+I$)
Inoltre
- φ è iniettivo
- φ è surgettivo $\iff$ f è surgettivo).

<u>Dim</u> Tutto è OK per il teo. di omomorfismo sui gruppi, eccetto la verifica che φ è anche un omomorfismo di anelli.

Ricordo come era definita φ
$$\varphi(x+I) = f(x).$$
Devo verificare
$$\varphi\big(\underbrace{(x+I)(y+I)}_{\|}\big) = \varphi(x+I)\cdot\varphi(y+I)$$
$$f(xy) = \varphi(xy+I) = f(x)f(y) \qquad \text{OK.}$$

<u>Oss.</u> Gli ideali sono tutti e soli i nuclei degli omomorfismi.
(Per vedere che sono tutti, basta considerare $\pi: A \to A/I$).

Supponiamo ora che A, B siano anelli con unità (risp. alla moltiplicazione) $(1_A, 1_B)$

È vero che $f(1) = 1$?

Esempio $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$

$$f(x) = 3x$$

$$f(x+y) = 3(x+y) = 3x + 3y = f(x) + f(y)$$

$$f(xy) = 3xy = 3x \cdot 3y$$

$$f(\overline{1}) = \overline{3}$$

Def Si dice che un anello A è un dominio d'integrità se:

- A è commutativo (la moltiplicazione è comm.)
- A ha un'unità (1)
- "non esistono" divisori di zero, cioè
  $xy = 0 \Rightarrow x = 0$ oppure $y = 0$.

(Un divisore di zero è un elemento $\boxed{x \neq 0}$ tale che $\exists\, y \neq 0$ con $xy = 0$).

Prop. Se $f : A \to B$ è un omomorfismo di anelli con unità (non banale) e B è un dominio d'integrità, allora $f(1) = 1$.

Dim. Supponiamo $f(1) = b$

Allora $f(x) = f(1 \cdot x) = f(1) \cdot f(x) = b\, f(x)$

$1 \cdot f(x) = f(x) = b f(x)$

$(1-b) f(x) = 0$

$\Rightarrow$ $1-b=0$ oppure $f(x) = 0$

$\Downarrow$

$b=1$ (tesi) $\quad$ $f(x)$ non è uguale a zero sempre per ipotesi.

Nel seguito, consideriamo anelli COMMUTATIVI con UNITÀ

Ideale generato da un sottoinsieme S.

1° caso $\quad S = \{x\}$.

L'ideale generato da S, (x) è

$$I = \{ax \mid a \in A\}.$$

Infatti, I è un ideale:

$0 \in I \quad 0 = 0 \cdot x$

$ax + bx = (a+b)x \in I$

$-ax = (-a)x$

sgr I $\quad$ Ass. $\quad b(ax) = (ba)x$

Inoltre è il più piccolo: ogni ideale che contenga x deve contenere anche tutti gli elementi ax (proprietà di assorbimento).

2° caso $\quad S$ finito, $S = \{x_1, \ldots, x_n\}$

L'ideale generato da S, $(x_1, x_2, \ldots, x_n)$ è

$$\{a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \mid a_i \in A\}.$$

(Verifica facile che è un ideale, e poi è il più piccolo perché $x_i \in I \Rightarrow a_i x_i \in I \Rightarrow$

$\Rightarrow \sum a_i x_i \in I$.

<u>3° caso</u> S qualsiasi $S = \{x_\lambda\}_{\lambda\in\Lambda}$.

Ideale generato da S : $(x_\lambda)_{\lambda\in\Lambda}$

$$\left\{ a_1 x_{\lambda_1} + \dots + a_n x_{\lambda_n} \;\middle|\; n\in\mathbb{N} \quad a_i\in A \quad x_{\lambda_i}\in S \right\}$$

I, J ideali di $\mathbb{Z}$ $\quad I=(m),\ J=(n)$

$$(m,n) = \{ am+bn \mid a,b\in\mathbb{Z}\} = (d)$$

d → MCD

OPERAZIONI SU IDEALI.

- intersezione $\quad I, J$ ideali di $A \Rightarrow I\cap J$ è un ideale

- il più piccolo ideale che contiene I, J è
$$I+J = \{x+y \mid x\in I,\ y\in J\}.$$

(Le somme sono ovviamente necessarie e in più sono sufficienti perché l'insieme delle somme forma un ideale : $(x+y)+(x'+y') = (x+x')+(y+y')$ ... ecc)

<u>Prodotto di ideali</u>

$I \cdot J$ = ideale <u>generato</u> dai prodotti xy, $x\in I$, $y\in J$.

attenzione!

$= \{ a_1 x_1 y_1 + \dots + a_n x_n y_n \mid n \in \mathbb{N} \ a_i \in A \ x_i \in I \ y_i \in J \}$

$I = J = (x, y) \in \mathbb{R}[x, y]$

$x^2 + y^2 \in I \cdot J$ ma non è un prodotto.

<u>Oss</u> $I \cdot J \subseteq I \cap J$.

<u>Dim.</u> Basta verificare che tutti i generatori di $I \cdot J$ appartengono a $I \cap J$.

$x \in I \ y \in J \Rightarrow xy \in I \quad xy \in J$

per le proprietà di assorbimento.

<u>Prop.</u> Se $I + J = A$ allora $I \cdot J = I \cap J$.

<u>Dim</u> $I + J = A \Rightarrow \exists x \in I \ \exists y \in J$ tali che

$x + y = 1$.

Bisogna far vedere $I \cap J \subseteq I \cdot J$.

Sia $a \in I \cap J$

Moltiplico e ottengo

$$\underbrace{ax}_{\in I \cdot J} + \underbrace{ay}_{\in I \cdot J} = a$$

$\Rightarrow a = ax + ay \in I \cap J$.