ARITMETICA 23 NOV 2017

Note Title 11/23/2017

Oss. $f: G \to G'$ omomorfismo.
Sia $x \in G$ un elemento di ordine finito.
Allora $f(x)$ ha ordine finito e inoltre
$\text{ord}(f(x)) \mid \text{ord}(x)$.

Dim. $\text{ord}(x) = n$. Quindi $x^n = e$

$$[f(x)]^n = f(x^n)$$
$$[f(x)]^n = \underbrace{f(x) \cdot \dots \cdot f(x)}_{n \text{ volte}} = f(x^n) = e'$$

Quindi n è multiplo di $\text{ord}\, f(x)$,
o, equivalentemente, $\text{ord}\, f(x) \mid n$.

Teorema (di Cauchy, per gruppi abeliani).
Sia G un gruppo finito, di ordine n.
Sia p un numero primo tale che $p \mid n$.
Allora esiste $x \in G$ tale che $\text{ord}(x) = p$.

Esempio: $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non ha elementi di ordine 4.

Dim $p \mid n \Rightarrow n = p \cdot m$
Induzione su m.
Caso iniziale: $m = 1$ $(n = p)$
G è ciclico e ha un elemento di ordine 1 (e' ovvio) e tutti gli altri elementi di ordine p.
$< m \Rightarrow m$.

Sia $x \in G$ $x \neq e$.
Consideriamo $H = \langle x \rangle$
Gruppo abeliano $\Rightarrow H \trianglelefteq G \Rightarrow$ posso fare G/H.

$$|H| \cdot |G/H| = |G| = pm$$

1° caso $p \mid \text{ord}(H)$

Notando che H è un gruppo ciclico, sappiamo che H possiede un sottogruppo (ciclico) di ordine d per ogni divisore di $\text{ord}(H)$
Quindi esiste un sottogruppo di H (e quindi un sottogruppo di G) di ordine p.
Questo sottogruppo contiene elementi di ordine p.

2° caso $p \nmid \text{ord}(H)$ ma $p \mid \text{ord}(G/H)$

$\text{ord}(G/H) = pm'$ con $m' < m$
Infatti, $x \neq e \Rightarrow |H| > 1$.
$|G/H| < |G|$

Per ipotesi induttiva, G/H possiede un elemento di ordine p.

$$\pi : G \to G/H \quad \text{(proiezione canonica)}$$

(surgettiva) $\quad x \mapsto xH$ di ordine p

$$\text{ord}(xH) \mid \text{ord}(x)$$

Considero $K = \langle x \rangle$

K è ciclico, di ordine multiplo di p.
Come prima, K contiene un sottogruppo (ciclico) di ordine p. → FINE.

Esercizio Sia G un gruppo abeliano finito e sia $H < G$ tale che

① $(\text{ord}(H), \text{ord}(G/H)) = 1$

② Sia H che G/H sono ciclici.

Allora anche G è ciclico.

Soluzione $|G| = n \quad |H| = a \quad |G/H| = b$

$n = ab \qquad (a, b) = 1.$

1° fatto $\exists\, x \in G \ (x \in H)$ di ordine a (H è ciclico).

2° fatto $\exists\, \bar{y} \in G/H$ di ordine b.

$\exists\, y \in G : \pi(y) = \bar{y}$.

$\text{ord}(\bar{y}) \mid \text{ord}(y)$.

Considerando $K = \langle y \rangle$ (ciclico) ho che in G c'è un elemento di ordine b.

Consideriamo $g = xy$

Tesi: $\text{ord}(g) = ab = |G|$.

$$g^{ab} = (xy)^{ab} = \underbrace{xy \cdot xy \cdots xy}_{ab \text{ volte}} \overset{G \text{ abeliano}}{=}$$

$$= x^{ab} \cdot y^{ab} = e \cdot e = e$$

Questo dice che $\text{ord}(xy) \mid ab$.

Chiamiamo $d = \text{ord}(xy)$

$(xy)^d = x^d y^d = e.$

$x^d = (y^d)^{-1} = y^{-d}$

$\in$ $\in$

$H = \langle x \rangle$ $K = \langle y \rangle$

$ord(H) = a$ $ord(K) = b.$

$x^d = y^{-d} \in H \cap K$ $ord(H \cap K) \mid (a,b) = 1.$

$\Rightarrow H \cap K = \{e\}.$

$x^d = e$ $y^{-d} = e \Rightarrow y^d = e.$

$\Rightarrow a \mid d$, $b \mid d$

$(a,b) = 1 \Rightarrow ab \mid d$ CVD.

ANELLI

Def Un anello è un insieme A munito di due operazioni $(+, \cdot)$ con le seguenti proprietà:

(1) Rispetto all'operazione $+$, A è un gruppo abeliano.
Notazione: l'elemento neutro si chiamerà 0.

(2) L'operazione $\cdot$ è ASSOCIATIVA.

(3) Valgono le proprietà distributive:
$a(b+c) = ab + ac$ $(b+c)a = ba + ca$

Tipi di anelli secondo le proprietà della moltiplicaz.

- moltiplicazione commutativa → ANELLO COMMUTATIVO
- esistenza di un elemento neutro per la moltiplicazione (che verrà chiamato 1)
  → ANELLO CON UNITÀ o ANELLO UNITARIO.

Le due cose insieme danno un
ANELLO COMMUTATIVO CON UNITÀ.

Esempi: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m\mathbb{Z}$.
(Polinomi),
(Non commutativi: matrici $n \times n$ $(n>1)$
a coefficienti in un campo).
(Senza unità: $2\mathbb{Z}$)

Oss. In un anello A
$$0 \cdot x = x \cdot 0 = 0 \quad \forall x \in A$$
Infatti, $0 \cdot x = (0+0)x = 0 \cdot x + 0 \cdot x$
$$\Rightarrow 0 \cdot x = 0.$$

Oss. 2 Se A è un anello con unità
di almeno 2 elementi, allora $0 \neq 1$
Infatti, se fosse $0 = 1$, avrei
$$x = 1 \cdot x = 0 \cdot x = 0 \quad \forall x \in A$$
assurdo.

In particolare, A non può essere un
gruppo rispetto alla moltiplicazione, perché

0 non ha un inverso

Invece $A - \{0\}$ può essere un gruppo.

P. esempio se A è un campo

$A = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$.

Più in generale, se A possiede un'unità, posso considerare

$$A^* = \{x \in A \mid x \text{ ha un'inverso}\}$$

$\rightarrow A^*$ è UN GRUPPO.

Es. $(\mathbb{Z}/m\mathbb{Z})^*$ $\quad (\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*)$

Def. Un elemento x di un anello A si dice un DIVISORE DI ZERO se $\exists\, y \in A$, $y \neq 0$ tale che $xy = 0$ (oppure $yx = 0$).

Oss. Con la definizione precedente, in ogni anello con almeno due elementi, 0 è un divisore di 0.

- Se 0 è L'UNICO DIVISORE DI ZERO (BANALE) A si dice PRIVO DI DIVISORI di ZERO oppure (se è commutativo con identità) DOMINIO DI INTEGRITÀ

  (Es: CAMPI, POLINOMI, $\mathbb{Z}$)

- Ma, in molti casi, ci sono altri divisori di zero

  $A = \mathbb{Z}/6\mathbb{Z}$ $\qquad \bar{2} \cdot \bar{3} = \bar{0}$

Oss. Se D è l'insieme dei divisori di zero di un anello A, allora $D \cap A^* = \emptyset$.

Dim Banale se $A^* = \emptyset$ (A non ha 1)

Se no, sia, per assurdo

$$x \in D \cap A^*$$

$x \in D \Rightarrow \exists\, y \in A,\ y \neq 0$ t.c. $xy = 0$ *

$x \in A^* \Rightarrow \exists\, z \in A$ t.c. $zx = 1$. *

Allora

$$y = 1 \cdot y = (zx)y = z(xy) = z\,0 = 0$$

ASSURDO

* le ragionamento è simmetrico se scambiamo l'ordine.

Gruppi	$\longleftrightarrow$	Anelli
Sottogruppi	$\longleftrightarrow$	Sottoanelli
sottogruppi normali	$\longleftrightarrow$	Ideali

Def. Un sottoinsieme B di un anello A si dice un sottoanello di A se è esso stesso un anello con le operazioni indotte da A. (In particolare, $x, y \in B \Rightarrow x+y \in B,\ xy \in B$)

Es. $3\mathbb{Z}$ è un sottoanello di $\mathbb{Z}$

$\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$,

$4\mathbb{Z}/20\mathbb{Z}$ è un sottoanello di $\mathbb{Z}/20\mathbb{Z}$

Def Un ideale I di un anello A è un sottoinsieme di A tale che:

(1) I è un sottogruppo di A rispetto a $+$

(2) $\forall x \in A \quad \forall i \in I \qquad xi \in I \,,\; ix \in I$

(proprietà di assorbimento della moltiplicazione)

Esempio $m\mathbb{Z}$ è un ideale di $\mathbb{Z}$

mentre $\mathbb{Z}$ non è un ideale di $\mathbb{Q}$

$$\underset{\in \mathbb{Q}}{\frac{1}{3}} \cdot \underset{\in \mathbb{Z}}{1} = \frac{1}{3} \notin \mathbb{Z}$$

Anelli quoziente

I ideale di A

A/I = insieme delle classi laterali rispetto a $+$.

Operazioni

$$(x+I) + (y+I) = x+y+I \quad \text{(la solita)}$$

$$(x+I)\cdot(y+I) = xy+I$$

BEN DEFINITA?

Supponiamo $x'+I = x+I \qquad y'+I = y+I$

$$x' = x + i_1 \quad (i_1 \in I) \qquad y' = y + i_2 \quad (i_2 \in I)$$

$$x'y' = (x+i_1)(y+i_2) = xy + i_1 y + x i_2 + i_1 i_2$$

$\in I \qquad \in I \qquad \in I$

$x'y' \in xy + I$

$x'y' + I = xy + I$

Matrici

Ideale sinistro $\quad xI \subseteq I \quad \forall x$

Ideale destro $\quad Ix \subseteq I \quad \forall x$

Ideale proprio (o ideale bilatero)

$xI \subseteq I$ e $Ix \subseteq I \quad \forall x$

SIN. $\quad \ker f \trianglerighteq W \subset V \quad W$ sottospazio

DEL. $\quad \operatorname{Im} f \trianglelefteq W \subset V \quad$ "

BILATERO SOLO $\{0\}$ e TUTTE LE MATRICI.