

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>

© Scuola Normale Superiore, Pisa, 1940, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

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 $\mathbf{G}$ si dice regolare se, dato un qualunque intero positivo α e una qualsiasi coppia di elementi P e Q di $\mathbf{G}$, chiamato $\mathbf{L}$ il sottogruppo generato da P e Q , è sempre possibile trovare degli elementi $S_3, S_4, \dots, S_r$, tutti appartenenti al derivato di $\mathbf{L}$ e soddisfacenti all'equazione

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

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 $\mathbf{G}$ è un p -gruppo regolare, gli elementi di $\mathbf{G}$ il cui ordine divide p^β (β intero qualunque) formano gruppo ».

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

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

Allora, se l'indice di $\mathbf{S}$ in $\mathbf{H}$ è p^x , e q è il più piccolo fattore primo di g diverso da p , $\mathbf{G}$ 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 $\mathbf{G}$ un gruppo semplice d'ordine g , ed $\mathbf{H}$ un suo sottogruppo di SYLOW d'ordine p^α regolare. Se q è il più piccolo fattore primo di g diverso da p , $\mathbf{G}$ 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 $\mathbf{H}$. Essendo $\mathbf{H}$ regolare, per la b) del paragrafo 1, le operazioni di $\mathbf{H}$ il cui ordine divide p^{r-1} formano un sottogruppo $\mathbf{R}$, che, per la sua stessa definizione, è caratteristico in $\mathbf{H}$. Evidentemente, la potenza p -esima di una qualsiasi operazione di $\mathbf{H}$ non contenuta in $\mathbf{R}$, è in $\mathbf{R}$. Sia $\mathbf{S}$ un qualsiasi sottogruppo di $\mathbf{H}$, invariante massimo in esso (vale a dire di indice p in $\mathbf{H}$) e contenente $\mathbf{R}$. Evidentemente $\mathbf{S}$ contiene il derivato di $\mathbf{H}$, perchè $\frac{\mathbf{H}}{\mathbf{S}}$ è abeliano; inoltre tutte le operazioni di $\mathbf{H}$ non contenute in $\mathbf{S}$ hanno periodo assoluto p^r (perchè non sono in $\mathbf{R}$) e periodo relativo p (perchè le loro potenze p -esime devono stare in $\mathbf{R}$ e quindi in $\mathbf{S}$). Pertanto, dal nostro teorema anzi citato, segue che $\mathbf{G}$ non ha più 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 $\mathbf{H}$ non contenute in $\mathbf{S}$ è costante ($=p^{r-1}$) il rapporto tra periodo assoluto e periodo relativo rispetto ad $\mathbf{S}$.

3. - Ricordiamo la seguente definizione introdotta da HALL:

Sia un gruppo $\mathbf{G}$ e un suo sottogruppo $\mathbf{H}$. Dicesi centralizzante di $\mathbf{H}$ in $\mathbf{G}$ il sottogruppo costituito da tutte le operazioni di $\mathbf{G}$ permutabili con ogni operazione di $\mathbf{H}$.

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

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

È noto ⁽³⁾ che $\mathbf{A}$ 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 $\mathbf{A}$ è $(p^2-1)(p^2-p)$, e ogni sua sostituzione è della forma

$$\begin{aligned} x_1' &\equiv a_{11}x_1 + a_{12}x_2 \\ x_2' &\equiv a_{21}x_1 + a_{22}x_2 \end{aligned} \quad (\text{mod } p)$$

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

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

In $\mathbf{A}$ inoltre è contenuto un sottogruppo $\mathbf{C}$ d'ordine $p-1$ generato dalla sostituzione

$$\begin{aligned} x_1' &\equiv zx_1 \\ x_2' &\equiv zx_2 \end{aligned} \quad (\text{mod } p),$$

ove z è una radice primitiva (mod p). $\mathbf{C}$ è il centrale di $\mathbf{A}$.

Ogni sostituzione di $\mathbf{C}$ 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 $\mathbf{C}$ 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 $\mathbf{C}$.

$\mathbf{S}$ e $\mathbf{C}$ hanno a comune un sottogruppo $\mathbf{I}$ d'ordine 2, costituito dall'identità e dalla sostituzione

$$\begin{aligned} x_1' &\equiv -x_1 \\ x_2' &\equiv -x_2 \end{aligned} \quad (\text{mod } p).$$

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

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

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

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

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

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

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 $\mathbf{G}$ 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 $p_1 \geq a$, sono tutti regolari, e quindi pel secondo teorema del paragrafo 2, se $\mathbf{G}$ è semplice, il numero delle operazioni di $\mathbf{G}$ 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 $\mathbf{G}$ è semplice, il numero delle operazioni il cui ordine è divisibile per p_k ($r < k \leq m$) non supera $\frac{g}{p_1}$.

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

Il numero delle operazioni contenute nel centralizzante di almeno un sottogruppo d'ordine p_k non supera pertanto $\frac{g}{np_k} \cdot \bar{m}p_k \leq \frac{g}{p_1}$; d'altra parte ogni operazione di $\mathbf{G}$ 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 $\mathbf{G}$ sia semplice, le operazioni di $\mathbf{G}$ il cui ordine è divisibile per p_i ($1 < i \leq r$).

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

Siano rispettivamente $\mathbf{N}$, d'ordine np_i^2 ed $\mathbf{M}$ d'ordine $\bar{m}p_i^2$ il normalizzante e il centralizzante di $\mathbf{P}_i^{(2)}$ in $\mathbf{G}$. Se $\mathbf{G}$ è semplice, $\mathbf{N}$ è più vasto di $\mathbf{M}$ ⁽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 $\bar{\mathbf{N}}$ del gruppo di automorfismi di $\mathbf{P}_i^{(2)}$. Ma $\bar{n}$ è primo con $2p_i$; quindi $\bar{\mathbf{N}}$, 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 $\mathbf{N}$ siano più vasti di $\mathbf{M}$.

(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 $\mathbf{G}$ è un gruppo risolubile d'ordine $h \cdot k$, dove h è primo con k , si ha che:

- 1). $\mathbf{G}$ ha almeno un sottogruppo d'ordine h .
- 2). Due sottogruppi di $\mathbf{G}$ d'ordine h sono coniugati.
- 3). Ogni sottogruppo di $\mathbf{G}$ il cui ordine divide h sta almeno in un sottogruppo d'ordine h .
- 4). Il numero l_h dei sottogruppi di $\mathbf{G}$ d'ordine h può essere espresso come prodotto di fattori ciascuno dei quali (i) è $\equiv 1 \pmod{\text{qualche fattore primo di } h}$, (ii) è una potenza di un numero primo e divide uno dei fattori principali di $\mathbf{G}$ ».

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

Decomponiamo $\mathbf{M}$ secondo $\mathbf{D}$ e i suoi laterali nel seguente modo:

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

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

Sarà poi

$$\mathbf{N} = \mathbf{M} + \mathbf{M}N_2 + \dots + \mathbf{M}N_n$$

ove $N_2, \dots, N_n$ sono opportune operazioni di $\mathbf{N}$. Avremo allora

$$\mathbf{N} = (\mathbf{D} + \mathbf{D}P_2 + \dots + \mathbf{D}P_{p_i^2}) + (\mathbf{D} + \dots + \mathbf{D}P_{p_i^2})N_2 + \dots + (\mathbf{D} + \dots + \mathbf{D}P_{p_i^2})N_n$$

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

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

Pertanto tra $\mathbf{N}^*$ e $\bar{\mathbf{N}}$ c'è un isomorfismo meriedrico, e a $\bar{\mathbf{P}}_i^{(2)}$ corrisponde in $\bar{\mathbf{N}}$ l'identità. $\frac{\mathbf{N}^*}{\bar{\mathbf{P}}_i^{(2)}}$, coincidendo con $\frac{\mathbf{N}}{\bar{\mathbf{M}}}$, 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 $\bar{\mathbf{P}}_i^{(2)}$ risolubile, si ha che $\mathbf{N}^*$ è risolubile, e quindi, pel teorema anzi riportato di HALL, ha un sottogruppo $\mathbf{N}^{(4)}$ d'ordine $\bar{n}$, che ha solo l'identità a comune con $\bar{\mathbf{P}}_i^{(2)}$. Quindi a $\mathbf{N}^{(4)}$ corrisponderà in $\bar{\mathbf{N}}$ un sottogruppo d'ordine $\bar{n}$ oloedricamente isomorfo ad $\mathbf{N}^{(4)}$; esso dovrà coincidere con $\bar{\mathbf{N}}$. Dunque $\mathbf{N}^{(4)}$ è oloedricamente isomorfo con $\bar{\mathbf{N}}$.

Consideriamo $\mathbf{N}^*$, e vediamo quante sono le operazioni di $\bar{\mathbf{P}}_i^{(2)}$ permutabili con qualche operazione di $\mathbf{N}^{(4)}$. Notiamo intanto che non esiste, oltre l'identità, nessuna operazione di $\mathbf{N}^{(4)}$ che sia permutabile con tutte le operazioni di $\bar{\mathbf{P}}_i^{(2)}$. 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 $\bar{\mathbf{P}}_i^{(2)}$, quindi N^* dovrebbe essere in $\bar{\mathbf{P}}_i^{(2)}$, e, dovendo anche essere, per ipotesi, in $\mathbf{N}^{(4)}$, è l'identità, come s'era detto.

Una operazione di $\mathbf{N}^{(4)}$ permutabile con una operazione P di $\bar{\mathbf{P}}_i^{(2)}$, è permutabile con tutte le operazioni del sottogruppo ciclico d'ordine p_i generato da P .

Sia $\mathbf{P}_{i,1}^{(4)}$ un sottogruppo d'ordine p_i di $\bar{\mathbf{P}}_i^{(2)}$ e sia $\mathbf{Z}_1$ il sottogruppo costituito da tutte le operazioni di $\mathbf{N}^{(4)}$ permutabili con tutte le operazioni di $\mathbf{P}_{i,1}^{(4)}$.

Sia $\mathbf{P}_{i,2}^{(4)}$ un altro sottogruppo di $\bar{\mathbf{P}}_i^{(2)}$ che abbia ordine p_i , e si definisca $\mathbf{Z}_2$ rispetto ad esso come si è definito $\mathbf{Z}_1$ rispetto a $\mathbf{P}_{i,1}^{(4)}$.

Così per ogni sottogruppo $\mathbf{P}_{i,j}^{(4)}$ d'ordine p_i di $\bar{\mathbf{P}}_i^{(2)}$ 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 $\mathbf{P}_{i,1}^{(4)}$ e di $\mathbf{P}_{i,2}^{(4)}$ e quindi con tutte le operazioni del sottogruppo da essi generato, che è $\bar{\mathbf{P}}_i^{(2)}$; ma abbiamo visto più sopra che $\mathbf{N}^{(4)}$ non ha altre operazioni, oltre l'identità, che siano permutabili con ogni operazione di $\bar{\mathbf{P}}_i^{(2)}$, pertanto M deve coincidere con l'identità.

Sia N una operazione di $\mathbf{Z}_1$ diversa dall'identità. $\mathbf{N}^{(4)}$, essendo isomorfo oloedricamente ad $\bar{\mathbf{N}}$, è abeliano; pertanto N è permutabile con $\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3$. Essendo poi $\bar{\mathbf{P}}_i^{(2)}$ invariante in $\mathbf{N}^*$, sarà N permutabile con il sottogruppo di $\bar{\mathbf{P}}_i^{(2)}$ formato da tutte le operazioni di $\bar{\mathbf{P}}_i^{(2)}$ permutabili con ogni operazione di $\mathbf{Z}_1$, cioè permutabile con $\mathbf{P}_{i,1}^{(4)}$. Analogamente si vede che N deve essere permutabile con $\mathbf{P}_{i,2}^{(4)}$.

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

1°) N muta in sè anche tutte le operazioni di $\mathbf{P}_{i,2}^{(1)}$. Ma ciò non può essere, perchè N appartarrebbe 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 $\mathbf{P}_{i,2}^{(1)}$, in una sua potenza P_2^x . Ma allora N non può mutare in sè $\mathbf{P}_{i,3}^{(1)}$. Infatti se è P_1 un'operazione generatrice di $\mathbf{P}_{i,1}^{(1)}$, e P_3 un'operazione generatrice di $\mathbf{P}_{i,3}^{(1)}$, 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 $\mathbf{P}_i^{(2)}$). 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 $\mathbf{P}_{i,3}^{(1)}$ 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 $\mathbf{P}_i^{(2)}$ 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 $\bar{\mathbf{P}}_i^{(2)}$, i cui centralizzanti in $\mathbf{N}^*$ sarebbero più vasti di $\bar{\mathbf{P}}_i^{(2)}$. Ma se $\mathbf{P}_{i,1}^{(1)}$ è un sottogruppo d'ordine p_i di $\bar{\mathbf{P}}_i^{(2)}$ il cui centralizzante $\mathbf{I}_1$ in $\mathbf{N}^*$ è più ampio di $\bar{\mathbf{P}}_i^{(2)}$, si ha che $\mathbf{N}^{(1)}$ ha qualche operazione, oltre l'identità, a comune con $\mathbf{I}_1$, cioè ha qualche operazione permutabile con $\mathbf{P}_{i,1}^{(1)}$, oltre l'identità. Ma abbiamo visto che ciò non può capitare per più di due sottogruppi di $\bar{\mathbf{P}}_i^{(2)}$ d'ordine p_i , dal che si deduce, procedendo a ritroso, che *in $\mathbf{P}_i^{(2)}$ 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 $\mathbf{G}$, ogni sottogruppo d'ordine p_i^2 di $\mathbf{L}$ appartiene al centrale del proprio normalizzante in $\mathbf{L}$.

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

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, $\mathbf{L}$ il normalizzante di P in $\mathbf{G}$, deve esistere in $\mathbf{L}$ 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 $\mathbf{N}$ il normalizzante ed $\mathbf{M}$ il centralizzante di $\mathbf{P}_i^{(2)}$ in $\mathbf{G}$, deve esistere in $\mathbf{N}$ qualche operazione non di $\mathbf{M}$ permutabile con P , ossia il centralizzante del gruppo ciclico d'ordine p_i generato da P , in $\mathbf{N}$, è più vasto di $\mathbf{M}$. 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 $\mathbf{G}$ 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 $\mathbf{G}$ 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 $\mathbf{G}$ 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 $\mathbf{G}$ 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 $\mathbf{G}$ per una operazione, permutabile con essa, il cui ordine non è divisibile per p_i ; e calcoliamoci $\nu_2(P)$.

Sia $\mathbf{L}$, d'ordine lp_i^2 (l non divisibile per p_i^2) il normalizzante di P in $\mathbf{G}$. Detto $\mathbf{P}$ il sottogruppo d'ordine p_i generato da P , decomponiamo $\mathbf{L}$ secondo $\mathbf{P}$ e i suoi laterali. Evidentemente $\mathbf{P}$ appartiene al centrale di $\mathbf{L}$, quindi ogni operazione di $\mathbf{L}$ è permutabile con ogni operazione di $\mathbf{P}$. In ogni laterale c'è al più una operazione il cui ordine è primo con p_i . Se infatti L è una operazione di $\mathbf{L}$ 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 $\mathbf{G}$ 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 $\mathbf{G}$ è eguale all'indice di $\mathbf{L}$ in $\mathbf{G}$, 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 $\mathbf{G}$ un gruppo d'ordine $p^a \cdot s$ (p primo ed s non divisibile per p). $\mathbf{H}$ sia un sottogruppo di $\mathbf{G}$ d'ordine p^a abeliano. Se in $\mathbf{H}$ c'è un elemento non identico che è contenuto anche nel centrale del normalizzante di $\mathbf{H}$, $\mathbf{G}$ ha un sottogruppo invariante, il cui ordine è divisibile per s ».

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

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 $\mathbf{G}$.

Il numero di tali classi in $\mathbf{G}$ è eguale al numero delle classi di operazioni d'ordine p_i del tipo 2°, coniugate rispetto a $\mathbf{G}$, in $\mathbf{P}_i^{(2)}$, perchè i sottogruppi d'ordine p_i^2 in $\mathbf{G}$ 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 $\mathbf{N}$, e quindi in $\mathbf{G}$, ad almeno p_1 operazioni del medesimo tipo, si ha che il numero di classi di operazioni, coniugate rispetto a $\mathbf{G}$, d'ordine p_i del tipo 2° di $\mathbf{P}_i^{(2)}$ e quindi di $\mathbf{G}$ 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 $\mathbf{M}$ in $\mathbf{N}$ è $\geq p_1^2$. Infatti, il normalizzante $\mathbf{B}$ di P in $\mathbf{N}$ deve essere più vasto di $\mathbf{M}$ perchè P è del tipo 2°; quindi l'indice di $\mathbf{M}$ in $\mathbf{B}$ è $\geq p_1$; d'altra parte $\mathbf{B}$ non

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

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

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

Se chiamo $\mathbf{L}$ il normalizzante di P in $\mathbf{G}$, d'ordine lp_i^2 , si ha che $\mathbf{P}_i^{(2)}$ appartiene al centrale del proprio normalizzante in $\mathbf{L}$, e quindi, per un teorema di BURNSIDE ⁽³⁾, c'è in $\mathbf{L}$ un $\bar{\mathbf{L}}$, d'ordine l , invariante. Ad ogni operazione di $\mathbf{L}$ non contenuta in $\bar{\mathbf{L}}$ corrisponde in $\frac{\mathbf{L}}{\bar{\mathbf{L}}}$ un'operazione d'ordine p_i ; da cui segue che $\bar{\mathbf{L}}$ contiene tutte le operazioni di $\mathbf{L}$ il cui ordine non è divisibile per p_i . Pertanto il numero delle operazioni di $\mathbf{L}$ 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 $\mathbf{G}$ è eguale all'indice di $\mathbf{L}$ in $\mathbf{G}$, 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 $\mathbf{G}$ 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 $\mathbf{N}$; e questo numero non supera $\frac{p_i^2}{\bar{n}}$, ove $\bar{n}$ è l'indice di $\mathbf{M}$ in $\mathbf{N}$, perchè, essendo P del tipo 1°, il normalizzante di P in $\mathbf{N}$ è $\mathbf{M}$. Quindi $\nu_1(p_i)$ non supera $\frac{g}{p_i^2} \cdot \frac{p_i^2}{\bar{n}} = \frac{g}{\bar{n}}$. Ma $\bar{n}$ è in genere $\geq p_1$, e se $\mathbf{G}$ contiene operazioni del tipo 2° è anche, come s'è visto alla fine della a) di questo paragrafo, $\bar{n} \geq p_1^2$.

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 $\mathbf{G}$ operazioni d'ordine p_i del tipo 2°, mentre non supera $\frac{g}{p_1}$ nel caso contrario. In ogni caso però $\nu(p_i) \leq \frac{2g}{p_1} + \frac{g}{p_1^2}$; e quindi, nel caso che i sotto-

⁽³⁾ 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 ⁽⁴⁰⁾ 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 di $\mathbf{N}$, dovrà essere $n > \overline{m}$, ossia $n \geq \overline{m}p_1$. 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 $\frac{g}{np_i^2} \cdot \overline{m}p_i^2 \leq \frac{g}{p_1}$, perchè $n \geq \overline{m}p_1$.

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 $r < s \leq m$) non supera $\frac{g}{p_1}$; il numero delle operazioni il cui ordine è divisibile per p_i (ove è $1 < i \leq r$) 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

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

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

⁽⁴⁰⁾ W. K. TURKIN, l. c. ⁽⁸⁾.

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

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

il che è assurdo.

Quindi $\mathbf{G}$ 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 $\frac{g}{p}$, ove $\bar{p}$ è il più piccolo fattore di g , dopo p .*

Sia $\mathbf{G}$ un tale gruppo, e sia $\mathbf{P}_3$ un sottogruppo di SYLOW di $\mathbf{G}$ d'ordine p^3 . Esso, per un teorema di BURNSIDE ⁽⁴⁾ deve, essendo $\mathbf{G}$ semplice, essere abeliano.

Calcoliamo prima il numero delle operazioni di $\mathbf{G}$ 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 $\mathbf{N}$ il normalizzante di P . Essendo $\mathbf{P}_3$ abeliano, P è invariante in $\mathbf{P}_3$, e quindi l'ordine di $\mathbf{N}$ è della forma $p^3 \cdot h$, ove h non è divisibile per p . Supponiamo prima $h > 1$. Sia $\mathbf{R}$ il normalizzante di $\mathbf{P}_3$ in $\mathbf{N}$. Ogni operazione di $\mathbf{R}$ determina un automorfismo in $\mathbf{P}_3$, per il quale P e le sue potenze sono mutate in sè. Sia poi $\mathbf{S}$ il centralizzante di $\mathbf{P}_3$ in $\mathbf{N}$; voglio far vedere che $\mathbf{S}$ coincide con $\mathbf{R}$, vale a dire che tutte le operazioni di $\mathbf{R}$ trasformano in sè ogni operazione di $\mathbf{P}_3$. Supponiamo che ciò non sia, e indichiamo con R quella tra le operazioni di $\mathbf{R}$ non contenute in $\mathbf{S}$ 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, $\geq p+2$. Quindi $\mathbf{R}$ coincide con $\mathbf{S}$, e pertanto $\mathbf{P}_3$ appartiene in $\mathbf{N}$ al centrale del proprio normalizzante,

⁽⁴⁾ W. BURNSIDE, l. c. (4).

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

Se poi è $h=1$, c'è in $\mathbf{G}$ 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 $\mathbf{G}$ il cui ordine non è divisibile per p , permutabili con P , è h .

Il numero delle operazioni coniugate a P in $\mathbf{G}$ è uguale all'indice di $\mathbf{N}$ in $\mathbf{G}$, cioè $\frac{g}{hp^3}$. Quindi il numero delle operazioni di $\mathbf{G}$ 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 $\mathbf{G}$. 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 $\mathbf{L}$ di $\mathbf{P}_3$ in $\mathbf{G}$. Per un teorema di TURKIN già riportato ⁽¹²⁾, se $\mathbf{G}$ è semplice, e P è una operazione qualunque di $\mathbf{P}_3$, ci deve essere in $\mathbf{L}$ 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 $\mathbf{L}$ è al più $\frac{p^3}{p}$, e tale è anche il numero delle classi di operazioni coniugate il cui ordine è una potenza di p in $\mathbf{G}$. 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 $\frac{g}{p^3} \cdot \frac{p^3}{p} = \frac{g}{p}$ 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 $\frac{g}{p}$ le operazioni il cui ordine è divisibile per p , c. d. d. ⁽¹³⁾.

7. - TEOREMA II. — *Ogni gruppo $\mathbf{G}$ 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 $p_1 \geq m+r$ e $p_2 \geq \beta$.*

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 $\bar{g}$ è un divisore di g non divisibile per p_1^3 , essendo $p_2 > p_1 \geq m+r-1$, e quindi $p_2 \geq m+r$, ogni gruppo di ordine $\bar{g}$ 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 $\mathbf{G}$ 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 $\mathbf{G}$ fosse semplice, il numero delle operazioni di $\mathbf{G}$ il cui ordine è divisibile per p_i (ove è $2 < i \leq r$) non supererebbe $\frac{2g}{p_i} + \frac{g}{p_i^2}$; il numero delle operazioni di $\mathbf{G}$ il cui ordine è divisibile per p_k (ove è $r < k \leq m$) non supererebbe $\frac{g}{p_k}$; 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^α) che, se $\mathbf{G}$ fosse semplice, il numero delle operazioni di $\mathbf{G}$ 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 $\mathbf{G}$ il cui ordine è divisibile per p_1 non supererebbe, se $\mathbf{G}$ 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 $\mathbf{G}$ fosse semplice

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

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

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

il che è assurdo. Quindi $\mathbf{G}$ è risolubile, c. d. d.