ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

GUIDO ZAPPA

Sui gruppi risolubili d'ordine dispari

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 2^e série, tome 9, n° 2 (1940), p. 147-161

<http://www.numdam.org/item?id=ASNSP_1940_2_9_2_147_0>

SUI GRUPPI RISOLUBILI D'ORDINE DISPARI

di GUIDO ZAPPA (Roma).

1. - In una sua ben conosciuta memoria, HALL (1) dava la seguente definizione:

« Il p-gruppo **G** si dice regolare se, dato un qualunque intero positivo α e una qualsiasi coppia di elementi P e Q di **G**, chiamato **L** il sottogruppo generato da P e Q, è sempre possibile trovare degli elementi S_3, S_4,...., S_r, tutti appartenenti al derivato di **L** e soddisfacenti all'equazione

$$(PQ)^{p^\alpha} = P^{p^\alpha} Q^{p^\alpha} S_3^{p^\alpha} S_4^{p^\alpha} \ldots\ldots S_r^{p^\alpha} \text{ ».}$$

Più oltre egli dimostrava che:

a). « Ogni p-gruppo il cui ordine è minore o uguale a p^p è regolare »; e che

b). « Se **G** è un p-gruppo regolare, gli elementi di **G** il cui ordine divide p^β (β intero qualunque) formano gruppo ».

2. - In una mia nota precedente (2) davo il seguente teorema:

« Sia **G** un gruppo semplice d'ordine g, ed **H** un suo sottogruppo di SYLOW d'ordine p^α. Sia poi **S** un sottogruppo invariante di **H**, contenente il derivato **H'** di **H**, e tale che tutte le operazioni di **H** non contenute in **S** abbiano eguale il rapporto tra periodo assoluto e periodo relativo rispetto ad **S**.

Allora, se l'indice di **S** in **H** è p^x, e q è il più piccolo fattore primo di g diverso da p, **G** non contiene più di

$$g\left(\frac{1}{p^x} + \frac{1}{q}\right)$$

operazioni, il cui ordine è una potenza di p ».

---

(1) P. HALL: *A contribution to the theory of groups of prime-power orders.* Proc. of London Math. Soc., Serie 2, Vol. 36 (1934), pp. 29-95.

(2) G. ZAPPA: *Un teorema sui gruppi semplici.* Rendiconti del Seminario Mat. della R. Università di Roma, Serie IV, Vol. 2, Fasc. 3 (1938).

Da questo teorema segue facilmente l'altro:

Sia **G** *un gruppo semplice d'ordine* g, *ed* **H** *un suo sottogruppo di* SYLOW *d'ordine* p^α *regolare. Se* q *è il più piccolo fattore primo di* g *diverso da* p, **G** *non ha più di*

$$g\left(\frac{1}{p}+\frac{1}{q}\right)$$

operazioni, il cui ordine è una potenza di p.

Sia infatti p^r il massimo ordine delle operazioni di **H**. Essendo **H** regolare, per la *b*) del paragrafo 1, le operazioni di **H** il cui ordine divide p^{r-1} formano un sottogruppo **R**, che, per la sua stessa definizione, è caratteristico in **H**. Evidentemente, la potenza p-esima di una qualsiasi operazione di **H** non contenuta in **R**, è in **R**. Sia **S** un qualsiasi sottogruppo di **H**, invariante massimo in esso (vale a dire di indice p in **H**) e contenente **R**. Evidentemente **S** contiene il derivato di **H**, perchè $\frac{\mathbf{H}}{\mathbf{S}}$ è abeliano; inoltre tutte le operazioni di **H** non contenute in **S** hanno periodo assoluto p^r (perchè non sono in **R**) e periodo relativo p (perchè le loro potenze p-esime devono stare in **R** e quindi in **S**). Pertanto, dal nostro teorema anzi citato, segue che **G** non ha plù di

$$g\left(\frac{1}{p}+\frac{1}{q}\right)$$

operazioni, il cui ordine è una potenza di p, visto che per tutte le operazioni di **H** non contenute in **S** è costante ($=p^{r-1}$) il rapporto tra periodo assoluto e periodo relativo rispetto ad **S**.

3. - Ricordiamo la seguente definizione introdotta da HALL:

Sia un gruppo **G** *e un suo sottogruppo* **H**. *Dicesi* **centralizzante** *di* **H** *in* **G** *il sottogruppo costituito da tutte le operazioni di* **G** *permutabili con ogni operazione di* **H**.

Sia **N** il normalizzante ed **M** il centralizzante di **H** in **G**. È noto come ogni operazione di **N** determini un automorfismo in **H**, e quindi **N** è isomorfo ad un sottogruppo **S** del gruppo di automorfismi di **H**. Le operazioni di **N** a cui corrisponde in **S** l'identità sono tutte e sole le operazioni di **M**; quindi $\frac{\mathbf{N}}{\mathbf{M}}$ è oloedricamente isomorfo ad **S**.

4. - LEMMA. — *Sia* **P** *un gruppo d'ordine* p^2 *del tipo* (1, 1) (*p primo dispari*) *e sia* **A** *il gruppo di automorfismi di* **P**. *Ogni sottogruppo di* **A**, *il cui ordine è primo con* $2p$, *è abeliano.*

È noto (3) che **A** può essere rappresentato come gruppo lineare omogeneo

(3) W. BURNSIDE: *Theory of groups*, 1ª edizione, Cambridge 1897, p. 244 e Cap. XIV.

(mod p) su due variabili. L'ordine di **A** è $(p^2-1)(p^2-p)$, e ogni sua sostituzione è della forma

$$\begin{aligned} x_1' &\equiv a_{11}x_1 + a_{12}x_2 \\ x_2' &\equiv a_{21}x_1 + a_{22}x_2 \end{aligned} \pmod{p}$$

con determinante $\not\equiv 0 \pmod{p}$.

È noto ancora che le sostituzioni il cui determinante è l'unità formano un sottogruppo **S** invariante in **A**; il gruppo fattoriale $\frac{\mathbf{A}}{\mathbf{S}}$ è ciclico d'ordine $p-1$.

In **A** inoltre è contenuto un sottogruppo **C** d'ordine $p-1$ generato dalla sostituzione

$$\begin{aligned} x_1' &\equiv zx_1 \\ x_2' &\equiv \quad zx_2 \end{aligned} \pmod{p},$$

ove z è una radice primitiva (mod p). **C** è il centrale di **A**.

Ogni sostituzione di **C** ha per determinante il quadrato di una radice (mod p), e viceversa, se z^2 è il quadrato di una radice (mod p), esiste una sostituzione di **C** che ha per determinante z^2. È noto dalla teoria dei numeri che ogni radice che appartiene ad un esponente dispari (mod p) è quadrato di un'altra radice; quindi ogni radice che appartiene ad un esponente dispari è determinante di una sostituzione di **C**.

S e **C** hanno a comune un sottogruppo **I** d'ordine 2, costituito dall'identità e dalla sostituzione

$$\begin{aligned} x_1' &\equiv -x_1 \\ x_2' &\equiv \quad -x_2 \end{aligned} \pmod{p}.$$

Inoltre **S** ha ordine $(p+1)(p^2-p)$; **C** ha ordine $p-1$, ed ogni operazione di **S** è permutabile con ogni operazione di **C**. Quindi **S** e **C** generano un sottogruppo **R** di **A** che ha ordine $\frac{1}{2}(p^2-1)(p^2-p)$.

Si noti che, moltiplicando tutte le sostituzioni di **S** per una sostituzione di **A** il cui determinante è uguale ad una certa radice z (mod p) si ottengono tutte e sole le sostituzioni di **A** il cui determinante è uguale a z. Quindi tutte le sostituzioni di **A** il cui determinante appartiene ad un esponente dispari sono contenute in **R**. E poichè il periodo del determinante divide il periodo della sostituzione corrispondente, segue che tutte le sostituzioni di **A** aventi periodo dispari sono contenute in **R**.

Sia ora **H** un sottogruppo di **A** il cui ordine è primo con $2p$. Le sostituzioni di **H** hanno tutte periodo dispari, quindi **H** è in **R**.

Consideriamo il fattoriale $\frac{\mathbf{R}}{\mathbf{I}} = \bar{\mathbf{R}}$. Tra **R** e $\bar{\mathbf{R}}$ passa un isomorfismo meriedrico, in cui a **C** corrisponde $\frac{\mathbf{C}}{\mathbf{I}} = \bar{\mathbf{C}}$, e ad **S** corrisponde $\frac{\mathbf{S}}{\mathbf{I}} = \bar{\mathbf{S}}$. Ad **H** corrisponderà in $\bar{\mathbf{R}}$ un sottogruppo $\bar{\mathbf{H}}$ isomorfo ad **H**. L'isomorfismo tra **H** e $\bar{\mathbf{H}}$ è olo-

edrico, altrimenti l'indice di meriedria dovrebbe essere 2, il che è impossibile, perchè l'ordine di $\mathbf{H}$ è dispari. Se quindi dimostro che $\overline{\mathbf{H}}$ è abeliano, ho che anche $\mathbf{H}$ è abeliano.

Evidentemente $\overline{\mathbf{S}}$ e $\overline{\mathbf{C}}$ non hanno elementi comuni oltre l'identità; e pertanto $\overline{\mathbf{R}}$ è il prodotto diretto di $\overline{\mathbf{S}}$ per $\overline{\mathbf{C}}$. Ogni operazione di $\overline{\mathbf{R}}$ si può quindi in uno ed un sol modo mettere sotto la forma $S \times C$, ove S è una conveniente operazione di $\overline{\mathbf{S}}$, e C di $\overline{\mathbf{C}}$.

Sia ora $H = S \times C$ una operazione di $\overline{\mathbf{H}}$; il periodo di H è primo con $2p$, e tale dovrà essere anche il periodo di S e quello di C, poichè è $H^x = 1$ allora e solo allora che è $S^x = 1$ e $C^x = 1$. Se si ha $H_1 = S_1 \times C_1$ e $H_2 = S_2 \times C_2$, (con H_1, H_2 di $\overline{\mathbf{H}}$; S_1, S_2 di $\overline{\mathbf{S}}$; C_1, C_2 di $\overline{\mathbf{C}}$) si ha anche $H_1 H_2 = S_1 \cdot S_2 \times C_1 \cdot C_2$. Quindi le operazioni di $\overline{\mathbf{S}}$ che compaiono come fattori nelle operazioni di $\overline{\mathbf{H}}$ formano un sottogruppo $\overline{\mathbf{S}}$, e le analoghe operazioni di $\overline{\mathbf{C}}$ un sottogruppo $\overline{\mathbf{C}}$.

Il prodotto $\overline{\mathbf{S}} \times \overline{\mathbf{C}}$ è un sottogruppo di $\overline{\mathbf{R}}$ che contiene $\overline{\mathbf{H}}$; se pertanto dimostro che $\overline{\mathbf{S}} \times \overline{\mathbf{C}}$ è abeliano, ho dimostrato il lemma.

È noto che $\overline{\mathbf{S}}$ è oloedricamente isomorfo con il gruppo delle sostituzioni lineari fratte (mod p) su una variabile che abbiano determinante eguale a 1. Questo gruppo è tale che tutti i suoi sottogruppi il cui ordine è primo con $2p$ sono ciclici. D'altra parte $\overline{\mathbf{S}}$, essendo costituito di operazioni il cui ordine è primo con $2p$, ha un ordine primo con $2p$; ed essendo in $\overline{\mathbf{S}}$, è ciclico. $\overline{\mathbf{C}}$ poi è anch'esso ciclico, perchè lo era $\mathbf{C}$; quindi $\overline{\mathbf{S}} \times \overline{\mathbf{C}}$, quale prodotto diretto di due gruppi ciclici, è abeliano, e tale è anche $\overline{\mathbf{H}}$ e $\mathbf{H}$, c. d. d.

5. - TEOREMA I. — *Ogni gruppo il cui ordine è della forma*

$$g = p_1^{\alpha}\, p_2^2 \ldots p_r^2\, p_{r+1} \ldots p_m \quad (\text{con } p_1, p_2, \ldots, p_m \text{ numeri primi dispari distinti}),$$

è risolubile, purchè sia $p_1 \geqslant \alpha$; $p_1 \geqslant m + r + 1$.

5. 1. - Una volta dimostrato che un tale gruppo, che chiameremo $\mathbf{G}$, non è semplice, è facile provare che esso è risolubile. Infatti poichè ogni gruppo il cui ordine divide g si trova nelle stesse condizioni del teorema, possiamo procedere per induzione ammettendo la risolubilità di ogni gruppo il cui ordine divide g. Se $\mathbf{G}$ non è semplice esso conterrà un sottogruppo invariante proprio $\mathbf{H}$. Gli ordini di $\mathbf{H}$ e di $\frac{\mathbf{G}}{\mathbf{H}}$ dividono g; quindi $\mathbf{H}$ e $\frac{\mathbf{G}}{\mathbf{H}}$ sono risolubili; sarà pertanto risolubile anche $\mathbf{G}$, e i fattori di composizione di $\mathbf{G}$ sono dati dai fattori di composizione di $\mathbf{H}$ più i fattori di composizione di $\frac{\mathbf{G}}{\mathbf{H}}$.

Basterà quindi provare che $\mathbf{G}$ non è semplice, il che faremo senza ricorrere al procedimento di induzione.

Faremo la dimostrazione per assurdo, supponendo $\mathbf{G}$ semplice. Se il più piccolo fattore primo di g è diverso da p_1, vale a dire compare in g alla prima o alla

seconda potenza, si ha che **G** non è semplice, per un noto teorema di BURNSIDE (4). Possiamo pertanto supporre che p_1 sia il più piccolo fattore primo di g.

Per la *a*) del paragrafo 1, i sottogruppi di SYLOW d'ordine p_1^a, essendo $p_1 \geqslant a$, sono tutti regolari, e quindi pel secondo teorema del paragrafo 2, se **G** è semplice, il numero delle operazioni di **G** il cui ordine divide p_1^a non supera

$$g\left(\frac{1}{p_1}+\frac{1}{\bar{p}}\right)$$

ove $\bar{p}$ è il più piccolo fattore primo di g, diverso da p_1.

Inoltre, se **G** è semplice, il numero delle operazioni il cui ordine è divisibile per p_k $(r<k\leqslant m)$ non supera $\frac{g}{p_1}$.

Infatti, sia $\mathbf{P}_k$ un sottogruppo d'ordine p_k di **G**, e siano **N**, d'ordine np_k, ed **M**, d'ordine $\bar{m}p_k$, rispettivamente il normalizzante e il centralizzante di $\mathbf{P}_k$ in **G**. Se **N** coincide con **M**, $\mathbf{P}_k$ appartiene al centrale del proprio normalizzante, e **G**, per un teorema di BURNSIDE (5), non è semplice. Se **G** è semplice, deve essere **N** più ampio di **M**, ossia $n \geqslant \bar{m}p_1$.

Il numero delle operazioni contenute nel centralizzante di almeno un sottogruppo d'ordine p_k non supera pertanto $\frac{g}{np_k} \cdot \bar{m}p_k \leqslant \frac{g}{p_1}$; d'altra parte ogni operazione di **G** il cui ordine è divisibile per p_k ha una sua potenza d'ordine p_k, con la quale è permutabile, e quindi appartiene al centralizzante di un sottogruppo di SYLOW d'ordine p_k; pertanto anche il numero delle operazioni il cui ordine è divisibile per p_k non supera $\frac{g}{p_1}$, c. d. d.

5. 2. - Vediamo ora quante sono al massimo, nel caso che **G** sia semplice, le operazioni di **G** il cui ordine è divisibile per p_i $(1<i\leqslant r)$.

Sia $\mathbf{P}_i^{(2)}$ un sottogruppo di SYLOW di **G** d'ordine p_i^2 $(1<i\leqslant r)$. Consideriamo prima il caso in cui $\mathbf{P}_i^{(2)}$ *non sia ciclico*; esso sarà allora abeliano del tipo (1, 1).

Siano rispettivamente **N**, d'ordine np_i^2 ed **M** d'ordine $\bar{m}p_i^2$ il normalizzante e il centralizzante di $\mathbf{P}_i^{(2)}$ in **G**. Se **G** è semplice, **N** è più vasto di **M** (6), e quindi $\frac{n}{\bar{m}}=\bar{n}>1$. $\frac{\mathbf{N}}{\mathbf{M}}=\bar{\mathbf{N}}$ ha ordine $\bar{n}$, e, come si vede in base alle osservazioni del paragrafo 3, è oloedricamente isomorfo a un sottogruppo $\bar{\bar{\mathbf{N}}}$ del gruppo di automorfismi di $\mathbf{P}_i^{(2)}$. Ma $\bar{n}$ è primo con $2p_i$; quindi $\bar{\bar{\mathbf{N}}}$, per il lemma, è abeliano, e così $\bar{\mathbf{N}}$.

5. 3. - Facciamo ora vedere che *in* $\mathbf{P}_i^{(2)}$ *non esistono più di due sottogruppi d'ordine* p_i *i cui centralizzanti in* **N** *siano più vasti di* **M**.

---

(4) W. BURNSIDE: *On some properties of Groups of Odd Order*. Proc. of the London Math. Soc., Vol. XXXIII (1901), p. 357 e seg.

(5) W. BURNSIDE l. c. (4).

(6) W. BURNSIDE l. c. (4).

Ricordiamo il seguente teorema di HALL (7) sui gruppi risolubili:

« Se **G** è un gruppo risolubile d'ordine $h \cdot k$, dove h è primo con k, si ha che:

1). **G** ha almeno un sottogruppo d'ordine h.

2). Due sottogruppi di **G** d'ordine h sono coniugati.

3). Ogni sottogruppo di **G** il cui ordine divide h sta almeno in un sottogruppo d'ordine h.

4). Il numero l_h dei sottogruppi di **G** d'ordine h può essere espresso come prodotto di fattori ciascuno dei quali (*i*) è $\equiv 1$ (mod. qualche fattore primo di h), (*ii*) è una potenza di un numero primo e divide uno dei fattori principali di **G** ».

Essendo $\mathbf{P}_i^{(2)}$ nel centrale di **M**, per un teorema già citato di BURNSIDE, in **M** c'è un sottogruppo invariante **D** di ordine $\overline{m}$. Ogni operazione di **D**, essendo in **M**, è permutabile con ogni operazione di $\mathbf{P}_i^{(2)}$; pertanto **M** è dato dal prodotto diretto $\mathbf{D} \times \mathbf{P}_i^{(2)}$. Per una nota proprietà dei prodotti diretti, ogni operazione di **M** non contenuta in **D** ha un ordine divisibile per p_i. Da ciò segue che in **M** non esistono, oltre **D**, altri sottogruppi d'ordine $\overline{m}$. Infatti un tale sottogruppo, se fosse diverso da **D**, dovrebbe contenere qualche operazione il cui ordine è divisibile per p_i, il che non può essere, perchè $\overline{m}$ è primo con p_i. Pertanto **D** è caratteristico in **M**, ed essendo **M** invariante in **N**, si ha che **D** è invariante in **N**.

Decomponiamo **M** secondo **D** e i suoi laterali nel seguente modo:

$$\mathbf{M} = \mathbf{D} + \mathbf{D}P_2 + \ldots + \mathbf{D}P_{p_i^2}$$

ove $P_2, \ldots, P_{p_i^2}$ sono le operazioni di $\mathbf{P}_i^{(2)}$. Tale scrittura è possibile perchè **D** e $\mathbf{P}_i^{(2)}$ non hanno elementi in comune.

Sarà poi

$$\mathbf{N} = \mathbf{M} + \mathbf{M}N_2 + \ldots + \mathbf{M}N_{\overline{n}}$$

ove $N_2, \ldots, N_{\overline{n}}$ sono opportune operazioni di **N**. Avremo allora

$$\mathbf{N} = \left(\mathbf{D} + \mathbf{D}P_2 + \ldots + \mathbf{D}P_{p_i^2}\right) + \left(\mathbf{D} + \ldots + \mathbf{D}P_{p_i^2}\right)N_2 + \ldots + \left(\mathbf{D} + \ldots + \mathbf{D}P_{p_i^2}\right)N_{\overline{n}}$$

e sviluppando i prodotti abbiamo una decomposizione di **N** secondo **D** e i suoi laterali. I complessi $\mathbf{D}, \ldots, \mathbf{D}P_{p_i^2}, \mathbf{D}N_2, \ldots, \mathbf{D}P_{p_i^2}N_2, \ldots, \mathbf{D}P_{p_i^2}N_{\overline{n}}$ sono gli elementi di $\frac{\mathbf{N}}{\mathbf{D}} = \mathbf{N}^*$, che ha ordine $\overline{n}p_i^2$. I complessi $\mathbf{D}, \ldots, \mathbf{D}P_{p_i^2}$ formano un sottogruppo di $\mathbf{N}^*$ isomorfo oloedricamente a $\mathbf{P}_i^{(2)}$; sia esso detto $\overline{\mathbf{P}}_i^{(2)}$. Consideriamo $\frac{\mathbf{N}^*}{\overline{\mathbf{P}}_i^{(2)}}$. Esso ha per elementi i complessi: $\left(\mathbf{D} + \ldots + \mathbf{D}P_{p_i^2}\right), \ldots, \left(\mathbf{D} + \ldots + \mathbf{D}P_{p_i^2}\right)N_{\overline{n}}$, ossia $\mathbf{M}, \mathbf{M}N_2, \ldots, \mathbf{M}N_{\overline{n}}$, e quindi altro non è che $\frac{\mathbf{N}}{\mathbf{M}} = \overline{\mathbf{N}}$.

---

(7) P. HALL: *On the soluble groups*. Journal of the L. M. S. III (1928), p. 98.

Pertanto tra $\mathbf{N}^*$ e $\overline{\mathbf{N}}$ c'è un isomorfismo meriedrico, e a $\overline{\mathbf{P}}_i^{(2)}$ corrisponde in $\overline{\mathbf{N}}$ l'identità. $\frac{\mathbf{N}^*}{\overline{\mathbf{P}}_i^{(2)}}$, coincidendo con $\frac{\mathbf{N}}{\mathbf{M}}$, è isomorfo ad un sottogruppo, d'ordine primo con $2p_i$, del gruppo di automorfismi di $\mathbf{P}_i^{(2)}$, e quindi, per il lemma, è abeliano, vale a dire anche risolubile; essendo poi anche $\overline{\mathbf{P}}_i^{(2)}$ risolubile, si ha che $\mathbf{N}^*$ è risolubile, e quindi, pel teorema anzi riportato di HALL, ha un sottogruppo $\mathbf{N}^{(1)}$ d'ordine $\overline{n}$, che ha solo l'identità a comune con $\overline{\mathbf{P}}_i^{(2)}$. Quindi a $\mathbf{N}^{(1)}$ corrisponderà in $\overline{\mathbf{N}}$ un sottogruppo d'ordine $\overline{n}$ oloedricamente isomorfo ad $\mathbf{N}^{(1)}$; esso dovrà coincidere con $\overline{\mathbf{N}}$. Dunque $\mathbf{N}^{(1)}$ è oloedricamente isomorfo con $\overline{\mathbf{N}}$.

Consideriamo $\mathbf{N}^*$, e vediamo quante sono le operazioni di $\overline{\mathbf{P}}_i^{(2)}$ permutabili con qualche operazione di $\mathbf{N}^{(1)}$. Notiamo intanto che non esiste, oltre l'identità, nessuna operazione di $\mathbf{N}^{(1)}$ che sia permutabile con tutte le operazioni di $\overline{\mathbf{P}}_i^{(2)}$. Infatti una tale operazione, N^*, dovrebbe provenire, nell'isomorfismo tra $\mathbf{N}$ e $\mathbf{N}^*$, da un'operazione N, la quale dovrebbe trasformare una generica operazione P di $\mathbf{P}_i^{(2)}$ in una operazione del tipo DP, ove D è in $\mathbf{D}$. Ma ogni operazione di $\mathbf{N}$ trasforma $\mathbf{P}_i^{(2)}$ in sè, quindi $D=1$, perchè DP deve essere in $\mathbf{P}_i^{(2)}$. N quindi, essendo permutabile con P e analogamente con tutte le operazioni di $\mathbf{P}_i^{(2)}$, dovrebbe essere in $\mathbf{M}$. Nell'isomorfismo tra $\mathbf{N}$ e $\mathbf{N}^*$, ad $\mathbf{M}$ corrisponde $\overline{\mathbf{P}}_i^{(2)}$, quindi N^* dovrebbe essere in $\overline{\mathbf{P}}_i^{(2)}$, e, dovendo anche essere, per ipotesi, in $\mathbf{N}^{(1)}$, è l'identità, come s'era detto.

Una operazione di $\mathbf{N}^{(1)}$ permutabile con una operazione P di $\overline{\mathbf{P}}_i^{(2)}$, è permutabile con tutte le operazioni del sottogruppo ciclico d'ordine p_i generato da P.

Sia $\mathbf{P}_{i,1}^{(1)}$ un sottogruppo d'ordine p_i di $\overline{\mathbf{P}}_i^{(2)}$ e sia $\mathbf{Z}_1$ il sottogruppo costituito da tutte le operazioni di $\mathbf{N}^{(1)}$ permutabili con tutte le operazioni di $\mathbf{P}_{i,1}^{(1)}$.

Sia $\mathbf{P}_{i,2}^{(1)}$ un altro sottogruppo di $\overline{\mathbf{P}}_i^{(2)}$ che abbia ordine p_i, e si definisca $\mathbf{Z}_2$ rispetto ad esso come si è definito $\mathbf{Z}_1$ rispetto a $\mathbf{P}_{i,1}^{(1)}$.

Così per ogni sottogruppo $\mathbf{P}_{i,j}^{(1)}$ d'ordine p_i di $\overline{\mathbf{P}}_i^{(2)}$ sarà definito il corrispondente $\mathbf{Z}_j$. Dico che tutti i $\mathbf{Z}_j$, due al più esclusi, si riducono all'identità. Supponiamo che ciò non sia, e che vi siano almeno tre $\mathbf{Z}_j$, per esempio $\mathbf{Z}_1$, $\mathbf{Z}_2$, $\mathbf{Z}_3$, che non si riducono all'identità. Vedremo che ciò è assurdo.

Si noti intanto che due qualunque $\mathbf{Z}_j$ non possono avere operazioni in comune oltre l'identità. Sia infatti M una operazione comune a $\mathbf{Z}_1$ e $\mathbf{Z}_2$; esso deve essere permutabile con tutte le operazioni di $\mathbf{P}_{i,1}^{(1)}$ e di $\mathbf{P}_{i,2}^{(1)}$ e quindi con tutte le operazioni del sottogruppo da essi generato, che è $\overline{\mathbf{P}}_i^{(2)}$; ma abbiamo visto più sopra che $\mathbf{N}^{(1)}$ non ha altre operazioni, oltre l'identità, che siano permutabili con ogni operazione di $\overline{\mathbf{P}}_i^{(2)}$, pertanto M deve coincidere con l'identità.

Sia N una operazione di $\mathbf{Z}_1$ diversa dall'identità. $\mathbf{N}^{(1)}$, essendo isomorfo oloedricamente ad $\overline{\mathbf{N}}$, è abeliano; pertanto N è permutabile con $\mathbf{Z}_1$, $\mathbf{Z}_2$, $\mathbf{Z}_3$. Essendo poi $\overline{\mathbf{P}}_i^{(2)}$ invariante in $\mathbf{N}^*$, sarà N permutabile con il sottogruppo di $\overline{\mathbf{P}}_i^{(2)}$ formato da tutte le operazioni di $\overline{\mathbf{P}}_i^{(2)}$ permutabili con ogni operazione di $\mathbf{Z}_1$, cioè permutabile con $\mathbf{P}_{i,1}^{(1)}$. Analogamente si vede che N deve essere permutabile con $\mathbf{P}_{i,2}^{(1)}$

e con $\mathbf{P}^{(1)}_{i,3}$. In particolare inoltre N, essendo in $\mathbf{Z}_1$, è permutabile con tutte le operazioni di $\mathbf{P}^{(1)}_{i,1}$. Ora possono darsi due casi:

1°) N muta in sè anche tutte le operazioni di $\mathbf{P}^{(1)}_{i,2}$. Ma ciò non può essere, perchè N apparterrebbe nello stesso tempo a $\mathbf{Z}_1$ e $\mathbf{Z}_2$, mentre, come s'è visto sopra, $\mathbf{Z}_1$ e $\mathbf{Z}_2$ non possono avere operazioni comuni oltre l'identità.

2°) N muta P_2, generatrice di $\mathbf{P}^{(1)}_{i,2}$, in una sua potenza P_2^x. Ma allora N non può mutare in sè $\mathbf{P}^{(1)}_{i,3}$. Infatti se è P_1 un'operazione generatrice di $\mathbf{P}^{(1)}_{i,1}$, e P_3 un'operazione generatrice di $\mathbf{P}^{(1)}_{i,3}$, si può scrivere $P_3 = P_1^a P_2^b$ con a e b convenientemente scelti (dato che, come si nota immediatamente, P_1 e P_2 costituiscono una base per $\overline{\mathbf{P}}^{(2)}_i$). Ma poichè P_1 è trasformata in sè da N (essendo N di $\mathbf{Z}_1$), mentre P_2 è trasformata da N in P_2^x, segue che P_3 è trasformata in $P_1^a P_2^{bx}$, che non è potenza di P_3. Pertanto $\mathbf{P}^{(1)}_{i,3}$ non è trasformato in sè da N, contro quando avevamo dimostrato. Anche questo secondo caso è quindi assurdo.

Esistono dunque al più due $\mathbf{Z}_j$ che non si riducono all'identità.

Ora siamo in grado di provare che, come abbiamo già affermato, non esistono in $\mathbf{P}^{(2)}_i$ più di due sottogruppi d'ordine p_i i cui centralizzanti in $\mathbf{N}$ siano più vasti di $\mathbf{M}$. Se infatti esistessero più di due sottogruppi di tal tipo, si avrebbe, per l'isomorfismo tra $\mathbf{N}$ e $\mathbf{N}^*$, che in $\mathbf{N}^*$ ci sarebbero più di due sottogruppi d'ordine p_i, naturalmente contenuti in $\overline{\mathbf{P}}^{(2)}_i$, i cui centralizzanti in $\mathbf{N}^*$ sarebbero più vasti di $\overline{\mathbf{P}}^{(2)}_i$. Ma se $\mathbf{P}^{(1)}_{i,1}$ è un sottogruppo d'ordine p_i di $\overline{\mathbf{P}}^{(2)}_i$ il cui centralizzante $\mathbf{I}_1$ in $\mathbf{N}^*$ è più ampio di $\overline{\mathbf{P}}^{(2)}_i$, si ha che $\mathbf{N}^{(1)}$ ha qualche operazione, oltre l'identità, a comune con $\mathbf{I}_1$, cioè ha qualche operazione permutabile con $\mathbf{P}^{(1)}_{i,1}$, oltre l'identità. Ma abbiamo visto che ciò non può capitare per più di due sottogruppi di $\overline{\mathbf{P}}^{(2)}_i$ d'ordine p_i, dal che si deduce, procedendo a ritroso, che *in* $\mathbf{P}^{(2)}_i$ *non vi sono più di due sottogruppi i cui centralizzanti in* $\mathbf{N}$ *siano più vasti di* $\mathbf{M}$.

5. 4. - Ora possiamo procedere a contare le operazioni di $\mathbf{G}$ il cui ordine è divisibile per p_i (sempre nel caso che i sottogruppi d'ordine p_i^2 non siano ciclici) con un'eventuale maggiorazione.

Ogni operazione A di $\mathbf{G}$ il cui ordine è divisibile per p_i, per esempio kp_i (k primo con p_i) avrà una sua potenza A^k, il cui ordine è p_i, ed un'altra, A^{p_i} il cui ordine è primo con p_i. Le operazioni A^k e A^{p_i} generano tutto il sottogruppo ciclico generato da A, e pertanto potrà scriversi $A = (A^k)^x \cdot (A^{p_i})^y$, ove x e y sono convenienti esponenti. Si noti poi che A^k e A^{p_i} sono fra loro permutabili.

Si può quindi concludere che *ogni operazione il cui ordine è divisibile per* p_i *può darsi come prodotto di una operazione d'ordine* p_i *per una operazione* (*che può anche ridursi all'identità*) *il cui ordine non è divisibile per* p_i, *permutabile con essa.*

Dividiamo ora in due categorie le operazioni d'ordine p_i.

Diremo che una operazione P, d'ordine p_i, *è del tipo 1°, se, detto* $\mathbf{L}$ *il*

normalizzante di P in **G**, *ogni sottogruppo d'ordine p_i^2 di* **L** *appartiene al centrale del proprio normalizzante in* **L**.

Si noti appena che, se ciò avviene per un sottogruppo d'ordine p_i^2 di **L**, ciò avviene per tutti, poichè, pel teorema di SYLOW, i sottogruppi d'ordine p_i^2 sono coniugati in **L**.

Diremo che una operazione P d'ordine p_i *è del tipo 2° se non è del tipo 1°*.

Se una operazione è del tipo 1° (2°) anche tutte le sue potenze appartengono allo stesso tipo.

Si osservi che, se P è una operazione del tipo 2°, $\mathbf{P}_i^{(2)}$ un sottogruppo d'ordine p_i^2 che la contiene, **L** il normalizzante di P in **G**, deve esistere in **L** qualche operazione permutabile con $\mathbf{P}_i^{(2)}$ ma nello stesso tempo non permutabile con ogni operazione di $\mathbf{P}_i^{(2)}$. In altri termini, detto **N** il normalizzante ed **M** il centralizzante di $\mathbf{P}_i^{(2)}$ in **G**, deve esistere in **N** qualche operazione non di **M** permutabile con P, ossia il centralizzante del gruppo ciclico d'ordine p_i generato da P, in **N**, è più vasto di **M**. Abbiamo visto nel paragrafo 5. 3. che ciò può avvenire al più per due sottogruppi d'ordine p_i di $\mathbf{P}_i^{(2)}$, quindi si può concludere che in $\mathbf{P}_i^{(2)}$ non vi sono più di $2(p_i-1)$ operazioni del tipo 2°.

Indichiamo ora con $\nu(p_i)$ il numero delle operazioni di **G** che possono darsi come prodotto di una operazione d'ordine p_i per una operazione il cui ordine non è divisibile per p_i permutabile con essa. Indichiamo poi con $\nu_1(p_i)$ il numero di operazioni di **G** che possono darsi come prodotto di una operazione d'ordine p_i del tipo 1° per una operazione permutabile con essa il cui ordine non è divisibile per p_i; e con $\nu_2(p_i)$ il numero delle operazioni di **G** che possono darsi come prodotto di una operazione d'ordine p_i del tipo 2° per una operazione, permutabile con essa, il cui ordine non è divisibile per p_i. Evidentemente è $\nu(p_i)=\nu_1(p_i)+\nu_2(p_i)$; e $\nu(p_i)$ è eguale al numero delle operazioni di **G** il cui ordine è divisibile per p_i, per quello che abbiamo osservato precedentemente.

a). Calcoliamo il massimo valore che può assumere $\nu_2(p_i)$. Sia P una operazione d'ordine p_i del tipo 2°. Indichiamo con $\nu_2(P)$ il numero delle operazioni che possono darsi come prodotto di P o di una sua coniugata rispetto a **G** per una operazione, permutabile con essa, il cui ordine non è divisibile per p_i; e calcoliamoci $\nu_2(P)$.

Sia **L**, d'ordine lp_i^2 (l non divisibile per p_i^2) il normalizzante di P in **G**. Detto **P** il sottogruppo d'ordine p_i generato da P, decomponiamo **L** secondo **P** e i suoi laterali. Evidentemente **P** appartiene al centrale di **L**, quindi ogni operazione di **L** è permutabile con ogni operazione di **P**. In ogni laterale c'è al più una operazione il cui ordine è primo con p_i. Se infatti L è una operazione di **L** il cui ordine è primo con p_i, tutte le operazioni appartenenti allo stesso laterale di L sono della forma $P^x \cdot L$. Ma poichè P^x ed L sono permutabili, e i loro ordini sono primi tra loro, ne segue che è $(P^x \cdot L)^y=1$ allora e solo allora che è $(P^x)^y=1$ ed $L^y=1$; essendo poi P^x d'ordine p_i, si ha che y deve essere

divisibile per p_i. Quindi, oltre L, non vi sono nel laterale operazioni d'ordine primo con p_i.

Da ciò segue che il numero delle operazioni di **G** il cui ordine non è divisibile per p_i, permutabili con P, non supera lp_i; e quindi non supera lp_i il numero delle operazioni che possono darsi come prodotto di P per una operazione il cui ordine non è divisibile per p_i, permutabile con P.

Il numero delle operazioni coniugate a P in **G** è eguale all'indice di **L** in **G**, ossia $\frac{g}{lp_i^2}$. Ne segue che $\nu_2(P)$ non supera $lp_i \frac{g}{lp_i^2} = \frac{g}{p_i}$.

Ricordiamo il seguente teorema di TURKIN [8]:

« Sia **G** un gruppo d'ordine $p^\alpha \cdot s$ (p primo ed s non divisibile per p). **H** sia un sottogruppo di **G** d'ordine p^α abeliano. Se in **H** c' è un elemento non identico che è contenuto anche nel centrale del normalizzante di **H**, **G** ha un sottogruppo invariante, il cui ordine è divisibile per s ».

Applicando questo teorema nel nostro caso, abbiamo che, se **G** è semplice, e indichiamo con $\mathbf{P}_i^{(2)}$ un sottogruppo d'ordine p_i^2 che contiene P, e con **N** il normalizzante di $\mathbf{P}_i^{(2)}$, P non appartiene al centrale di **N**, ossia P non è invariante in **N**. Il numero delle operazioni coniugate a P in **N** deve dividere l'ordine di **N**, e quindi non è inferiore a p_1; inoltre esse sono tutte in $\mathbf{P}_i^{(2)}$, perchè questo è l'unico sottogruppo d'ordine p_i^2 in **N**.

Il numero $\nu_2(p_i)$ non supera il prodotto del massimo valore che può essere assunto da $\nu_2(P)$ per il numero delle classi di operazioni coniugate d'ordine p_i del tipo 2° in **G**.

Il numero di tali classi in **G** è eguale al numero delle classi di operazioni d'ordine p_i del tipo 2°, coniugate rispetto a **G**, in $\mathbf{P}_i^{(2)}$, perchè i sottogruppi d'ordine p_i^2 in **G** sono tra loro coniugati a causa del teorema di SYLOW, e quindi ogni operazione di $\mathbf{P}_i^{(2)}$ è coniugata ad almeno una operazione di ogni altro sottogruppo d'ordine p_i^2.

Il numero delle operazioni del tipo 2° in $\mathbf{P}_i^{(2)}$ è, come abbiamo visto, al massimo $2(p_i-1)<2p_i$; inoltre poichè, come abbiamo indicato, ogni operazione del tipo 2° di $\mathbf{P}_i^{(2)}$ è coniugata in **N**, e quindi in **G**, ad almeno p_1 operazioni del medesimo tipo, si ha che il numero di classi di operazioni, coniugate rispetto a **G**, d'ordine p_i del tipo 2° di $\mathbf{P}_i^{(2)}$ e quindi di **G** non supera $\frac{2p_i}{p_1}$. E poichè, come si vide, $\nu_2(P)$ non supera $\frac{g}{p_i}$, si ha che $\nu_2(p_i)$ non supera $\frac{g}{p_i} \cdot \frac{2p_i}{p_1} = \frac{2g}{p_1}$.

Si noti che, se $\mathbf{P}_i^{(2)}$ contiene realmente operazioni del tipo 2°, l'indice di **M** in **N** è $\geqslant p_1^2$. Infatti, il normalizzante **B** di P in **N** deve essere più vasto di **M** perchè P è del tipo 2°; quindi l'indice di **M** in **B** è $\geqslant p_1$; d'altra parte **B** non

---

[8] W. K. TURKIN: *Ein neues Kriterium der Einfachheit einer endlichen Gruppe.* Math. Ann., 111, p. 281.

può coincidere con **N**, altrimenti, per il teorema di TURKIN ultimamente riportato, **G** non è semplice; quindi l'indice di **B** in **N** è $\geqslant p_1$; e l'indice di **M** in **N** è $\geqslant p_1^2$.

b). Calcoliamo ora il massimo valore che può assumere $\nu_1(p_i)$. Se P è una operazione d'ordine p_i del tipo 1° di **G**, indichiamo con $\nu_1(P)$ il numero delle operazioni che possono darsi come prodotto di P o di una sua coniugata per una operazione, permutabile con essa, il cui ordine non è divisibile per p_i. Calcoliamoci $\nu_1(P)$.

Sia P una operazione del tipo 1° d'ordine p_i di **G**. Se $\mathbf{P}_i^{(2)}$ è un sottogruppo d'ordine p_i^2 che contiene quell'operazione, ed **N** è il normalizzante di $\mathbf{P}_i^{(2)}$, mentre **M** è il centralizzante del medesimo, dovrà, come abbiamo visto, ogni operazione di **N** permutabile con P essere in **M**.

Se chiamo **L** il normalizzante di P in **G**, d'ordine lp_i^2, si ha che $\mathbf{P}_i^{(2)}$ appartiene al centrale del proprio normalizzante in **L**, e quindi, per un teorema di BURNSIDE (9), c'è in **L** un $\overline{\mathbf{L}}$, d'ordine l, invariante. Ad ogni operazione di **L** non contenuta in $\overline{\mathbf{L}}$ corrisponde in $\frac{\mathbf{L}}{\overline{\mathbf{L}}}$ un'operazione d'ordine p_i; da cui segue che $\overline{\mathbf{L}}$ contiene tutte le operazioni di **L** il cui ordine non è divisibile per p_i. Pertanto il numero delle operazioni di **L** il cui ordine non è divisibile per p_i è l; ed è quindi l anche il numero delle operazioni che possono darsi come prodotto di P per una operazione il cui ordine non è divisibile per p_i permutabile con P. E poichè il numero delle operazioni coniugate a P in **G** è eguale all'indice di **L** in **G**, cioè $\frac{g}{lp_i^2}$, si ha che $\nu_1(P) = l \cdot \frac{g}{lp_i^2} = \frac{g}{p_i^2}$.

Il numero $\nu_1(p_i)$ non supera il prodotto del massimo valore preso da $\nu_1(P)$, cioè $\frac{g}{p_i^2}$, per il numero delle classi di operazioni coniugate d'ordine p_i in **G** del tipo 1°; il numero di tali classi non supera il numero delle classi di operazioni di $\mathbf{P}_i^{(2)}$ del tipo 1° coniugate rispetto ad **N**; e questo numero non supera $\frac{p_i^2}{\overline{n}}$, ove $\overline{n}$ è l'indice di **M** in **N**, perchè, essendo P del tipo 1°, il normalizzante di P in **N** è **M**. Quindi $\nu_1(p_i)$ non supera $\frac{g}{p_i^2} \cdot \frac{p_i^2}{\overline{n}} = \frac{g}{\overline{n}}$. Ma $\overline{n}$ è in genere $\geqslant p_1$, e se **G** contiene operazioni del tipo 2° è anche, come s'è visto alla fine della *a*) di questo paragrafo, $\overline{n} \geqslant p_1^2$.

Riunendo i risultati *a*) e *b*) si può concludere che $\nu(p_i)$ non supera $\frac{2g}{p_1} + \frac{g}{p_1^2}$ se vi sono in **G** operazioni d'ordine p_i del tipo 2°, mentre non supera $\frac{g}{p_1}$ nel caso contrario. In ogni caso però $\nu(p_i) \leqslant \frac{2g}{p_1} + \frac{g}{p_1^2}$; e quindi, nel caso che i sotto-

(9) W. BURNSIDE, l. c. (4).

gruppi d'ordine p di $\mathbf{G}$ non siano ciclici, si ha che il numero delle operazioni di $\mathbf{G}$ il cui ordine è divisibile per p_i non supera $\frac{2g}{p_1}+\frac{g}{p_1^2}$.

5. 5. - Supponiamo ora che i sottogruppi di SYLOW il cui ordine è p_i^2 siano ciclici. Determiniamo anche in questo caso un massimo per il numero di operazioni il cui ordine è divisibile per p_i.

Sia A una qualunque operazione di $\mathbf{G}$ il cui ordine è divisibile per p_i. Nel gruppo ciclico generato da A c'è un sottogruppo anch'esso ciclico d'ordine p_i, che chiamiamo $\mathbf{P}_i^{(1)}$, il quale deve essere contenuto in un sottogruppo almeno $\mathbf{P}_i^{(2)}$ d'ordine p_i^2. Allora $\mathbf{P}_i^{(1)}$ è costituito, oltre che dall'identità, da tutte le operazioni d'ordine p_i di $\mathbf{P}_i^{(2)}$. Poichè A è permutabile con tutte le sue potenze, A è nel centralizzante di $\mathbf{P}_i^{(1)}$. Sia P^{p_i} un'operazione generatrice di $\mathbf{P}_i^{(1)}$. Per un teorema di TURKIN ([10]) ultimamente riportato, se $\mathbf{G}$ è semplice, dovrà P^{p_i} essere coniugata a qualche altra operazione di $\mathbf{P}_i^{(2)}$ d'ordine p_i, cioè a qualche altra operazione di $\mathbf{P}_i^{(1)}$; in altre parole, se $\mathbf{M}$ è il centralizzante di $\mathbf{P}_i^{(1)}$ ed $\mathbf{N}$ il normalizzante del medesimo, dovrà essere $\mathbf{N}$ più ampio di $\mathbf{M}$, cioè, detto $\overline{m}p_i^2$ l'ordine di $\mathbf{M}$ e np_i^2 l'ordine $\mathbf{N}$, dovrà essere $n>\overline{m}$, ossia $n\geqslant\overline{m}p_1$. Le operazioni permutabili con tutte le operazioni di $\mathbf{P}_i^{(1)}$ sono in numero di $\overline{m}p_i^2$; le operazioni permutabili con tutte le operazioni di $\mathbf{P}_i^{(1)}$ o di un trasformato sono $\frac{g}{np_i^2}\cdot\overline{m}p_i^2\leqslant\frac{g}{p_1}$, perchè $n\geqslant\overline{m}p_1$.

Poichè ogni operazione il cui ordine è divisibile per p_i è contenuta nel centralizzante di $\mathbf{P}_i^{(1)}$ o di un suo trasformato, segue che il numero di tali operazioni non supera $\frac{g}{p_1}$, e quindi non supera nemmeno $\frac{2g}{p_1}+\frac{g}{p_1^2}$. Quindi anche nel caso di $\mathbf{P}_i^{(2)}$ ciclici, il numero delle operazioni il cui ordine è divisibile per p_i non supera $\frac{2g}{p_1}+\frac{g}{p_1^2}$.

5. 6. - Se pertanto $\mathbf{G}$ è un gruppo semplice, il numero delle operazioni il cui ordine è divisibile per p_s (ove è $r<s\leqslant m$) non supera $\frac{g}{p_1}$; il numero delle operazioni il cui ordine è divisibile per p_i (ove è $1<i\leqslant r$) non supera $\frac{2g}{p_1}+\frac{g}{p_1^2}$; infine il numero delle operazioni il cui ordine divide p_1^a non supera $g\left(\frac{1}{p_1}+\frac{1}{\overline{p}}\right)$, ove $\overline{p}$ è il più piccolo fattore primo di g dopo p_1.

In queste categorie rientrano tutte le operazioni di $\mathbf{G}$; dovrà quindi essere

$$g\leqslant g\left(\frac{1}{p_1}+\frac{1}{\overline{p}}\right)+g\cdot\frac{m-r}{p_1}+g\left(\frac{2(r-1)}{p_1}+\frac{r-1}{p_1^2}\right)$$

$$1\leqslant\frac{r-1}{p_1^2}+\frac{(m-r)+2r-1}{p_1}+\frac{1}{\overline{p}}$$

([10]) W. K. TURKIN, l. c. ([8]).

ed anche, dato $p_1 \geqslant m+r+1$, visto che $m+r+1>r-1$, e $\bar{p}>p$

$$1<\frac{r-1}{p_1^2}+\frac{m+r}{p_1}<\frac{p_1}{p_1^2}+\frac{m+r}{p_1}=\frac{m+r+1}{p_1}\leqslant\frac{p_1}{p_1}=1$$

il che è assurdo.

Quindi **G** non è semplice e, per quanto abbiamo osservato all'inizio della dimostrazione, è risolubile, c. d. d.

6. - LEMMA. — *In ogni gruppo semplice, d'ordine* $g=p^3\cdot\bar{g}$, *(ove* p *è un numero primo dispari, e* $\bar{g}$ *è primo con* p *e con tutti i numeri primi minori di* p*) il numero delle operazioni il cui ordine è divisibile per* p *non supera* $\frac{g}{\bar{p}}$, *ove* $\bar{p}$ *è il più piccolo fattore di* g, *dopo* p.

Sia **G** un tale gruppo, e sia $\mathbf{P}_3$ un sottogruppo di SYLOW di **G** d'ordine p^3. Esso, per un teorema di BURNSIDE ([11]) deve, essendo **G** semplice, essere abeliano.

Calcoliamo prima il numero delle operazioni di **G** che possono darsi come prodotto di una operazione fissata P (diversa dall'identità) di $\mathbf{P}_3$ per una operazione il cui ordine non è divisibile per p, permutabile con P.

Sia **N** il normalizzante di P. Essendo $\mathbf{P}_3$ abeliano, P è invariante in $\mathbf{P}_3$, e quindi l'ordine di **N** è della forma $p^3\cdot h$, ove h non è divisibile per p. Supponiamo prima $h>1$. Sia **R** il normalizzante di $\mathbf{P}_3$ in **N**. Ogni operazione di **R** determina un automorfismo in $\mathbf{P}_3$, per il quale P e le sue potenze sono mutate in sè. Sia poi **S** il centralizzante di $\mathbf{P}_3$ in **N**; voglio far vedere che **S** coincide con **R**, vale a dire che tutte le operazioni di **R** trasformano in sè ogni operazione di $\mathbf{P}_3$. Supponiamo che ciò non sia, e indichiamo con R quella tra le operazioni di **R** non contenute in **S** che trasforma in sè il maggior numero di operazioni di $\mathbf{P}_3$. Le operazioni di $\mathbf{P}_3$ trasformate in sè da R formano un sottogruppo di ordine p o p^2. Nel primo caso le operazioni di $\mathbf{P}_3$, non lasciate ferme da R, sono $p^3-p=(p+1)p(p-1)$, nel secondo caso $p^3-p^2=p^2(p-1)$. Ma R dovrà determinare, sulle operazioni di $\mathbf{P}_3$ non lasciate ferme, una sostituzione regolare cioè costituita di cicli aventi egual numero di lettere, altrimenti una potenza di R, pur non lasciando ferme tutte le operazioni di $\mathbf{P}_3$, lascerebbe ferme più operazioni che R, contro l'ipotesi su R. L'ordine di questa sostituzione dovrà da un lato, per l'osservazione fatta al paragrafo 3, dividere l'ordine di $\frac{\mathbf{R}}{\mathbf{S}}$, quindi anche $\bar{g}$; e d'altro lato esso, essendo la sostituzione regolare, dovrà dividere il numero delle operazioni di $\mathbf{P}_3$ non lasciate ferme, vale a dire $(p+1)p(p-1)$, o $p^2(p-1)$, il che porta a un assurdo perchè per ipotesi $\bar{g}$ è divisibile solo per fattori primi maggiori di p, ossia, visto che p è dispari, $\geqslant p+2$. Quindi **R** coincide con **S**, e pertanto $\mathbf{P}_3$ appartiene in **N** al centrale del proprio normalizzante,

---

([11]) W. BURNSIDE, l. c. ([4]).

onde per un teorema di BURNSIDE già citato, **N** ha un sottogruppo invariante d'ordine h che contiene tutte e sole le operazioni di **N** tali che il loro ordine è primo con p. Il numero delle operazioni di **G** il cui ordine non è divisibile per p, permutabili con P, è h.

Se poi è $h=1$, c'è in **G** la sola identità che sia permutabile con P e abbia un ordine non divisibile per p; quindi, anche in questo caso, il numero delle operazioni di **G** il cui ordine non è divisibile per p, permutabili con P, è h.

Il numero delle operazioni coniugate a P in **G** è uguale all'indice di **N** in **G**, cioè $\frac{g}{hp^3}$. Quindi il numero delle operazioni di **G** che possono darsi come prodotto di P o di una sua coniugata per una operazione permutabile con essa e il cui ordine non è divisibile per p è al più $\frac{g}{hp^3} \cdot h = \frac{g}{p^3}$.

Calcoliamo ora il numero delle classi di operazioni coniugate il cui ordine è una potenza di p in **G**. Ragionando in modo analogo che nel teorema I, paragrafo 5. 4. si vede che detto numero non supera il numero delle classi di operazioni di $\mathbf{P}_3$ coniugate rispetto al normalizzante **L** di $\mathbf{P}_3$ in **G**. Per un teorema di TURKIN già riportato ([12]), se **G** è semplice, e P è una operazione qualunque di $\mathbf{P}_3$, ci deve essere in **L** una operazione che trasforma P in un'altra operazione di $\mathbf{P}_3$. Quindi il numero delle classi di operazioni di $\mathbf{P}_3$ coniugate rispetto ad **L** è al più $\frac{p^3}{\bar{p}}$, e tale è anche il numero delle classi di operazioui coniugate il cui ordine è una potenza di p in **G**. Essendo, come s'è visto, al più $\frac{g}{p^3}$ il numero delle operazioni che possono darsi come prodotto di P o di una sua coniugata per una operazione permutabile con P il cui ordine non è divisibile per p, segue che sono al più $\frac{g}{p^3} \cdot \frac{p^3}{\bar{p}} = \frac{g}{\bar{p}}$ le operazioni che possono darsi come prodotto di una operazione il cui ordine è una potenza di p per una operazione il cui ordine non è divisibile per p permutabile con essa; e quindi sono al più $\frac{g}{\bar{p}}$ le operazioni il cui ordine è divisibile per p, c. d. d. ([13]).

7. - TEOREMA II. — *Ogni gruppo* **G** *il cui ordine è della forma* $g=p_1^3 p_2^\beta p_3^2 \dots p_r^2 p_{r+1} \dots p_m$, *ove* p_1 *è il più piccolo fattore di* g, *è risolubile, purchè sia* $p_1 \geqslant m+r$ e $p_2 \geqslant \beta$.

Si osservi anzitutto che, se $\bar{g}$ è un divisore di g divisibile per p_1^3, ogni gruppo di ordine $\bar{g}$ soddisfa alle condizioni del teorema; se poi $\bar{\bar{g}}$ è un divisore di g non divisibile per p_1^3, essendo $p_2 > p_1 \geqslant m+r-1$, e quindi $p_2 \geqslant m+r$, ogni gruppo di ordine $\bar{\bar{g}}$ soddisfa alle condizioni del teorema precedente I e

---

([12]) W. K. TURKIN, l. c. ([8]).

([13]) Casi particolari di questo lemma sono stati già dimostrati e applicati, e figurano in diversi lavori di BURNSIDE e di TURKIN.

quindi è risolubile. Possiamo pertanto procedere per induzione, ammettendo la risolubilità di ogni gruppo il cui ordine divide g.

Con procedimento del tutto eguale a quello del teorema I si mostra che basta dimostrare che **G** non è semplice. Si procede poi, come nel teorema I, per assurdo e si prova in modo analogo a quello del teorema I che, se **G** fosse semplice, il numero delle operazioni di **G** il cui ordine è divisibile per p_i (ove è $2<i\leqslant r$) non supererebbe $\frac{2g}{p_1}+\frac{g}{p_1^2}$; il numero delle operazioni di **G** il cui ordine è divisibile per p_k (ove è $r<k\leqslant m$) non supererebbe $\frac{g}{p_1}$; si prova ancora, (in modo analogo a quello usato nella dimostrazione del teorema I per stabilire il numero delle operazioni il cui ordine divide p_1^a) che, se **G** fosse semplice, il numero delle operazioni di **G** il cui ordine divide p_2^β non supererebbe $g\left(\frac{1}{p_2}+\frac{1}{p_1}\right)$. Il numero poi delle operazioni di **G** il cui ordine è divisibile per p_1 non supererebbe, se **G** fosse semplice, per il lemma precedente, $\frac{g}{\bar{p}}$, ove $\bar{p}$ è il più piccolo fattore primo di g, dopo p_1.

Dovrebbe quindi essere, se **G** fosse semplice

$$g\leqslant g\left\{\frac{2(r-2)}{p_1}+\frac{r-2}{p_1^2}+\frac{1}{\bar{p}}+\frac{1}{p_2}+\frac{1}{p_1}+\frac{m-r}{p_1}\right\}=g\left\{\frac{m+r-3}{p_1}+\frac{r-2}{p_1^2}+\frac{1}{\bar{p}}+\frac{1}{p_2}\right\}$$

ed anche, essendo $\bar{p}>p_1$, $p_2>p_1$, $p_1\geqslant m+r>r-2$

$$g<g\left\{\frac{m+r-1}{p_1}+\frac{r-2}{p_1^2}\right\}=g\left\{1-\frac{p_1-(r-2)}{p_1^2}\right\}<g$$

il che è assurdo. Quindi **G** è risolubile, c. d. d.

LEONIDA TONELLI - *Direttore responsabile.* Finito di stampare il 13 aprile 1940-XVIII.