

# RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

GUIDO ZAPPA

## **Determinazione dei gruppi finiti in omomorfismo strutturale con un gruppo ciclico**

*Rendiconti del Seminario Matematico della Università di Padova,*  
tome 18 (1949), p. 140-162

[http://www.numdam.org/item?id=RSMUP\\_1949\\_\\_18\\_\\_140\\_0](http://www.numdam.org/item?id=RSMUP_1949__18__140_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1949, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) 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/>

## DETERMINAZIONE DEI GRUPPI FINITI IN OMOMORFISMO STRUTTURALE CON UN GRUPPO CICLICO

*Memoria (\*) di GUIDO ZAPPA (a Napoli).*

Secondo un indirizzo recentemente introdotto nella teoria dei gruppi da O. ORE, molte proprietà dei gruppi vengono ricondotte a proprietà delle *strutture* costituite da tutti i loro sottogruppi, o da tutti i sottogruppi soddisfacenti ad una data condizione (ad es. sottogruppi normali). Donde l'opportunità di studiare tali strutture. Ciò anche allo scopo di arrivare ad una nuova classificazione dei gruppi, non più rispetto all'ordinario isomorfismo, ma rispetto ad una relazione di equivalenza che raggruppi in una stessa classe non solo tutti i gruppi isomorfi ad uno dato, bensì anche altri gruppi; cosa che consentirà di arrivare a classificare più agevolmente categorie di gruppi oggi difficilmente dominabili a causa della grande varietà di tipi.

Si è pertanto introdotto il concetto di isomorfismo strutturale. Vengono detti strutturalmente isomorfi due gruppi quando è stabilita una corrispondenza biunivoca tra i sottogruppi dei due gruppi tale che all'intersezione di due sottogruppi corrisponde l'intersezione dei sottogruppi omologhi, e all'unione, l'unione. Ciò equivale a dire, come si dimostra in modo immediato, che due gruppi sono strutturalmente isomorfi se è data una corrispondenza biunivoca tra i sottogruppi dei due gruppi conservante le appartenenze.

L'isomorfismo strutturale è stato studiato da vari autori. Recentemente P. M. WHITMAN <sup>(1)</sup> ha considerato anche l'omo-

(\*) Pervenuta in Redazione il 26 settembre 1948.

(1) *Groups with a cyclic group as lattice-homomorph.* Annals of Mathematics, II ser., vol. 48 (1948) pp. 347-351.

morfismo strutturale. Dicesi omomorfismo strutturale tra due gruppi  $G$  e  $G'$  una corrispondenza univoca tra i sottogruppi di  $G$  e quelli di  $G'$ , tale che ogni sottogruppo di  $G'$  provenga da almeno un sottogruppo di  $G$ , e che all'intersezione, e all'unione, di due sottogruppi di  $G$  corrisponda l'intersezione, e rispettivamente l'unione, dei sottogruppi omologhi di  $G'$ . Il WHITMAN ha studiato i gruppi in omomorfismo strutturale con un gruppo ciclico, dimostrando che se un gruppo finito  $G$  è strutturalmente omomorfo ad un gruppo ciclico  $G'$ , esiste un sottogruppo ciclico di  $G$  strutturalmente isomorfo a  $G'$ .

Nel presente lavoro, riprendendo il problema posto da WHITMAN, arrivo, in un primo momento, alla determinazione di tutti i gruppi finiti in omomorfismo strutturale con un gruppo ciclico d'ordine  $p^\alpha$  ( $p$  primo) e, successivamente, a quella di tutti i gruppi in omomorfismo strutturale con un gruppo ciclico qualunque. Si noti, in particolare, che se  $G$  è in omomorfismo strutturale con un gruppo ciclico  $P'$  qualunque, è  $G = S \cup R$ , ove  $R$  è normale, l'ordine di  $S$  è primo con quello di  $R$ , ed  $S$  o è ciclico, o appartiene ad un altro tipo ben determinato. La costruzione di tutti i gruppi in omomorfismo strutturale con un dato gruppo ciclico risulta poi immediata.

Si osservi che, mentre due gruppi isomorfi nel senso ordinario sono anche isomorfi strutturalmente, due gruppi omomorfi nel senso ordinario non sono omomorfi strutturalmente: ad es. un gruppo non ciclico d'ordine  $p^2$  è omomorfo ad un gruppo d'ordine  $p$  nel senso ordinario, ma non lo è strutturalmente. Potrà essere pertanto opportuno considerare in seguito, anzichè questo tipo di omomorfismo strutturale, che possiamo chiamare *omomorfismo strutturale forte*, anche un altro tipo, che potrà dirsi *omomorfismo strutturale debole* e che è definito come una corrispondenza univoca tra i sottogruppi di un gruppo  $G$  e quelli di un gruppo  $G'$ , la quale conserva le appartenenze, e tale che ogni gruppo di  $G'$  proviene da almeno un gruppo di  $G$ . Nel caso dell'isomorfismo, i due tipi, come s'è visto, coincidono. L'omomorfismo ordinario rientra come caso particolare nell'omomorfismo strutturale debole.

### § 1. - Preliminari.

1. - *Dati due gruppi  $G$  e  $G'$  si dice che tra essi intercorre un omomorfismo di struttura, quando è data una legge che faccia corrispondere ad ogni sottogruppo di  $G$  uno, ed un solo sottogruppo di  $G'$ , di modo che:*

a) *Se ai sottogruppi  $A$  e  $B$  di  $G$  corrispondono i sottogruppi  $A'$  e  $B'$  di  $G'$ , all'intersezione  $A \cap B$  di  $A$  e  $B$  corrisponde l'intersezione  $A' \cap B'$  di  $A'$  e  $B'$ , e all'unione  $A \cup B$  corrisponde l'unione  $A' \cup B'$ .*

b) *Ogni sottogruppo di  $G'$  è il corrispondente di almeno un sottogruppo di  $G$ .*

Si dirà anche, in tal caso, che  $G$  è *strutturalmente omomorfo* a  $G'$ .

Dato un isomorfismo di struttura tra  $G$  e  $G'$ , il sottogruppo corrispondente di un qualsiasi sottogruppo  $A$  di  $G$  si indicherà col simbolo  $A'$ , od anche col simbolo  $f(A)$ . La a) della definizione ora data può quindi esprimersi così:

$$f(A \cap B) = f(A) \cap f(B)$$

$$f(A \cup B) = f(A) \cup f(B).$$

Facciamo ora la seguente osservazione, che giocherà in tutta la nostra nota:

*Dati due gruppi finiti  $G$  e  $G'$  in omomorfismo di struttura, e preso un qualsiasi sottogruppo  $A'$  di  $G'$ , tra i sottogruppi di  $G$  che hanno per corrispondente  $A'$  ne esistono due, che rappresenteremo con le notazioni  $f^{-1}(A')$ ,  $f_{-1}(A')$ , tali che condizione necessaria e sufficiente perchè ad un sottogruppo  $A$  di  $G$  corrisponda  $A'$  è che  $A$  stia in  $f^{-1}(A')$  e contenga  $f_{-1}(A')$ .*

Infatti, essendo  $G$  finito, i sottogruppi di  $G$  che hanno per corrispondente  $A'$  sono in numero finito. In base alla a), alla loro intersezione deve corrispondere  $A' \cap A' \cap \dots \cap A'$ , cioè  $A'$  stesso, e, analogamente, alla loro unione corrisponde ancora  $A'$ . La loro intersezione sia  $f_{-1}(A')$ , e la loro unione  $f^{-1}(A')$ . Ogni sottogruppo di  $G$  che ha per corrispondente  $A'$  è eviden-

temente in  $f^{-1}(A)$  e contiene  $f_{-1}(A)$ . Viceversa, un sottogruppo contenuto in  $f^{-1}(A)$  e contenente  $f_{-1}(A)$  ha per omologo un sottogruppo contenuto in  $A'$  e contenente  $A'$ , vale a dire  $A'$  stesso.

## § 2. - Gruppi in omomorfismo strutturale con un gruppo ciclico d'ordine $p^\alpha$ .

2. - Sia ora  $G$  un gruppo finito in omomorfismo di struttura con un gruppo  $P'$  ciclico d'ordine  $p^\alpha$ , ove  $p$  è un numero primo. Sia  $\lambda$  un generatore di  $P'$ , e si ponga  $P'_1 = \{\lambda^p\}$ ,  $P'_2 = \{\lambda^{p^2}\}$ , ...,  $P'_{\alpha-1} = \{\lambda^{p^{\alpha-1}}\}$ ,  $P'_\alpha = \{\lambda^{p^\alpha}\} \equiv E'$ , ove con  $E'$  si è indicato il sottogruppo identico di  $P'$ .

Dimostriamo anzitutto che

$f_{-1}(P')$  è un gruppo ciclico d'ordine  $q^\beta$ , ove  $q$  è un numero primo.

Se infatti ciò non fosse,  $f_{-1}(P')$  potrebbe ottenersi come unione di due suoi sottogruppi propri  $A$  e  $B$ . Ma allora si avrebbe anche  $A' \cup B' = P'$ , il che non può essere, perchè  $A'$ , a causa definizione di  $f_{-1}(P')$ , non può coincidere con  $P'$ , e deve quindi essere un suo sottogruppo proprio, vale a dire contenuto in  $P'_1$ ; altrettanto avverrebbe di  $B'$ , e anche di  $A' \cup B'$ ; pertanto  $A' \cup B' = P'$  sarebbe in  $P'_1$ , il che è assurdo. Da ciò segue l'asserto.

Poniamo  $P = f_{-1}(P')$ , e chiamiamo  $l$  un generatore di  $P$ .

In modo analogo si dimostra che  $f_{-1}(P'_1)$  è ciclico ed ha per ordine la potenza di un numero primo; ma poichè esso deve stare in  $P$ , si avrà che  $f_{-1}(P'_1) = P_1$ , ove è  $P_1 = \{l^{q^{r_1}}\}$ , essendo  $r_1 \geq 1$ . Analogamente,  $f_{-1}(P'_2) = P_2 = \{l^{q^{r_2}}\}$ , con  $r_2 > r_1, \dots, f_{-1}(P'_i) = P_i = \{l^{q^{r_i}}\}$  con  $r_i > r_{i-1}, \dots$ . Ne segue che deve essere  $\beta \geq \alpha$ .

Sia ora  $H = f^{-1}(E')$ . Evidentemente  $H$  non contiene  $P_{\alpha-1}$ , perchè  $f(P_{\alpha-1}) = P'_{\alpha-1} \neq E'$ . Invece, preso un elemento  $g$  di  $G$ , non contenuto in  $H$ , si ha che  $\{g\}$  non è in  $H$  è quindi ha per omologo in  $P'$  un sottogruppo non identico, vale a dire

un sottogruppo  $P'_i$ , con  $i \leq \alpha - 1$ . Ne segue che tale omologo contiene  $P'_{\alpha-1}$ , e quindi  $\{g\}$  contiene  $P_{\alpha-1}$ . Pertanto  $g$  ha tra le sue potenze l'elemento  $l^{q^r\alpha-1}$ , generatore di  $P_{\alpha-1}$ .

Concludendo:

*Ogni elemento  $g$  di  $G$ , non contenuto in  $H = f^{-1}(E')$ , ha tra le sue potenze l'elemento  $l^{q^r\alpha-1}$ , e viceversa.*

Poniamo, per brevità,  $l^{q^r\alpha-1} = l_{\alpha-1}$ . Ogni elemento di  $H$ , evidentemente, trasforma  $H$  in sè. Ma poichè  $H$  contiene tutti gli elementi che non hanno per potenza  $l_{\alpha-1}$ , ed essi soli, si ha che ogni elemento  $g$  fuori di  $H$ , avendo  $l_{\alpha-1}$  tra le sue potenze, trasforma ogni elemento che ha  $l_{\alpha-1}$  tra le sue potenze in un elemento godente della stessa proprietà, e quindi trasforma ogni elemento che non ha  $l_{\alpha-1}$  tra le sue potenze in un elemento godente della stessa proprietà, vale a dire trasforma un elemento di  $H$  in un elemento di  $H$ . Pertanto:

*Il sottogruppo  $H = f^{-1}(E')$  è normale in  $G$ .*

In modo analogo si dimostra che  $f^{-1}(P'_i)$  è costituito da tutti e soli gli elementi, che non hanno per potenza  $l^{q^ri-1}$ . Posto  $l^{q^ri-1} = l_{i-1}$ , e  $f^{-1}(P'_i) = (H_i)$ , si ha quindi:

*Ogni elemento  $g$  di  $G$ , non contenuto in  $H_i = f^{-1}(P'_i)$  ha tra le sue potenze l'elemento  $l_{i-1}$ , e viceversa.*

Si ha anche, analogamente al caso precedente:

*Il sottogruppo  $H_i = f^{-1}(P'_i)$  è normale in  $G$ .*

### 3. - Mostriamo ora che

*Ogni elemento di  $H_1$  (quindi anche di  $H_2, \dots, H$ ) è permutabile con  $l$ .*

Detto infatti  $h_1$  un elemento di  $H_1$ , si ha che l'elemento  $h_1 \cdot l$  non è in  $P$ , perchè  $h_1$  non vi è, ed  $l$  vi è. Pertanto (n. 2),  $h_1 \cdot l$  deve avere per potenza  $l$ , e quindi deve essere permutabile con  $l$ . Ma allora anche  $h_1 = (h_1 \cdot l) \cdot l^{-1}$  è permutabile con  $l$ .

D'altra parte anche ogni elemento fuori di  $H_1$ , avendo tra le sue potenze  $l$ , è permutabile con  $l$ , e pertanto:

*Il sottogruppo  $P$  appartiene al centro di  $G$ .*

È evidente che  $l_{i-1}$  non appartiene ad  $H_i$ , mentre  $l_{i-1}^q$  vi appartiene. Posto  $Q_i = \{l_{i-1}^q\}$  abbiamo quindi

$$H_i \cap P = Q_i$$

e analogamente

$$H \cap P = Q_{\alpha-1}.$$

Mostriamo ora che:

*Il sottogruppo  $Q_i$  è un sottogruppo di SYLOW di  $H_i$  (e analogamente,  $Q_{\alpha-1}$  è un sottogruppo di SYLOW di  $H$ ).*

Procediamo per assurdo. Se  $Q_i$  non è sottogruppo di SYLOW di  $H_i$ , si dovrà trovare un sottogruppo  $S$  di SYLOW di  $H_i$ , contenente  $Q_i$ . Sia  $h_i$  un elemento di  $S$ , non contenuto in  $Q_i$ . L'elemento  $l_{i-1} \cdot h_i$  non è contenuto in  $H_i$ , perchè  $l_{i-1}$  non lo è, mentre  $h_i$  lo è. Pertanto (n. 2) deve esistere un  $x$  tale che  $(l_{i-1} \cdot h_i)^x = l_{i-1}$ . Ma  $l_{i-1}$ , essendo in  $P$ , è nel centro di  $G$ , quindi si ha  $(l_{i-1} \cdot h_i)^x = l_{i-1}^x h_i^x$ . Dovrà pertanto aversi

$$l_{i-1}^x h_i^x = l_{i-1}$$

cioè

$$(1) \quad h_i^x = l_{i-1}^{1-x}.$$

Si ha quindi che  $h_i^x$  è in  $P_{i-1}$ . Ma poichè  $h_i$  non è, per ipotesi in  $Q_i$ , esso non è nemmeno in  $P_{i-1}$ , essendo, come abbiamo visto,  $H_i \cap P_{i-1} = H_i \cap P = Q_i$ . Trovandosi invece  $h_i^x$  in  $P_{i-1}$ , ed essendo l'ordine di  $h_i$  una potenza di  $q$ , deve essere  $x$  multiplo di  $q$ . Ma allora  $1 - x$  è primo con  $q$ , quindi  $l_{i-1}$  è potenza di  $l_{i-1}^{1-x}$ , e di conseguenza  $l_{i-1}$  è potenza di  $h_i$  (1). Ma ciò è assurdo, perchè  $h_i$  è in  $H_i$ , il quale è formato da tutti e soli gli elementi, che non hanno  $l_{i-1}$  tra le loro potenze.

Resta così dimostrato che  $Q_i$  è sottogruppo di SYLOW di  $H_i$ .

Il sottogruppo  $Q_i$  è pertanto un sottogruppo di SYLOW di  $H_i$ , ed appartiene al centro di  $H_i$  stesso. Per un noto teorema di BURNSIDE (\*)  $H_i$  contiene allora un sottogruppo caratteristico

(2) Cfr., ad es.: G. SCORZA, *Gruppi astratti*, Roma, ed. Cremonese 1944, pagg. 226.

$R$ , il cui indice in  $H_i$  eguaglia l'ordine di  $Q_i$ . Esso contiene tutti e soli gli elementi di  $H_i$  il cui ordine è primo con  $q$ . Essendo  $H_i$  normale in  $G$ , si ha che anche  $R$  è normale in  $G$ . È appena il caso di notare che qualunque valore di  $i$  si consideri, si ottiene sempre lo stesso sottogruppo  $R$ , il quale giace in tutti i sottogruppi  $H_i$ . Infatti il sottogruppo  $R$  ottenuto a partire da un dato  $H_i$  sta in  $H$ , perchè nessun suo elemento ha per potenza  $l_{\alpha-1}$  (n. 2), e quindi coincide col sottogruppo  $R$  che si ottiene a partire da  $H$ . Concludendo.

*Gli elementi di uno e quindi di tutti i sottogruppi  $H_i$ , aventi un ordine primo con  $q$ , formano un sottogruppo normale  $R$  di  $G$ .*

Essendo tanto  $Q_\alpha$  che  $R$  normali in  $H$ , ed essendo essi privi di elementi non identici in comune, si ha  $H = R \times Q_\alpha$ . Ogni elemento di  $H$  non contenuto in  $R$  è dato dal prodotto di un elemento  $\rho$  di  $R$  per un elemento  $\xi$  non identico di  $Q_\alpha$ . Poichè  $\rho$  e  $\xi$  hanno ordini primi tra loro, si ha che  $\rho\xi$  ha per potenza  $\xi$ ; e poichè ogni elemento non identico di  $Q_\alpha$ , quindi anche  $\xi$ , ha per potenza, se  $Q_\alpha$  non è identico, l'elemento  $l^{q\beta-1}$ , otteniamo che, o  $Q_\alpha$  è identico, e quindi  $R = H$ , oppure ogni elemento di  $H$  non contenuto in  $R$  ha per potenza  $l^{q\beta-1}$ . In ambedue i casi possiamo affermare che ogni  $R$  contiene tutti e soli gli elementi di  $H$  non aventi tra le loro potenze  $l^{q\beta-1}$ . Poichè poi ogni elemento di  $G$  non contenuto in  $H$  ha per potenza  $l_{\alpha-1}$ , quindi anche  $l^{q\beta-1}$  che è potenza di  $l_{\alpha-1}$ , si ottiene che:

*Il sottogruppo  $R$  è costituito da tutti e soli gli elementi di  $G$  non aventi  $l^{q\beta-1}$  tra le loro potenze.*

4. - Consideriamo ora l'omomorfismo tra  $G$  e  $\frac{G}{R} \equiv \bar{G}$ .

All'elemento  $l^{q\beta-1}$ , che chiameremo, per brevità,  $l_{\beta-1}$ , corrisponde in  $\bar{G}$  un elemento  $\bar{l}_{\beta-1}$ ; e ogni elemento non identico di  $\bar{G}$ , proveniendo da un elemento di  $G$  non contenuto in  $R$ , deve avere tra le sue potenze  $\bar{l}_{\beta-1}$ . Occorre quindi, a tal punto, studiare la struttura di un gruppo  $\bar{G}$  tale che ogni suo elemento non identico abbia tra le sue potenze un elemento fisso  $\bar{l}_{\beta-1}$ .

Tutti i sottogruppi non identici di  $\bar{G}$  contengono  $\bar{l}_{p-1}$ , quindi  $\bar{G}$  è necessariamente un  $p$  — gruppo, altrimenti due sottogruppi di SYLOW di  $G$  d'ordine diverso non potrebbero contenere ambedue l'elemento  $\bar{l}_{p-1}$ , poichè non hanno elementi non identici in comune.

Se  $\bar{G}$  è abeliano, esso è certamente ciclico, perchè in un gruppo abeliano che non sia ciclico, si possono sempre trovare due elementi (ad es. due diversi generatori di una base) non aventi potenze in comune, oltre l'identità.

Supponiamo ora, invece,  $\bar{G}$  non abeliano. Considerando una successione decrescente di sottogruppi non abeliani di  $\bar{G}$ , ciascuno di indice primo nel precedente, si arriva ad un sottogruppo  $\bar{S}$  non abeliano, tale che ogni suo sottogruppo proprio sia abeliano. Sia  $\bar{T}$  un sottogruppo di indice primo di  $\bar{S}$ . Esso, essendo abeliano, e dovendo ogni suo elemento contenere  $\bar{l}_{p-1}$ , è ciclico. Ogni sottogruppo di  $\bar{T}$  è allora caratteristico in  $\bar{T}$ ; e poichè, essendo  $\bar{S}$  un  $p$  — gruppo,  $\bar{T}$  è normale in  $\bar{S}$ , si ha che ogni sottogruppo di  $\bar{T}$  è normale in  $\bar{S}$ . Essendo poi  $\bar{T}$  un qualunque sottogruppo d'indice primo in  $\bar{S}$  si ha, al variare di  $\bar{T}$ , che ogni sottogruppo di  $\bar{S}$  è normale in  $\bar{S}$ . Ma allora  $\bar{S}$ , essendo, per ipotesi, non abeliano, è hamiltoniano, ha per ordine una potenza di 2, e contiene il gruppo dei quaternioni. Pertanto:

*Se l'ordine di  $\bar{G}$  è dispari,  $\bar{G}$  è ciclico (ed ha per ordine la potenza di un numero primo); se invece l'ordine di  $\bar{G}$  è pari,  $\bar{G}$  o è ciclico d'ordine  $2^s$  ( $s$  intero), o è un gruppo d'ordine  $2^s$  contenente il gruppo dei quaternioni.*

Approfondiamo il caso in cui  $\bar{G}$  non è ciclico. Se  $\bar{G}$  ha ordine 8, esso è necessariamente il gruppo dei quaternioni. Se  $\bar{G}$  ha ordine 16, dall'esame dei tipi, tutti noti, dei gruppi non abeliani d'ordine 16, si vede che affinchè  $\bar{G}$  goda della proprietà voluta, deve potersi generare mediante due elementi  $g_1$  e  $g_2$ , legati dalle relazioni (\*)

$$g_1^2 = 1 \quad g_2^2 = g_1^4 \quad g_2^{-1} g_1 g_2 = g_1^{-1}.$$

(\*) Cfr., ad es.: W. BURNSIDE, Theory of groups, Cambridge, 1897, pp. 88-89 (n. 74).

Dimostreremo ora che, se  $G$  ha ordine  $2^s$ , esso deve potersi generare mediante due elementi  $g_1, g_2$  legati dalle relazioni

$$(2) \quad g_1^{2^{s-1}} = 1, \quad g_2^2 = g_1^{2^{s-2}}, \quad g_2^{-1} g_1 g_2 = g_1^{-1}.$$

Poichè ciò è vero per  $s = 4$ , dimostreremo la cosa per induzione rispetto ad  $s$ . Notiamo anzitutto che in un gruppo definito dalle (2) tutti gli elementi non contenuti in  $\{g_1\}$  hanno il quadrato eguale a  $g_1^{2^{s-2}}$ , e quindi periodo 4. Infatti, un tale elemento può mettersi sotto la forma  $g_1^x g_2$ , e si ha

$$(g_1^x g_2)^2 = g_1^x g_2 g_1^x g_2 = g_1^x g_2^2 g_2^{-1} g_1^x g_2 = g_1^x g_2^2 g_1^{-x} = g_1^{2^{s-2}}.$$

Pertanto  $\{g_1\}$  è un sottogruppo caratteristico del gruppo.

Sia ora un gruppo  $\overline{G}$  d'ordine  $2^s$ , godente della proprietà che tutti i suoi elementi hanno in comune una potenza non identica, e tale che, per ipotesi, ogni suo sottogruppo o è ciclico, o è del tipo definito dalle (2). Vogliamo provare che anche  $\overline{G}$ , se non è ciclico, è di tal tipo.

Facciamo anzitutto vedere che  $\overline{G}$  ha un sottogruppo ciclico d'indice 2. Sia  $\overline{G}_1$  un sottogruppo d'indice 2 di  $\overline{G}$ . Se esso è ciclico, la cosa è già provata. Supponiamo che sia, invece, del tipo definito dalle (2). Allora  $\overline{G}_1$  contiene, per quanto si è osservato or ora, un sottogruppo  $\overline{S}$  ciclico d'ordine  $2^{s-2}$ , caratteristico in  $\overline{G}_1$  e normale in  $\overline{G}$ , perchè, come è ben noto,  $\overline{G}_1$  è normale in  $\overline{G}$ . Se esiste in  $\overline{G}$ , un elemento  $\gamma$  che abbia periodo relativo 4 rispetto a  $\overline{S}$ , si ha che  $\{\gamma^2, \overline{S}\}$  ha ordine  $2^{s-1}$ , quindi, o è ciclico, e la cosa è dimostrata, o è del tipo definito dalle (2). In tal caso, detto  $\sigma$  un generatore di  $\overline{S}$ , deve aversi  $\gamma^{-2} \sigma \gamma^2 = \sigma^{-1}$ . Poichè  $\overline{S}$  è normale in  $\overline{G}$ , anche  $\gamma$  deve mutare  $\sigma$  in una sua potenza: sia ad es.  $\gamma^{-1} \sigma \gamma = \sigma^x$ . Di qui segue  $\gamma^{-2} \sigma \gamma^2 = \sigma^{x^2}$ .

Essendo, d'altra parte,  $\gamma^{-2} \sigma \gamma^2 = \sigma^{-1}$ , si ottiene  $\sigma^{x^2} = \sigma^{-1}$ , cioè  $x^2 \equiv -1 \pmod{2^{s-2}}$ , congruenza che non può esser soddisfatta per alcun valore di  $x$ . Pertanto, si giunge ad un assurdo, e di conseguenza, se esiste un elemento  $\gamma$  di periodo relativo 4 rispetto a  $\overline{S}$ , necessariamente  $\overline{G}$  ha un sottogruppo ciclico d'in-

dice 2. Se poi non esiste un tale elemento  $\gamma$ , siano  $\delta_1$  e  $\delta_2$  due elementi di  $\overline{G}$  aventi periodo relativo 2 rispetto ad  $\overline{S}$ , ed appartenenti a diversi laterali di  $\overline{S}$ . Se  $\delta_1$ , o  $\delta_2$ , è permutabile con  $\sigma$ , si ha che  $\{\delta_1, \overline{S}\}$  o  $\{\delta_2, \overline{S}\}$ , dovendo essere abeliano, è ciclico, e il nostro asserto è dimostrato.

Se invece  $\{\delta_1, \overline{S}\}$  e  $\{\delta_2, \overline{S}\}$  non sono ciclici, dovrà aversi  $\delta_1^{-1} \sigma \delta_1 = \sigma^{-1}$ , e  $\delta_2^{-1} \sigma \delta_2 = \sigma^{-1}$ , perchè tanto  $\{\delta_1, \overline{S}\}$  che  $\{\delta_2, \overline{S}\}$  sono del tipo definito dalle (2). Ma allora  $(\delta_1 \delta_2)^{-1} \sigma (\delta_1 \delta_2) = \sigma$ , onde il sottogruppo  $\{\delta_1 \delta_2, \overline{S}\}$  è ciclico. In ogni caso resta quindi provato che  $\overline{G}$  ha un sottogruppo ciclico  $\overline{G}_1$  di indice 2.

Sia ora  $g_1$  un generatore di  $\overline{G}_1$ , e sia  $g_2$  un elemento di  $\overline{G}$  non contenuto in  $\overline{G}_1$ . Se  $g_2$  è permutabile con  $g_1$ ,  $\overline{G}$  è abeliano, quindi ciclico. In caso contrario, si avrà

$$g_2^{-1} g_1 g_2 = g_1^x$$

con  $x$  dispari, da cui segue

$$g_2^{-2} g_1 g_2^2 = g_1^{x^2}.$$

Ma  $g_2^2$  è in  $\overline{G}_1$ , quindi si ha anche

$$g_2^{-2} g_1 g_2^2 = g_1$$

ossia  $g_1^{x^2} = g_1$ , vale a dire

$$x^2 \equiv 1 \pmod{2^{s-1}}$$

da cui segue

$$(x+1)(x-1) \equiv 0 \pmod{2^{s-1}}.$$

Dei due numeri  $x+1$ ,  $x-1$ , uno non è divisibile per 4. Quindi si avrà

$$x \equiv 1 \pmod{2^{s-2}}$$

oppure

$$x \equiv -1 \pmod{2^{s-2}}.$$

Si otterrà quindi, per  $x$ , uno dei quattro valori  $1, 2^{s-2} - 1,$

$2^{s-2} + 1, -1$ . Va anzitutto scartato il valore  $x = 1$ , per cui  $g_2$  risulta permutabile con  $g_1$ .

Se è  $x = 2^{s-2} - 1$ , si avrà, qualunque sia  $y$ ,

$$g_2^{-1} g_1^{2y} g_2 = g_1^{y \cdot 2^{s-1} - 2y} = g_1^{-2y}$$

e si avrà  $g_1^{2y} = g_1^{-2y}$  se e solo se è  $y = 2^{s-2}$ . Poichè d'altra parte  $g_1$  e  $g_2$  devono avere una potenza in comune, e tale potenza deve essere permutabile con  $g_2$ , si ha che deve essere

$$g_2^2 = g_1^{2^{s-2}}.$$

Ma allora si ha

$$(g_2 g_1)^2 = g_2 g_1 g_2 g_1 = g_2^2 g_1^{2^{s-2}-1} g_1 = g_2^2 g_1^{2^{s-2}} = g_1^{2^{s-1}} = 1$$

contro l'ipotesi che  $g_2 g_1$  abbia una potenza a comune con  $g_1$ . Il caso  $x = 2^{s-2} - 1$  resta quindi scartato.

Sia ora  $x = 2^{s-2} + 1$ . È allora

$$g_2^{-1} g_1^2 g_2 = g_1^{2^{s-1} + 2} = g_1^2.$$

Pertanto  $\{g_1^2, g_2\}$  è abeliano, quindi ciclico, e quindi potrà trovarsi un elemento, che potremo supporre essere lo stesso  $g_2$ , per cui è

$$g_2^2 = g_1^2, \quad g_2^{-1} g_1 g_2 = g_1^{2^{s-2} + 1}.$$

Ma allora si ha

$$\begin{aligned} (g_2 g_1^{2^{s-3}-1})^2 &= g_2 g_1^{2^{s-3}-1} g_2 g_1^{2^{s-3}-1} = g_2 g_1^{-1} g_2 g_1^{-1} g_1^{2^{s-3}} = \\ &= g_2^2 g_1^{2^{s-3}-1} g_1^{-1} g_1^{2^{s-2}} = g_1^2 g_1^{2^{s-2}} g_1^{-2} g_1^{2^{s-2}} = 1 \end{aligned}$$

contro l'ipotesi che ogni elemento di  $\overline{G}$  abbia una potenza a comune con  $g_1$ . Anche il caso  $x = 2^{s-2} - 1$  va quindi scartato. Resta il caso  $x = -1$ , nel quale  $\overline{G}$  può generarsi mediante gli elementi  $g_1$  e  $g_2$  legati dalle relazioni

$$g_1^{2^{s-1}} = 1, \quad g_2^2 = g_1^{2^{s-2}}, \quad g_2^{-1} g_1 g_2 = g_1^{-1}$$

come avevamo affermato. Anche il gruppo dei quaternioni rientra in questo tipo.

Giungiamo pertanto alla seguente conclusione :

*Un gruppo  $\overline{G}$  in cui tutti gli elementi non identici hanno una potenza comune, diversa dall'identità, o è ciclico d'ordine  $p^s$  ( $p$  primo) o ha ordine  $2s$  ( $s \geq 3$ ) e può generarsi mediante due elementi  $g_1, g_2$ , legati dalle relazioni :*

$$(2) \quad g_1^{s-1} = 1, \quad g_2^s = g_1^{s-2}, \quad g_2^{-1} g_1 g_2 = g_1^{-1}.$$

Viceversa, ogni gruppo ciclico d'ordine  $p^s$  ( $p$  primo) o del tipo dato dalle (2) è tale che tutti gli elementi hanno una potenza diversa dall'identità in comune. Infatti, se il gruppo è ciclico, ciò è evidente; se invece è del tipo dato dalle (2) si ha che ogni elemento non contenuto in  $\{g_1\}$  è della forma  $g_1^x g_2$ , e si ha  $(g_1^x g_2)^s = g_1^x g_2 g_1^x g_2 = g_1^x g_1^{-x} g_2^s = g_2^s = g_1^{s-2}$ . Poichè anche tutti gli elementi non identici di  $\{g_1\}$  hanno per potenza  $g_1^{s-2}$ , la cosa resta provata (\*).

5. - Torniamo ora al gruppo  $G$  in omomorfismo di struttura col gruppo  $P'$ . Vedemmo, all'inizio del n. 4, che tutti gli elementi di  $\overline{G} = \frac{G}{R}$  hanno per potenza l'elemento  $\bar{l}_{\beta-1}$  omologo di  $l_{\beta-1}$ . Pertanto, in base a quanto abbiamo ora dimostrato,  $\frac{G}{R}$  è un gruppo ciclico d'ordine la potenza di un numero primo, oppure un gruppo d'ordine una potenza di 2 e definito dalle relazioni (2). Poichè  $G$  contiene l'elemento  $l$  che ha ordine  $q^\beta$  e non è in  $R$ , l'ordine di  $\frac{G}{R}$  deve essere  $q^s$ , con  $s \geq \beta$ . Il gruppo  $G$  contiene sottogruppi di SYLOW isomorfi a  $\frac{G}{R}$ , uno dei quali,  $S$ , contiene  $l$ . Ricordando che  $l$  appartiene al centro di  $G$  (n. 3) e notando che  $S \cup R = G$ , si ha il teorema :

(\*) [Aggiunto in bozze. Mi sono accorto, dopo presentato il lavoro, che il risultato di questo n. 4 era da tempo noto (Op. cit. in (3), II ed., 1911, pag. 182). Ho conservato però egualmente la dimostrazione per comodità del lettore].

Se  $G$  è un gruppo finito in omomorfismo di struttura con un gruppo ciclico d'ordine  $p^\alpha$  ( $p$  primo), si ha  $G = S \cup R$ , ove  $R$  è un sottogruppo normale, mentre  $S$  è un sottogruppo di Sylow di  $G$  d'ordine  $q^s$  ( $q$  primo,  $s \geq \alpha$ ). Inoltre  $S$  è ciclico, oppure, se  $\alpha = 1$ ,  $q = 2$ , è un gruppo generabile mediante due elementi  $g_1$  e  $g_2$ , legati dalle relazioni

$$(2) \quad g_1^{s-1} = 1, \quad g_2^2 = g_1^{s-2}, \quad g_2^{-1} g_1 g_2 = g_1^{-1}.$$

Infine l'ordine di  $R$  è primo con  $q$  (onde  $R \cap S = E$ ), e se  $S$  è ciclico e generato dall'elemento  $b$ , si ha  $b^{\alpha s - \beta} = l$  permutabile con ogni elemento di  $R$  ( $\beta \geq \alpha$ ), mentre se  $S$  è del tipo dato dalle (2),  $g_1^{s-2} = l$  è permutabile con ogni elemento di  $R$ .

6. - Ci proponiamo ora di invertire questo teorema. Si abbia, in primo luogo, un gruppo  $G = S \cup R$ , ove  $S$  è ciclico d'ordine  $q^s$ ,  $R$  è un sottogruppo normale di ordine primo con  $q$ , e, detto  $b$  un generatore di  $S$ ,  $b^{\alpha s - \beta}$  è permutabile con ogni elemento di  $R$ . Vogliamo far vedere che  $G$  può porsi in omomorfismo strutturale con un gruppo  $P'$  ciclico d'ordine  $p^\alpha$  con  $p$  primo e  $\alpha \leq \beta$ .

Essendo  $\beta \geq \alpha$ , possiamo determinare  $\alpha - 1$  interi positivi  $r_1 < r_2 < \dots < r_{\alpha-1} < \beta$ , e poniamo  $P_i = \{l^{r_i}\}$  ( $i=1, \dots, \alpha-1$ ),  $P = \{l\}$ , ove si è posto  $l = b^{\alpha s - \beta}$ . Posto poi, per brevità,  $l_i = l^{r_i}$ , si ponga anche  $Q_i = \{l_{i-1}^q\}$ , ( $i=2, \dots, \alpha$ ) e  $Q_1 = \{l^q\}$ . Infine si introducano i gruppi  $H_i = Q_i \times R$ , ( $i=1, \dots, \alpha$ ) e si scriva, più semplicemente  $H_\alpha = H$ .

Detto  $\lambda$  un generatore di  $P'$ , si ponga  $P'_i = \{\lambda^{p^i}\}$  ( $i=1, \dots, \alpha$ ). Si stabilisca ora una corrispondenza univoca  $f$  tra i sottogruppi di  $G$  e quelli di  $P'$  nel modo seguente: se  $A$  è un sottogruppo di  $G$  che non contiene  $P_{\alpha-1}$ , sia  $f(A) = P'_\alpha = E'$ ; se  $A$  contiene  $P_i$ , ma non  $P_{i-1}$  ( $i=2, \dots, \alpha-1$ ), sia  $f(A) = P'_i$ ; se  $A$  contiene  $P_1$ , ma non  $P$ , sia  $f(A) = P'_1$ ; se infine  $A$  contiene  $P$ , sia  $f(A) = P'$ . Evidentemente, ad ogni sottogruppo di  $G$

corrisponde, per effetto di  $f$ , uno ed uno solo sottogruppo di  $P'$ , mentre ogni sottogruppo di  $P'$  proviene da almeno un sottogruppo di  $G$ .

Vogliamo ora far vedere che  $f$  è un omomorfismo di struttura. A tal fine basta dimostrare che se  $A$  e  $B$  sono due sottogruppi di  $G$ , e  $A'$  e  $B'$  i loro corrispondenti in  $P'$ , ad  $A \cup B$  corrisponde  $A' \cup B'$ , e ad  $A \cap B$  corrisponde  $A' \cap B'$ .

Anzitutto osserviamo che è, per definizione,  $f_{-1}(P'_i) = P_i$  ( $i = 1, \dots, \alpha - 1$ ),  $f_{-1}(E') = E$ ,  $f_{-1}(P') = P$ . Ora mostreremo che *tutti e soli i sottogruppi di  $G$  che non contengono  $P_{i-1}$  sono in  $H_i$*  ( $i = 1, \dots, \alpha$ , ove si è posto per comodità,  $P_0 = P$ ).

Sia infatti  $A$  un sottogruppo di  $G$  non contenente  $P_{i-1}$ , e sia  $q^\alpha \cdot m$ , con  $m$  primo con  $q$ , l'ordine di  $A$ . Essendo  $R$  normale in  $G$ , e di indice  $q^\alpha$ , tutti i sottogruppi di SYLOW di  $G$  di ordine primo con  $q$  sono in  $R$ . Pertanto anche i sottogruppi di SYLOW di  $A$  d'ordine primo con  $q$  sono in  $R$ . La loro unione è un sottogruppo  $M$  d'ordine  $m$  contenuto ancora in  $R$ , e si ha anzi, più precisamente,  $A \cap R = M$ .

Il sottogruppo  $P$ , essendo nel centralizzante di  $H$  e normale in  $S$ , appartiene a tutti i sottogruppi di SYLOW di  $G$  d'ordine  $q^\alpha$ , perchè è normale in  $G$ . E poichè  $S$ , e così i suoi coniugati, sono ciclici, ogni elemento di  $S$ , o di un suo coniugato, che non sia in  $P$ , ha per potenza  $l$ . Poichè  $A$  non contiene  $P_{i-1}$ , esso non contiene  $l$ . Pertanto  $A$  non contiene alcun elemento di  $S$ , o di un suo coniugato, che non sia in  $P$ , e quindi  $A$  ha un solo sottogruppo di SYLOW il cui ordine è potenza di  $q$ , e tale sottogruppo, che diremo  $T$ , non contiene  $P_{i-1}$ , e di conseguenza è in  $Q_i$ . Il sottogruppo  $A$  è allora dato dal prodotto diretto  $T \times M$ , e poichè  $M$  è in  $R$ , e quindi in  $H_i$ , e  $T$  è in  $Q_i$ , e quindi in  $H_i$ , anche  $A$  è in  $H_i$ . Viceversa, un gruppo contenuto in  $H_i$  non contiene  $P_{i-1}$ , perchè nemmeno  $H_i$  lo contiene.

Ne segue che è  $f^{-1}(P'_i) = H_i$  ( $i = 1, \dots, \alpha$ ). Si ha poi, evidentemente,  $f^{-1}(P') = G$ .

Siano ora  $A$  e  $B$  due sottogruppi di  $G$ , e si abbia  $f(A) = P'_i$ ,  $f(B) = P'_j$ , con  $i \geq j$ . Per il modo in cui è stato definito  $f$ , si ha che  $A$  contiene  $P_i$ , ma non  $P_{i-1}$ , e che  $B$  contiene  $P_j$ , ma non  $P_{j-1}$ . Poichè è  $i \geq j$ ,  $P_j$  contiene  $P_i$ , e quindi l'intersezione di  $A$  e  $B$  contiene  $P_i$ , poichè  $A$  e  $B$  lo conten-

gono, ma non contiene  $P_{i-1}$ , perchè  $A$  non lo contiene. Segue che  $f(A \cap B) = P'_i$ , e poichè è  $P'_i \cap P'_j = P'_i$ , perchè  $P'_j$ , contiene  $P'_i$ , si ha che  $f(A \cap B) = f(A) \cap f(B)$ .

Poichè  $A$  contiene  $P_i$ , ma non  $P_{i-1}$ , si ha che  $A$  sta in  $H_i$ , ma non sta in  $H_{i+1}$ . Analogamente  $B$  sta in  $H_j$ , ma non in  $H_{j+1}$ . Poichè è  $i \geq j$ , si ha che  $H_j$  contiene  $H_i$ , e pertanto  $A \cup B$  è in  $H_j$ , poichè  $A$  e  $B$  vi sono, mentre non è in  $H_{j+1}$  perchè  $B$  non vi è. Ma allora  $A \cup B$  non contiene  $P_{i-1}$ , mentre contiene  $P_i$ . E da ciò segue che ad  $A \cup B$  corrisponde in  $P'$  il sottogruppo  $P'_j$ , che è il congiungente di  $P'_i$  e  $P'_j$ , e pertanto  $f(A \cup B) = f(A) \cup f(B)$ . Il ragionamento sussiste, con minime varianti di simboli, anche se è  $i = \alpha$ , o è  $j = 0$ .

Se  $S$  è generato da due elementi  $g_1$  e  $g_2$  legati dalle (2), si ragiona allo stesso modo. Si porrà, in tal caso,  $g_1^{s-2} = l$ , onde  $Q_1 \equiv P_2 \equiv E$ ,  $H_1 \equiv H \equiv R$ . Anche in tal caso ogni elemento di  $S$ , o di un suo coniugato, che non sia in  $P$ , ha per potenza  $l$ . Tolti questi punti, tutto il ragionamento è identico. Il teorema del n. prec. è così invertito, e possiamo concludere:

*Condizione necessaria e sufficiente perchè un gruppo finito  $G$  sia in omomorfismo di struttura con un gruppo ciclico  $P'$  d'ordine  $p^\alpha$  ( $p$  primo) è che sia  $G = S \cup R$ , ove  $R$  è un sottogruppo normale, ed  $S$  è un sottogruppo d'ordine  $q^s$  ( $s \geq \alpha$ ,  $q$  numero primo, che non divida l'ordine di  $R$ ), appartenente ad uno dei tipi seguenti:*

1) Ciclico, tale che se  $b$  è un suo generatore,  $b^{\alpha-\beta}$  ( $\beta \geq \alpha$ ) è permutabile con ogni elemento di  $R$ .

2) Se è  $\alpha = 1$ ,  $q = 2$ , generabile mediante due elementi  $g_1, g_2$ , legati dalle relazioni

$$g_1^{s-1} = 1, \quad g_1^{s-2} = g_2^2, \quad g_2^{-1} g_1 g_2 = g_1^{-1}$$

con  $g_1^{s-2}$  permutabile con ogni elemento di  $R$ .

Si noti in particolare che un gruppo ciclico d'ordine  $q^s \cdot k$ , con  $q$  primo,  $s \geq \alpha$ ,  $k$  primo con  $q$ , è in omomorfismo di struttura con un gruppo ciclico d'ordine  $p^\alpha$  ( $p$  primo).

§ 3. – **Gruppi in omomorfismo strutturale con un gruppo ciclico qualunque.**

7. – Si abbia ora un gruppo  $G$  in omomorfismo di struttura con un gruppo ciclico  $P'$  d'ordine  $m$  qualunque.

Sia  $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , con  $p_1, \dots, p_k$  numeri primi distinti. Il gruppo  $P'$  sarà dato dal prodotto diretto  $P'_1 \times P'_2 \times \dots \times P'_k$  ove  $P'_i$  ( $i = 1, \dots, k$ ) è un sottogruppo di SYLOW di  $P'$  d'ordine  $p_i^{\alpha_i}$ .

In base all'osservazione che chiude il n. prec., è possibile porre un omomorfismo di struttura  $\omega_i$  tra  $P'$  e  $P'_i$ . Basta, a tal fine, far corrispondere a ciascun sottogruppo  $A'$  di  $P'$  il sottogruppo  $A' \cap P'_i$ . Detto  $\tau$  l'omomorfismo strutturale tra  $G$  e  $P'$ , si ottiene, tra  $G$  e  $P'_i$ , l'omomorfismo strutturale  $\tau\omega_i$ , prodotto di  $\tau$  ed  $\omega_i$ .

Pertanto è  $G = S'_i \cup R_i$ , ove  $S'_i$  è un sottogruppo di SYLOW d'ordine  $q_i^{s_i}$  ( $s_i \geq \alpha_i$ ,  $q_i$  primo), ciclico o del tipo definito dalle (2), ed  $R_i$  un sottogruppo normale d'ordine primo con  $q_i$ . Inoltre  $S'_i$  deve contenere un elemento  $l_i$  d'ordine  $q_i^{\beta_i}$  ( $\alpha_i \leq \beta_i \leq s_i$ ) permutabile con ogni elemento di  $R_i$ , tale che tutti gli elementi di  $S'_i$  non contenuti in  $\{l_i\}$  hanno per potenza  $l_i$ .

A  $S'_i$  corrisponde in  $P'_i$ , per effetto di  $\tau\omega_i$ ,  $P'_i$  stesso, quindi, stante la definizione di  $\omega_i$ , a  $S'_i$  corrisponde in  $P'$ , per effetto di  $\tau$ , un sottogruppo contenente  $P'_i$ . Ma  $\tau\omega_i$  muta  $\{l_i\}$  in  $P'_i$ , quindi  $\tau$  muta  $\{l_i\}$  in un sottogruppo non identico  $\{l'_i\}$ . E poichè ogni sottogruppo  $S'_i$  non giacente in  $\{l_i\}$  contiene  $\{l_i\}$  stesso, così l'omologo di  $S'_i$  di  $S'_i$  in  $\tau$  deve esser tale che ogni suo sottogruppo non giacente in  $\{l'_i\}$  contiene  $\{l'_i\}$ . Ciò è possibile solo se  $S'_i$  è di SYLOW, e pertanto, poichè  $S'_i$  deve contenere  $P'_i$ , coincide addirittura con esso.

Otteniamo così che  $G$  contiene un sottogruppo di SYLOW  $S_i$ , ciclico o del tipo definito dalle (2), ed un sottogruppo  $R_i$ , normale, il cui ordine è primo con l'ordine,  $q_i^{s_i}$ , di  $S_i$ , tali che  $G = R_i \cup S_i$ . Inoltre  $S_i$  contiene un elemento  $l_i$  d'ordine

$q_i^{\beta_i}$  ( $\alpha_i \leq \beta_i \leq s_i$ ) permutabile con ogni elemento di  $R_i$ , e tale che ogni elemento di  $S_i$  non contenuto in  $\{l_i\}$  ha per potenza  $l_i$ . Ciò si ha per ogni valore di  $i$ .

L'omomorfismo strutturale  $\tau \omega_i$  fa corrispondere a  $S_j$  ( $j \neq i$ ) l'identità, perchè  $\tau$  fa corrispondere ad  $S_j$  il sottogruppo  $P'_j$ , e  $\omega_i$  fa corrispondere a  $P'_j$  la sua intersezione con  $P'_i$ , cioè l'identità. Poichè invece  $\tau \omega_i$  fa corrispondere ad  $S_i$  il sottogruppo  $P'_i$ , si ha che  $S_j \neq S_i$ ,  $q_i \neq q_j$  e quindi  $R_j \neq R_i$ . Pertanto  $S_i$  sta in  $R_j$ , ed  $S_j$  sta in  $R_i$ . L'indice di  $R_i$  in  $G$  è  $q_i^{s_i}$ , quello di  $R_j$  è  $q_j^{s_j}$ ; inoltre, essendo  $R_i \cup S_i = G$ , ed giacendo  $S_i$  in  $R_j$ , si ha  $R_i \cup R_j = G$ . Si ha allora che il sottogruppo  $R_{i,j} = R_i \cap R_j$ , anch'esso normale in  $G$  come  $R_i$  ed  $R_j$ , ha indice  $q_i^{s_i}$  in  $R_j$ , e quindi indice  $q_i^{s_i} q_j^{s_j}$  in  $G$ . Così procedendo, si dimostra che se è  $i \neq j \neq k$ , l'intersezione  $R_{i,j,k}$  di  $R_i$ ,  $R_j$ ,  $R_k$  è normale in  $G$  ed ha in esso indice  $q_i^{s_i} q_j^{s_j} q_k^{s_k}, \dots$ , e così via; e finalmente l'intersezione  $R_{1,2,\dots,k}$  di  $R_1, R_2, \dots, R_k$  è normale in  $G$  ed ha indice  $q_1^{s_1} q_2^{s_2} \dots q_k^{s_k}$ . Poniamo, per brevità  $R_{1,2,\dots,k} = R$ .

Consideriamo ora il fattoriale  $\bar{G} = \frac{G}{R}$ , d'ordine  $q_1^{s_1} \dots q_k^{s_k}$ .

Poichè  $R_{1,2,\dots,t-1,t+1,\dots,k}$  è normale in  $G$  si ha che

$$\bar{S}_i = \frac{R_{1,2,\dots,t-1,t+1,\dots,k}}{R}$$

è normale in  $\bar{G}$ . Ma  $\bar{S}_i$  è isomorfo ad  $S_i$ , come si vede subito. Pertanto è  $\bar{G} = \bar{S}_1 \times \bar{S}_2 \times \dots \times \bar{S}_k$  con  $\bar{S}_i$  isomorfo ad  $S_i$  ( $i = 1, \dots, k$ ).

**8.** - Poichè  $S_1, S_2, \dots, S_k$  sono sottogruppi di SYLOW relativi a numeri primi distinti, uno solo di essi può avere per ordine una potenza di 2 e quindi non essere ciclico. Supponiamo, in un primo tempo, che tutti i sottogruppi  $S_i$ , e quindi anche i sottogruppi  $\bar{S}_i$  siano ciclici. Allora  $\bar{G}$ , quale prodotto diretto di gruppi ciclici di ordini primi tra loro, è ciclico, e può esser generato da un elemento  $\bar{b}$  d'ordine  $n = q_1^{s_1} q_2^{s_2} \dots q_k^{s_k}$ . Se  $b^*$  è un

elemento di  $G$  cui corrisponde  $\bar{b}$  nell'omomorfismo tra  $G$  e  $\bar{G}$ , l'ordine di  $b^*$  è divisibile per  $n$ , e poichè  $n$  è primo con l'ordine di  $r$ , l'ordine di  $b^*$  è dato dal prodotto di  $n$  per un numero primo con  $n$ . Una potenza di  $b^*$ , che diremo  $b$ , e a cui corrisponde ancora  $\bar{b}$  in  $\frac{G}{R}$ , ha esattamente ordine  $n$ . Il gruppo  $S$  generato da  $b$  è il prodotto diretto di  $k$  sottogruppi di SYLOW di  $G$ , di ordini rispettivamente  $q_1^{s_1}, \dots, q_k^{s_k}$ , e che sono coniugati ad  $S_1, S_2, \dots, S_k$ .

Scegliendo opportunamente i gruppi  $S_i$ , tra i sottogruppi di SYLOW di dato ordine, si può addirittura supporre che sia  $S = S_1 \times S_2 \times \dots \times S_k$ .

Si consideri ora l'elemento  $l = l_1 \cdot l_2 \cdot \dots \cdot l_k$ . Esso appartiene al centro di  $G$ , perchè vi appartengono  $l_1, \dots, l_k$ , avendosi  $l_i$  normale in  $S_i$  (perchè  $S_i$  è ciclico), e permutabile con ogni elemento di  $R_i$ . Pertanto  $l$  è permutabile con ogni elemento di  $R$ . L'elemento  $l$ , essendo in  $S_1 \times S_2 \times \dots \times S_k = S$ , è una potenza di  $b$ . Poichè l'ordine di  $b$  è  $q_1^{s_1} \dots q_k^{s_k}$ , mentre quello di  $l$  è  $q_1^{\beta_1} \dots q_k^{\beta_k}$ , si ha che  $\{l\}$  coincide con  $\left\{ b^{q_1^{s_1 - \beta_1} \cdot q_2^{s_2 - \beta_2} \cdot \dots \cdot q_k^{s_k - \beta_k}} \right\}$ . Possiamo quindi supporre che sia  $l = b^{q_1^{s_1 - \beta_1} \cdot \dots \cdot q_k^{s_k - \beta_k}}$ .

Riassumendo, quando tutti i sottogruppi  $S_i$  son ciclici, si ha che è  $G = S \cup R$ , ove  $S$  è un gruppo ciclico d'ordine  $q_1^{s_1} \dots q_k^{s_k}$  ( $q_1, \dots, q_k$  primi;  $s_i \geq \alpha_i$ ) mentre  $R$  è un sottogruppo normale di  $G$ , il cui ordine è primo con  $q_1, \dots, q_k$ . Inoltre, detto  $b$  un generatore di  $S$ , si ha che l'elemento

$$l = b^{q_1^{s_1 - \beta_1} \cdot q_2^{s_2 - \beta_2} \cdot \dots \cdot q_k^{s_k - \beta_k}} \quad (\beta_i \geq \alpha_i)$$

è permutabile con ogni elemento di  $R$ .

9. - Supponiamo ora invece che uno dei sottogruppi  $S_i$ , ad esempio  $S_1$ , non sia ciclico. Esso allora deve essere necessariamente del tipo definito dalle (2); ed altrettanto deve avvenire di  $\bar{S}_1$ , mentre i sottogruppi  $S_2, \dots, S_k$ , e così  $\bar{S}_2, \dots, \bar{S}_k$  sono

ciclici. Si può allora dimostrare, ragionando su  $R_1$  come si è ragionato nel n. prec. su  $G$ , che è  $R_1 = T \cup R$ , ove  $T$  è un sottogruppo ciclico d'ordine  $q_2^{s_2} \dots q_k^{s_k}$ . Sia  $t$  un generatore di  $T$ . A  $T$  corrisponde in  $\overline{G}$  un elemento  $\overline{t}$ .

Consideriamo ora il sottogruppo  $R_{2,3,\dots,k} = S_1 \cup R$ .

L'elemento  $\overline{t}$  trasforma ogni elemento di  $\overline{S}_1$  in sè, perchè  $\overline{t}$  è in  $\overline{S}_2 \times \overline{S}_3 \times \dots \times \overline{S}_k$  che è permutabile elemento per elemento con  $\overline{S}_1$ , e pertanto  $t$  trasforma un elemento  $\gamma$  di  $S_1$  in un elemento del tipo  $\gamma\rho$ , con  $\rho$  in  $R$ . Di conseguenza si ha  $t^{-1} S_1 t = S_1^*$ , ove  $S_1^*$  è un sottogruppo contenuto in  $S_1 \cup R$ , cioè in  $R_{2,3,\dots,k}$ , ed anzi è un sottogruppo di SYLOW di quest'ultimo. Esisterà allora un elemento  $\varphi$  di  $R_{2,3,\dots,k}$ , che possiamo supporre in  $R$ , tale che  $\varphi^{-1} S_1^* \varphi = S_1$ . Allora si ha  $(t\varphi)^{-1} S_1 (t\varphi) = S_1$ , onde l'elemento  $v = t\varphi$  trasforma  $S_1$  in sè. L'elemento  $v$  ha per corrispondente in  $\overline{G}$ , al pari di  $t$ , l'elemento  $\overline{v}$ , e poichè  $\overline{t}$  ha ordine  $q_2^{s_2} \dots q_k^{s_k}$ , l'ordine di  $v$  è della forma  $q_2^{s_2} \dots q_k^{s_k} \cdot d$ , con  $d$  primo con  $q_2, \dots, q_k$ . Pertanto una potenza  $u = v^d$  di  $v$  ha ordine  $q_2^{s_2} \dots q_k^{s_k}$ . L'elemento  $u$ , al pari di  $v$ , trasforma ogni elemento  $\gamma$  di  $S_1$  in un elemento del tipo  $\gamma\rho$  con  $\rho$  di  $R$ ; ma poichè  $u$ , al pari di  $v$ , deve trasformare  $S_1$  in sè,  $\rho$  deve essere in  $S_1$ , e quindi è  $\rho = 1$ , e  $u$  è permutabile con ogni elemento di  $S_1$ .

Il gruppo  $S_1$  sia generato dagli elementi  $g_1$  e  $g_2$  legati dalle relazioni

$$g_1^{s_1-1} = 1 \quad g_2^2 = g_1^{s_2-2} \quad g_2^{-1} g_1 g_2 = g_1^{-1}.$$

Gli elementi  $g_1, g_2$  e  $u$  generano un sottogruppo  $S$  d'ordine  $2^{s_1} \cdot q_2^{s_2} \dots q_k^{s_k}$ , e si ha, evidentemente,  $G = S \cup R$ . Inoltre tanto  $g_1^{s_1-2}$  che  $u^{q_2^{s_2-\beta_2} \cdot q_3^{s_3-\beta_3} \dots q_k^{s_k-\beta_k}}$  ( $\beta_i \geq \alpha_i$ ) sono permutabili con ogni elemento di  $R$ . Posto, per maggior semplicità,  $g_1 = c, g_2 = d$ , otteniamo che, in questo caso è  $G = S \cup R$ , ove  $S$  è un gruppo d'ordine  $2^{s_1} \cdot q_2^{s_2} \dots q_k^{s_k}$  generato dagli elementi  $c, d, u$ , legati dalle relazioni

$$c^{2^{s_1-1}} = 1, \quad d^{2^2} = c^{2^{s_1-2}}, \quad u^{q_2^{s_2} \cdots q_k^{s_k}} = 1,$$

$$cu = uc, \quad du = ud, \quad d^{-1}cd = c^{-1}.$$

ed  $R$  è un sottogruppo normale d'ordine primo con  $2, q_1, \dots, q_k$ , e inoltre tanto  $c^{2^{s_1-2}}$  che  $u^{q_2^{s_2-\beta_2} \cdots q_k^{s_k-\beta_k}}$  ( $\beta_i \geq \alpha_i$ ) sono permutabili con ogni elemento di  $R$ .

**10.** - Ora invertiremo i risultati degli ultimi due nn., dimostrando che un gruppo  $G$  soddisfacente alle condizioni indicate alla fine del n. 8 è strutturalmente omomorfo ad un gruppo ciclico d'ordine  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  ( $\alpha_i \leq \beta_i$ ), e che un gruppo soddisfacente alle condizioni indicate alla fine del n. 9 è strutturalmente omomorfo ad un gruppo ciclico d'ordine  $2 \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$  ( $\alpha_i \leq \beta_i$ ).

Si abbia in primo luogo un gruppo  $G$  soddisfacente alle condizioni del n. 8, cioè tale che è  $G = S \cup R$ , con  $S$  ciclico d'ordine  $q_1^{s_1} \dots q_k^{s_k}$ ,  $R$  normale d'ordine primo con  $q_1, q_2, \dots, q_k$ , e che, se  $b$  è un generatore di  $S$ , l'elemento

$$b^{q_1^{s_1-\beta_1} \cdot q_2^{s_2-\beta_2} \cdots q_k^{s_k-\beta_k}}$$

sia permutabile con ogni elemento di  $R$ . Sia  $P'$  un gruppo ciclico d'ordine  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  ( $\alpha_i \leq \beta_i$ ). Indichiamo con  $P'_1, P'_2, \dots, P'_k$  i sottogruppi di SYLOW di  $G$  di ordini  $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$  rispettivamente. Stabiliamo anzitutto un omomorfismo di struttura  $\omega_i$  tra  $G$  e  $P'_i$  ( $i = 1, \dots, k$ ). Notiamo a tal fine che il minimo sottogruppo di  $G$  contenente  $R$  e  $b^{q_i^{s_i}}$ , sottogruppo che diremo  $R_i$ , è normale in  $G$ , perchè  $b$ , trasformando ogni sua potenza in sè ed  $R$ , che è normale, in sè, trasforma di conseguenza in sè  $R_i$ , ed ogni elemento di  $R$  trasforma in sè  $R_i$  perchè vi giace. Inoltre  $R_i$  ha indice  $q_i^{s_i}$  in  $G$ , e, posto  $b_i = b^{q_1^{s_1} \cdots q_{i-1}^{s_{i-1}} q_{i+1}^{s_{i+1}} \cdots q_k^{s_k}}$ , si ha che  $\{b_i\}$  è un sottogruppo di SYLOW  $S_i$  di  $G$  d'ordine  $q_i^{s_i}$ , ed è  $G = S_i \cup R_i$ . Infine l'e-

lemento  $b_i^{q_i^{s_i} - \beta_i}$  è una potenza di  $b^{q_1^{s_1 - \beta_1} \dots q_k^{s_k - \beta_k}}$ , e quindi è permutabile con ogni elemento di  $R$ ; ma è permutabile anche con  $b^{q_i^{s_i}}$ , e pertanto trasforma in sè ogni elemento di  $R_i$ . Sono così soddisfatte tutte le condizioni del teorema del n. 6, e pertanto si può porre un omomorfismo strutturale  $\omega_i$  tra  $G$  e  $P'_i$  ( $i = 1, \dots, k$ ).

Si costruisca ora una corrispondenza univoca  $\tau$  tra  $G$  e  $P'$  nel modo seguente. Preso un sottogruppo  $A$  di  $G$ , se  $\omega_i$  fa corrispondere ad  $A$  il sottogruppo  $A'_i$  di  $P'_i$ ,  $\tau$  fa corrispondere ad  $A$  il sottogruppo  $A' = A'_1 \times A'_2 \times \dots \times A'_k$ .

Mostriamo ora che  $\tau$  è un omomorfismo di struttura. Anzitutto, per la stessa definizione di  $\tau$ , ad ogni sottogruppo di  $G$  corrisponde uno ed un solo sottogruppo di  $P'$ . Inoltre, preso un sottogruppo  $A'$  di  $P'$ , esso può porsi in uno ed un solo modo sotto la forma  $A' = A'_1 \times A'_2 \times \dots \times A'_k$ , ove  $A'_i$  a un opportuno sottogruppo di  $P'_i$ . Il minimo sottogruppo di  $G$  cui  $\omega_i$  fa corrispondere  $A'_i$  in  $P'_i$  è contenuto in  $S_i$ ; sia esso  $A_i$ . Preso  $j \neq i$ , si ha  $A_j$  permutabile, elemento per elemento, con  $A_i$ , perchè di analoga proprietà gode  $S_j$  nei confronti di  $S_i$ . Il sottogruppo  $A = A_1 \times A_2 \times \dots \times A_k$  ha per corrispondente  $A'$  in  $P'$ , per effetto di  $\omega_i$ , perchè è  $A \cap S_i = A_i$ , e ad  $A_i$  corrisponde, per effetto di  $\omega_i$ ,  $A'_i$ . Quindi ad  $A$  corrisponde  $A'$  per effetto di  $\tau$ , e di conseguenza ogni sottogruppo di  $P'$  proviene, per effetto di  $\tau$ , da qualche sottogruppo di  $G$ .

Infine, siano  $A$  e  $B$  due sottogruppi di  $G$ , e siano  $A' = A'_1 \times A'_2 \times \dots \times A'_k$ ,  $B' = B'_1 \times B'_2 \times \dots \times B'_k$  gli omologhi di  $A$  e  $B$  per effetto di  $\tau$  ( $A'_i$  e  $B'_i$  in  $P'_i$ ). Ad  $A \cap B$ , l'omomorfismo  $\omega_i$  fa corrispondere  $A'_i \cap B'_i$ , quindi  $\tau$  fa corrispondere ad  $A \cap B$  il sottogruppo  $(A'_1 \cap B'_1) \times (A'_2 \cap B'_2) \times \dots \times (A'_k \cap B'_k)$ , che coincide con  $(A'_1 \times A'_2 \times \dots \times A'_k) \cap (B'_1 \times B'_2 \times \dots \times B'_k) = A' \cap B'$ . In breve,  $\tau$  fa corrispondere  $A' \cap B'$  ad  $A \cap B$  e, come si vede in modo analogo, fa corrispondere  $A' \cup B'$  ad  $A \cup B$ .

Sono pertanto soddisfatte da  $\tau$  le tre condizioni cui deve soddisfare una corrispondenza perchè sia un omomorfismo strutturale. Quindi  $\tau$  è un omomorfismo strutturale.

Si abbia, in secondo luogo, un gruppo  $G$  soddisfacente alle condizioni del n. 9, cioè tale che  $G = S \cup R$ , ove  $S$  è un gruppo d'ordine  $2^{s_1} \cdot q_2^{s_2} \cdots q_k^{s_k}$ , generato dagli elementi  $c, d, u$ , legati dalle relazioni

$$\begin{aligned} c^{2^{s_1-1}} &= 1, \quad d^2 = c^{2^{s_1-2}}, \quad u^{q_2^{s_2} \cdots q_k^{s_k}} = 1; \\ cu &= uc, \quad du = ud, \quad d^{-1}cd = c^{-1} \end{aligned}$$

ed  $R$  un sottogruppo normale d'ordine primo con  $2, q_1, \dots, q_k$ , e inoltre tanto  $c^{2^{s_1-2}}$  quanto  $u^{q_2^{s_2-\beta_2} \cdots q_k^{s_k-\beta_k}}$  sono permutabili con ogni elemento di  $R$ . Sia poi  $P'$  un gruppo ciclico d'ordine  $2 \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$  ( $\alpha_i \leq \beta_i \leq s_i$ ). Vogliamo dimostrare che si può porre un omomorfismo strutturale tra  $G$  e  $P'$ .

A tal fine, detti  $P'_1, P'_2, \dots, P'_k$  i sottogruppi di SYLOW di  $P'$  di ordini  $2, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ , si ponga, in base al n. 6, un omomorfismo strutturale  $\omega_i$  tra  $G$  e  $P'_i$  ( $i = 2, \dots, k$ ) in modo simile a quello tenuto nel caso precedente, con la differenza che in questo caso il sottogruppo  $R_i$  è il minimo contenente  $c, d, u^{q_i^{s_i}}$  ed  $R_i$ , mentre l'elemento  $b_i$  è dato da  $u^{q_2^{s_2} \cdots q_{i-1}^{s_{i-1}} q_{i+1}^{s_{i+1}} \cdots q_k^{s_k}}$ . L'elemento  $b_i^{q_i^{s_i-\beta_i}}$  risulta nel nostro caso potenza di  $u^{q_2^{s_2-\beta_2} \cdots q_k^{s_k-\beta_k}}$ , e quindi è permutabile con ogni elemento di  $R$ , ma è permutabile anche con  $u^{q_i^{s_i}}$ , con  $c$  e con  $d$ , e quindi è permutabile con ogni elemento di  $R_i$ .

Sono così soddisfatte le condizioni perchè esista un omomorfismo di struttura  $\omega_i$  tra  $G$  e  $P'_i$  ( $i = 2, \dots, k$ ).

Si consideri poi il sottogruppo  $R_1$ , minimo contenente  $u$  ed  $R$ , e il sottogruppo  $S_1$ , generato da  $c$  e  $d$ . Quest'ultimo è del tipo dato dalle (2) del n. 4, e inoltre  $c^{2^{s_1-2}}$  è permutabile con  $u$  e con ogni elemento di  $R$ , cioè con ogni elemento di  $R_1$ . Sono quindi soddisfatte le condizioni perchè esista un omomorfismo di struttura  $\omega_1$  tra  $G$  e  $P'_1$ . Da questo punto in poi, la dimostrazione si conduce come nel caso precedente.

Si giunge così al seguente teorema:

*Condizione necessaria e sufficiente perchè un gruppo  $G$  sia in omomorfismo strutturale con un gruppo  $P'$  ciclico d'ordine  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  ( $p_1, p_2, \dots, p_k$  numeri primi) è che sia  $G = S \cup R$ , dove  $R$  è un sottogruppo normale, ed  $S$  è un sottogruppo d'ordine  $q_1^{s_1} \cdot q_2^{s_2} \dots q_k^{s_k}$  ( $q_1, q_2, \dots, q_k$  numeri primi che non dividano l'ordine di  $R$ ;  $s_1 \geq \alpha_1, \dots, s_k \geq \alpha_k$ ), appartenente ad uno dei tipi seguenti:*

1) *Ciclico, tale che se  $b$  è un suo generatore esistano dei numeri  $\beta_1, \dots, \beta_k$  per cui  $b^{q_1^{s_1 - \beta_1} \dots q_k^{s_k - \beta_k}}$  ( $\alpha_i \leq \beta_i \leq s_i$ ) sia permutabile con ogni elemento di  $R$ .*

2) *Se è  $\alpha_1 = 1, q_1 = 2$ , generabile mediante tre elementi  $c, d, u$ , legati dalle relazioni*

$$c^{2^{s_1 - 1}} = 1, \quad d^2 = c^{2^{s_1 - 2}}, \quad u^{q_2^{s_2} \dots q_k^{s_k}} = 1;$$

$$cu = uc, \quad du = ud, \quad d^{-1}cd = c^{-1}$$

*e tale che esistano dei numeri  $\beta_1, \dots, \beta_k$ , per cui  $c^{2^{s_1 - 2}}$ , e  $u^{q_2^{s_2 - \beta_2} \dots q_k^{s_k - \beta_k}}$  siano permutabili con ogni elemento di  $R$ .*