Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Giovanni Zacher

Una caratterizzazione reticolare della finitezza dell'indice di un sottogruppo in un gruppo

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **69** (1980), n.6, p. 317–323.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1980_8_69_6_317_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1980.

Teoria dei gruppi. — *Una caratterizzazione reticolare della finitezza dell'indice di un sottogruppo in un gruppo.* Nota di GIOVANNI ZACHER (*), presentata (**) dal Socio G. SCORZA DRAGONI.

SUMMARY. — A lattice characterization of the finiteness of the index of a subgroup in a group is given, and some consequences are derived.

Nello studio delle proiettività di un gruppo G su un gruppo $\overline{G}$, vale a dire degli isomorfismi tra il reticolo L(G) di tutti i sottogruppi di G e quello L($\overline{G}$) di $\overline{G}$, ha un notevole interesse sapere se la finitezza dell'indice di un sottogruppo H di G è un invariante proiettivo o meno.

Scopo principale della presente Nota è di provare che effettivamente dal reticolo L(G) si può riconoscere se è finito o meno l'indice [G : H] di un sottogruppo H di G; qualche utile conseguenza sarà pure messa in evidenza.

Premettiamo alcune convenzioni di notazione.

Se $\sigma : G \to \overline{G}$ è una proiettività, se $X \leq G$ e $\bar{g} \in \overline{G}$, per il sottogruppo $X^{\sigma\bar{g}\sigma^{-1}}$ di G si scriverà $X^{\bar{g}}$ e porremo $X_{\overline{G}} = \bigwedge_{\bar{g} \in \overline{G}} X^{\bar{g}}$; $H \underset{d}{\leq} G$ sta per H sottogruppo di Dedekind (1) di G, $H \underset{q}{\leq} G$: H quasinormale in G, $H \lessdot G$: H sottogruppo massimo di G, [G/H]: intervallo di estremi G, H; per il resto la notazione è quella standard di teoria dei gruppi.

LEMMA 1. *Sia* $\sigma : G \to \overline{G}$ *una proiettività del gruppo* G *su quello* $\overline{G}$, *ed* N *un sottogruppo normale e d'indice primo in* G. *Allora l'indice di* N^σ *in* $\overline{G}$ *è pure un numero primo* (2).

Dimostrazione. Poichè $N \underset{d}{\lessdot} G$, per concludere basterà far vedere che N^σ ha indice finito in $\overline{G}$ [3].

Se $N^\sigma \lhd \overline{G}$, la conclusione è banale.

Sia dunque $N^\sigma \ntriangleleft G$. Posto $G = \langle N, a \rangle$ e $\langle \bar{a} \rangle = \langle a \rangle^\sigma$, abbiamo $\overline{G} = \langle \overline{N}, \bar{a} \rangle$ e da $\overline{N}^{\bar{a}^i} \underset{d}{\lessdot} \overline{G}$ segue $\overline{N}^{\bar{a}^i} \wedge \langle \bar{a} \rangle = \langle \bar{a}^q \rangle$ ove q è un primo, per cui $\bar{a}^q \in \overline{N} \wedge \overline{N}^{\bar{a}} \wedge \cdots \wedge \overline{N}^{\bar{a}^{q-1}} = \overline{T}$ e $\overline{T} \lhd \langle \bar{a}, \overline{T} \rangle = \overline{H}$ e da $\overline{T} < \overline{X} \leq \overline{N}^{\bar{a}^i}$ segue $\overline{X}^{\bar{a}^j} \neq \overline{X}$ per $0 < j \leq q - 1$ avendosi $\bigwedge_i \overline{X}^{\bar{a}^i} = \overline{T}$. Ora $\overline{N} \vee \overline{H} = \langle \overline{N}, \bar{a} \rangle = \overline{G}$ e cosi da $\overline{T} \lessdot \overline{H}$ e $\overline{N} \wedge \overline{H} \geq \overline{T}$ segue pure $\overline{N} \wedge \overline{H} = \overline{T}$.

(*) Ind. dell'A: Istituto di Algebra e Geometria, Via Belzoni 7, 35100 Padova.

(**) Nella seduta del 6 dicembre 1980.

(1) Ricordiamo che H si dice un sottogruppo di Dedekind in G se e solo se per due qualunque sottogruppi X, Y di G, da $H \leq X$ segue $H \vee (X \wedge Y) = (H \vee Y) \wedge X$ e da $X \leq Y$ segue $X \vee (H \wedge Y) = (X \vee H) \wedge Y$.

(2) La prima dimostrazione di questo teorema ho saputo essere stata indicata da I. A. Rips (Aggiunto sulle bozze di stampa: di questa dimostrazione ho ricevuto copia quando la mia Nota era stata già presentata all'Accademia Lincea).

Pertanto in G avremo le relazioni:

$$\text{(1)} \qquad H \vee N = G\,,\, T = H \wedge N \lhd\cdot H\,,\, N^{\bar{a}^i} \underset{d}{<} G\,,\, \bigwedge_i N^{\bar{a}^i} = T$$

$$\text{e da } T < X \leq N^{\bar{a}^i} \text{ segue } X^{\bar{a}^j} \neq X \text{ non appena } 0 < j \leq q - 1.$$

Poniamo per semplicità $N_i = N^{\bar{a}^i}$, $i = 0, 1, \cdots, q-1$ e per $0 \leq i_1 < i_2 \cdots < i_s \leq q - 1$ $(s \leq q)$, $I_{i_1 i_2 \cdots i_s} = N_{i_1} \wedge N_{i_2} \wedge \cdots \wedge N_{i_s}$. L'insieme

$$\mathscr{F} = \{G\,,\, I_{i_1 \cdots i_s} \mid 0 \leq i_1 < i_2 \cdots < i_s \leq q - 1\,,\, 1 \leq s \leq q\}$$

si ordina parzialmente per inclusione; in esso le catene hanno lunghezza al più q e soddisfano alla condizione di Jordan-Dedekind, per cui in modo naturale si può parlare per i suoi elementi di dimensione e codimensione [1]: tutto ciò segue dal fatto che $N^{\bar{a}^i} \underset{d}{<} G$. Se l è la lunghezza massima delle catene di $\mathscr{F}$, scelto un naturale d con $1 \leq d < l$, fra gli elementi di $\mathscr{F}$ di dimensione d, prendiamo, per fissare le idee:

$$I_{1,2 \cdots s} = N_1 \wedge \cdots \wedge N_s;$$

in tale rappresentazione non sarà restrittivo supporre che non si può semplificare agli estremi nel senso che

$$N_1 \wedge N_2 \wedge \cdots \wedge N_s \lessdot N_1 \wedge N_2 \wedge \cdots \wedge N_{s-1}$$

(si legga G se $s - 1 = 0$) e $N_1 \wedge N_2 \wedge \cdots \wedge N_s \lessdot N_2 \wedge \cdots \wedge N_s$ (si legga G se $s < 2$).

Abbiamo ora:

$$I_{0,1 \cdots s-1} = N \wedge N_1 \wedge N_2 \cdots \wedge N_{s-1} = (N_1 \wedge \cdots N_s)^{\bar{a}^{q-1}} = I_{1,2 \cdots s}^{\bar{a}^{q-1}} \neq I_{1,2 \cdots s}$$

e $\dim(I_{0,1 \cdots s-1}) = \dim(I_{1,2 \cdots s})$; è poi $I_{0 \cdots s-1} \leq I_{1,2 \cdots s-1}$ e $I_{1,2 \cdots s} \leq I_{1,2 \cdots s-1}$ e poichè $\dim(I_{1,2 \cdots s-1}) = d - 1$, si avrà

$$I_{0,1 \cdots s-1} \lessdot I_{1,2 \cdots s-1}\,,\, I_{1,2 \cdots s} \lessdot I_{1,2 \cdots s-1} \text{ e } I_{0,1 \cdots s-1} \neq I_{1 \cdots s}\,;$$

da qui segue:

$$\text{(2)} \qquad (I_{0,1 \cdots s-1} = I_{1,2 \cdots s}^{\bar{a}^{q-1}}) \vee I_{1,2 \cdots s} = I_{1,2 \cdots s-1}$$

e poichè $I_{0,1 \cdots s-1} = N \wedge N_1 \wedge \cdots \wedge N_{s-1} = N \wedge I_{1,2 \cdots s}$, è pure

$$\text{(3)} \qquad I_{0,1 \cdots s-1} \lhd I_{1,2 \cdots s-1}\,.$$

A questo punto non è difficile provare che se $I_{1,2 \cdots s} \neq T$, allora la chiusura $I_{1,2 \cdots s}^{\langle \bar{a} \rangle} = G$. Infatti ciò è banalmente vero se $s = 1$, ossia se cod. $I_{1 \cdots s} = 1$. Usiamo induzione su cod. Sia allora $1 < d = $ cod. $I_{1,2 \cdots s}$. Per (2) abbiamo $I_{1,2 \cdots s-1} = I_{0,1 \cdots s-1} \vee I_{1,2 \cdots s}$ con cod. $I_{1,2 \cdots s-1} = d - 1$; per cui, per ipotesi induttiva,

$$G = I_{1,2 \cdots s-1}^{\langle \bar{a} \rangle} = I_{0,1 \cdots s-1}^{\langle \bar{a} \rangle} \vee I_{1,2 \cdots s}^{\langle \bar{a} \rangle} = I_{12, \cdots s}^{\langle \bar{a} \rangle} \vee I_{1,2 \cdots s}^{\langle \bar{a} \rangle}\,.$$

Sia ora $I_{1,2\cdots s} > T$; poichè $I_{1,2\cdots s}^{\langle\bar{a}\rangle} = G$, esiste un k tale che $R = I_{1,2\cdots s}^{\bar{a}^k} \not< N$. Sarà $T < R$ e $R \vee N = G$ per cui

$$(4) \qquad R \wedge N = T \lhd R .$$

Ancora da $(R \vee H)^\sigma = R^\sigma \vee H^\sigma = R^\sigma \vee \langle\bar{a}\rangle \geq R^\sigma \vee R^{\sigma\bar{a}} \vee \cdots \vee R^{\sigma\bar{a}^{q-1}}$ segue

$$(5) \qquad R \vee H \geq R^{\sigma\bar{a}^0\sigma^{-1}} \vee \cdots \vee R^{\sigma\bar{a}^{q-1}\sigma^{-1}} = (I_{1,2\cdots s}^{\bar{a}^k})^{\langle\bar{a}\rangle} = G .$$

Tenendo allora presente (1), (4) e (5) si ricavano le relazioni:

$$(6) \qquad R \wedge H = R \wedge N = H \wedge N = T \ , \ K \vee H = K \vee N = H \vee N = G .$$

Pertanto $T \lhd H \vee R = G$.

Proviamo che G/T è un gruppo finito. Da $R = I_{1,2\cdots s}^{\bar{a}^k}$ e $T < R$ segue che $I_{1,2\cdots s}^{\bar{a}^i}/T$ $i = 0, 1, \cdots, q-1$ è finito. Usiamo ora induzione su $d = \dim(I_{1,2\cdots s})$ e sia $d > 1$. Allora da (2) e (3) si ha

$$I_{1,2\cdots s-1}/T = I_{0,1\cdots s-1}/T \vee I_{1,2\cdots s}/T ,$$

ossia si tratta di un gruppo estensione finita mediante un gruppo finito essendo tali per ipotesi induttiva sia $I_{1,2\cdots s}/T$ che $I_{0,1\cdots s-1}/T$, in quanto la loro dimensione è $d-1$. Dunque N/T e così anche G/T è finito. Poichè in base alle relazioni (6), l'intervallo $[G/T]$ non è distribuitivo, il gruppo finito G/T non è ciclico. Pertanto esistono in numero finito sottogruppi M_i con $i = 1, 2, \cdots, n$, tali che $G = N \cup M_1 \cup \cdots \cup M_n$ è una unione insiemistica non riducibile; ma allora si ha pure che

$$\bar{G} = N^\sigma \cup M_1^\sigma \cup \cdots \cup M_n^\sigma$$

è una unione insiemistica finita non riducibile di $\bar{G}$; in virtù allora di (4, 4) in [2] si conclude che $[\bar{G} : N^\sigma] < \infty$. //

TEOREMA A. *Sia* $\sigma : G \to \bar{G}$ *una proiettività e sia* $H \leq K \leq G$. *Allora* $[K : H] < \infty$ *se e solo se* $[K^\sigma : H^\sigma] < \infty$.

Dimostrazione. Sia $[K : H] < \infty$ e sia $H = H_0 \lessdot H_1 \lessdot \cdots \lessdot H_n = K$ una catena completa da H a K. Se $H_{i-1} \lhd H_i$ è $[H_i^\sigma : H_{i-1}^\sigma] < \infty$ per il Lemma 1. Altrimenti considerato $H_i/(H_{i-1})_{H_i}$, tale gruppo è finito non ciclico, per cui $H_i = H_{i-1} \cup M_1 \cup \cdots \cup M_n$ è una unione insiemistica irriducibile di certi sottogruppi in numero finito e quindi tale sarà pure la rappresentazione $H_i^\sigma = H_{i-1}^\sigma \cup \cdots \cup M_n^\sigma$ e dunque, per il citato teorema di Neumann [2], sarà $[H_i^\sigma : H_{i-1}^\sigma] < \infty$. Da qui avendosi $[K^\sigma : H^\sigma] = \prod_{1}^{n}{}_i [H_i^\sigma : H_{i-1}^\sigma]$ si vede che $[K^\sigma : H^\sigma] < \infty$. Similmente per il viceversa. //

Con Schmidt [4] scriveremo che $G \in P(n, p)$, $1 \leq n \leq \infty$, p un primo, se e solo se G è un p-gruppo abeliano elementare d'ordine p^n oppure anche, per $n \geq 2$, un gruppo $G = A\langle t\rangle$ con A gruppo abeliano elementare d'ordine

p^{n-1}, t un elemento d'ordine q, q un primo, e $t^{-1} at = a^r$ per ogni $a \in A$ con $r^q \equiv 1 \mod. p$, $r \not\equiv 1 \mod. p$.

Ciò ricordato passiamo a dimostrare il seguente

LEMMA 2. *Sia* $\sigma : G \to \overline{G}$ *una proiettività ed* N *un sottogruppo normale di* G. *Se* $G/N \in P(n, p)$ *allora* $N_{\overline{G}}$ *è normale in* G *e se* N^σ *non è tale in* $\overline{G}$, *i gruppi* $G/N_{\overline{G}}$ *e* $\overline{G}/N^\sigma_{\overline{G}}$ *appartengono alla classe* $P(n+1, s)$ *ove* $s \geq p$ *ed* $s = p$ *non appena* $n \geq 2$.

Dimostrazione. Se $n = 1$, è $N^\sigma \underset{d}{<} \overline{G}$ e dunque essendo per il Lemma 1 $[\overline{G} : N^\sigma] < \infty$, [3] ci garantisce che $[\overline{G} : N^\sigma] = s$, un primo. Se ora $N^\sigma \ntriangleleft \overline{G}$, si ha per [3] che $\overline{G}/N^\sigma_{\overline{G}} \in P(2, s)$ per cui l'intervallo $[G/N_{\overline{G}}]$ contiene tre gruppi distinti N, H_1, H_2 con $N_{\overline{G}} = N \wedge H_1 = N \wedge H_2$ e $H_1 \vee H_2 = G$ sicchè $N_{\overline{G}} \triangleleft G$ e $G/N_{\overline{G}}$ apparterrà a $P(2, s)$ ove $s \geq p$.

Sia ora n maggiore di uno. Esistono sottogruppi $M \triangleleft \cdot G$, $N \triangleleft \cdot N_i$ con $M \wedge N_i = N$ e $\bigvee_i N_i = G$. Da $(M_{\overline{G}} \wedge N)^\sigma = \overline{M}_{\overline{G}} \wedge \overline{N}_i \triangleleft \bigvee_i \overline{N}_i = \overline{G}$ e $\overline{M}_{\overline{G}} \wedge \overline{N} \leq \overline{N}$ segue $\overline{N}_{\overline{G}} = \overline{M}_{\overline{G}} \wedge \overline{N}$ e dunque anche $N_{\overline{G}} = M_{\overline{G}} \wedge N \triangleleft G$ come pure per il Teorema A l'indice $[G : N_{\overline{G}}] < \infty$. Non sarà restrittivo supporre $N_{\overline{G}} = \{1\}$ ed $N \neq \{1\}$. Tenuto presente che da $G/N \in P(n, p)$, $n \geq 2$ segue $N^\sigma \triangleleft \overline{G}$ non appena $N^\sigma \underset{q}{\leq} \overline{G}$, e che $[G/N]$ è un reticolo irriducibile, usando th. 3.4 in [5] non è difficile concludere che $G/N_{\overline{G}} \in P(n+1, p)$ e dunque pure $\overline{G}/N^\sigma_{\overline{G}} \in P(n+1, p)$. //

TEOREMA 3. *Sia* N *un sottogruppo normale di* G, $[G : N] = q$ e $P(G)$ *il gruppo delle autoproiettività di* G. *Allora il gruppo* $G/\bigwedge_{\sigma \in P(G)} N^\sigma$ *soddisfa ad una delle seguenti condizioni*:

i) $G/\bigwedge_{\sigma \in P(G)} N^\sigma \in P(n, p)$, $n \geq 2$, $q \leq p$ *e* $q = p$ *se e solo se è un P-gruppo abeliano*.

ii) *è un gruppo i cui sottogruppi finitamente generati sono ciclici Hölderiani*.

iii) *è un gruppo abeliano senza torsione di rango* 1 *e residualmente finito*.

Dimostrazione. Per $\sigma \in P(G)$ è $N^\sigma < G$ e $[G : N^\sigma] < \infty$ per il Lemma 1. Pertanto per [3] è $\overline{G}'' \leq N^\sigma$ e dunque, posto $T = \bigwedge_{\sigma \in P(G)} N^\sigma$ è G/T un gruppo con $G'' \leq T$, ossia metabeliano. Ragionando ora modulo T potremo supporre $T = \{1\}$. Distinguiamo due casi:

a) Esiste un gruppo $H \triangleleft G$, $H < N$ e $G/H \in P(2, p)$.

Questo avviene certamente se per un $\sigma \in P(G)$ è $N^\sigma \ntriangleleft G$ oppure $N^\sigma \neq N^{\sigma_1}$ e $[G : N^\sigma] = [G : N^{\sigma_1}]$. Da $\bigwedge_{\sigma \in P(G)} N^\sigma = \{1\}$ segue $\bigwedge_{\sigma \in P(G)} H^\sigma = \{1\}$. In virtù del Lemma 2 è $G/(H^\sigma)_G \in P(i, p)$ $i = 2$ o 3 a secondo che $H^\sigma \triangleleft G$ o $H^\sigma \ntriangleleft \overline{G}$. Pertanto $G \hookrightarrow \Pi\, P(i, p)$ per cui G/G' è periodico e G' è un p-gruppo abeliano elementare sicchè G è un gruppo periodico risolubile, dunque localmente finito. La teoria delle autoproiettività singolari quale sviluppata per i gruppi finiti [7] non è difficile vedere che si applica anche ai gruppi localmente finiti, per cui possiamo concludere che G è un P–gruppo.

b) $N^\sigma \lhd G$ per ogni $\sigma \in P(G)$.

Il gruppo G è abeliano e quindi se è periodico e non P–gruppo, sarà localmente ciclico Hölderiano. Se G è misto, per th. 3, II in [7], G non può contenere 2 elementi aperiodici indipendenti, per cui se è senza torsione sarà di rango 1 ed ovviamente residualmente finito. Sia infine G misto con il sottogruppo periodico $B \neq \{1\}$. Pocihè B è L–invariante, avendosi $\bigwedge_\sigma N^\sigma = \{1\}$, dovrà essere $BN = G$ e dunque $[B : B \wedge N] = q$. Ma ora esiste un $H \lhd G$ con $G/H \in P(2, q)$, e si ha il caso *a*) e dunque G è periodico, una contraddizione. //

Veniamo ora ad una caratterizzazione reticolare della finitezza dell'indice di un sottogruppo H in un gruppo G

TEOREMA B. *Un sottogruppo* H *ha indice finito in* G *se e solo se esiste una catena completa finita da* H *a* G: $H = H_0 < H_1 < \cdots < H_n = G$ *tale che per* $H_j, j = 1, 2, \cdots, n$ *è soddisfatta una delle seguenti condizioni*:

i) H_j *è unione insiemistica irriducibile di* H_{j-1} *e un numero finito di sottogruppi di* H_j.

ii) $\left[H_j / \bigwedge_{\sigma \in P(H_j)} H_{j-1}^\sigma\right]$ *è un'algebra di Boole atomica.*

iii) $\left[H_j / \bigwedge_{\sigma \in P(H_j)} H_{j-1}^\sigma\right]$ *è modulare senza torsione di rango* 1.

Dimostrazione. Necessità. Poniamo per semplicità $L = H_{j-1}$, $K = H_j$. Se $L \ntriangleleft K$, il gruppo K/L_K è finito non ciclico. Ne segue che $K = \bigcup_i M_i$ è una unione irriducibile finita di sottogruppi massimi fra i quali si può includere L. Se $L \lhd K$ sarà $[K : L] = p$, e in virtù del Teorema 3 sarà presente uno dei casi ivi considerati. Da qui ora si perviene facilmente alla necessità delle condizioni. Viceversa se è presente il caso i), in virtù di (4,4) in [2] si conclude che $[K : L] < \infty$; se infine è presente ii) o iii), sarà $L \lhd K$ e da $L < K$ si conclude che $[K : L] < \infty$. //

Una conseguenza immediata delle nostre considerazioni è che la classe dei gruppi residualmente finiti è proiettivamente invariante. Vogliamo mettere in evidenza ancora tre corollari dei risultati esposti.

COROLLARIO 1. *Sia* $\sigma : G \to \overline{G}$ *una proiettività ed* N *un sottogruppo normale di* G *con* G/N *ciclico infinito. Allora* N^σ *è normale in* $\overline{G}$ *e* $\overline{G}/N^\sigma$ *è ciclico infinito.*

Dimostrazione. Sia $N < M_p \lessdot G$ ove $[G : M_p] = p$, un primo. Sarà $M_p^\sigma \underset{d}{<} \overline{G}$ e per Lemma 1 $[\overline{G} : M_p^\sigma] < \infty$, per cui [3] $\overline{G}'' \leq \bigwedge_p M_p^\sigma$. Ora da $N = \bigwedge_p M_p$ segue $\overline{G}'' \leq \bigwedge_p M_p^\sigma = N^\sigma$; il gruppo $\overline{G}/\overline{G}''$ è un $\mathfrak{X}^s$–gruppo e in $\overline{G}/\overline{G}''$ il sottogruppo di Dedekind $N^\sigma/\overline{G}''$ ha un complemento ciclico infinito: in base al Th. A in [6] si conclude che $N^\sigma \lhd \overline{G}$. //

COROLLARIO 2. *Sia* $\sigma : G \to \overline{G}$ *una proiettività ed* N *un sottogruppo normale perfetto o privo di sottogruppi d'indice finito. Allora* N^σ *è sottogruppo normale di* $\overline{G}$.

Dimostrazione. Sia $\bar{g} \in \overline{G}$ che non normalizza N^σ. Per il corollario 1 sarà $[\langle \bar{g}, N^\sigma \rangle : N^\sigma] < \infty$ per cui $[N^\sigma : N^{\sigma\bar{g}} \wedge N^\sigma] < \infty$; ma allora per il Teorema A è $[N : N^{\bar{g}} \wedge N] < \infty$ ed è anche $N^{\bar{g}} \wedge N \underset{d}{<} N$; ma ciò [3] porta in ogni caso ad una contraddizione alle ipotesi. //

Seguendo Suzuki [7], una proiettività $\sigma : G \to \overline{G}$ si dice che *conserva gli indici* se da $H \leq K \leq G$ e K ciclico segue $[K : H] = [K^\sigma : H^\sigma]$; si dice che *conserva strettamente gli indici* se da $H \leq K \leq G$ segue $[K : H] = [K^\sigma : H^\sigma]$.

COROLLARIO 3. *Sia* $\sigma : \overline{G} \to G$ *una proiettività. Allora* σ *conserva strettamente gli indici se e solo se conserva gli indici.*

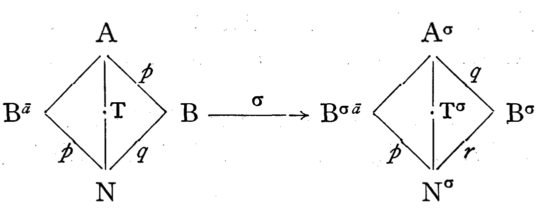
Dimostrazione. Sia $H \leq K \leq G$ e $[K : H] < \infty$. Visto che $[K : H_K] < \infty$ e $[K : H] = [K : H_K]/[H : H_K]$, non sarà restrittivo supporre $H \lhd K$; sia $H = H_0 \lhd\cdot H_2 \lhd\cdot \cdots \lhd\cdot H_n = K$ una serie di composizione da H a K. Consideriamo il fattore generico $H_i/H_{i-1} = A/B$ e distinguiamo due casi:

a) A/B è un gruppo (finito) semplice non abeliano.

Sarà $B^\sigma \underset{d}{<} A^\sigma$ e per teorema A, $[A^\sigma : B^\sigma] < \infty$. Se ora B^σ non è normale in A^σ esiste un sottogruppo di Dedekind L^σ di A^σ con $B^\sigma < L^\sigma \underset{d}{<} A^\sigma$; ma allora è pure $B < L \underset{d}{<} A$ e questo è in contrasto con la semplicità del gruppo A/B [3]. Dunque $B^\sigma \lhd A^\sigma$ e così $[A : B] = [A^\sigma : B^\sigma]$ per un risultato di Suzuki [7].

b) A/B è d'ordine primo.

Sarà $A = \langle a, B \rangle$ e $[A : B] = p$, un primo. Se $B^\sigma \lhd A^\sigma$ da $[A : B] = [\langle a \rangle : \langle a^p \rangle] = [\langle a \rangle^\sigma : \langle a^p \rangle^\sigma] = [\langle \bar{a} \rangle : \langle \bar{a}^p \rangle] = [\langle \bar{a} \rangle : A \wedge \langle \bar{a} \rangle] = [A^\sigma : B^\sigma]$, si conclude. Resta da vedere che effettivamente $B^\sigma \lhd A^\sigma$. Se $B^\sigma \ntriangleleft A^\sigma$ si hanno i diagrammi:



$q > r = p$.

Visto che $[B : N] = q$ tutti gli altri sottogruppi T di A che coprono N hanno ordine p e poichè $N^\sigma \lhd T^\sigma$ sarà $[T^\sigma : N^\sigma] = p$. Così il P–gruppo A^σ/N^σ è p–abeliano elementare per cui $B^\sigma \lhd A^\sigma$, una contraddizione.

Resta così provata la sufficienza della condizione. La necessità è ovvia. //

BIBLIOGRAFIA

[1] BIRKHOFF G. (1948) – *Lattice theory*, Colloquim Publ. vol. 25, New York.

[2] NEUMANN B. H. (1954) – *Groups covered by permutable subsets*, « Jour. of the London Math. Soc. », *29*.

[3] SCHMIDT R. (1964) – *Modulare Untergruppen endlicher Gruppen*, « Illinois Jour. of Math. », vol. 13.

[4] SCHMIDT R. (1980) – *Untergruppenverbände involutorisch erzeugter Gruppen*, « Rend. del Seminario Mat. dell'Università di Padova », vol. 63.

[5] SCHMIDT R. (1975) – *Normal subgroups and lattice isomorphisms of finite groups*, « Proc. of the London Math. Soc. », vol. 30.

[6] STONEHEWER S. E. (1976) – *Modular subgroup structure in infinite groups* « Proc. London Math. Soc. », *3*, vol. 132.

[7] SUZUKI M. (1956) – *Structure of a group and the structure of its lattice of subgroups*, Springer Verlag, Berlin.