p-GRUPPI

Da questo momento G sarà gruppo finito e p sarà un numero primo di $\mathbb{N}$

Def: G è un p-gruppo se $|G| = p^n$

Osservazione: Sia G un p-gruppo

i) $H \leq G \Rightarrow H$ è un p-gruppo

ii) $H \triangleleft G \Rightarrow G/H$ è un p-gruppo

Proposizione: G p-gruppo che agisce su X con $|X| \not\equiv 0 \pmod p \Rightarrow \exists\, x \in X$ tale che $g(x) = x$ per ogni $g \in G$

[l'azione di G ammette un punto fisso]

Dim:
$$|X| = \sum_{x \in \Gamma} |G : \mathrm{stab}_G(x)|$$
con Γ che contiene esattamente 1 elemento per orbita

Se non ci sono punti fissi: $\mathrm{stab}_G(x) \neq G \ \forall x \in \Gamma$

per cui

$$|\mathrm{stab}_G(x)| < |G| \quad \text{e} \quad |G : \mathrm{stab}_G(x)| = \frac{|G|}{|\mathrm{stab}_G(x)|} > 1$$

per ogni $x \in \Gamma$

Da questo si ricava che $|G : stab_G(x)|$ è una potenza non banale di p $\forall x \in \Gamma$

cioè $p \mid |G : stab_G(x)| \quad \forall x \in \Gamma$

Se così fosse $|X| = \sum_{x \in \Gamma} |G : stab_G(x)|$

sarebbe multiplo di p, cosa che non può accadere perché $|X| \not\equiv 0 \bmod p$

□

Teorema: Sia G p-gruppo e $H \triangleleft G$

Se $H \neq \{1_G\}$ allora $H \cap Z(G) \neq \{1_G\}$

In particolare se $G \neq \{1_G\}$ allora $Z(G) \neq \{1_G\}$

[i p-gruppi hanno centro non banale]

Dim: • G agisce per coniugazione su H

• siccome $(1_G)^g = 1_G$ per ogni G

G agisce su $H \setminus \{1_G\}$ per coniugazione

e $|H \setminus \{1_G\}| = p^n - 1$ per cui

$|H \setminus \{1_G\}| \not\equiv 0 \pmod p$

- l'azione ha punto fisso

i.e. $\exists\, h \in H \setminus \{1_G\}$ t.c. $h^g = h \;\forall g \in G$

cioè $\exists\, h \in H \setminus \{1_G\}$ tc $gh = hg \;\forall g \in G$

$\Rightarrow$

$\exists\, h \neq \{1_G\}$ tc $h \in H \cap Z(G)$ □

Teorema Sia G p-gruppo, $H \leq G$

allora o $H \lhd G$ oppure $\exists\, g \in G$ tc $H^g \neq H$ e $H^g \leq N_G(H)$

Dim. Supponiamo H non normale allora

- $N_G(H) \neq G$ e $|\{H^g \mid g \in G\}| = \dfrac{|G|}{|N_G(H)|} = p^k$ con $k > 0$

Definiamo $\Gamma = \{H^g \mid g \in G \text{ e } H^g \neq H\}$

Allora $|\Gamma| = p^k - 1 \not\equiv 0 \mod p$

e

H agisce su Γ

(infatti se $(H^g)^x = H$ con $x \in H$ allora $H^g = H^{x^{-1}} = H$)

$\Rightarrow$ H fisse un elemento in Γ

↑ prop. inizio lezione

$\Rightarrow \exists\, g \in G$ t.c H normalizze $H^g \neq H$

$\Rightarrow H \subseteq N_G(H^g) \Rightarrow H^{g^{-1}} \subseteq (N_G(H^g))^{g^{-1}} = N_G(H)$

con $H^{g^{-1}} \neq H$ (perchè $H^g \neq H$)

Teorema Se $H \leq G$, G p-gruppo e $H \neq G$ allora $N_G(H) \neq H$ (i.e. H è un sottogruppo proprio di $N_G(H)$)

Dim se $H \trianglelefteq G$ allora $N_G(H) = G \neq H$ per ipotesi

se H non è normale in G esiste $x \in G$ tale che $H^x \leq N_G(H)$ e $H \neq H^x$ quindi $N_G(H) \neq H$

Corollario G p-gruppo $M \leq G$ massimale (i.e. $M \neq G$ e se $M \leq M' \leq G$ allora $M = M'$ o $M' = G$)

allora $M \triangleleft G$ e $G/M \cong \mathbb{Z}_p$ $(|G:M| = p)$

Dimostrazione: $M \leq N_G(M) \leq G$

per cui o $N_G(M) = M$ impossibile per teorema precedente

o $N_G(M) = G \Rightarrow M \triangleleft G$

Inoltre abbiamo la seguente biezione

$$\{\text{sottogruppi di } G/M\} \xleftrightarrow{\text{biezione}} \{\text{sottogruppi di } G \text{ contenenti } M\}$$

$$= \{M, G\} \quad (M \text{ massimale})$$

Allora G/M non ha sottogruppi propri non banali $\Rightarrow$ G/M ciclico di ordine primo $\Rightarrow G \cong \mathbb{Z}_p$

(vedi primo foglio di esercizi)

(G/M p-gruppo)

Def. 1) $H \leq G$ se H p-gruppo (i.e. $|H| = p^k$)

allora H si dice **p-sottogruppo** di G

2) Sia G gruppo t.c $|G| = p^n m$ con $MCD(p,m) = 1$

se $H \leq G$ con $|H| = p^n$ allora H si dice

un **p-sottogruppo di Sylow** (o **p-Sylow**) di G

Esempio : A_4 $\quad |A_4| = 12 = 2^2 \cdot 3$

$S = \langle (1,2,3) \rangle \cong \mathbb{Z}_3 \quad |S| = 3$

$\Rightarrow$ S è un 3-Sylow

$H = \langle Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$|H| = 4 = 2^2 \quad \Rightarrow$ H è un 2-Sylow

Nell'esempio esistono p-Sylow per ogni p

[se p non dividesse $|G|$ allora formalmente possiamo considerare $\{1\}$ come p-Sylow ma è poco rilevante infatti di solito si consideravano solo i p-Sylow non banali]

È vero sempre? Teoremi di Sylow !! (prossima lezione)

[secondo il Sozuki il "più fondamentale" risultato per i gruppi finiti]