SU UNA CLASSE DI GRUPPI FINITI INTRODOTTA DA McLAIN

In memoria di G. A. Miller

DI
GUIDO ZAPPA

In un recente lavoro[1] McLAIN ha studiato diverse interessanti classi di gruppi finiti, caratterizzate dall'esistenza di sottogruppi di dato ordine. Una delle più notevoli è quella dei gruppi verificanti la proprietà da lui chiamata A1: un gruppo finito G si dice verificare la proprietà A1 quando, comunque si scelga un sottogruppo H di G, e comunque si prenda un intero m che divida l'ordine di G e sia divisibile per l'ordine di H, esiste un sottogruppo di G d'ordine m che contiene H.

McLAIN ha determinato varie proprietà che sono equivalenti alla proprietà A1, ma di più facile studio; tra queste la proprietà A3, consistente nel fatto che il normalizzante di ogni sottogruppo H del gruppo ha un indice che non è divisibile per alcun numero primo che sia minore di tutti i divisori dell'ordine di H. Si ha facilmente che i gruppi verificanti A3, e quindi A1, sono particolari gruppi supersolubili.

La difficoltà di determinare tutti i gruppi verificanti A1 consiste fra l'altro nel fatto che, come ha mostrato con un esempio lo stesso McLAIN, se un gruppo verifica A1, non necessariamente ogni suo sottogruppo la verifica.

Il McLAIN ha fatto vedere tra l'altro che un gruppo finito verifica A1 se e soltanto se è risolubile e ogni suo sottogruppo di HALL[2] il cui ordine sia divisibile per due soli numeri primi distinti, verifica anch'esso A1. Pertanto, una volta determinati tutti i gruppi d'ordine $p^\alpha q^\beta$ (p, q primi) verificanti A1, non dovrebbe essere difficile determinare tutti i gruppi finiti verificanti A1.

La presente nota costituisce appunto un primo studio dei gruppi d'ordine $p^\alpha q^\beta$ verificanti A1.

Supposto $p > q$, un gruppo finito G d'ordine $p^\alpha q^\beta$ che verifica A1 e quindi A3 ha evidentemente un sottogruppo normale P d'ordine p^α. Dopo alcune osservazioni preliminari (n. 1), determino facilmente (n. 2) tutti i gruppi in questione nel caso in cui P sia abeliano. Passo poi (n. 3) all'esame del caso, alquanto più complesso, in cui la serie centrale discendente di P ha lunghezza 2, e determino (3.5) una condizione necessaria perchè un gruppo d'ordine $p^\alpha q^\beta$ ($p > q$) col sottogruppo d'ordine p^α a serie centrale discendente

---

Received February 4, 1959. The editors regret that this paper was received too late to be included in the G. A. Miller Memorial Issue.

[1] D. H. McLAIN, *The existence of subgroups of given order in finite groups*, Proc. Cambridge Philos. Soc., vol. 53 (1957), pp. 278–285.

[2] Ricordiamo che dicesi *sottogruppo di* HALL di un gruppo finito, un sottogruppo il cui ordine sia primo con l'indice.

di lunghezza 2, verifichi A1. Tale condizione chiarisce abbastanza bene la struttura di tali gruppi, ed è probabilmente anche sufficiente. Infine, nel n. 4, impongo l'ulteriore condizione che il derivato di P abbia ordine p; i teoremi 4.3 e 4.4 forniscono una condizione necessaria e sufficiente affinchè un gruppo d'ordine $p^\alpha q^\beta$ con sottogruppo d'ordine p^α a derivato d'ordine p verifichi A1. Tale condizione permette di costruire tutti i gruppi di questo tipo.

Incidentalmente, vengono anche determinati (4.1) tutti i p-gruppi (del resto, forse già noti) col derivato d'ordine p e coincidente col centro.

In tutta la nota, con p, q si indicheranno numeri primi tali che $p > q$.

1. Osservazioni preliminari

Introduciamo anzitutto alcune definizioni, che ricalcano quelle poste da McLain nel lavoro citato.

Diremo che un gruppo finito G gode della *proprietà* A1 quando ogni sottogruppo H di G è contenuto in sottogruppi di ogni ordine possibile, quando cioè, comunque si scelga un sottogruppo H di G, e comunque si prenda un intero m che divida l'ordine di G e sia divisibile per l'ordine di H, esiste un sottogruppo di G d'ordine m che contiene H.

Diremo che un gruppo finito G gode della *proprietà* A3 quando, comunque si scelga un sottogruppo H di G, e comunque si prenda un numero primo p che divida l'ordine di G e sia minore di tutti i divisori primi dell'ordine di H, il normalizzante di H contiene almeno un sottogruppo di Sylow di G relativo a p.

Si ha che:

1.1 (McLain, l.c.) *Un gruppo finito gode della proprietà* A1 *se e solo se gode della proprietà* A3.

Si ha pure che:

1.2 (McLain, l.c., Lemma 6) *Un gruppo finito G verifica* A1 *se e solo se è risolubile e per ogni coppia, p_i, p_j, di divisori primi distinti dell'ordine di G, uno, e quindi ognuno, dei sottogruppi di G d'ordine $p_i^\alpha p_j^\beta$ (ove p_i^α, p_j^β sono le massime potenze di p_i, p_j che dividono l'ordine di G) verifica* A1.

Ancora, si nota subito che:

1.3. *Se un gruppo finito G verifica* A1, *ed N è un suo sottogruppo normale, anche G/N verifica* A1.

Sia infatti K/N un sottogruppo di G/N. Sia n l'ordine di N, g quello di G, k quello di K. Sarà allora g/n l'ordine di G/N, e k/n quello di K/N. Sia h un intero che divide g/n ed è divisibile per k/n. Allora $l = hn$ divide g ed è divisibile per k. Poichè G verifica A1, esiste un sottogruppo L di G d'ordine l, contenente K. Di conseguenza L contiene N, e si ha che L/N è un sottogruppo di G/N d'ordine $h = l/n$ e contenente K/N, come si voleva.

Portiamo ora la nostra attenzione sui gruppi finiti, verificanti la proprietà A1, e aventi ordine $p^\alpha q^\beta$, con p, q primi distinti tali che $p > q$. In base ad 1.2, dalla conoscenza dei gruppi di tale tipo si può risalire facilmente alla conoscenza di tutti i gruppi finiti godenti della proprietà A1.

Sia G un gruppo finito verificante A1, d'ordine $p^\alpha q^\beta$. Necessariamente G verifica, in base ad 1.1, anche la A3, onde un sottogruppo di SYLOW P di G d'ordine p^α ha il normalizzante di ordine divisibile per q^β; pertanto P è normale in G, ed è l'unico sottogruppo di SYLOW del suo ordine.

Proviamo ora che:

1.4 *Se G è un gruppo d'ordine $p^\alpha q^\beta$ $(p > q)$ verificante* A1, *P il suo (unico) sottogruppo di* SYLOW *d'ordine p^α, g un elemento qualunque di G, e C il centro di P, esiste un intero s tale che, comunque si prenda un elemento c di C, si abbia $g^{-1}cg = c^s$.*

Sia D un qualunque sottogruppo di C. In base ad 1.1, G verifica la A3 onde, essendo l'ordine di D una potenza di p ed essendo $q < p$, l'ordine del normalizzante $N(D, G)$ di D in G è divisibile per q^β; essendo poi D normale in P, l'ordine di $N(D, G)$ è divisibile per p^α. Pertanto l'ordine di $N(D, G)$ è divisibile per $p^\alpha q^\beta$, onde $N(D, G) = G$, e D è normale in G. Pertanto g, come ogni altro elemento di G, trasforma in sè ogni sottogruppo D di C, ed essendo C abeliano, deve esistere un intero s, dipendente in generale da g, tale che, comunque si prenda un elemento c di C, si abbia $g^{-1}cg = c^s$.

Da 1.3 e 1.4 segue che:

1.5. *Se G è un gruppo d'ordine $p^\alpha q^\beta$ $(p > q$ numeri primi$)$ verificante* A1, *P è il suo (unico) sottogruppo di* SYLOW *d'ordine p^α, g è un elemento qualunque di G e C_i, C_{i+1} $(C_i \subset C_{i+1})$ sono due termini consecutivi della serie centrale ascendente o discendente di P, esiste un intero s tale che, comunque si prenda un elemento c di C_{i+1}, si abbia $g^{-1}cg = c^s h$, con h in C (e dipendente in generale da c).*

Infatti, essendo C_i caratteristico in P e P normale in G, è C_i normale in G. Inoltre, per 1.3, G/C_i verifica A1, e P/C_i ne è il sottogruppo di SYLOW relativo a p, mentre C_{i+1}/C_i è contenuto nel centro di P/C_i. Pertanto, se indichiamo con $\bar{g}$ l'omologo di g nell'omomorfismo naturale ϑ di G su G/C_i, si ha, in base a 1.4, che esiste un intero s tale che, comunque si prenda un elemento $\bar{c}$ di C_{i+1}/C_i, è $\bar{g}^{-1}\bar{c}\bar{g} = \bar{c}^s$. Se ora c è un qualunque elemento di C_{i+1}, e facciamo coincidere $\bar{c}$ con l'omologo di c per effetto di ϑ, da $\bar{g}^{-1}\bar{c}\bar{g} = \bar{c}^s$ discende $g^{-1}cg = c^s h$, con h in C_i, (ove s non dipende dall'elemento c, mentre h in generale ne dipende).

Pertanto 1.5 è dimostrato.

2. Gruppi d'ordine $p^\alpha q^\beta$ verificanti A1 col sottogruppo d'ordine p^α abeliano

Sia ora G un gruppo d'ordine $p^\alpha q^\beta$, verificante A1, il cui (unico) sottogruppo di SYLOW P d'ordine p^α sia abeliano.

Allora P coincide col proprio centro, onde, in base ad 1.4, se g è un elemento qualunque di G, esiste un intero s, dipendente in generale da g, tale che, comunque si prenda un elemento c di P, si abbia $g^{-1}cg = c^s$.

Il centralizzante H di P in G ha indice q^γ in G, con $\gamma \leqq \beta$. Inoltre G/H è isomorfo al gruppo A degli automorfismi ottenuti trasformando gli elementi di P mediante quelli di G. Poichè, in base a quanto si è visto, un automorfismo di P che appartenga ad A porta ogni elemento di P nella sua s-esima potenza, G/H è isomorfo ad un sottogruppo del gruppo degli automorfismi di un p-gruppo ciclico; e di conseguenza G/H è ciclico, e il suo ordine, essendo primo con p, è un divisore di $p - 1$. Se Q è un sottogruppo di SYLOW di G d'ordine q^β, si ha che $H \cap Q$ è normale in Q e $Q/(H \cap Q)$ è isomorfo a G/H, quindi ciclico d'ordine q^γ divisore di $p - 1$. Posto $H \cap Q = M$, e detto g un elemento di Q cui corrisponde, nell'omomorfismo naturale di Q sopra Q/M, un generatore di quest'ultimo, si ha $Q = \{M, g\}$ con $g^{-1}Mg = M$, e g^{q^γ} in M. Sarà inoltre, comunque si prenda un elemento c di P, $g^{-1}cg = c^s$ con s intero appartenente all'esponente $q^\gamma \pmod p$.

Concludendo:

2.1. *Se G è un gruppo d'ordine $p^\alpha q^\beta$ $(p > q)$ verificante* A1 *a sottogruppo di* SYLOW *d'ordine p^α abeliano, è $G = PQ$, con Q sottogruppo di* SYLOW *d'ordine q^β tale che $Q = \{M, g\}$, $PM = P \times M$, $g^{-1}Mg = M$, g^{q^γ} è la minima potenza di g contenuta in M, con q^γ divisore di $p - 1$, e, qualunque sia l'elemento c di P, è $g^{-1}cg = c^s$ con s indipendente da c e appartenente all'esponente $q^\gamma \pmod p$.*

Viceversa:

2.2. *Un gruppo d'ordine $p^\alpha q^\beta$ dotato di sottogruppo di* SYLOW *P d'ordine p^α normale abeliano, e tale che $G = PQ$, ove P e Q soddisfano alle condizioni indicate in* 2.1., *verifica* A1.

Infatti, (MCLAIN, l.c., Theorem 3) un tale gruppo gode addirittura della proprietà che, comunque si prendano due suoi sottogruppi H e K con $H \subset K$, esistono sottogruppi di ogni possibile ordine contenenti H e contenuti in K.

3. Gruppi d'ordine $p^\alpha q^\beta$ verificanti A1 con sottogruppo d'ordine p^α a derivato contenuto nel centro

Sia ora G un gruppo d'ordine $p^\alpha q^\beta$, verificante A1, in cui il sottogruppo (unico) P d'ordine p^α abbia il derivato K contenuto nel centro di P. Se g è un qualunque elemento di G, esiste, in base a 1.5, un intero r tale che, comunque si prenda un elemento b di P, è $g^{-1}bg = b^r k$, con k in K, ed esiste del pari, in base ad 1.4, un intero s tale che, comunque si prenda un elemento c di K, è $g^{-1}cg = c^s$. Siano ora a, b due elementi di P (necessariamente non contenuti in K) tali che $b^{-1}a^{-1}ba = k$, con k in K. Sarà $g^{-1}ag = a^r k_1$, $g^{-1}bg = b^r k_2$, con k_1, k_2 convenienti elementi di K, onde, tenuto conto del fatto che K è contenuto nel centro di P, si ha

$$k^s = g^{-1}kg = g^{-1}(b^{-1}a^{-1}ba)g = k_2^{-1}b^{-r}k_1^{-1}a^{-r}b^r k_1 a^r k_2 = b^{-r}a^{-r}b^r a^r = k^{r^2}.$$

Pertanto:

3.1. *Se k è il commutatore di due elementi di P, è $k^s = k^{r^2}$, onde $s \equiv r^2 \pmod{p}$.*

Sia ora Q un sottogruppo di SYLOW di G d'ordine q^β; sarà $G = PQ$. Se b è un elemento di P, il normalizzante di $\{b\}$ in G, in base a 1.1, contiene un sottogruppo $\bar{Q}$ d'ordine q^β, che risulterà, in base al teorema di SYLOW, coniugato a Q in G; e poichè in ogni laterale di Q in G c'è un elemento di P, esisterà un elemento d di P tale che $d^{-1}\bar{Q}d = Q$. Di conseguenza il normalizzante di $\{d^{-1}bd\}$ in G contiene Q. Ma $d^{-1}bd$ è in bK, essendo d e b in P, e pertanto:

3.2. *Se Q è un sottogruppo di* SYLOW *di G d'ordine q^β, in ogni laterale di K in P c'è un elemento trasformato in una qualche sua potenza da ogni elemento di Q.*

Se è $G = P \times Q$, G verifica sicuramente A1, perchè verifica A3. Supponiamo che invece non sia $G = P \times Q$. Se H è il centralizzante di P in G, H non potrà allora contenere Q. Se g è un elemento di Q, non contenuto in H, dovrà aversi, per ogni b di P, non contenuto in K, $g^{-1}bg = b^r k$, con k in K ed $r \not\equiv 1 \pmod{p}$. Infatti, per 1.5 sarà intanto $g^{-1}bg = b^r k$, con k in K ed r intero conveniente non dipendente da b, ed inoltre, per 1.4, sarà, per ogni elemento c di K, $g^{-1}cg = c^s$, con s intero conveniente non dipendente da c; e, in base a 3.1, sarà $r^2 \equiv s \pmod{p}$. Se fosse $r \equiv 1 \pmod{p}$, sarebbe anche $s \equiv 1 \pmod{p}$, onde g indurrebbe in $\{c\}$ un automorfismo il cui ordine è potenza di p. Essendo l'ordine di g primo con p, dovrebbe essere g permutabile con c, cioè con ogni elemento di K; per analoghe ragioni g dovrebbe indurre l'automorfismo identico in P/K, e pertanto dovrebbe aversi $g^{-1}bg = bk$; ma essendo g di ordine primo con p, dovrebbe essere addirittura $g^{-1}bg = b$, per ogni b di P, contro l'ipotesi che g non sia nel centralizzante H di P in G.

Mostriamo ora che, se non è $G = P \times Q$, in ogni laterale di K in P diverso da K c'è un solo elemento mutato in una sua potenza da ogni elemento di Q. Sia infatti g un elemento di Q non contenuto nel centralizzante H di P in G, e sia Kb un laterale di K in P diverso da K (onde è $b \neq 1$). In base a 3.2, c'è in Kb almeno un elemento, che potremo supporre sia proprio b, tale che $g^{-1}bg = b^r$, con r intero conveniente; e non essendo g in H, è $r \not\equiv 1 \pmod{p}$.

Sia b^{p^x} la minima potenza di b contenuta in K. Sarà $g^{-1}b^{p^x}g = b^{rp^x}$; ma essendo d'altra parte b^{p^x} in K, è $g^{-1}b^{p^x}g = b^{sp^x}$. Sarà allora $b^{rp^x} = b^{sp^x}$ cioè $(b^{p^x})^r = (b^{p^x})^s$. Se fosse $b^{p^x} \neq 1$, sarebbe $r \equiv s \pmod{p}$; avendosi, per 3.1, $s \equiv r^2 \pmod{p}$, sarebbe $r^2 \equiv r \pmod{p}$, vale a dire $r \equiv 0 \pmod{p}$ o $r \equiv 1 \pmod{p}$. Poichè invece, come si è visto, è $r \not\equiv 1 \pmod{p}$, ed è, evidentemente, $r \not\equiv 0 \pmod{p}$, dovrà essere necessariamente $b^{p^x} = 1$, cioè $\{b\} \cap K = 1$.

Se kb è un qualunque elemento di Kb, diverso da b, cioè con $k \neq 1$, sarà $g^{-1}kbg = k^s b^r$. Se kb fosse trasformato da g in una sua potenza, sarebbe

$g^{-1}kbg = (kb)^t = k^t b^t$, con t intero conveniente. Sarebbe allora $k^s b^r = k^t b^t$, cioè $k^{t-s} = b^{r-t}$; e poichè $\{b\} \cap K = 1$, sarebbe $k^{t-s} = b^{r-t} = 1$, onde $s \equiv t \pmod p$, $r \equiv t \pmod p$, da cui seguirebbe $s \equiv r \pmod p$. Essendo, in base a 3.1, $s \equiv r^2 \pmod p$, sarebbe $r^2 \equiv r \pmod p$; il che, come si è visto, non può avvenire. Pertanto, se g muta b in una sua potenza, non può mutare in una sua potenza kb, con $k \neq 1$. Concludendo:

3.3. *Se non è* $G = P \times Q$, *in ogni laterale di* K *in* P *c'è uno ed un solo elemento* b *trasformato in una qualche sua potenza da ogni elemento di* Q; *e si ha* $\{b\} \cap K = 1$.

Vogliamo ora far vedere che:

3.4. *Se non è* $G = P \times Q$, *tutti gli elementi di un medesimo laterale di* K *in* P *diverso da* K *sono coniugati tra loro in* P.

Sia infatti b l'unico elemento del laterale Kb (diverso da K) che sia trasformato in una sua potenza da ogni elemento di Q, e sia kb un qualunque elemento di Kb. Poichè G verifica A3, il normalizzante di $\{kb\}$ in G contiene un coniugato $\bar{Q}$ di Q; e poichè in ogni laterale di $\bar{Q}$ c'è un elemento di P, esisterà in P un elemento d tale che $d^{-1}\bar{Q}d = Q$. Allora il normalizzante di $\{d^{-1}kbd\}$ contiene Q, onde $d^{-1}kbd$ è trasformato in una sua potenza da ogni elemento di Q. Ma, essendo d in P, al pari di kb, si ha che $d^{-1}kbd$ è in Kkb, cioè in Kb; e poichè b è l'unico elemento di Kb trasformato in una sua potenza da ogni elemento di Q, deve essere $d^{-1}kbd = b$. Essendo d in P, ed essendo kb un qualunque elemento di Kb, 3.4 è dimostrato.

Si noti che, poichè ogni elemento di Kb è coniugato a b in P, ogni elemento di K risulta commutatore di una coppia di elementi di P (uno dei quali è b) onde, in base a 3.1, si ha che, *se non è* $G = P \times Q$, *comunque si prenda un elemento* c *di* K, *è* $c^s = c^{r^2}$ (ove r ed s conservano il significato che hanno in 3.1).

Si noti ancora che *se non è* $G = P \times Q$, *e* $\bar{b}$ *è un qualunque elemento di* P *non contenuto in* K, *è* $\{\bar{b}\} \cap K = 1$. Infatti, detto b l'elemento di $K\bar{b}$ che è mutato in sè da ogni elemento di Q, si ha, in base a 3.3, che $K \cap \{b\} = 1$, e, in base a 3.4, che b è coniugato a $\bar{b}$.

Possiamo riassumere i risultati ottenuti sin qui in questo numero nel modo seguente:

3.5. *Se* G *è un gruppo d'ordine* $p^\alpha q^\beta$ *verificante* A1, *e se il sottogruppo (unico)* P *di* SYLOW *di* G *d'ordine* p^α *ha il derivato contenuto nel centro di* P, *indicato con* Q *un sottogruppo di* SYLOW *di* G *d'ordine* q^β, *si presenta uno dei due casi seguenti*:

(a) *È* $G = P \times Q$;

(b) *Detto* K *il derivato di* P, *tutti gli elementi di un medesimo laterale di* K *in* P *che sia diverso da* K *sono coniugati tra loro in* P *e si può trovare in ciascun laterale* K_i *di* K *in* P *diverso da* K *un elemento* b_i *in modo che*: (i) *ciascun elemento* g *di* Q *trasforma ogni elemento* b_i *in una sua potenza* b_i^r, *ove* r *dipende*

da g ma non da b_i, e trasforma ciascun elemento c di K in c^{r^2}; (ii) *per qualche elemento g di Q risulta $r \not\equiv 1 \pmod{p}$*; (iii) *comunque si prenda un elemento b contenuto in P ma non in K, è $\{b\} \cap K = 1$.*

Osserviamo ancora che:

3.6. *Se non è $G = P \times Q$, K coincide col centro di P.*

Infatti, K è per ipotesi contenuto nel centro di P; d'altra parte, ogni elemento b di P non contenuto in K è coniugato in P a tutti gli elementi di Kb, e quindi non può appartenere al centro di P.

4. Caso particolare in cui il sottogruppo P d'ordine p^α ha il derivato d'ordine p

Sia ora G un gruppo d'ordine $p^\alpha q^\beta$ verificante A1 in cui il sottogruppo P d'ordine p^α abbia il derivato K d'ordine p. Allora necessariamente K, essendo normale in P e d'ordine p, è contenuto nel centro di P, onde sussistono le ipotesi del numero precedente. Sia Q sottogruppo di SYLOW di G d'ordine q^β. Supponiamo che non sia $G = P \times Q$. Allora, in base a 3.6, K coincide col centro di P, e inoltre, in base a 3.4, gli elementi di un medesimo laterale di K in P diverso da K sono tutti coniugati tra loro in P. Del resto, un qualunque gruppo P d'ordine p^α col derivato K d'ordine p e coincidente col centro è tale che gli elementi di un laterale Kb di K in P diverso da K sono coniugati tra loro: infatti, se b è un elemento di P non contenuto in K, b non è normale in P, ed è quindi coniugato ad almeno p elementi di P; e poichè i coniugati di b in P sono tutti in Kb, si ha che tutti gli elementi di Kb sono coniugati a b, e quindi tra loro, in P. Si pone pertanto innanzitutto, per determinare la struttura di G, il problema di trovare i p-gruppi col derivato d'ordine p e coincidente col centro. Orbene si ha che:

4.1. *Se P è un gruppo d'ordine p^α (p dispari) col derivato K d'ordine p e coincidente col centro di P, è $\alpha = 2l + 1$, con $l \geqq 1$, e P ammette un sistema di $2l + 1$ generatori $k, a_1, d_1, a_2, d_2, \cdots, a_l, d_l$. Se P non possiede elementi d'ordine p^2, i generatori sono legati dalle relazioni*

$$\text{(A)}\qquad \begin{gathered} a_i^p = d_i^p = k^p = 1 \qquad (i = 1, \cdots, l), \\ d_i a_i = a_i d_i k \qquad (i = 1, \cdots, l), \\ a_i a_j = a_j a_i, \quad d_i d_j = d_j d_i, \quad d_i a_j = a_j d_i \\ (i \neq j;\ i = 1, \cdots, l;\ j = 1, \cdots, l). \end{gathered}$$

Se invece P possiede elementi d'ordine p^2, i generatori sono legati dalle relazioni

$$\text{(B)}\qquad \begin{gathered} a_1^p = k, \quad d_1^p = k^p = a_i^p = d_i^p = 1 \qquad (i = 2, \cdots, l), \\ d_i a_i = a_i d_i k \qquad (i = 1, \cdots, l), \\ a_i a_j = a_j a_i, \quad d_i d_j = d_j d_i, \quad d_i a_j = a_j d_i \\ (i \neq j;\ i = 1, \cdots, l;\ j = 1, \cdots, l). \end{gathered}$$

Sia P un gruppo che verifichi le ipotesi del teorema. Mostriamo in primo luogo che:

4.2. *Se a è un elemento di P, a^p è in K.*

Sia infatti b un qualunque elemento di P. Si avrà $b^{-1}ab = a\bar{k}$, con $\bar{k}$ in K. Essendo K il centro di P, si avrà $b^{-1}a^2b = (a\bar{k})^2 = a\bar{k}a\bar{k} = a^2\bar{k}^2$, e così di sèguito, e pertanto $b^{-1}a^pb = a^p\bar{k}^p$. Ma avendo K ordine p, è $\bar{k}^p = 1$, onde, $b^{-1}a^pb = a^p$, e a^p risulta permutabile con ogni elemento b di P, cioè contenuto in K. Poichè K ha ordine p, da 4.2 discende che il periodo di un elemento di P non supera mai p^2 e che P/K è un gruppo abeliano elementare. Sia a_1 un elemento di P non contenuto in K, che supporremo di periodo p^2 se in P esistono elementi di tal periodo. Poichè a_1 è coniugato ai p elementi di Ka_1 e ad essi soltanto, il normalizzante N_1 di a_1 ha indice p in P, onde, detto b_1 un elemento di P non permutabile con a_1, è $P = \{b_1, N_1\}$. Il normalizzante M_1 di b_1 in P ha anch'esso indice p in P ed è distinto da N_1 perchè non contiene a_1: onde $L_1 = M_1 \cap N_1$ ha indice p^2 in P, e si ha $P = \{a_1, b_1, L_1\}$. Se non è $L_1 = K$, esisterà un elemento a_2 di L_1 non contenuto in K. Non può a_2 appartenere al centro di L_1, altrimenti, essendo permutabile anche con a_1 e b_1, sarebbe normale in P e quindi contenuto in K. Il normalizzante N_2 di a_2 in L_1 ha allora indice p in L_1. Sia b_2 un elemento di L_1 non contenuto in N_2; il normalizzante M_2 di b_2 in L_1 non contiene a_2, quindi ha indice p in L_1, ed è distinto da N_2; e pertanto $L_2 = M_2 \cap N_2$ ha indice p^2 in L_1, e quindi indice p^4 in P, e si ha $L_1 = \{a_2, b_2, L_2\}$ e di conseguenza $P = \{a_1, b_1, a_2, b_2, L_2\}$. Si noti che a_1 e b_1 non sono permutabili tra loro, come non lo sono a_2 e b_2, mentre a_1 e b_1 sono ambedue permutabili con a_2 e b_2, e gli elementi di L_2 sono permutabili con a_1, a_2, b_1, b_2. Se non è $L_2 = K$, si seguita allo stesso modo. Alla fine si determinano $2l$ elementi $a_1, \cdots, a_l, b_1, \cdots, b_l$, tali che $P = \{a_1, b_1, a_2, b_2, \cdots, a_l, b_l, K\}$, K ha indice p^{2l} in P, e a_i non è permutabile con b_i mentre lo è con a_j e con b_j, per ogni $j \neq i$. Si ha intanto che P ha ordine p^{2l+1}.

Scambiando eventualmente a_i con b_i, possiamo ridurci al caso in cui, se dei due elementi a_i, b_i ve ne è uno ed uno solo di periodo p^2, questo sia a_i $(i = 1, \cdots l)$.

Distinguiamo ora due casi:

(a) P non contiene elementi d'ordine p^2. Allora, si avrà che

$$a_i^p = b_i^p = k^p = 1, \qquad b_i a_j = a_j b_i, \qquad b_i b_j = b_j b_i, \qquad a_i a_j = a_j a_i \quad (i, j = 1, \cdots, l;\ i \neq j), \tag{1}$$

ove con k si è indicato un generatore di K.

Si avrà inoltre $b_i a_i = a_i b_i k^{x_i}$, con $0 < x_i < p$. Se y_i è l'intero (che esiste ed è unico) tale che $0 < y_i < p$, $x_i y_i \equiv 1 \pmod p$, si ha, tenuto conto del fatto che k è nel centro di P:

$$b_i^{y_i} a_i = a_i b_i^{y_i} k^{x_i y_i} = a_i b_i^{y_i} k. \tag{2}$$

Ponendo allora $d_i = b_i^{y_i}$, si avrà

$$P \equiv \{a_1, d_1, \cdots, a_l, d_l, k\}.$$

Inoltre, dalle (1) discende che è

$$a_i^p = d_i^p = k^p = 1, \qquad d_i a_j = a_j d_i, \qquad a_i a_j = a_j a_i, \qquad d_i d_j = d_j d_i \quad (i, j = 1, \cdots, l; i \neq j),$$

e dalle (2), che è

$$d_i a_i = a_i d_i k \qquad (i = 1, \cdots, l).$$

Pertanto, in tal caso P è generato dagli elementi $a_1, d_1, \cdots, a_l, d_l, k$, verificanti le (A), come si voleva.

(b) P contiene elementi d'ordine p^2. In tal caso, dato il modo in cui abbiamo scelto gli elementi a_i e b_i $(i = 1, \cdots, l)$ sarà $a_1^p \neq 1$, e sarà $b_i^p = 1$ tutte le volte che è $a_i^p = 1$ $(i = 2, \cdots, l)$. Possiamo allora supporre per fissare le idee, senza ledere la generalità, che sia $a_1^p \neq 1$, $a_2^p \neq 1, \cdots, a_m^p \neq 1$, $a_{m+1}^p = \cdots = a_l^p = 1$. Sostituendo eventualmente ad $a_1, a_2, \cdots, a_m$ delle loro potenze, che chiameremo ancora $a_1, \cdots, a_m$, possiamo ridurci al caso in cui sia $a_1^p = a_2^p = \cdots = a_m^p = k$, con k conveniente elemento $\neq 1$ di K.

Allora $\{a_i, b_i\}$ $(i = 1, \cdots, m)$ è un gruppo non abeliano d'ordine p^3 con elementi d'ordine p^2, la cui struttura è ben nota: potrà trovarsi in esso un elemento h_i tale che $\{a_i, b_i\} = \{a_i, h_i\}$, $h_i^p = 1$, $h_i a_i h_i^{-1} = a_i^{p+1} = a_i k$ $(i = 1, \cdots, m)$. Inoltre, ragionando come nel caso (a), si vede che può determinarsi in $\{a_i, b_i\}$ $(i = m+1, \cdots, l)$ un elemento h_i tale che $h_i^p = 1$, $\{a_i, b_i\} = \{a_i, h_i\}$, $h_i a_i h_i^{-1} = a_i k$.

Avremo allora

$$P \equiv \{a_1, h_1, \cdots, a_l, h_l, k\}$$

$$\text{con } a_1^p = a_2^p = \cdots = a_m^p = k, \quad a_{m+1}^p = \cdots = a_l^p = 1, \quad h_1^p = \cdots = h_l^p = 1;$$

$$h_i a_i = a_i h_i k \qquad (i = 1, \cdots, l),$$

$$a_i a_j = a_j a_i, \qquad h_i h_j = h_j h_i, \qquad h_i a_j = a_j h_i \quad (i, j = 1, \cdots, l; i \neq j).$$

Mostriamo ora che ci si può ridurre al caso $m = 1$.

Si ponga infatti

$$\bar{a}_i = a_i \text{ per } i = 1 \text{ e per } i > m, \qquad \bar{a}_i = a_1^{-1} a_i \text{ per } 2 \leqq i \leqq m,$$

$$d_1 = h_1 h_2 \cdots h_m, \qquad d_i = h_i \text{ per } i = 2, \cdots, l.$$

Si verifica subito che è

$$P \equiv \{\bar{a}_1, d_1, \bar{a}_2, d_2, \cdots, \bar{a}_l, d_l, k\},$$

$$\bar{a}_1^p = k, \qquad \bar{a}_i^p = 1 \text{ per } 2 \leqq i \leqq m, \qquad d_i^p = 1 \text{ per } 1 \leqq i \leqq m,$$

$$\bar{a}_i \bar{a}_j = \bar{a}_j \bar{a}_i, \qquad d_i d_j = d_j d_i, \qquad \bar{a}_i d_j = d_j \bar{a}_i \quad \text{per } i, j = 1, \cdots, l; i \neq j;$$

$$d_i \bar{a}_i = \bar{a}_i d_i k \qquad (i = 1, \cdots, l).$$

Scrivendo ora a_i in luogo di $\bar{a}_i$, si ottiene che P è generato dagli elementi $a_1, d_1, \cdots, a_r, d_r, k$, legati dalle relazioni (B) di cui all'enunciato. Il teorema 4.1 è così dimostrato.

Sia ora di nuovo G un gruppo d'ordine $p^\alpha q^\beta$ verificante A1, tale che il derivato K del sottogruppo di SYLOW P di G d'ordine p^α abbia ordine p. Allora la struttura di P è fornita dal teorema 4.1 ed è $K = \{k\}$. Ma poichè, in base a (3.5), comunque si prenda un elemento b contenuto in P ma non in K, dev'essere $\{b\} \cap K = 1$, sarà in particolare $\{a_1\} \cap K = 1$, onde non potrà aversi $a_1^p = k$, e di conseguenza P non potrà presentare il caso (B) del teorema 4.1. Ne segue che P sarà generato dagli elementi $a_1, a_2, \cdots, a_l, b_1, \cdots, b_l, k$, legati dalle relazioni:

$$\text{(A)}\qquad \begin{gathered} a_i^p = b_i^p = k^p = 1 \qquad (i = 1, \cdots, l), \\ b_i a_i = a_i b_i k \qquad (i = 1, \cdots, l), \\ a_i a_j = a_j a_i, \quad b_i a_j = a_j b_i, \quad b_i b_j = b_j b_i \\ (i \neq j;\ i, j = 1, \cdots, l). \end{gathered}$$

Vogliamo ora mostrare che esiste un sottogruppo d'ordine q^β di G ciascun elemento del quale trasformi ciascuno degli elementi $a_1, b_1, \cdots, a_l, b_l$ in una sua potenza.

Sia a tal fine Pg un laterale di P in G. Si avrà, in base a 1.5,

$$g^{-1} a_i g = a_i^s k^{x_i}, \qquad g^{-1} b_i g = b_i^s k^{y_i} \qquad (i = 1, \cdots, l).$$

Sia ora t_i un intero tale che $t_i s \equiv x_i \pmod p$, e u_i un intero tale che $u_i s \equiv -y_i \pmod p$ $(i = 1, \cdots, l)$. Allora, posto

$$g' = g a_1^{u_1} b_1^{t_1} a_2^{u_2} b_2^{t_2} \cdots a_l^{u_l} b_l^{t_l},$$

si ha, in base alle (A)

$$\begin{aligned} g'^{-1} a_i g' &= b_l^{-t_l} a_l^{-u_l} \cdots b_1^{-t_1} a_1^{-u_1} g^{-1} a_i g a_1^{u_1} b_1^{t_1} \cdots a_l^{u_l} b_l^{t_l} \\ &= b_i^{-t_i} a_i^s k^{x_i} b_i^{t_i} = a_i^s k^{-st_i} k^{x_i} = a_i^s, \end{aligned}$$

e analogamente

$$g'^{-1} b_i g' = a_i^{-u_i} b_i^s k^{y_i} a_i^{u_i} = b_i^s k^{su_i} k^{y_i} = b_i^s.$$

Ma g' è nel laterale $gP = Pg$, onde in ogni laterale di P c'è un elemento permutabile con $\{a_1\}, \{b_1\}, \cdots, \{a_l\}, \{b_l\}$. Detta pertanto S l'intersezione dei normalizzanti di $\{a_1\}, \{b_1\}, \cdots, \{a_l\}, \{b_l\}$, si ha allora che in ogni laterale di P in G c'è un elemento di S, onde è $G = PS$. Ne consegue che in S c'è un sottogruppo Q d'ordine q^β. Evidentemente, è allora $G = PQ$, ed ogni elemento g di Q trasforma a_i, b_i $(i = 1, \cdots, l)$ in a_i^s, b_i^s, con s dipendente da g, ma non da a_i, b_i, e trasforma k in k^{s^2} (in base a 3.1).

Sia M l'intersezione di Q col centralizzante di P in G. Allora Q/M è isomorfo al gruppo degli automorfismi indotti in P dagli elementi di Q. Se un elemento di Q è permutabile con a_1, esso è permutabile anche con

$b_1, a_2, \cdots, a_l, b_l$ (avendosi, per esso, $s = 1$) e con k, onde è in M. Ne segue che il gruppo degli automorfismi indotti in P dagli elementi di Q è isomorfo al gruppo degli automorfismi da essi indotti in $\{a_1\}$, onde è ciclico, e il suo ordine divide $p - 1$. Si ha allora $Q = \{M, g\}$, con g conveniente elemento di Q, ed è $g^{-1}a_i g = a_i^s$, $g^{-1}b_i g = b_i^s$, $g^{-1}kg = k^{s^2}$, e, detto q^γ il periodo relativo di g rispetto ad M, si ha che q^γ divide $p - 1$, ed s appartiene all'esponente $q^\gamma \pmod p$.

Possiamo concludere pertanto col teorema:

4.3. *Condizione necessaria perchè un gruppo G d'ordine $p^\alpha q^\beta$ $(p > q)$ a sottogruppo d'ordine p^α con derivato d'ordine p, verifichi* A1, *è che G contenga un solo sottogruppo P (necessariamente normale) d'ordine p^α, e*: (i) *sia $G = P \times Q$ con Q d'ordine q^β; oppure*: (ii) *P sia generato da $2l + 1$ (l intero $\geqq 1$) elementi $a_1, b_1, \cdots, a_l, b_l, k$, verificanti le* (A) *del teorema* 4.2 (*onde è $\alpha = 2l + 1$*), *e si abbia $G = PQ$, con Q sottogruppo d'ordine q^β, tale che $Q = \{M, g\}$, $PM = P \times M$, $g^{-1}a_i g = a_i^s$, $g^{-1}b_i g = b_i^s$, $g^{-1}kg = k^{s^2}$, M d'indice q^γ in Q, con q^γ divisore di $p - 1$, ed s appartenente all'esponente $q^\gamma \pmod p$.*

Ci resta ora infine da invertire il teorema 4.3, da dimostrare cioè che la condizione necessaria, di cui all'enunciato di detto teorema, è anche sufficiente.

Sia G un gruppo d'ordine $p^\alpha q^\beta$ verificante detta condizione. Se è $G = P \times Q$, G verifica A3, e quindi verifica A1, come si voleva. Supponiamo pertanto che non sia $G = P \times Q$. Basterà dimostrare che G verifica A3, cioè che l'ordine del normalizzante $N(H)$ in G di un qualunque sottogruppo H di P è divisibile per q^β. Sarà sufficiente provare che $G = PN(H)$, perchè di conseguenza, essendo P d'ordine p^α, l'ordine di $N(H)$ dovrà essere divisibile per q^β. Detto K il sottogruppo generato da k, il quale è nello stesso tempo centro e derivato di P, si ha che se H contiene K, H è addirittura normale in G. Sia infatti $H \supseteqq K$. Siano $\bar{a}_i, \bar{b}_i$ $(i = 1, \cdots, l)$ gli omologhi di a_i, b_i nell'omomorfismo naturale di G su G/K. Ogni elemento di G induce in P/K un automorfismo che porta $\bar{a}_i, \bar{b}_i$ rispettivamente in $\bar{a}_i^t, \bar{b}_i^t$, con t intero conveniente non dipendente da i. Poichè P/K è abeliano elementare, e gli elementi $\bar{a}_i, \bar{b}_i$ $(i = 1, \cdots, l)$ ne costituiscono una base, tale automorfismo porta ogni elemento di P/K nella sua potenza t-esima, e quindi muta in sè ogni sottogruppo di P/K. Pertanto ogni sottogruppo di P/K è normale in G/K, onde ogni sottogruppo H di P che contenga K è normale in G.

Sia ora H un sottogruppo di P non contenente K. Essendo K d'ordine p, è $H \cap K = 1$, onde il derivato di H è il sottogruppo unità, e H risulta abeliano elementare.

Se H ha ordine 1, esso è certo normale in G. Possiamo pertanto procedere per induzione rispetto all'ordine p^h di H. Supporremo allora che, se R è un sottogruppo di P d'ordine $\leqq p^{h-1}$, ed $N(R)$ il suo normalizzante, si abbia $G = PN(R)$, e dimostreremo che è $G = PN(H)$.

Sia a un elemento di H diverso da 1, e sia $A \equiv \{a\}$. L'elemento a non è in K, quindi non è normale in P. I coniugati di a in P sono tutti in Ka.

Poichè il numero di tali coniugati uguaglia l'indice in P del normalizzante di a in P, e quindi è $= p$, si ha che tutti e soli gli elementi di Ka sono coniugati ad a in P, onde esiste un elemento b di P tale che $b^{-1}ab = ak$. Il normalizzante di b in P ha anch'esso indice p in P, e, non contenendo a e quindi neppure H, interseca quest'ultimo secondo un sottogruppo L d'indice p in H e non contenente a. Poichè H è abeliano elementare, sarà $A \cap L = 1$, $A \cup L = H$, quindi $H = A \times L$.

Sia Pg un laterale di P in G. Poichè L ha ordine p^{h-1}, per l'ipotesi d'induzione esiste in Pg un elemento, che potremo pensare sia proprio g, contenuto nel normalizzante $N(L)$ di L. Si avrà allora $g^{-1}Lg = L$. Sarà poi $g^{-1}ag = a^z h^x$, con z primo con p: infatti, detti $\bar{g}$, $\bar{a}$ gli omologhi di g, a nell'omomorfismo naturale di G su G/K, si ha $\bar{g}^{-1}\bar{a}\bar{g} = \bar{a}^z$, con z primo con p, perchè, come si è visto, ogni sottogruppo di P/K è normale in G/K.

Essendo z primo con p, esiste un intero t tale che $0 \leqq t < p$ e $zt \equiv -x \pmod{p}$. Si avrà allora, ricordando che $b^{-1}ab = ak$ e che k è nel centro di P:

$$(gb^t)^{-1}a(gb^t) = b^{-t}g^{-1}agb^t = b^{-t}a^z k^x b^t = b^{-t}a^z b^t k^x = a^z k^{zt} k^x = a^z k^{-x} k^x = a^z.$$

Sarà quindi $(gb^t)^{-1}A(gb^t) = A$. Essendo poi L nel normalizzante di b, ogni elemento di L è permutabile con b, onde $b^{-1}Lb = L$. Poichè g è in $N(L)$, è anche $g^{-1}Lg = L$. Sarà pertanto $(gb^t)^{-1}L(gb^t) = L$. Segue allora:

$$(gb^t)^{-1}H(gb^t) = (gb^t)^{-1}(A \times L)(gb^t)$$

$$= [(gb^t)^{-1}A(gb^t)] \times [(gb^t)^{-1}L(gb^t)] = A \times L = H.$$

L'elemento gb^t è quindi in $N(H)$. Ma essendo b^t in P, si ha che gb^t è, al pari di g, in Pg. Data l'arbitrarietà del laterale Pg di P, si ha che in ogni laterale di P in G c'è un elemento di $N(H)$. Sarà allora $G = PN(H)$, come si voleva.

Si ha pertanto che:

4.4. *La condizione necessaria, di cui in* 4.3, *affinchè un gruppo d'ordine* $p^\alpha q^\beta$ (p, q *primi*, $p > q$) *con sottogruppo d'ordine* p^α *a derivato d'ordine* p, *verifichi* A1, *è anche sufficiente.*

FIRENZE, ITALIA