

GRUPPI QUASI-ABELIANI (*)

GUIDO ZAPPA

SUMMARY. — Americanus O. Ore, nuper doctrinam de abstractis classibus in generaliore doctrina de structuris inseruit. Qua nova ratione, classes sunt potius subclassium quam elementorum acervi, ita ut praecipuum momentum detur non studio classium abelianarum, sed classium quas Auctor quasi-abelianas vocat, scilicet in quibus duae subclasses inter se permutari semper possint. Priore hac dissertatione Auctor recenset omnia genera classium quasi-abelianarum, quae e duobus tantum elementis gigni possint, in altera expositurus dissertatione classes quasi-abelianas, quae e finito elementorum numero gigni possint.

Nel recente indirizzo dato da O. ORE alla teoria dei gruppi, secondo il quale le proprietà dei gruppi vengono collegate con le proprietà delle strutture ⁽¹⁾, viene ad assumere grande importanza, in luogo del concetto di sottogruppo invariante o normale di un gruppo, quello di sottogruppo quasi-normale (cioè permutabile con ogni altro sottogruppo del gruppo) ⁽²⁾.

Diverse proprietà dei sottogruppi quasi-normali vengono studiate, nelle memorie citate, dallo stesso ORE, il quale tra l'altro introduce diversi concetti che hanno il parallelo nell'usuale teoria dei sottogruppi normali, come, ad esempio, quello di *quasi-centro* (sottogruppo generato da tutti i sottogruppi ciclici permutabili con ogni sottogruppo del gruppo) che corrisponde al noto concetto di centro.

(*) Nota presentata dall'Accademico Pontificio Ugo Amaldi nella tornata del 20 febbraio 1942.

(1) [1] OYSTEN ORE, *Structures and group theory*, I, Duke Mathematical Journal, 3, pagg. 149-174 (1937).

[2] OYSTEN ORE, *Structures and group theory*, II, Duke Mathematical Journal, 4, pagg. 247-269 (1938).

[3] OYSTEN ORE, *Contributions to the theory of groups of finite order*, Duke Mathematical Journal, 5, pagg. 431-460 (1939).

(2) *Op. cit.* [1] in ⁽¹⁾, pag. 162.

Nel presente lavoro vengono introdotti i gruppi *quasi-abeliani* (gruppi in cui due sottogruppi son sempre permutabili tra loro, ovvero ogni sottogruppo è quasi-normale), che corrispondono ai gruppi abeliani dell'usuale teoria. Il loro studio ha evidentemente interesse, oltre che in sè, anche per tutto l'ordine di idee introdotto dalle ricerche di Ore.

In questo lavoro vengono determinati tutti i possibili tipi di gruppi quasi-abeliani, d'ordine finito o infinito, generabili mediante due elementi. In una nota successiva ci proponiamo di trovare i tipi di gruppi quasi abeliani generabili mediante un numero finito di elementi.

1. DEFINIZIONE. *Un gruppo G si dice QUASI-ABELIANO quando due suoi sottogruppi qualunque sono sempre permutabili tra loro.*

Prima di determinare tutti i gruppi quasi-abeliani con due generatori, esamineremo il caso particolare in cui il sottogruppo ciclico generato da ciascuno dei due generatori, se finito, ha per ordine la potenza di un numero primo.

2. Sia in primo luogo G un gruppo quasi-abeliano, con due generatori, a e b , il primo dei quali sia aperiodico, mentre l'altro abbia periodo p^α (con p primo e α intero positivo) di modo che si abbia $b^{p^\alpha} = 1$.

Mostriamo anzitutto che $\{b\}^{(1)}$ è normale in G . Infatti, nel caso contrario è $a^{-1}ba = \bar{b}$, con \bar{b} non appartenente a $\{b\}$. Allora $\{b, \bar{b}\}$ dovrebbe essere più vasto di $\{b\}$, e dovrebbe avere, d'altra parte, ordine finito, perchè tali sono gli ordini di $\{b\}$ e $\{\bar{b}\}$, e perchè questi due sottogruppi devono essere permutabili tra loro. Ma dovendo essere permutabili anche $\{a\}$ e $\{b, \bar{b}\}$, l'indice in G dell'intersezione $\{a\} \wedge \{b, \bar{b}\}$ tra $\{a\}$ e $\{b, \bar{b}\}$, in $\{b, \bar{b}\}$, dovrebbe eguagliare l'indice di $\{a\}$ in G , il quale indice, non avendo a e \bar{b} potenze non identiche in comune perchè uno d'ordine finito e l'altro aperiodico, è eguale all'ordine di $\{b\}$. E allora l'indice di $\{a\} \wedge \{b, \bar{b}\}$ in $\{b, \bar{b}\}$ verrebbe ad essere eguale all'ordine di $\{\bar{b}\}$, cioè minore dell'ordine di $\{b, \bar{b}\}$, onde l'ordine di $\{a\} \wedge \{b, \bar{b}\}$ sarebbe > 1 . Cioè $\{a\}$ e $\{b, \bar{b}\}$ avrebbero elementi non identici a comune, il che è assurdo, una volta che a è aperiodico, mentre $\{b, \bar{b}\}$ ha ordine finito. Quindi $\{b\}$ è normale in G .

(1) Indicheremo, in generale, con $\{x, y, \dots, z\}$ il sottogruppo generato dagli elementi x, y, \dots, z .

Si avrà pertanto $b^{-1} a^{-1} a b = b^k$, con k intero. Ma dico, di più, che k è divisibile per p . Infatti, se ciò non è, il gruppo generato da a^{-1} e da $b^{-1} a^{-1} b$, contenendo b^k , contiene anche b , che in tal caso è potenza di b^k ; e contenendo anche a , coincide con G . Onde i due sottogruppi $\{a^{-1}\}$ e $\{b^{-1} a^{-1} b\}$ verrebbero ad essere coniugati nel loro congiungente. Ma allora questi due sottogruppi non possono essere permutabili ⁽¹⁾, contro l'ipotesi che G sia quasi-abeliano.

Giungiamo pertanto alla conclusione che, se G è un gruppo abeliano generato da due elementi di cui il primo a , è aperiodico, mentre l'altro, b , ha ordine p^x , si deve avere $a^{-1} b a = b^{1+x}$, con x intero.

3. Consideriamo ora un gruppo quasi-abeliano con due generatori a e b ambedue aperiodici. Possiamo allora distinguere due casi:

a) a e b non hanno potenze non identiche a comune.

Si avrà:

$$[1] \quad b a = a^x b^y$$

perchè $\{a\}$ e $\{b\}$ son permutabili. Inoltre, essendo anche $\{a^x\}$ e $\{b\}$ permutabili, ogni elemento di $\{a^x, b\}$ può porsi sotto la forma $(a^x)^m b^n$, con m ed n interi convenienti. Tra questi elementi, i soli che appartengono ad $\{a\}$ sono quelli con $n=0$, perchè $\{a\}$ e $\{b\}$ hanno per ipotesi a comune la sola identità. Cioè $\{a\} \wedge \{a^x, b\} = \{a^x\}$. Ma dalla [1] segue che in $\{a^x, b\}$ c'è ba , e quindi a , onde a dev'essere potenza di a^x , e di conseguenza si ha $x=\pm 1$. Analogamente si ottiene $y=\pm 1$.

Sia $x=1$, $y=-1$. Si ha allora, dalla [1], $a^{-1} b a = b^{-1}$, onde $(a b)^2 = a b a \bar{b} = a^2$, e di conseguenza G può generarsi mediante gli elementi a ed $a b$, i quali hanno una potenza non identica in comune. Si cade pertanto nel caso β) considerato più sotto. Analogamente si procede se $x=-1$, $y=1$.

Sia invece $x=y=-1$. Allora è $b a = a^{-1} b^{-1} = (b a)^{-1}$, onde ba ha ordine 2. Poichè inoltre $\{a, b\} = \{a, b a\}$, si ha che G può generarsi mediante due elementi, uno d'ordine 2, l'altro aperiodico. Il gruppo è pertanto del tipo considerato nel numero precedente.

Se infine $x=y=1$, il gruppo è abeliano, e precisamente è un gruppo abeliano libero con due generatori.

⁽¹⁾ O. ORB, *op. cit.* [3] in ⁽¹⁾, pag. 434.

β) a e b abbiano potenze non identiche a comune. Allora, se $\{a, b\}$ non è ciclico, contiene elementi d'ordine finito non identici.

Supponiamo infatti $a^m = b^n$, con un m intero positivo ed un n intero, e supponiamo pure che nessuna potenza di a con esponente positivo minore di m sia in $\{b\}$.

Se m ed n hanno almeno un fattore primo p a comune, esisterà una potenza c di a tale che $c^p = a^m$, e una potenza d di b tale che $d^p = b^n$. Allora $\{c, d\}/\{c^m\}$ è un p -gruppo d'ordine p o p^2 , quindi abeliano, e di conseguenza si ha $dc = cd c^{px} d^{py}$, con x e y interi, ossia, tenendo conto del fatto che $d^p = c^p$, si ha $c^{-1} dc = d^{1+p(x+y)}$, quindi $c^{-1} d^p c = d^{p+ p^2(x+y)}$. E poichè d^p , essendo eguale a c^p e potenza di c , è permutabile con c , dev'essere $x+y=0$, da cui segue $dc = cd$. Onde $\{c, d\}$ è abeliano, ed in esso l'elemento cd^{-1} , (il quale è diverso dall'identità perchè c , potenza di a con esponente positivo minore di m , non può coincidere con d che è potenza di b) ha periodo finito p avendo $(cd^{-1})^p = c^p d^{-p} = c^p d^p = 1$. Quindi, se m ed n non son primi tra loro, $G = \{a, b\}$ ha elementi d'ordine finito.

Se m ed n sono invece primi tra loro, consideriamo il gruppo fattoriale $\{a, b\}/\{a^m\}$. Esso è abeliano, come risulta dal lemma che passiamo a dimostrare.

LEMMA. *Un gruppo quasi-abeliano finito è speciale* ⁽¹⁾.

Se H è un gruppo quasi-abeliano finito, non vi possono infatti essere in esso due sottogruppi di SYLOW del medesimo ordine, perchè due tali sottogruppi, pel teorema di SYLOW, sono coniugati in ogni sottogruppo che li contenga, quindi anche nel loro congiungente, e pertanto non possono essere permutabili tra loro, contro l'ipotesi su H . Il lemma è quindi dimostrato.

In base ad esso, il gruppo $\{a, b\}/\{a^m\}$, che evidentemente è quasi-abeliano e finito, risulta speciale. Esso, d'altra parte, è il congiungente dei due gruppi $\{a\}/\{a^m\}$ e $\{b\}/\{b^n\}$, i quali son ciclici e hanno gli ordini primi tra loro. Ma due sottogruppi di ordini primi tra loro di un gruppo speciale sono permutabili elemento per elemento, dunque $\{a, b\}/\{a^m\}$ è un prodotto diretto dei due gruppi ciclici $\{a\}/\{a^m\}$ e $\{b\}/\{b^n\}$, cioè è abeliano.

⁽¹⁾ Chiamiamo, come è d'uso, *speciale* un gruppo finito quando ogni suo sottogruppo di SYLOW è normale.

Da ciò segue $b^{-1} a b = a^{1+mk}$, con k intero. E allora è anche $b^{-1} a^m b = a^{m(1+mk)} = a^{m+m^2k}$. Ma a^m , essendo eguale a b^n , è permutabile con b , onde dev'essere $k=0$, $ab=ba$, cioè $G=\{a, b\}$ abeliano.

E allora, essendo m ed n primi tra loro, esistono due interi x e y tali che $mx+ny=1$. Da ciò segue $(b^x a^y)^n = b^{nx} a^{ny} = a^{mx} a^{ny} = a^{mx+ny} = a$, come anche $(b^x a^y)^m = b^{mx} \cdot a^{my} = b^{mx} \cdot b^{ny} = b^{mx+ny} = b$ e pertanto $b^x a^y$, avendo a e b tra le sue potenze, genera da solo tutto G , che risulta ciclico infinito.

È pertanto dimostrato che, nel caso β), il gruppo $G=\{a, b\}$, se non è ciclico, contiene elementi d'ordine finito.

In quest'ultima ipotesi, gli elementi d'ordine finito di G devono formare un sottogruppo normale N .

Infatti, il congiungente di due sottogruppi finiti di G è ancora un sottogruppo finito di G , perchè i due sottogruppi son tra loro permutabili; quindi gli elementi di G aventi ordine finito formano intanto un sottogruppo. Questo sottogruppo è poi normale, perchè, per la sua stessa definizione, è caratteristico.

Evidentemente N è il più ampio sottogruppo finito di G . Da ciò segue che G/N non ha elementi d'ordine finito, altrimenti, detto M/N il sottogruppo formato da tali elementi, M sarebbe un sottogruppo finito di G più ampio di N .

Pertanto G/N , che è quasi abeliano, ed è generato dagli elementi \bar{a} e \bar{b} omologhi rispettivamente di a e b nell'omomorfismo tra G e G/N , dovrà essere ciclico. Cioè uno dei due elementi \bar{a} e \bar{b} , per esempio \bar{b} , dovrà esser eguale ad una potenza \bar{a}^r di \bar{a} . Di conseguenza è $b = a^r \cdot v$, con v in N . Ma allora G può generarsi coi soli elementi a e v , di cui il primo è aperiodico, mentre l'altro è periodico, appartenendo ad N .

Il sottogruppo $\{v\}$, quale gruppo ciclico finito, è il prodotto diretto di più sottogruppi ciclici il cui ordine è potenza di un numero primo: si avrà cioè $v = v_1^{s_1} v_2^{s_2} \dots v_h^{s_h}$, con v_1, v_2, \dots, v_h elementi il cui periodo è dato rispettivamente da potenze dei numeri primi distinti p_1, p_2, \dots, p_h . Ma $\{a, v_i\}$ ($i=1, \dots, h$), è quasi abeliano e appartiene al tipo considerato nel n. 2; onde si avrà $a^{-1} v_i a = v_i^{1+p_1 x_i}$, ossia $a^{-1} v a = \prod v_i^{s_i(1+p_i x_i)} = v^t$, ove t è un intero conveniente.

In tal caso, G potrà anche generarsi mediante gli elementi a, v_1, v_2, \dots, v_h , ciascuno dei quali è aperiodico, o ha per ordine la potenza di un numero primo.

Concludendo, il caso β) dà luogo ai seguenti possibili tipi di gruppi:

A) Gruppi abeliani liberi con uno o due generatori.

B) Gruppi generabili anche mediante un elemento a aperiodico ed altri elementi v_1, v_2, \dots, v_h , di ordini rispettivamente $p_1^{r_1}, p_2^{r_2}, \dots, p_h^{r_h}$ (p_1, p_2, \dots, p_h primi distinti) tali che $v_i v_j = v_j v_i$ ($i, j = 1, 2, \dots, h$), $a^{-1} v_i a = v_i^{1+p_i^{r_i}}$ ($i = 1, 2, \dots, h$).

4. Dal lemma dimostrato incidentalmente nel numero precedente discende che se G è un gruppo quasi-abeliano generato da due elementi a e b di ordini rispettivamente p^α, q^β , con p e q numeri primi distinti, G è addirittura abeliano.

5. Passiamo infine all'esame del caso in cui G è generato da due elementi a e b , di ordini rispettivamente p^α e p^β , p essendo un numero primo.

Se p^δ è l'ordine dell'intersezione di $\{a\}$ e $\{b\}$, sarà $p^{\alpha+\beta-\delta}$ l'ordine di $G = \{a, b\}$. Ma l'intersezione di $\{a\}$ e $\{b\}$, coincide con l'intersezione di $\{a^p\}$ e $\{b^p\}$, poichè, evidentemente, nè a è in $\{b\}$, nè b in $\{a\}$. Onde necessariamente, l'ordine di $\{a^p, b^p\}$ è $p^{\alpha-1+\beta-1-\delta} = p^{\alpha+\beta-2-\delta}$, e l'indice di $\{a^p, b^p\}$ in $\{a, b\}$ è p^2 . Analogamente si vede che l'indice di $\{a^p, b^p\}$ in $\{a, b^p\}$, come pure in $\{a^p, b\}$, è p , onde $\{a^p, b^p\}$ è normale sia in $\{a, b^p\}$ che in $\{a^p, b\}$, perchè un sottogruppo di indice p di un p -gruppo è sempre normale. Pertanto $\{a^p, b^p\}$ è addirittura normale in $\{a, b\}$, e quindi $\{a, b\}/\{a^p, b^p\}$ è un gruppo d'ordine p^2 .

Ma i gruppi d'ordine p^2 son tutti abeliani; quindi, detti \bar{a} e \bar{b} i corrispondenti di a e b nell'omomorfismo tra $\{a, b\}$ e $\{a, b\}/\{a^p, b^p\}$, si ha $\bar{b} \bar{a} = \bar{a} \bar{b}$, cioè $b a = a b c$, con c in $\{a^p, b^p\}$. Essendo poi $\{a^p\}$ e $\{b^p\}$ permutabili, è $c = (a^p)^x (b^p)^y = a^{px} b^{py}$, onde $b a = a b a^{px} b^{py}$, con x e y interi.

Giungiamo pertanto alla seguente conclusione:

Se G è un gruppo quasi-abeliano generato da due elementi a e b di ordini p^α e p^β (p primo) si ha

$$b a = a b a^{px} b^{py}.$$

Ogni potenza p -esima di un elemento di $\{a, b\}$ si esprime, evidentemente, in funzione di a^p, b^p e dei commutatori di G . Ma ognuno di tali commutatori è in $\{a^p, b^p\}$, perchè ivi è il commutatore di a e b , come risulta dalla [2]. Quindi:

Ogni potenza p -esima di un elemento di $\{a, b\}$ è in $\{a^p, b^p\}$.

Se nè a^p è in $\{b\}$, nè b^p in $\{a\}$, applicando ad $\{a^p, b^p\}$ i ragionamenti fatti intorno ad $\{a, b\}$, si ha che ogni potenza p -esima di un elemento di $\{a^p, b^p\}$, quindi anche ogni potenza p^2 -esima di un elemento di $\{a, b\}$, dev'essere in $\{a^{p^2}, b^{p^2}\}$. Ma ciò è vero anche se, ad esempio, a^p è in $\{b\}$, poichè in tal caso ogni potenza p -esima di un elemento di $\{a, b\}$ è in $\{b^p\}$ e ogni potenza p -esima di un elemento di $\{a^p, b^p\}$ è in $\{b^{p^2}\}$, cioè in $\{b^{p^2}, a^{p^2}\}$. In generale, seguitando si ottiene che:

Ogni potenza p^i -esima (i intero qualunque) di un elemento di $\{a, b\}$ è in $\{a^{p^i}, b^{p^i}\}$.

E poichè tra le potenze p^i -esime degli elementi di $\{a, b\}$ ci sono a^{p^i} e b^{p^i} , i quali generano insieme $\{a^{p^i}, b^{p^i}\}$, si può anche dire che $\{a^{p^i}, b^{p^i}\}$ è il più piccolo sottogruppo che contiene tutte le potenze p^i -esime degli elementi di $\{a, b\}$.

6. Sia ora $\alpha \leq \beta$. Dimostriamo che

Il sottogruppo $\{a^{p^{\beta-1}}, b^{p^{\beta-1}}\}$ appartiene al centro di $\{a, b\}$.

Se a e b hanno una potenza non identica in comune, si ha $\{a^{p^{\beta-1}}, b^{p^{\beta-1}}\} = \{b^{p^{\beta-1}}\} = \{a^{p^{\alpha-1}}\}$, e il teorema è evidente.

Supponiamo pertanto che a e b non abbiano potenze non identiche in comune, di modo che sia $p^{\alpha+\beta}$ l'ordine di $\{a, b\}$. Il gruppo $\{a^{-1}ba, b\}$, non può coincidere con $\{a, b\}$, perchè $\{a^{-1}ba\}$ e $\{b\}$, essendo per ipotesi permutabili, non sono coniugati nel loro congiungente, di modo che a non è in $\{a^{-1}ba, b\}$. Segue che l'ordine di $\{a^{-1}ba, b\}$ è al massimo $p^{\alpha+\beta-1}$. Esso d'altra parte dev'essere $p^{2\beta-\varepsilon}$, ove p^ε è l'ordine dell'intersezione di $\{a^{-1}ba\}$ e $\{b\}$. Da $\alpha \leq \beta$ segue allora $\varepsilon \geq 1$, onde $\{a^{-1}ba\}$ e $\{b\}$ devono avere a comune almeno p elementi, tra cui necessariamente quelli di $\{b^{p^{\beta-1}}\}$ che coincide con $\{(a^{-1}ba)^{p^{\beta-1}}\}$, ossia con $\{a^{-1}b^{p^{\beta-1}}a\}$. Pertanto si ha che a trasforma in sè $\{b^{p^{\beta-1}}\}$, sottogruppo d'ordine p che viene in tal modo ad essere normale in $\{a, b\}$, e quindi, per una nota proprietà dei p -gruppi, fa parte del centro di $\{a, b\}$. Se $\alpha = \beta$, in modo analogo si conclude che $\{a^{p^{\alpha-1}}\}$ appartiene al centro di $\{a, b\}$; ma ciò è vero anche se $\alpha < \beta$, perchè in tal caso $a^{p^{\alpha-1}} = 1$; onde in ogni caso $\{a^{p^{\beta-1}}, b^{p^{\beta-1}}\}$, al pari di $\{a^{p^{\beta-1}}\}$ e di $\{b^{p^{\beta-1}}\}$, appartiene al centro di $\{a, b\}$, c. d. d.

7. Dimostriamo ora che:

Se G è un gruppo quasi-abeliano d'ordine $p^{2\alpha}$ generato da due elementi a e b , ciascuno di ordine p^α , privi di potenze non identiche comuni, tutti e soli gli elementi che sono potenze p^i -esime di elementi di G sono gli elementi di $\{a^{p^i}, b^{p^i}\}$.

Notiamo anzitutto che le potenze p^{a-1} -esime degli elementi di $\{a^p, b^p\}$, sono, giusta il n. 5, in $\{a^{p^a}, b^{p^a}\}$, ossia sono identiche, onde l'ordine degli elementi di $\{a^p, b^p\}$ non supera mai p^{a-1} . Analogamente si vede che l'ordine degli elementi di $\{a^{p^i}, b^{p^i}\}$ non supera p^{a-i} ($1 \leq i \leq \alpha$).

Inoltre, ogni elemento d di $\{a, b\}$ che non sia in $\{a^p, b^p\}$, ha la sua potenza p -esima in $\{a^p, b^p\}$, ma non in $\{a^{p^2}, b^{p^2}\}$. Infatti, se d^p fosse in $\{a^{p^2}, b^{p^2}\}$, per quanto s'è osservato ora, esso avrebbe ordine al più p^{a-2} , onde d avrebbe al più ordine p^{a-1} . D'altra parte, d , non essendo in $\{a^p, b^p\}$, può porsi sotto la forma $a^h b^k$, ove uno almeno dei due numeri h e k , poniamo h , non è divisibile per p . Di conseguenza $\{b, d\}$ contiene b ed a^h , indi a (perchè a è potenza di a^h), cioè coincide con $\{a, b\}$. Ma ciò non può essere se l'ordine di d non supera p^{a-1} , perchè in tal caso l'ordine di $\{d, b\}$ non supererebbe p^{2a-1} , onde $\{d, b\}$ non potrebbe coincidere con $\{a, b\}$. Resta quindi dimostrato che d^p è in $\{a^p, b^p\}$ ma non in $\{a^{p^2}, b^{p^2}\}$.

In base al n. 5, l'indice di $\{a^p, b^p\}$ in $\{a, b\}$ è p^2 , onde gli elementi di $\{a, b\}$ non contenuti in $\{a^p, b^p\}$ sono $p^{2a} - p^{2a-2} = p^{2a-2}(p^2 - 1)$. E, in base alle ipotesi, si vede analogamente che gli elementi di $\{a^p, b^p\}$ non contenuti in $\{a^{p^2}, b^{p^2}\}$ sono $p^{2a-4}(p^2 - 1)$.

Siano ora d e δ due elementi di $\{a, b\}$ non contenuti in $\{a^p, b^p\}$, i quali abbiano la medesima potenza p -esima. Sarà allora $\{d, \delta\}$ un gruppo d'ordine p^{a+1} , che dovrà avere a comune con $\{a\}$ un sottogruppo d'ordine p almeno. Onde $\{a^{p^{a-1}}\}$ e analogamente $\{b^{p^{a-1}}\}$ indi $\{a^{p^{a-1}}, b^{p^{a-1}}\}$ è in $\{d, \delta\}$. D'altra parte, non avendo $\{a^{p^{a-1}}\}$ e $\{b^{p^{a-1}}\}$ elementi non identici comuni, $d^{p^{a-1}}$ non può essere contemporaneamente in $\{a^{p^{a-1}}\}$ e in $\{b^{p^{a-1}}\}$. Supponiamo che $d^{p^{a-1}}$ non sia in $\{a^{p^{a-1}}\}$. Allora $\{d, a^{p^{a-1}}\}$ ha ordine di p^{a-1} e quindi coincide con $\{d, \delta\}$. Onde si ha $\delta = d' \cdot c$, con c elemento (di $\{a^{p^{a-1}}\}$, indi) di $\{a^{p^{a-1}}, b^{p^{a-1}}\}$. Pel n. 6, c è nel centro di $\{a, b\}$, indi è permutabile con d , e pertanto si ha $\delta^p = (d' c)^p = d'^p c^p = d'^p$, perchè $c^p = 1$. Ma l è primo con p , altrimenti $\delta = d' \cdot c$ sarebbe in $\{a^p, b^p\}$ contro l'ipotesi; inoltre da $\delta^p = d'^p$ e da $\delta^p = d'^p$ segue $d'^p = d^p$, cioè $d^{(l-1)p} = 1$, ossia $l-1 \equiv 0 \pmod{p^{a-1}}$. Pertanto è $\delta = d^{1+s \cdot p^{a-1}} \cdot c = d \cdot d^{sp^{a-1}} \cdot c$, con s intero. L'elemento $\gamma = d^{sp^{a-1}} \cdot c$ è in $\{a^{p^{a-1}}, b^{p^{a-1}}\}$, al pari di c e di $d^{p^{a-1}}$. Onde si ha $\delta = d \cdot \gamma$, con γ in $\{a^{p^{a-1}}, b^{p^{a-1}}\}$. Viceversa da $\delta = d \cdot \gamma$, con γ in $\{a^{p^{a-1}}, b^{p^{a-1}}\}$, segue $\delta^p = d^p \gamma^p = d^p$.

Pertanto fissato un elemento d , gli elementi δ i quali hanno la stessa potenza p -esima che d sono tutti e soli gli elementi del tipo $d \cdot \gamma$, con γ in $\{a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\}$: e poichè l'ordine di quest'ultimo sottogruppo è p^2 , segue che sono p^2 gli elementi di $\{a, b\}$, i quali danno luogo alla stessa potenza p -esima.

Essendo $p^{2\alpha-2}(p^2-1)$ gli elementi di $\{a, b\}$ non contenuti in $\{a^p, b^p\}$, saranno $p^{2\alpha-4}(p^2-1)$ le loro potenze p -esime distinte. Esse d'altra parte devono esser tutte in $\{a^p, b^p\}$ senza essere in $\{a^{p^2}, b^{p^2}\}$; e gli elementi di $\{a^p, b^p\}$ non contenuti in $\{a^{p^2}, b^{p^2}\}$ sono esattamente $p^{2\alpha-4}(p^2-1)$. Onde ogni elemento di $\{a^p, b^p\}$ non contenuto in $\{a^{p^2}, b^{p^2}\}$ è potenza p -esima di un elemento di $\{a, b\}$ non contenuto in $\{a^p, b^p\}$.

Dal che si deduce subito il teorema in generale.

8. Passiamo a dimostrare che:

Se G è un gruppo quasi-abeliano d'ordine $p^{\alpha+\beta}$ generato da due elementi a e b d'ordini p^α e p^β ($\alpha \leq \beta$) non aventi potenze non identiche in comune, detto y un qualunque intero $< p^\beta$, tra le potenze di $a^k b$ (k intero qualunque) ve ne è una della forma $a^{kx} b^y$, con x intero conveniente.

Giusta il n. 5, la potenza p^β -esima di $a^k b$ è in $\{a^{p^\beta}, b^{p^\beta}\}$, quindi è identica, onde l'ordine di $a^k b$ divide p^β . D'altra parte quest'ordine deve essere non minore di p^β , poichè $\{a, a^k b\}$ contiene a e b , e coincide quindi con G , onde l'ordine di $a^k b$ è proprio p^β .

Ogni potenza di $a^k b$ ha la forma $a^{kx} b^z$, con $z \leq p^\beta$. Se dimostro che alle p^β potenze di $a^k b$ corrispondono valori z tutti diversi, questi valori saranno tutti e soli gli interi $\leq p^\beta$, e quindi tra essi vi sarà anche il numero y prefissato. Onde il teorema sarà provato.

Tutto si riduce pertanto a dimostrare che non vi possono essere due diverse potenze di $a^k b$, siano $a^{kx} b^y$, $a^{kt} b^y$, che diano luogo al medesimo y . E ciò risulta dal fatto che, altrimenti, del pari che $a^{kx} b^y$ e $a^{kt} b^y$, anche $a^{kx} b^y (a^{kt} b^y)^{-1} = a^{k(x-t)}$ lo sarebbe. Ma $a^k b$, avendo ordine p^β e generando insieme con a tutto G , non può avere potenze non identiche a comune con a . Onde verrebbe ad essere $a^{k(x-t)} = 1$, cioè $a^{kx} = a^{kt}$, quindi anche $a^{kx} b = a^{kt} b$, contro l'ipotesi. Il teorema è pertanto completamente dimostrato.

9. Dimostriamo ora il seguente teorema, che segna il punto culminante della trattazione:

Se G è un gruppo quasi-abeliano con due generatori a e b di ordini p^α e p^β rispettivamente (p primo), esso ha un sottogruppo normale ciclico N , tale che il fattoriale G/N risulti anch'esso ciclico.

Dimostreremo il teorema per induzione, ammettendolo vero per gruppi il cui ordine divide l'ordine di G . Distingueremo vari casi:

I) Presa una qualunque coppia di elementi, che insieme generino tutto G , essi hanno sempre una potenza non identica a comune. Allora, in particolare, ciò deve capitare ad a e b , onde sarà $\{a^{p^{\alpha-1}}\} = \{b^{p^{\alpha-1}}\}$. Posto $\{a^{p^{\alpha-1}}\} = C$, si ha che G/C è un gruppo quasi-abeliano con due generatori costituiti dagli elementi \bar{a} e \bar{b} , che corrispondono ad a e b nell'omomorfismo tra G e G/C , e pertanto per esso vale il teorema. Vale a dire G/C ha un sottogruppo normale N/C ciclico, tale che il fattoriale G/N risulti anch'esso ciclico. Sia δ un elemento generatore di N/C ; vi sarà allora in G/C un elemento γ , tale che $G/C = \{\gamma, \delta\}$.

Siano rispettivamente g e d due elementi di G , cui corrispondono in G/C gli elementi γ e δ . Sarà $g = a^m b^n$ e $d = a^r b^s$, e di conseguenza $\gamma = \bar{a}^m \bar{b}^n$ e $\delta = \bar{a}^r \bar{b}^s$ (m, n, r, s interi convenienti). Non potranno ambedue i numeri m ed r esser divisibili per p , altrimenti si avrebbe $\{\gamma, \delta\} = \{\bar{a}^p, \bar{b}^p\}$, mentre deve essere $\{\gamma, \delta\} = \{\bar{a}, \bar{b}\}$ per ipotesi. Analogamente, n ed s non posson essere ambedue divisibili per p . Ne segue che $\{g, d\}$ contiene a e b , e quindi coincide con G .

Inoltre, dal fatto che m ed r non sono ambedue divisibili per p , segue che è o $\{a, g\} = G$, o $\{a, d\} = G$. Pertanto, stando all'ipotesi formulata in questo caso I), o $\{g\}$ o $\{d\}$ deve contenere $\{a^{p^{\alpha-1}}\}$ che è l'unico sottogruppo d'ordine p di $\{a\}$. Ma anche $\{g\}$ e $\{d\}$ devono per ipotesi avere a comune un sottogruppo d'ordine p , onde, in particolare, $\{d\}$ deve contenere $\{a^{p^{\alpha-1}}\} = C$.

L'elemento δ , generando il sottogruppo normale N/C , è trasformato da ogni elemento di G/C in una sua potenza; onde d è trasformato da ogni elemento di G in un elemento della forma $d^x \cdot c$, con c in C . Ma c , essendo in C è, per quanto s'è visto or ora, potenza di d , quindi d è trasformato in una sua potenza da ogni elemento di G . Segue che $\{d\}$ è un sottogruppo normale ciclico di G e coincide con N ; essendo poi G/N ciclico, ne discende, in questo caso, il teorema.

II) Esistano ora invece due elementi generatori di G , non aventi potenze non identiche a comune. Potremo supporre, senza ledere la generalità, che questi generatori siano a e b . Supponiamo inoltre, in primo luogo $\alpha < \beta$.

Evidentemente, l'ordine di G viene ad essere $p^{\alpha+\beta}$. Se è $\alpha = 1$, $\{b\}$ ha indice p in G , e pertanto è normale in esso, e dà luogo ad un fat-

toriale d'ordine p , quindi ciclico, onde il teorema è dimostrato. Possiamo pertanto supporre $\alpha > 1$.

Il sottogruppo $\{b^{p^{\beta-1}}\}$ è evidentemente normale in G . Posto pertanto $\{b^{p^{\beta-1}}\} = C$, il teorema vale, per ipotesi, per G/C , ossia G/C ha un sottogruppo normale N/C ciclico tale che anche G/N sia ciclico.

Se N è anch'esso ciclico, il teorema è dimostrato. Supponiamo pertanto che N non sia ciclico.

Detti \bar{a} e \bar{b} i corrispondenti di a e b nell'omomorfismo tra G e G/C , si ha che \bar{a} ha ordine $p^\alpha \leq p^{\beta-1}$, e \bar{b} ha ordine $p^{\beta-1}$. D'altra parte $\{\bar{a}, \bar{b}\} = G/C$, quindi, in base al n. 5, ogni elemento di G/C ha un ordine che divide $p^{\beta-1}$.

Detto δ un generatore di N/C dovrà esistere un elemento γ di G/C tale che $\{\gamma, \delta\} = G/C$. Per quanto s'è osservato or ora, sia l'ordine di γ che quello di δ divide $p^{\beta-1}$, cioè sia l'indice di $\{\gamma\}$ che quello di $\{\delta\}$ in G/C è divisibile per $\frac{p^{\alpha+\beta-1}}{p^{\beta-1}} = p^\alpha$. Ma se l'indice di $\{\gamma\}$ in G/C è divisibile per p^α , anche l'ordine di δ lo è.

Sia d un elemento cui corrisponde δ nell'omomorfismo tra G e G/C . Se $\{\delta\}$ contiene C , d genera tutto N , che è ciclico, contro quanto si è supposto. Pertanto $\{d\}$ non contiene C , e di conseguenza b e d non hanno potenze a comune. Segue che $\{b, d\}$ ha ordine $p^{\alpha+\beta}$ (perchè l'ordine di d è divisibile per p^α) e quindi coincide con G . Inoltre è evidente che l'ordine di d è esattamente p^α .

Se il commutatore di b e d è in C , essendo C in $\{b\}$, b è trasformato da d in una sua potenza, e pertanto $\{b\}$ è normale in G . Poichè esso evidentemente dà luogo a un fattoriale ciclico, il teorema è in tal caso provato.

Supponiamo invece che ciò non sia. Si avrà allora $b^{-1}db = d^{1+k} \cdot c$, con c in C e k non divisibile per p^α .

Posto $l = b^{p^{\beta-\alpha}}$, consideriamo il sottogruppo $\{d, l\}$, d'ordine $p^{2\alpha}$, generato dai due elementi d ed l d'ordine p^α . L'elemento $d^k \cdot c$, commutatore di b e c , è contenuto in esso.

In base al teorema del n. 7, applicato a $\{d, l\}$, l'elemento $d^k c$, posto $k = p^n \cdot h$, con h non divisibile per p , e, per quanto s'è detto, $n < \alpha$, è potenza p^n -esima di un elemento $l^x d^y$ contenuto in $\{d, l\}$, ma non in $\{d^p, l^p\}$. Dico inoltre che deve essere y non divisibile per p . Infatti, in caso contrario, si avrebbe $d^k c = (l^x d^y)^{p^n} = l^{x p^n} d^{z p^n}$, con z di-

visibile per p (n. 7), cioè, essendo c nel centro di G , $cd^k = l^{zp^n} d^{zn^n}$, ossia $k = zp^n$, e k sarebbe divisibile per p^{n+1} , contro l'ipotesi.

Detto pertanto u un numero tale che sia $yu \equiv 1 \pmod{p^n}$, che esiste perchè y è primo con p , dovrà esistere, in base al n. 8, un numero r , tale che sia $(l^x d^y)^r = l^{xs} d^{yu} = l^{xs} d$, con s intero conveniente. Inoltre r deve essere non divisibile per p , altrimenti $(l^x d^y)^r$, in base al n. 5, sarebbe in $\{l^y, d^y\}$, indi anche in $\{l, d^y\}$, e ciò non può essere, perchè, mentre l^{xs} è in $\{l, d^y\}$, d non vi è.

Segue che, come $l^{xs} d$ è potenza di $l^x d^y$, così anche $l^x d^y$ è potenza di $l^{xs} d$. E poichè $d^x c$ è potenza di $l^x d^y$, si ha che $d^k c$ è potenza di $l^{xs} d$, poniamo $d^x c = (l^{xs} d)^t$.

Ora, si ha $l^{-1} l^{xs} d l = l^{xs} l^{-1} d l = l^{xs} d \cdot d^k c = (l^{xs} d)^{t+1}$, onde $\xi = l^{xs} d$ è mutato da l in una sua potenza, cioè $\{\xi\}$ è normale in $\{l, \xi\}$. Ma $\{l, \xi\}$ contiene l e $l^{xs} d$, indi d , cioè coincide con G . Inoltre $G/\{\xi\}$ è ciclico, onde il teorema risulta dimostrato anche nel caso II).

III) Conservando l'ipotesi che esistano due elementi, che chiameremo a e b , di ordini p^α e p^β , senza potenze non identiche a comune, tali che $\{a, b\} = G$, supponiamo ora che sia $\alpha = \beta$, cosicchè G avrà ordine $p^{2\alpha}$.

Posto $C = \{a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\}$, consideriamo il gruppo fattoriale G/C , in cui, per l'ipotesi a base del processo d'induzione, vale il teorema.

Esiste pertanto in G/C un sottogruppo N/C ciclico e normale, tale anche G/N sia ciclico. Sia, come al solito, δ un generatore di N/C , e γ un elemento di G/C tale che sia $\{\gamma, \delta\} = G/C$.

Siano poi d e g due elementi di G , cui corrispondono rispettivamente δ e γ nell'omomorfismo tra G e G/C e siano \bar{a} e \bar{b} i corrispondenti di a e b in questo omomorfismo. Sarà $d = a^m b^n$, $g = a^r b^s$, indi anche $\delta = \bar{a}^m \bar{b}^n$, $\gamma = \bar{a}^r \bar{b}^s$, con m, n, r, s interi convenienti. Non potranno contemporaneamente m ed n , nè contemporaneamente r ed s esser divisibili per p , come si vede con un ragionamento analogo a quello fatto nel caso I). Segue che d e g generano insieme tutto G , cioè l'ordine di $\{d, g\}$ è $p^{2\alpha}$. D'altra parte l'ordine di d e quello di g non possono superare p^α (n. 5) quindi l'ordine di ciascuno di essi è esattamente p^α .

L'elemento γ trasforma per ipotesi δ in una sua potenza, quindi si avrà $g^{-1} d g = c d^{k+1}$, con c in C , ossia il commutatore di g e d è cd^k , od anche, notando che $\{g^{p^{\alpha-1}}, d^{p^{\alpha-1}}\} = C$, e che pertanto può porsi

$c = g^{u p^{a-1}} \cdot d^{v p^{a-1}}$ il commutatore di g e d è $g^{u p^{a-1}} d^{v p^{a-1} + k}$. Posto $u p^{a-1} = z$, $v p^{a-1} + k = t$, si ha che, se $t = 0$, d trasforma g in una sua potenza, onde $\{g\}$ è un sottogruppo normale di G con fattoriale ciclico, e il teorema è dimostrato.

Sia invece $t \neq 0$, cioè t non divisibile per p^a . Allora si vede, ricorrendo ai nn. 7 e 8, che $g^z d^t$ è potenza di un elemento della forma $g^w d$. Notando poi che è $g^{-1} g^w d g = g^w g^{-1} d g = g^w d g^z d^t = (g^w d)^{z+1}$, se si chiama x l'esponente da dare a $g^w d$ per ottenere $g^z d^t$, si ottiene che $g^w d$ è trasformata da g in sua potenza. Posto $g^w d = \xi$, si ottiene allora che (g, ξ) , contenendo g e $g^w d$, contiene g e d , e pertanto coincide con G , che in esso $\{\xi\}$ è normale e dà luogo a un fattoriale ciclico, e il teorema è provato.

Più precisamente, si ha che, come discende dalle proprietà dei p -gruppi, G può essere generato da due elementi g e d , il secondo dei quali generi da solo tutto N , legati dalle relazioni

$$d^{p^m} = 1, g^{p^n} = d^{p^s}, g^{-1} d g = d^{1+p^x}$$

con m, n, s, x , interi ≥ 0 tali che $s \leq m$, $x = p^r \cdot k$ (k primo con p), $s + r + 1 \geq m$, $m + r + 1 \geq n$.

La diseuguaglianza $s + r + 1 \geq m$ segue dal fatto che dev'essere $g^{-1} d^{p^s} g = d^{p^s}$, mentre l'altra $m + r + 1 \geq n$ dal fatto che dev'essere $g^{-p^n} d g^{p^n} = d$.

10. Ora possiamo determinare i possibili tipi di gruppi quasi-abeliani con due generatori, lasciando cadere l'ipotesi che ciascuno di essi, se periodico, abbia per ordine la potenza di un numero primo.

Sia in primo luogo G un gruppo quasi-abeliano generato da due elementi a e b , il primo dei quali aperiodico, il secondo di periodo $m = p^a q^b \dots r^v$, con p, q, \dots, r numeri primi distinti.

Allora può porsi $b = b_1 \cdot b_2 \dots b_h$, ove b_1 ha periodo p^a , b_2 periodo q^b , \dots , b_h periodo r^v . Inoltre i gruppi $\{a, b_1\}$, $\{a, b_2\}$, \dots , $\{a, b_h\}$, i quali sottogruppi di G , devono essere quasi-abeliani, e pertanto, in base al n. 2, deve aversi $a^{-1} b a = b_1^{1+p^{x_1}}$, $a^{-1} b_2 a = b_2^{1+q^{x_2}}$, \dots , $a^{-1} b_h a = b_h^{1+r^{x_h}}$, con x_1, x_2, \dots, x_h interi convenienti.

Ma allora G è del tipo B) considerato nel n. 3. Giungiamo pertanto alla conclusione che ogni gruppo quasi-abeliano, che non sia abe-

liano, con due generatori, uno dei quali aperiodico, è del tipo B) considerato nel n. 3.

Si supponga, di più, che uno dei fattori primi di m , poniamo p , sia eguale a 2; allora, conservando a x_1 il significato di poco fa, si ha che x_1 deve esser pari. Se infatti x_1 fosse dispari e $\alpha > 1$, detta l una potenza di b_1 , certo esistente, d'ordine 4, si avrebbe $a^{-1}la = l^{1+2x_1} = l^{-1}$; e allora si avrebbe anche $(al)^2 = alal = a^2$, onde l'intersezione di $\{a\}$ ed $\{al\}$ avrebbe indice 2 in $\{al\}$, mentre $\{a\}$ avrebbe indice 4 in $\{a, al\} = \{a, l\}$, e i sottogruppi $\{a\}$ ed $\{al\}$ non sarebbero permutabili tra loro, contro l'ipotesi. Se poi $\alpha = 1$, può porsi $x_1 = 0$, cioè pari.

Sia invece ora G un gruppo quasi-abeliano generato da due elementi a e b di ordini rispettivamente $m = p^{\alpha_1} q^{\beta_1} \dots r^{\gamma_1}$ e $n = p^{\alpha_2} q^{\beta_2} \dots r^{\gamma_2}$, con p, q, \dots, r numeri primi distinti, e $\alpha_1, \beta_1, \dots, \gamma_1, \alpha_2, \beta_2, \dots, \gamma_2$ interi positivi o nulli.

Allora può porsi $a = a_1 \cdot a_2 \dots a_h$, ove a_1 ha ordine p^{α_1} , a_2 ha ordine q^{β_1} , \dots , a_h ha ordine r^{γ_1} , e $b = b_1 \cdot b_2 \dots b_h$ con b_1 di ordine p^{α_2} , b_2 di ordine q^{β_2} , \dots , b_h di ordine r^{γ_2} . Inoltre, in base al lemma dimostrato al n. 3, G è dato dal prodotto diretto $\{a_1, b_1\} \times \{a_2, b_2\} \times \dots \times \{a_h, b_h\}$. Ciascuno dei gruppi $\{a_i, b_i\}$ ($i = 1, \dots, h$) è del tipo considerato nel n. 9.

Giungiamo pertanto alla conclusione che ogni gruppo quasi-abeliano con due generatori d'ordine finito è prodotto diretto di gruppi del tipo considerato nel n. 9.

11. Rovesciamo ora i risultati sin qui raggiunti, dimostrando che ogni gruppo dei tipi considerati nel numero precedente è quasi-abeliano.

Sia in primo luogo G un gruppo generato da due elementi a e b , il primo dei quali aperiodico, l'altro di periodo $m = p^{\alpha} q^{\beta} \dots r^{\gamma}$, con p, q, \dots, r numeri primi distinti; e supponiamo inoltre che, posto $b = b_1 b_2 \dots b_h$, ove b_1 ha periodo p^{α} , b_2 periodo q^{β} , \dots , b_h periodo r^{γ} , si abbia $a^{-1} b_1 a = b_1^{1+x_1}$, $a^{-1} b_2 a = b_2^{1+x_2}$, \dots , $a^{-1} b_h a = b_h^{1+x_h}$ con x_1, x_2, \dots, x_h interi; e che, se, ad esempio, è $p = 2$, sia x_1 pari.

Vogliamo dimostrare che G è quasi-abeliano. Faremo la dimostrazione nel caso $h = 1$, $m = p^{\alpha}$; il caso generale si tratta allo stesso modo, salvo qualche complicazione formale.

Basterà dimostrare che due qualunque sottogruppi ciclici di G sono tra loro permutabili. Siano rispettivamente $a'' b^s$ e $a' b^u$ i genera-

tori di due sottogruppi ciclici di G : dimostreremo che $\{a^r b^s\}$ e $\{a^t b^u\}$ son tra loro permutabili.

Notiamo anzitutto che è, qualunque sia l'intero v ,

$$(a^r b^s)^v = a^{rv} b^{sv} \text{ con } \mu = \frac{(1+px)^{rv} - 1}{(1+px)^r - 1}$$

ove s'è messo x in luogo di x_1 per semplicità. Se ora si pone $v = p^\alpha$, si vede subito che riesce μ divisibile per p^α , onde si ottiene

$$(a^r b^s)^{p^\alpha} = a^{rp^\alpha}.$$

Inoltre da ciò segue che a^{p^α} , quale potenza di a e di ab , è permutabile con a e con ab , indi anche con b , e pertanto appartiene al centro di G .

Ancora, a^{rp^α} appartiene ad $\{a^r b^s\}$, ed a^{tp^α} appartiene ad $\{a^t b^u\}$; onde a^{rp^α} appartiene all'intersezione di $\{a^r b^s\}$ e $\{a^t b^u\}$. Segue che, una volta dimostrato che $\{a^r b^s\}/\{a^{rp^\alpha}\}$ è permutabile con $\{a^t b^u\}/\{a^{tp^\alpha}\}$, sarà anche dimostrato $\{a^r b^s\}$ esser permutabile con $\{a^t b^u\}$.

Basta quindi dimostrare che è quasi-abeliano un gruppo con due generatori \bar{a} e \bar{b} , di ordini rispettivamente $rt p^\alpha$ e p^α e tali che $\bar{a}^{-1} \bar{b} \bar{a} = \bar{b}^{1+px}$, con x pari nel caso che sia $p=2$.

E ancora, si ha

$$\bar{a}^{-rp^\alpha} \bar{b} \bar{a}^{rp^\alpha} = \bar{b}^{(1+px)p^\alpha} = \bar{b}$$

onde, posto $rt = k \cdot p^\delta$, con k non divisibile per p , \bar{a} è dato dal prodotto di due elementi \bar{a}_1 e \bar{a}_2 , di ordini rispettivamente $p^{\delta+\alpha}$ e k , il secondo dei quali è permutabile con \bar{b} .

Segue che $\{\bar{a}, \bar{b}\} = \{\bar{a}_1, \bar{b}\} \times \{\bar{a}_2\}$; e una volta dimostrato che è quasi-abeliano $\{\bar{a}_1, \bar{b}\}$, risulterà subito che lo è anche $\{\bar{a}, \bar{b}\}$.

Tutto si riduce pertanto a dimostrare che è quasi-abeliano un p -gruppo con due generatori \bar{a}_1 e \bar{b} , di ordini rispettivamente $p^{\delta+\alpha}$ e p^α , tali che $\bar{a}_1^{-1} \bar{b} \bar{a}_1 = \bar{b}^{1+px}$, con x pari nel caso che sia $p=2$.

Poniamo, per semplicità, a in luogo di \bar{a}_1 , b in luogo di \bar{b} , $\mu = \delta + z$, lasciamo cadere le ipotesi che sia $\mu > \alpha$, e che $\{a\}$ e $\{b\}$ abbiano a comune la sola identità.

Basterà dimostrare che sono tra loro permutabili due sottogruppi ciclici generati uno da un elemento della forma $a b^{h p^e}$, l'altro da un elemento della forma $a^{h p^e} b$, con h e k primi con p , bastando, in caso contrario, sostituire ad a e b delle loro potenze convenienti, e a G un sottogruppo conveniente, per ridursi a questo caso.

Inoltre, $a b^{h p^e}$ trasforma, al pari di a , b in $b^{1 + p^e}$, e genera, assieme a b , tutto G . Onde, posto $a' = a b^{h p^e}$, l'elemento $a^{h p^e} b$ può indubbiamente porsi sotto la forma $a'^r b^s$. Tornando a chiamare a l'elemento a' , e notando che, per una ragione addotta poco fa, si può anche qui supporre $s = 1$, posto $r = l p^v$, con l primo con p , si vede che basterà dimostrare, sotto le stesse ipotesi di partenza, che sono permutabili i gruppi ciclici generati da a e da $a^{l p^v} b$.

Evidentemente, l'indice di $\{a\}$ in G eguaglia l'indice in $\{b\}$ dell'intersezione I di $\{a\}$ e $\{b\}$, perchè $\{a\}$ e $\{b\}$ son tra loro permutabili, $\{b\}$ essendo normale in G . Una volta dimostrato che l'indice in $\{a^{l p^v} b\}$ dell'intersezione J di $\{a\}$ e $\{a^{l p^v} b\}$ eguaglia quello di I in $\{b\}$, risulterà che l'indice di J in $\{a^{l p^v} b\}$ eguaglia quello di $\{a\}$ in G ($= \{a, a^{l p^v} b\}$) onde $\{a\}$ e $\{a^{l p^v} b\}$ risulteranno permutabili.

Tutto pertanto si riduce a dimostrare che l'indice di J in $\{a^{l p^v} b\}$ eguaglia quello di I in $\{b\}$; e ciò apparirà evidente una volta che si sarà provato che $(a^{l p^v} b)^{p^y}$, con y intero, è in $\{a\}$ allora e solo allora che b^{p^y} è in $\{a\}$.

Orbene, dalla relazione $a^{-1} b a = b^{1 + p^e}$, segue, posto $r = l p^v$,

$$\begin{aligned} (a^r b)^{p^y} &= a^{r p^y} b^{1 + (1 + p^e)^r + (1 + p^e)^{2r} + \dots + (1 + p^e)^{(p^y - 1)r}} \\ &= a^{r p^y} b^{\frac{(1 + p^e)^{r p^y} - 1}{(1 + p^e)^r - 1}} \end{aligned}$$

Fissiamo l'attenzione sopra l'esponente $\frac{(1 + p^e)^{r p^y} - 1}{(1 + p^e)^r - 1}$ di b nell'ultima espressione. Si ha

$$(1 + p^e)^{r p^y} - 1 = r p^y \cdot p^e + \binom{r p^y}{2} p^{2e} + \dots$$

Posto $x = p^t \cdot \theta$, con θ primo con p , si avrà, ricordando che $r = lp^v$,

$$(1 + px)^{r^{p^y}} - 1 = l\theta p^{t+v+y+1} + \frac{1}{2} (r^{p^y} - 1) l\theta^2 p^{2t+v+y+2} + \dots$$

Evidentemente, se p è dispari, i termini della detta somma successivi al primo hanno rispetto a p un grado maggiore di quello, $t+v+y+1$, del primo; e altrettanto può dirsi se, come si è supposto, per $p=2$, e x pari, cioè $t \geq 1$. Si avrà quindi

$$(1 + px)^{r^{p^y}} - 1 = H \cdot p^{t+v+y+1}$$

con H primo con p . Analogamente si ha

$$(1 + px)^r - 1 = K \cdot p^{t+v+1}$$

con K primo con p ; e di conseguenza

$$\frac{(1 + px)^{r^{p^y}} - 1}{(1 + px)^r - 1} = \frac{H}{K} \cdot p^y$$

ove $\frac{H}{K} = \lambda$ è primo con p . In conclusione

$$(a^r b)^{p^y} = a^{r^{p^y}} b^{\lambda p^y}$$

con λ primo con p .

Ne risulta che $(a^r b)^{p^y}$ è in $\{a\}$ allora e solo allora che $b^{\lambda p^y}$, cioè anche b^{p^y} , è ivi, come si doveva dimostrare. In conclusione, G risulta quasi-abeliano, come si voleva.

12. Sia ora G un gruppo del tipo considerato nel n. 9, generato cioè da due elementi a e b , tali che

$$b^{p^m} = 1, \quad a^{p^n} = b^{p^s}, \quad a^{-1} b a = b^{1+p^x}$$

con m, n, s, x interi positivi, tali che $s \leq m$, $x = p^r \cdot K$ (K primo con p), $s+r+1 \geq m$, $m+r+1 \geq n$.

Dal ragionamento del numero precedente discende intanto che G è quasi-abeliano, se p è dispari; come anche se $p=2$, ed x è pari.

Esaminiamo il caso $p=2$, x dispari. Si ha allora, facendo un calcolo analogo a quello del numero precedente

$$(ab)^{2^y} = a^{2^y} b^{2^{2^y} + 1}$$

se $y > 0$,

$$(ab)^{2^y} = a^{2^y} b^{2^{2^y}}$$

se $y = 0$.

Segue dalle considerazioni del numero precedente che, se G è quasi-abeliano, occorre che, ogniqualvolta sia $(ab)^{2^y}$ in $\{a\}$, anche b^{2^y} sia in $\{a\}$. Ora ciò, nel nostro caso, è possibile se e solo se b^2 è in $\{a\}$.

Se x è dispari, e b^2 è in $\{a\}$, si deve avere $a^{-1} b^2 a = b^2$. Ma d'altra parte è $a^{-1} b^2 a = b^{2(1+2x)} = b^{2+4x}$. Quindi dev'essere $b^4 = 1$, e di conseguenza $x=1$, $a^{-1} b a = b^3$, $b^3 = a^{2^{x-1}}$. Si ha allora $b^{-1} a b = a^{1+2^{x-1}}$, e il gruppo G è il gruppo generalizzato dei quaternioni, quindi hamiltoniano, e pertanto quasi-abeliano.

Giungiamo pertanto alla conclusione che i gruppi di cui al n. 9 sono quasi-abeliani nel caso che p sia dispari; mentre, nel caso $p=2$, detti gruppi sono quasi-abeliani se x è pari. Se poi $p=2$, e x è dispari, un gruppo del tipo di cui al n. 9 è abeliano allora e solo allora che esso è definito dalle relazioni $a^{2^{x-1}} = b^2$, $b^4 = 1$, $a^{-1} b a = b^3$. Inoltre i prodotti diretti di gruppi appartenenti a questi tipi, per valori distinti di p , sono tutti e soli i gruppi quasi-abeliani finiti con due generatori.

È superfluo avvertire che l'esistenza dei gruppi di cui ai nn. 11 e 12 discende dalla teoria dell'ampliamento.

13. Raccogliamo i risultati ottenuti nel seguente

TEOREMA. *Tutti e soli i gruppi quasi-abeliani generabili mediante due soli elementi, non abeliani, rientrano nei tipi seguenti:*

A) Gruppi generati dagli elementi a, b_1, b_2, \dots, b_h , legati dalle relazioni

$$b_1^{p^{\alpha}} = 1, b_2^{q^{\beta}} = 1, \dots, b_h^{r^{\gamma}} = 1 \quad (p, q, \dots, r \text{ numeri primi distinti})$$

$$a^{-1} b_1 a = b_1^{1+p\alpha_1}, a^{-1} b_2 a = b_2^{1+q\alpha_2}, \dots, a^{-1} b_h a = b_h^{1+r\alpha_h}$$

con $\alpha_1, \alpha_2, \dots, \alpha_h$ interi, e inoltre, se p (ad esempio) $= 2$, x_1 pari.

B) Gruppi generabili mediante due elementi a e b , legati dalle relazioni

$$b^{p^n} = 1, a^{p^s} = b^{p^s}, a^{-1} b a = b^{1+p^s}$$

con m, n, s, x interi positivi, tali che $s \leq m, x = p^r k$ (k primo con p), $s + r + 1 \geq m, m + r + 1 \geq n, r \geq 0$ se p è dispari, $r \geq 1$ se $p = 2$.

C) Gruppi generabili mediante due elementi a e b legati dalle relazioni

$$a^{2^n-1} = b^2, b^4 = 1, a^{-2} b a = b^3.$$

D) Prodotti diretti di gruppi del tipo C per gruppi del tipo B corrispondenti a valori dispari distinti di p .

14. OSSERVAZIONE. I nostri risultati sembrano a prima vista rientrare in quello ottenuto da G. A. MILLER ⁽¹⁾ attraverso il seguente teorema: « A necessary and sufficient condition that all the operators of a group which is generated by s and t can be represented in the form $s^p t^q$ is that at least one of these operators is transformed into a power of itself by other ». Ma se si approfondisce la cosa, si vede che il valoroso algebrista americano è in questo caso caduto in una lieve svista. Il teorema ora riportato infatti non è esatto. Consideriamo, ad esempio, il gruppo generato da due elementi a e b , legati dalle relazioni $a^{p^3} = b^{p^3} = 1, b^{-1} a b = a^{1+p}, p$ essendo un numero primo dispari: esso è quasi-abeliano, come risulta dal numero precedente. Esso può essere generato dagli elementi b e $d = b^p a$; e, essendo il gruppo quasi-abeliano, ogni suo elemento può mettersi sotto la forma $b^x d^y$. Si ha $b^{-1} d b = d a^p$, onde il commutatore di b e d è a^p , il quale, giusta il teorema di MILLER, dovrebbe esser potenza di b o di d . Ma a^p , evidentemente, non è potenza di b ; e non è neanche potenza di d , poichè se così fosse $\{d\}$ ed $\{a\}$ avrebbero a comune un sottogruppo d'ordine p^2 e pertanto $\{d, a\}$ avrebbe ordine p^4 , mentre esso, contenendo b^p ed a , deve avere ordine p^5 . Donde l'inesattezza del teorema. Non ci attardiamo ad indicare il punto della dimostrazione ov'è l'errore, poichè esso non può sfuggire ad un lettore che lo ricerchi attentamente.

⁽¹⁾ G. A. MILLER, *Groups whose operators are of the form $s^p t^q$* , Proceedings of the National Academy of Sciences, U. S. A., vol. 13 (1927), pagg. 758-759.