ALGEBRA 1 — 9 OTT 2018

Note Title 10/9/2018

Formula delle classi (di coniugio).

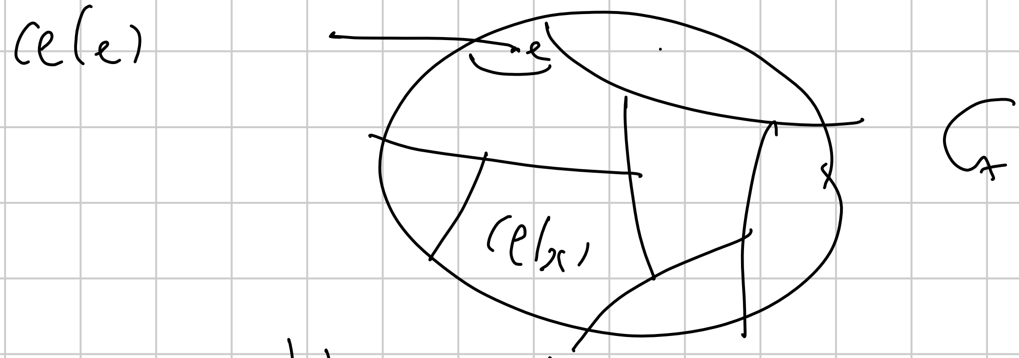
G gruppo finito.

(Le classi di coniugio sono le orbite dell'azione di G su G: $Cl(x) = \{gxg^{-1} \mid g \in G\}$)

→ Quindi sono una partizione di G.

$$|G| = \sum_{x \in R} |Cl(x)|$$

dove R è un insieme di rappresentanti delle classi di coniugio.



$$|Stab(x)|\,|Cl(x)| = |G|$$

$$Stab(x) = Z(x)$$

$$|Cl(x)| = \frac{|G|}{|Z(x)|}.$$

Termini $= 1$: $\dfrac{|G|}{|Z(x)|} = 1$ $\quad Z(x) = G$

cioè $x \in Z(G)$.

Separando i termini, ottengo:

$$\boxed{|G| = |Z(G)| + \sum_{x \in R'} \frac{|G|}{|Z(x)|}}$$

dove R è un insieme di rappresentanti delle classi di coniugio di elementi $\notin Z(G)$.

<u>Proprietà 1</u> Sia G un p-gruppo, cioè un gruppo la cui cardinalità è una potenza di un primo p, e sia $|G| > 1$.
Allora $Z(G) \neq \{e\}$. (non è banale).

<u>Dim.</u> Guardando gli addendi della formula delle classi, ho:

$$|G| = p^a$$

I termini a destra della somma sono tutti multipli di p. (sono potenze di $p > 1$). $\left(\frac{p^n}{\#}\right)$

Per differenza, $|Z(G)|$ è un multiplo di p. (quindi > 1).

<u>Oss.</u> Se $|G| = p^3$ e G non è abeliano, allora $|Z(G)| = p$.

Infatti $|Z(G)| = \begin{cases} 1 & \to \text{NO (formula delle classi)} \\ p & \\ p^2 & \text{ASSURDO} \\ p^3 & \to \text{NO } (G \text{ non è abeliano}) \end{cases}$

$G/Z(G)$ non è ciclico.

Proprietà 2 Se $|G| = p^2$, allora G è abeliano.

$$|Z(G)| = \begin{cases} 1 & \text{NO} \\ p & \text{NO} \quad (G/_{Z(G)} \text{ non è ciclico}) \\ p^2 & \text{SI} \end{cases}$$

Inoltre, $G \cong \mathbb{Z}/_{p^2\mathbb{Z}}$ (se è ciclico)

oppure $G \cong \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{p\mathbb{Z}}$.

Teorema (di Cauchy generale).
Se $|G| = n$ e p è un primo tale che $p \mid n$, allora esiste $x \in G$ tale che $\mathrm{ord}(x) = p$.

Dim. Sappiamo già che il teorema è vero nel caso G abeliano.
Usiamo l'induzione su $|G|$.
Supponiamo $|G| = pm$
e che il teorema sia vero per ogni gruppo H con $|H| = pm'$, $m' < m$
(passo base: $m = 1$).

1° caso $\exists\, x \in R'$ t.c. $|Z(x)|$ è un multiplo di p.
Funziona il passo induttivo: $\exists\, y \in Z(x)$ di ordine p.

2° caso $\forall\, x \in R'$ $|Z(x)|$ non è multiplo di p,
quindi $\left|\dfrac{G}{Z(x)}\right|$ è multiplo di p.

Allora, per differenza nella F.d.C., si ha che $|Z(G)|$ è multiplo di p.
$\longrightarrow$ Posso usare il teorema nel caso abeliano.

$A_4 < S_4$ $\qquad |A_4| = 12 \qquad |S_4| = 24$

gruppo alterno (= permutazioni pari)

$\{e\}$ $\qquad 1$

$\{(ab)(cd)\} = \{(12)(34),\ (13)(24),\ (14)(23)\}$ $\qquad 3$

$\{(abc)\} \to 8$ permutazioni

$\binom{4}{3} \cdot 2 = 8$ $\qquad \dfrac{8}{12}$

(Se si fissano k elementi, un ciclo con questi k elementi si può fare in $(k-1)!$ modi.

$(1\,2\,3 \dots k) = (2\,3 \dots k\,1)$ $\qquad \dfrac{k!}{k}$)

A_4 NON HA sottogruppi di ordine 6.

Se esistesse $H < A_4$ con $|H| = 6$, allora necessariamente avremmo $H \trianglelefteq A_4$.

Un sottogruppo normale è un'unione di classi di coniugio.

$(x \in H \Rightarrow gxg^{-1} \in H)$

Classi di coniugio in S_n e in A_n.

$\sigma \in A_n$ $\qquad |cl_{S_n}(\sigma)| = \dfrac{|S_n|}{|Z_{S_n}(\sigma)|} = \dfrac{n!}{|Z_{S_n}(\sigma)|}$

(*) $\qquad |cl_{A_n}(\sigma)| = \dfrac{|A_n|}{|Z_{A_n}(\sigma)|} = \dfrac{n!/2}{|Z_{A_n}(\sigma)|}$

Ho due casi:

(1) $Z_{A_n}(\sigma) = Z_{S_n}(\sigma)$

(cioè tutte le permutazioni che commutano con σ sono pari).

(2) $Z_{A_n}(\sigma) \neq Z_{S_n}(\sigma)$.

(cioè esiste una permutazione dispari che commuta con σ).

Se si verifica il caso (1), la formula (*) dà

$$|Cl_{A_n}(\sigma)| = \frac{n!/2}{|Z_{A_n}(\sigma)|} = \frac{n!/2}{|Z_{S_n}(\sigma)|} =$$

$$= \frac{|Cl_{S_n}(\sigma)|}{2}.$$

Se si verifica il caso 2, abbiamo:

$$Z_{A_n}(\sigma) = Z_{S_n}(\sigma) \cap A_n.$$

e vale la formula

$$|Z_{S_n}(\sigma) \cap A_n| \, |\underbrace{Z_{S_n}(\sigma) \cdot A_n}_{S_n}| = |Z_{S_n}(\sigma)| \cdot |A_n|$$

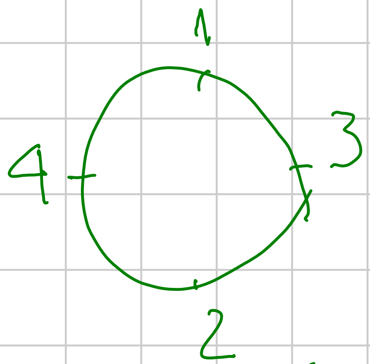
$$|Z_{A_n}(\sigma)| = |Z_{S_n}(\sigma) \cap A_n| = \frac{|Z_{S_n}(\sigma)| \cdot \frac{n!}{2}}{n!} = \frac{|Z_{S_n}(\sigma)|}{2}.$$

Quindi

$$|cl_{A_n}(\sigma)| = \frac{|A_n|}{|Z_{A_n}(\sigma)|} = \frac{n!/2}{\frac{|Z_{S_n}(\sigma)|}{2}}$$

$$= |cl_{S_n}(\sigma)|.$$

$\sigma = (12)(34)$



$\tau = (1324)$

$\tau^2 = \sigma$

τ commuta con σ, (τ è dispari)

Prendiamo, per esempio, $\sigma = (123)$

$Z_{S_n}(\sigma) = \langle \sigma \rangle$ $\quad |Z_{S_n}(\sigma)| = 3$

$\downarrow$ tutte permutazioni pari.

La suddivisione di A_4 in classi di coniugio è del tipo $1 + 3 + \underbrace{4 + 4}_{8}$

Con questi addendi NON SI FA 6

$\to$ NON ESISTE UN SOTTOGRUPPO DI ORDINE 6 in A_4.

<u>Proprietà 3</u> In un p-gruppo G esistono sottogruppi di ogni ordine divisore dell'ordine di G.

<u>Dim.</u> $|G| = p^n$. Induzione su n.

Casi iniziali $n = 0, 1$ banali.

Passo induttivo

Caso G abeliano

$\exists\, x \in G$: $ord(x) = p$ $\quad H = \langle x \rangle$

$H \trianglelefteq G$.

$\pi : G \to G/H$

(cerco $K < G$ $|K| = p^k$)

Basta considerare $K > H$ t.c. $|\pi(K)| = p^{k-1}$.
(Infatti G/H ha ordine < ordine di G, e per ipotesi induttiva esiste $K' < G/H$ di ordine p^{k-1})

$K = \pi^{-1}(K')$.

Caso generale (Possiamo supporre G non abeliano).

$$\pi : G \to G/Z(G)$$

$$|G| = p^n \qquad |Z(G)| = p^a \quad a \geq 1$$

$$|G/Z(G)| = p^{n-a}.$$

Cerco un sottogruppo di ordine p^k $(0 \leq k \leq n)$.

Se $k \leq a$, trovo questo sottogruppo già in $Z(G)$ (caso abeliano).

Se $k > a$, uso l'induzione:
$G/Z(G)$ possiede un sgr K' di ordine p^{k-a}.

e $\pi^{-1}(K')$ ha ordine p^k.

<u>Proprietà 4</u> G p-gruppo, $H < G$, $H \neq G$.
Allora $N(H) \supsetneq H$.

<u>Dim</u> Due casi.

1. $H \not\supseteq Z(G)$
2. $H \supseteq Z(G)$

Nel caso 1 ho che $N(H) \supseteq \begin{cases} H \\ Z(G) \end{cases}$
$N(H) \supseteq H \cdot Z(G) \supsetneq H$.

Nel caso 2 considero la proiezione:

$$\pi : G \to G/_{Z(G)} \qquad \pi(H) = H'$$

Per induzione sull'ordine, $N(H') = K' \supsetneq H'$

e $N(H) \underset{\downarrow}{=} \pi^{-1}(K') = K \supsetneq H$

esercizio