

### Teorema:

Dati  $G$  gruppo risolubile,  $H, N$  sottogruppi di  $G$ , si ha:

- 1)  $H$  è risolubile
- 2) Se  $N$  è normale in  $G$ , allora  $G/N$  è risolubile

Moltre, dati  $G$  gruppo,  $N$  sottogruppo normale di  $G$ , si ha:

$$N, G/N \text{ risolubili} \Rightarrow G \text{ è risolubile.}$$

### Dim.:

1)  $G$  risolubile  $\Rightarrow \exists$  serie abeliana  $H_0 = \{1\}, \dots, H_n = G$  t.c.  $H_0 \triangleleft \dots \triangleleft G$ . Sia  $H \subseteq G$  sottogruppo, consideriamo:

$$H_i' = H \cap H_i \quad (\Rightarrow H_0' = H \cap H_0, \dots)$$

si ha:

$$H_0' = \{1\} \trianglelefteq \dots \trianglelefteq H_n' = H.$$

Mostriamo ora che  $H_i'/H_{i-1}'$  è abeliano:

$$H_i'/H_{i-1}' = H_i/(H_{i-1} \cap H) \cong H_i/H_{i-1} \subseteq$$

$\Rightarrow H$  è risolubile.

Sia ora  $N$  normale in  $G$ :

$$H_0'' = N/N, H_1'' = H_1 N/N, \dots, H_i'' = H_i N/N$$

$\Rightarrow$  sono sottogruppi, mostriamo che sono abeliani:

$$H_i'' = H_i N/N \cong H_i/H_{i-1} N$$

$H_i''/H_{i-1}''$  è un quoziente di  $H_i/H_{i-1}$ , quindi

$\bar{e}$  abeliana

$\Rightarrow H_0'' = \frac{N}{N} \trianglelefteq \dots \trianglelefteq H_n'' = G/N$   $\bar{e}$  una serie abeliana.

$\Rightarrow G/N$   $\bar{e}$  risolubile.

2)  $N$  normale e risolubile in  $G$ ,  $G/N$  risolubile

$\Rightarrow \exists \{1\} = H_0 \trianglelefteq \dots \trianglelefteq H_n = N$  serie abeliana in  $N$

$\Rightarrow \exists \{1\} = \frac{N}{N} = \frac{K_0}{N} \trianglelefteq \dots \trianglelefteq \frac{K_m}{N} = G/N$  serie abeliana in  $G/N$  ( $K_i$  sottogruppo di  $G/K_i \supseteq N$ )

$\Rightarrow (K_i/N)/_{(K_{i-1}/N)} \cong K_i/K_{i-1}$   $\bar{e}$  abeliana

$\Rightarrow$  quindi:

$\{1\} = H_0 \trianglelefteq \dots \trianglelefteq H_n = N \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_m = G$

$\bar{e}$  una serie abeliana in  $G$

$\Rightarrow G$   $\bar{e}$  risolubile

q.e.d.

Teorema (di Cauchy):

Dato  $G$  gruppo finito,  $p$  primo t.c.  $p \mid |G|$ , si ha che  $G$  possiede un sottogruppo di ordine  $p$  e  $G$  possiede un elemento di ordine  $p$

Dim.

Devo trovare elementi di ordine  $p$ . Considero quindi:

$X \subseteq G^P$  formato dalle  $p$ -uple

$\hat{x} = (x_1, \dots, x_p) \in G^P$  t.c.  $x_1 \cdots x_p = 1$

$\Rightarrow X \neq \emptyset, (1, \dots, 1) \in X$

$\Rightarrow$  definiamo  $\varphi: X \rightarrow X$  t.c.  $\varphi(\hat{x}) = (x_2, \dots, x_p, x_1)$

(si ha che  $\beta(\hat{x}) \in X : x_1 \cdots x_p \cdot x_1 = x_1^{-1} (x_1 \cdots x_p) \cdot x_1 = x_1^{-1} x_1 = 1$ )

$\Rightarrow$  definiamo  $\sim$  t.c. :

$$\hat{x} \sim \hat{y} \Leftrightarrow \exists k \text{ t.c. } \hat{y} = \beta(\hat{x})^k$$

$$(\hat{y} = (x_{k+1}, \dots, x_p, x_1, \dots, x_k))$$

$\Rightarrow$  quanti sono gli elementi di  $[\hat{x}]_\sim$ ?

Sono 1 oppure p:

$$[\hat{x}]_\sim = \{\hat{x}\} \Leftrightarrow \hat{x} = (a, \dots, a)$$

$$\text{altrimenti } |[\hat{x}]_\sim| = p$$

Quindi  $\sim$  induce una partizione formata da singoletti e da insiemi di p elementi

$\Rightarrow |X| = \text{multiplo di } p$ , ausi  $|X| = |G|^{p-1}$

(si può scegliere arbitrariamente  $x_1, \dots, x_{p-1} \in G$  e allora  $(x_1, \dots, x_{p-1}, (x_1 x_2 \cdots x_{p-1})^{-1}) \in X$

$\Rightarrow$  Una classe di equivalenza con 1 solo elemento è  $[(1, \dots, 1)]_\sim$ , quindi ce ne sono almeno altre  $p-1$

q.e.d.

Per gruppi abeliani:

$$a^m b^m = (ab)^m \dots$$

$$\Rightarrow G_p = \{a \in G \mid a^{p^k} = 1 \text{ per un certo } k\}$$

Teatema (di Wielandt):

Dato  $G$  gruppo, se  $p^k \mid |G|$  con  $p$  primo, allora  $\exists H \leq G$  sottogruppo t.c.  $|H| = p^k$

Dim.

Consideriamo  $X = \text{insieme di tutti i sottoinsiemi di } G \text{ di cardinalità } p^k$ ,  $X \neq \emptyset$  ( $|G| = s \cdot p^k$ ). Definiamo su  $X$  l'azione di traslazione a sinistra:

$$a \in G, X \in X, aX = \{ax \mid x \in X\}$$

$\Rightarrow X \rightarrow aX$ ,  $x \mapsto ax$  è biettiva

$\Rightarrow$  siano  $O(x_1), \dots, O(x_m)$  le orbite distinte dell'azione.

$\Rightarrow$  sappiamo che  $|X| = \sum_{i=1}^m |O(x_i)| = \sum_{i=1}^m [G : G_{x_i}]$   
e  $|X| = \binom{n}{p^k}$  dove  $n = |G|$ , tuttavia:

$$\binom{n}{p^k} = \binom{n-1}{p^{k-1}} \frac{n}{p^k}$$

$\Rightarrow n = p^l q_0$  con  $p \nmid q_0$  e quindi  $k \leq l$

$\Rightarrow$  dimostriamo che  $\binom{n-1}{p^{k-1}}$  non è divisibile per  $p$ :

$$\binom{n-1}{p^{k-1}} = \frac{(n-1)!}{(p^{k-1})! (n-p^k)!} = \frac{(n-1)(n-2)\dots(n-p^{k-1})}{(p^{k-1}) \cdot (p^{k-2}) \dots 3 \cdot 2 \cdot 1}$$

$\Rightarrow$  per  $1 \leq s \leq p^{k-1}$  scriviamo  $s = p^{k_s} q_s$  con  $p \nmid q_s$  e  
 $n = p^k q$ , sicuramente  $k_s < k$

$$\Rightarrow \frac{n-s}{p^{k-s}} = \frac{p^k q - p^{k_s} q_s}{p^k - p^{k_s} q_s} = \frac{p^{k-k_s} q - q_s}{p^{k-k_s} - q_s} = \frac{p \cdot u_s - q_s}{p \cdot v_s - q_s}$$

$\Rightarrow \binom{n-1}{p^{k-1}} = \frac{p^u + r}{p^v + r}$  con  $r = \prod_s (-q_s)$ , quindi si ha:

$$\binom{n-1}{p^{k-1}} \in \mathbb{Z} \wedge pu+r \text{ non è divisibile per } p$$

$\Rightarrow \binom{n-1}{p^{k-1}}$  non è divisibile per  $p$

$\Rightarrow |X|$  è divisibile per  $p^{l-k}$  MA non per  $p^{l-k+1}$

$\Rightarrow \exists x_i \in X$  t.c.  $[G : G_{x_i}]$  non è divisibile per  $p^{l-k+1}$

sia  $Y = X_i$ .

$\Rightarrow$  per il Teorema di Lagrange si ha:

$$|G| = |G_Y| \cdot [G : G_Y]$$

$$\Rightarrow p^{\ell} q_0 = |G_Y| \cdot \underbrace{[G : G_Y]}_{\text{non divisibile per } p^{l-k+1}}$$

$\Rightarrow |G_Y|$  è divisibile per  $p^k$ .

$\Rightarrow$  se consideriamo  $f: G_Y \rightarrow Y$  t.c.  $f(a) = a_Y, y \in Y$   
osserviamo che  $f$  è iniettiva, quindi:

$$|G_Y| \leq |Y| = p^k$$

q.e.d.

Siano ora  $G$  gruppo,  $H \subseteq G$  sottogruppo. Dato  $a \in G$ ,  
se  $|H| = m$ , allora  $f_a(H) = aHa^{-1}$  ha ordine  $m$  (con  
 $f_a(x) = axa^{-1}$  coniugio di  $a$ )

Def. ( $p$ -Sylow):

Un  $p$ -sottogruppo di Sylow di  $G$  ( $p$ -Sylow) è un  
 $p$ -sottogruppo di  $G$  massimale: l'ordine di  $p$ -Sylow è  
la massima potenza di  $p$  che divide  $|G|$

Lemma:

Se  $H$  è un  $p$ -sottogruppo di  $G$  e  $P$  è un  $p$ -Sylow di  
 $G$ ,  $\exists a \in G$  t.c.  $H \subseteq aPa^{-1}$

Dim.:

Sia l'azione di  $H$  su  $X = G_p = \{aP \mid a \in G\}$

$$\Rightarrow h \cdot (\alpha P) = (h\alpha)P \Rightarrow |P| = p^k, [G:P] = q \text{ con } p \nmid q$$

$\Rightarrow$  consideriamo le orbite distinte  $O(\alpha_1 P), \dots, O(\alpha_r P)$

e siamo  $H_i = H_{\alpha_i} P$  gli stabilizzatori di  $\alpha_i P$

$$\Rightarrow q = \sum_{i=1}^r |O(\alpha_i P)| = \sum_{i=1}^r [H : H_i]$$

$\Rightarrow$  uno degli indici  $[H : H_i] = 1$ , quindi  $O(\alpha_i P) = \{\alpha_i P\}$

$\Rightarrow \alpha = \alpha_i$ , allora se  $b \in H$ ,  $b(\alpha P) = \alpha P \Rightarrow b\alpha \in \alpha P$

$$\Rightarrow b \in \alpha P \alpha^{-1} \Rightarrow H \subseteq \alpha P \alpha^{-1}$$

q.e.d.

Esempio (di p-Sylow):

$$1) |S_3| = 6 \Rightarrow 2\text{-Sylow} = \{<(12)>, <(13)>, <(23)>\}$$

$$3\text{-Sylow} = \{<(123)>\} = A_3$$

$$2) |S_4| = 24 \Rightarrow 2\text{-Sylow} \text{ devono avere ordine } 8,$$

$$3\text{-Sylow} = \{<(123)>, <(124)>, <(234)>, \dots\}$$

$\Rightarrow$  si dimostra che, se  $s_p$  è il numero di p-Sylow in  $G$ , allora  $s_p \mid \frac{|G|}{p^k}$  e  $s_p \equiv 1 \pmod{p}$

Teorema (di Sylow):

Dato  $G$  gruppo t.c.  $|G| = p^k q$  con  $p \nmid q$ ,  $k \geq 1$ ,  $p$  primo, si ha:

1)  $G$  possiede  $p$ -sottogruppi di Sylow (Teorema di Wielandt)

2)  $P, Q$  p-Sylow di  $G \Rightarrow \exists \alpha \in G$  t.c.  $Q = \alpha P \alpha^{-1}$

3) il numero  $s_p$  dei p-sylow di  $G$  è divisibile da  $q$

e si ha  $s_p \equiv 1 \pmod{p}$

Dim.:

(1), (2) già dimostrate sopra ✓

3) Consideriamo l'azione di  $G$  sull'insieme dei sottogruppi di  $G$  per conjugio. Allora  $s_p$  è la cardinalità dell'orbita di un  $p$ -Sylow. Quindi  $s_p = [G : N_G(P)]$  con  $N_G(P) = \{\alpha \in G \mid \alpha P \alpha^{-1} = P\}$ . Applicando Lagrange si ha:

$$s_p = [G : N_G(P)] = \frac{[G : P]}{[N_G(P) : P]} \text{ divisione di } q = [G : P] \quad \checkmark$$

Il sottogruppo  $P$  agisce sull'insieme  $\mathcal{P}$  dei  $p$ -Sylow per conjugio ( $\alpha Q = \alpha(Q\alpha^{-1})$ ). Allora si ha:

$O(P) = \{P\}$  unica orbita con un elemento.

Se prendiamo le orbite  $O(Q_1), \dots, O(Q_r)$  con  $Q_1 = P$  sappiamo che:

$$s_p = \sum_{i=1}^r |O(Q_i)| = 1 + \underbrace{\sum_{i=2}^r [P : P_{Q_i}]}_{\text{multipli di } p}$$

$$\Rightarrow s_p \equiv 1 \pmod{p} \quad \checkmark$$

q.e.d.

Esempio ( $S_4$ ):

$\Rightarrow |S_4| = 2^3 \cdot 3 \Rightarrow$  un 2-Sylow ha ordine 8:

$$s_2 \mid 3 \wedge s_2 \equiv 1 \pmod{2} \Rightarrow s_2 = 3$$

$\Rightarrow$  Uno dei 2-Sylow è  $D_4$ .

$\Rightarrow$  I 3-Sylow hanno ordine 3:

$$s_3 | 8 \wedge s_3 \equiv 1 \pmod{3} \Rightarrow s_3 = 4 \vee s_3 = 1$$

$\Rightarrow P = \langle (123) \rangle$  non è normale in  $S_4$  perché  
 $(14)(123)(14) = (1)(234) \notin S_4$

esercizio:

Dato  $p$  primo, allora un gruppo di ordine  $p^2$  è isomorfo a  $\mathbb{Z}/p^2\mathbb{Z}$  oppure a  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$\Rightarrow$  supponiamo che  $|G| = p^2$  e  $G$  non sia ciclica.

Allora  $G$  è abeliano. Siano  $a \in G$  di ordine  $p$ ,  $b \in G$  t.c.

$b \notin \langle a \rangle$ ,  $|\langle b \rangle| = p$ . Definiamo la funzione  $f$  t.c.:

$$\begin{aligned} f: \langle a \rangle \times \langle b \rangle &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

$\Rightarrow f$  è omomorfismo ( $G$  è abeliano), calcolando il Ker si ha:

$$(x, y) \in \text{Ker } f \Leftrightarrow xy = 1 \Leftrightarrow y = x^{-1}$$

$\Rightarrow y \in \langle a \rangle \cap \langle b \rangle \Rightarrow$  dato che  $|\langle a \rangle| = p$  si ha:

$$\langle a \rangle \cap \langle b \rangle = \{1\} \text{ OPPURE } \langle a \rangle \cap \langle b \rangle = \langle a \rangle$$

ma quest'ultima implicherebbe  $b \in \langle a \rangle \not\subseteq$

$\Rightarrow f$  iniettiva  $\Rightarrow f$  suriettiva  $\Rightarrow f$  isomorfismo

$$\Rightarrow \langle a \rangle \cong \mathbb{Z}/p\mathbb{Z} \cong \langle b \rangle \checkmark$$

N.B.

Nei gruppi abeliani, tutti i  $p$ -Sylow hanno ordine 1 (ovvero ogni  $p$ -Sylow è normale) !!!