Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei
Matematica e Applicazioni

Guido Zappa

Sui gruppi finiti i cui sottogruppi non normali hanno tutti lo stesso ordine, II

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **14** (2003), n.1, p. 13–21.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_2003_9_14_1_13_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 2003.

Rend. Mat. Acc. Lincei
s. 9, v. 14:13-21 (2003)

Teoria dei gruppi. — *Sui gruppi finiti i cui sottogruppi non normali hanno tutti lo stesso ordine*, II. Nota (*) del Socio GUIDO ZAPPA.

ABSTRACT. — *Finite groups in which all non normal subgroups have the same order*, II. Let p be a prime, n be an integer ≥ 1 and G be a non Abelian and non Hamiltonian finite p-group. G is said to be in $S(p^n)$ if all non normal subgroups of G have order p^n. In a previous *Note* [3] all groups in $S(p^n)$ (p odd, $n \geq 1$), in $S(2)$, and all groups of exponent 4 belonging to $S(4)$ were given. In the present *Note* all groups in $S(2^n)$ ($n \geq 2$) of exponent > 4 are given, and the classification of groups in $S(p^n)$ for all primes p and all integers $n \geq 1$ is completed.

KEY WORDS: p-group; Non normal subgroup; Exponent of a group.

RIASSUNTO. — Sia p un numero primo, n un intero ≥ 1, e G un p-gruppo finito non abeliano e non hamiltoniano. Si dice che G appartiene ad $S(p^n)$ se i sottogruppi non normali di G hanno tutti ordine p^n. In un *Nota* precedente [3] sono stati determinati tutti i gruppi appartenenti a $S(p^n)$ (p dispari, $n \geq 1$), tutti quelli appartenenti ad $S(2)$ e tutti i gruppi di esponente 4 appartenenti ad $S(4)$. Nella presente *Nota* si determinano tutti i gruppi appartenenti ad $S(2^n)$ ($n \geq 2$) e di esponente > 4, e in tal modo è completata la classificazione dei gruppi in $S(p^n)$ per tutti i numeri primi p e per tutti i valori di $n \geq 1$.

INTRODUZIONE

Sia p un numero primo ed n un intero ≥ 1. Sia $S(p^n)$ la classe di tutti i p-gruppi finiti, non abeliani né hamiltoniani, i cui sottogruppi non normali hanno tutti ordine p^n. In una *Nota* precedente [3], avente lo stesso titolo di questa, ho determinato tutti i gruppi G appartenenti ad $S(p^n)$ nei seguenti casi:

1) $p>2$, $n=1$; 2) $p=2$, $n=1$, 3) $p>2$, $n \geq 2$; 4) $p=2$, $n=2$, G di esponente 4.

Nel presente lavoro determino tutti i gruppi appartenenti ad $S(p^n)$ nei casi rimanenti, e precisamente trovo tutti i 2-gruppi appartenenti ad $S(4)$ di esponente ≥ 8, e tutti i gruppi appartenenti ad $S(2^n)$ per ogni $n \geq 3$. Precisamente, per $n=2$ ed esponente 2^m con $m \geq 3$ si ottengono il gruppo generalizzato dei quaternioni d'ordine 16 e i gruppi della forma: $G = \langle a, b \mid a^4 = b^{2^m} = 1, a^{-1}ba = b^{1+2^{m-1}} \rangle$ mentre per $n > 2$ si ottengono solo i gruppi della forma $G = \langle a, b \mid a^{2^n} = b^{2^m} = 1, a^{-1}ba = b^{1+2^{m-1}} \rangle$ con $n \leq m$. Questi risultati sono dati nel Teorema 1. Il Teorema 2 riunisce tutti i risultati delle due *Note* elencando tutti i gruppi appartenenti a $S(p^n)$ per ogni valore del numero primo p e dell'intero $n \geq 1$.

Tutti i gruppi considerati nella *Nota* sono supposti finiti.

Per le proprietà dei p-gruppi usate nelle dimostrazioni vedi [1].

Ringrazio vivamente il *referee* che, coi suoi suggerimenti, mi ha permesso di semplificare il processo dimostrativo.

(*) Presentata nella seduta del 14 marzo 2003.

Esempi notevoli

Definizione. Sia p un numero primo ed n un intero $\geqslant 1$. Un p-gruppo G è detto appartenente alla classe $S(p^n)$ se non è né abeliano né hamiltoniano e tutti i suoi sottogruppi non normali hanno ordine p^n.

Osservazione. Se $G \in S(p^n)$ i sottogruppi non normali di G di ordine p^n sono necessariamente ciclici, perché ogni sottogruppo non ciclico d'ordine p^n è unione insiemistica di sottogruppi di ordine $< p^n$, necessariamente normali, e quindi è normale.

Proposizione 1. *Sia G un 2-gruppo con un solo elemento di ordine 2. Allora $G \in S(2^n)$ se e solo se $n = 2$ e G è il gruppo generalizzato dei quaternioni d'ordine* 16:

$$G = \langle a, b \mid a^4 = 1, b^4 = a^2, a^{-1} ba = b^{-1} \rangle. \tag{1}$$

Dimostrazione. Un 2-gruppo G con un solo sottogruppo d'ordine 2 è ciclico, o è il gruppo dei quaternioni, o è un gruppo generalizzato dei quaternioni. Se $G \in S(2^n)$, G non è né abeliano né hamiltoniano. Poiché il gruppo dei quaternioni è hamiltoniano, segue che G è un gruppo generalizzato dei quaternioni.

Sia G il gruppo generalizzato dei quaternioni di ordine 16, dato dalla (1). Il sottogruppo $\langle a \rangle$ non è normale perché $[a, b] = b^2 \notin \langle a \rangle$. I sottogruppi d'ordine 8 di G sono normali perché massimali. In G c'è un solo sottogruppo d'ordine 2, necessariamente normale. Di conseguenza $G \in S(4)$, cioè $G \in S(2^n)$ per $n = 2$.

Sia ora G un gruppo generalizzato dei quaternioni di ordine 2^t con $t > 4$.
Si avrà

$$G = \langle a, b \mid a^4 = 1, b^{2^{t-2}} = a^2, a^{-1} ba = b^{-1} \rangle.$$

Il sottogruppo $\langle a \rangle$ ha ordine 4 e non è normale perché $[a, b] = b^2 \notin \langle a \rangle$. Il sottogruppo $\langle a, b^{2^{t-3}} \rangle$ ha ordine 8 e non è normale perché $[a, b] = b^2$ non è in $\langle a, b^{2^{t-3}} \rangle$. Pertanto G ha sottogruppi non normali di ordini differenti e non può appartenere ad alcun $S(2^n)$, comunque si prenda n.

Proposizione 2. *Un gruppo del tipo*

$$G = \langle a, b \mid a^{2^n} = b^{2^m} = 1, a^{-1} ba = b^{1 + 2^{m-1}} \rangle$$

con $n \geqslant 2$ e $m \geqslant 3$, appartiene ad $S(2^n)$ se e solo se $n \leqslant m$.

Dimostrazione. In primo luogo supponiamo $n > m$ e dimostriamo che allora $G \notin S(2^n)$. Evidentemente $\langle a \rangle$ non è normale. Inoltre si ha $a^{-2} ba^2 = b^{(1+2^{m-1})^2} = b^{1 + 2^m + 2^{2m-2}} = b$ perché $2m - 2 \geqslant m$, visto che $m \geqslant 3$. Pertanto $a^{2^{n-m}}$ è permutabile con b. Segue che $\langle a^{2^{n-m}} b \rangle$ ha ordine 2^m. Ma si ha $a^{-1} (a^{2^{n-m}} b)\, a = a^{2^{n-m}} b^{1+2^{m-1}}$ che non appartiene ad $\langle a^{2^{n-m}} b \rangle$. Pertanto G ha un sottogruppo non normale $\langle a^{2^{n-m}} b \rangle$ di ordine $2^m \neq 2^n$, e di conseguenza $G \notin S(2^n)$.

Sia ora $n \leqslant m$, e mostriamo che allora $G \in S(2^n)$. Il sottogruppo $\langle a \rangle$, d'ordine 2^n, non è normale. Poiché $|G| = 2^{n+m}$, ogni sottogruppo L di ordine $> 2^n$ incontra $\langle b \rangle$

secondo un sottogruppo di ordine ≥ 2 e quindi contiene $b^{2^{m-1}}$. Ma si ha $b^{2^{m-1}} = [a, b]$, quindi $\langle b^{2^{m-1}} \rangle = G'$, $L \geq G'$ e pertanto L è normale.

Da $[a, b] = b^{2^{m-1}}$ segue $[a^2, b] = [a, b^2] = 1$, e pertanto $\langle a^2, b^2 \rangle$ è contenuto nel centro di G. Ogni sottogruppo ciclico di G di ordine $< 2^n$ è contenuto in $\langle a^2, b^{2^{m-n+1}} \rangle \leq \langle a^2, b^2 \rangle$, e quindi è nel centro di G. Ogni sottogruppo non ciclico di ordine $< 2^n$ è generato da sottogruppi ciclici di ordine $< 2^n$, e di conseguenza è nel centro di G. Pertanto ogni sottogruppo di G di ordine $\neq 2^n$ è normale, e $G \in S(2^n)$.

Sottogruppo degli elementi di ordine ≤ 2 in un gruppo $G \in S(2^n)$

Dalla Proposizione 1 risulta che se $G \in S(2^n)$ e non coincide col gruppo generalizzato dei quaternioni d'ordine 16, in G vi sono almeno due elementi di ordine 2.

Un gruppo appartenente a $S(2^n)$ diverso dal gruppo generalizzato dei quaternioni di ordine 16 verrà detto *di tipo generale.*

Proposizione 3. *Sia G un gruppo appartenente ad $S(2^n)$ con $n \geq 2$ di tipo generale. Gli elementi di G di ordine* ≤ 2 *costituiscono un sottogruppo H di ordine* 4, *contenuto nel centro di G.*

Dimostrazione. Per ipotesi esiste un elemento $a \in G$ d'ordine 2^n con $\langle a \rangle$ non normale. Poiché G è di tipo generale, esiste in G un elemento b di ordine 2, diverso da $a^{2^{n-1}}$. Essendo $n \geq 2$, $\langle a^{2^{n-1}} \rangle$ ed $\langle b \rangle$ sono normali, quindi lo sono anche $a^{2^{n-1}}$ ed b. Ne segue che il sottogruppo $H = \langle a^{2^{n-1}}, b \rangle = \{1, a^{2^{n-1}}, b, a^{2^{n-1}} b\}$ è contenuto nel centro di G.

Il sottogruppo $\langle a, H \rangle$ ha ordine 2^{n+1}, quindi è normale in G e contiene tutti i coniugati di $\langle a \rangle$.

Supponiamo esista un elemento k d'ordine 2 non contenuto in $\langle a, H \rangle$. Allora $\overline{H} = \langle a, k \rangle$ ha ordine 2^{n+1} e quindi è normale, e contiene tutti i coniugati di $\langle a \rangle$. Allora i coniugati di $\langle a \rangle$ sono tutti in $H \cap \overline{H} = \langle a \rangle$, cioè $\langle a \rangle$ è l'unico coniugato di $\langle a \rangle$, contro l'ipotesi. Pertanto H contiene tutti e soli gli elementi di G di ordine ≤ 2, come si voleva.

Proposizione 4. *Sia G un gruppo appartenente ad $S(2^n)$ di tipo generale e di esponente 2^m $(2 \leq n \leq m, 3 \leq m)$, e sia H il sottogruppo generato dagli elementi di ordine* 2. *Allora H contiene il derivato G' di G. G è nilpotente di classe* 2.

Dimostrazione. In base alla Proposizione 3, H ha ordine 4 ed è contenuto nel centro di G. Distinguiamo tre casi

1° *caso*: $m > 3$.

Sia a un elemento di G con $\langle a \rangle$ non normale. Allora a ha ordine 2^n e $\langle a \rangle \cap H = \langle a^{2^{n-1}} \rangle$. Segue che $\langle a, H \rangle$ ha ordine 2^{n+1}, quindi è normale. Sia b un elemento di G con $\langle b \rangle$ normale. Allora anche $\langle b, H \rangle$ è normale. Segue che ogni sottogruppo ciclico di

$\frac{G}{H}$ è normale. Di conseguenza, ogni sottogruppo di $\frac{G}{H}$ è normale, e quindi $\frac{G}{H}$ è abeliano o hamiltoniano. Ma, essendo G di esponente 2^m con $m > 3$, $\frac{G}{H}$ è di esponente 2^{m-1} con $m-1 > 2$. Ne segue che $\frac{G}{H}$ ha elementi di ordine > 4, mentre un 2-gruppo hamiltoniano non ha elementi di ordine > 4. Ne segue che $\frac{G}{H}$ è abeliano, quindi $H \geqslant G'$.

2° *caso*: $n = m = 3$.

Siano $a, b \in G$. Se uno degli elementi a, b, p. es. a ha ordine 4, $\langle a \rangle$ è normale quindi $b^{-1}ab = a$ o $b^{-1}ab = a^3$. Di conseguenza $[a, b] = 1$ o $[a, b] = a^2$. In ogni caso $[a, b]$ ha ordine 1 o 2, quindi è in H.

Siano ora a e b ambedue di ordine 8. Poiché $\langle a, H \rangle$ è normale, si ha $b^{-1}ab = a^{1+2i}k$ con $i = \{0, 1, 2, 3\}$ e con $k \in H$. Ne segue $b^{-1}a^2b = a^{2+4i}k^2 = a^{2+4i}$, cioè $b^{-1}a^2b = a^2$ o $b^{-1}a^2b = a^6$. Pertanto $b^{-2}a^2b^2 = a^2$ onde $(a^2b^2)^2 = a^4b^4$, $(a^2b^2)^4 = 1$. Allora $\langle a^2b^2 \rangle$ è normale perché di ordine $\leqslant 4$. Supponiamo $b^{-1}a^2b = a^6$. Allora $b^{-1}a^2b^2b = a^2b^6$, che non è potenza di a^2b^2, e quindi $\langle a^2b^2 \rangle$ non è normale, contraddizione. Ne segue $b^{-1}a^2b = a^2$, quindi $i \in \{0, 2\}$. Pertanto $b^{-1}ab = ak$ o $b^{-1}ab = a^5k$, cioè $[a, b] = k \in H$ o $[a, b] = a^4k \in H$.

3° *caso*: $n = 2$, $m = 3$.

Siano $a, b \in G$. Se uno di essi, p. es. a, ha ordine 4, si ha $H = \langle a^2, k \rangle$ con k elemento di H d'ordine 2, diverso da a^2. Poiché $\langle a, H \rangle$ ha ordine 8, esso è normale, ossia $b^{-1}ab = a$ o $b^{-1}ab = a^3$, o $b^{-1}ab = ak$, o $b^{-1}ab = a^3k$. In ogni caso $[a, b] \in H$.

Supponiamo ora che a, b abbiano ambedue ordine 8. Allora $\langle a \rangle$ e $\langle b \rangle$ sono ambedue normali, onde $[a, b] \in \langle a \rangle \cap \langle b \rangle$. Se $[a, b]$ ha ordine 4, deve aversi $\langle a \rangle \cap \langle b \rangle = \langle a^2 \rangle = \langle b^2 \rangle$, quindi $[a, b] = a^2 = b^2$ o $[a, b] = a^2 = b^6$, o $[a, b] = a^6 = b^2$, o $[a, b] = a^6 = b^6$. Nel caso sia $[a, b] = a^2 = b^2$, si ha $b^{-1}ab = a^3$, quindi $b^{-1}a^2b = a^6$. Ma è $a^2 = b^2$, quindi $b^{-1}b^2b = b^6$, contraddizione. Allo stesso modo si escludono gli altri casi. Dovrà quindi essere $[a, b]$ di ordine 2, cioè $[a, b] = 1$ o $[a, b] = a^4 = b^4$. In ogni caso $[a, b]$, avendo ordine $\leqslant 2$, è in H cioè $G' \leqslant H$.

COROLLARIO 1. *Sia $G \in S(2^n)$ e di esponente 2^m, di tipo generale $(2 < n, 3 \leqslant m, n \leqslant m)$. Se $a \in G$, a^2 è nel centro di G. Se $a, b \in G$ si ha $(ab)^4 = a^4b^4$. Se $a, b \in G$ e $b = c^2$ con $c \in G$, si ha $(ab)^2 = a^2b^2$. Se $a^{2^r} = b^{2^r} = 1$, è anche $(ab)^{2^r} = 1$.*

DIMOSTRAZIONE. In base alle Proposizioni 3 e 4, G è nilpotente di classe 2 e G' è di esponente 2. Da [1, Hilfsatz III. 1. 3, p. 253], segue $[a^2, b] = [a, b^2] = 1$ e $(ab)^4 = a^4b^4[b, a]^6 = a^4b^4$. Quindi da $a^{2^t} = b^{2^t} = 1$ segue $(ab)^{2^t} = a^{2^t}b^{2^t} = 1$ per $t > 1$. Ciò è poi evidente per $t = 1$.

DETERMINAZIONE DEI GRUPPI DI ESPONENTE 2^m, APPARTENENTI AD $S(2^n)$, DI TIPO GENERALE, GENERABILI MEDIANTE DUE SOLI ELEMENTI

PROPOSIZIONE 5. *Sia G un gruppo di esponente 2^m, appartenente ad $S(2^n)$ di tipo generale, con $2 \leqslant n$, $3 \leqslant m$, $n \leqslant m$, generabile mediante due soli elementi. Allora si ha*

$$G = \langle a, b \mid a^{2^n} = b^{2^m} = 1,\ a^{-1}ba = b^{1+2^{m-1}} \rangle .$$

DIMOSTRAZIONE. Sia $G = \langle c, d \rangle$. Si avrà $[c, d] = k \neq 1$ e $G' = \langle k \rangle$. Poiché $\dfrac{G}{G'}$ è abeliano, possiamo scegliere c e d in modo che $\langle G'c \rangle \cap \langle G'd \rangle = \langle G' \rangle = \langle k \rangle$, quindi $\langle c \rangle \cap \langle d \rangle \leqslant \langle k \rangle$. In base al Corollario 1, uno degli elementi c, d, sia esso d, avrà ordine 2^m. Scegliamo poi c entro la classe laterale $G'c$ in modo che l'ordine di c sia il più piccolo possibile.

Dimostriamo che, sotto questa ipotesi, si ha $\langle c \rangle \cap \langle d \rangle = 1$. Supponiamo che, al contrario, sia $\langle c \rangle \cap \langle d \rangle = \langle k \rangle$. In base alla Proposizione 4, $k^2 = 1$ e k è nel centro di G. Detto 2^s l'ordine di c, si avrà $c^{2^{s-1}} = d^{2^{m-1}} = k$. Deve aversi $2^s \geqslant 4$, altrimenti c avrebbe ordine 2 e sarebbe nel centro di G, quindi è $s \geqslant 2$. Se $s > 2$, si ha $2^{s-1} \geqslant 4$. Allora, per il Corollario 1, è

$$(c^{-1} d^{2^{m-s}})^{2^{s-1}} = c^{-2^{s-1}} d^{2^{m-1}} = k^{-1} k = 1 .$$

Se invece $s = 2$, poiché è $m \geqslant 3$, si ha c permutabile con $d^{2^{m-s}}$, sempre in base al Corollario 1, onde $(c^{-1} d^{2^{m-s}})^2 = (c^{-1} d^{2^{m-2}})^2 = c^{-2} d^{2^{m-1}} = 1$. Si avrà allora $G = \langle c, d \rangle = \langle c^{-1} d^{2^{m-s}}, d \rangle$ con $c^{-1} d^{2^{m-s}}$ di ordine 2^{s-1}, contro l'ipotesi di minimo fatta su C. Possiamo quindi concludere che $\langle c \rangle \cap \langle d \rangle = 1$.

Distinguiamo ora due casi:

1) $n < m$.

Allora $\langle d \rangle$, avendo ordine $2^m \neq 2^n$, è normale, onde $k = [c, d] \in \langle d \rangle$, ossia $d^{2^{m-1}} = k$. Essendo $\langle c \rangle \cap \langle d \rangle = 1$, si ha che $k \notin \langle c \rangle$, quindi $\langle c \rangle$ non è normale. Pertanto si avrà $s = n$, e quindi $c^{-1}dc = dk = d.\ d^{2^{m-1}} = d^{1+2^{m-1}}$. Ne segue

$$G = \langle c, d \mid c^{2^n} = d^{2^m} = 1,\ c^{-1}dc = d^{1+2^{m-1}} \rangle .$$

2) $n = m$.

Avendosi $\langle c \rangle \cap \langle d \rangle = 1$, almeno uno dei sottogruppi $\langle c \rangle$, $\langle d \rangle$ non è normale.

Supponiamo $\langle c \rangle$ non normale e $\langle d \rangle$ normale. Allora $\langle c \rangle$ ha ordine $2^n = 2^m$. Avendosi $\langle d \rangle$ di ordine 2^m, e normale, si ha $d^{2^{m-1}} = k$ e quindi $c^{-1}dc = dk = d^{1+2^{m-1}} = d^{1+2^{n-1}}$ e di conseguenza

$$G = \langle c, d \mid c^{2^n} = d^{2^n} = 1,\ c^{-1}dc = d^{1+2^{n-1}} \rangle .$$

Supponiamo ora invece $\langle c \rangle$ normale e $\langle d \rangle$ non normale. Allora, ragionando come sopra si ottiene

$$G = \langle c, d \mid c^{2^s} = d^{2^n} = 1,\ d^{-1}cd = c^{1+2^{s-1}} \rangle .$$

Ma, in base alla Proposizione 2, se $s < n$ tale gruppo non appartiene ad $S(2^n)$. Dovrà quindi aversi $s = n$, e si ricade nell'alternativa precedente, salvo lo scambio tra c e d.

Supponiamo ora $\langle c \rangle$ e $\langle d \rangle$ ambedue non normali. Allora $s = n$ e $c^{2^{n-1}}$, $d^{2^{n-1}}$ sono due elementi d'ordine 2 diversi da $[c, d]$. Poiché in base alla Proposizione 3, G ha solo tre elementi d'ordine 2, sarà $[c, d] = c^{2^{n-1}} d^{2^{n-1}}$. Essendo $n = m$ e $m \geqslant 3$, si ha $n \geqslant 3$ onde, per il Corollario 1, $c^{2^{n-1}} d^{2^{n-1}} = (cd)^{2^{n-1}}$. Ponendo $cd = f$, si ha $G = \langle c, d \rangle = \langle c, f \rangle$ con $c^{-1} fc = c^{-1} cdc = c(c^{-1} dc) = cdk = (cd)^{1+2^{n-1}} = f^{1+2^{n-1}}$, e si ricade nella prima alternativa, salvo lo scambio di d con f. La proposizione è così dimostrata.

Caratterizzazione dei gruppi appartenenti ad $S(2^n)$, di esponente 2^m $(n \leqslant m)$ di tipo generale, per $n \geqslant 3$

Da [2, p. 55, Teorema 2.3.1 e Lemma 2.1.2] discende la seguente:

Proposizione 6 (Iwasawa). *Sia G un p-gruppo non hamiltoniano. Le seguenti affermazioni su G sono equivalenti:*

a) *Il reticolo $L(G)$ dei sottogruppi di G è modulare;*

b) *I sottogruppi di G sono a due a due permutabili;*

c) *G contiene un sottogruppo abeliano normale A a gruppo quoziente G/A ciclico, ed esistono un elemento $b \in G$ tale che $G = A\langle b \rangle$, ed un intero positivo s tale che $b^{-1}ab = a^{1+p^s}$ con $s \geqslant 2$ se $p = 2$.*

Da [2, p. 94, Teorema 2.5.9] discende la seguente

Proposizione 7 (Baer). *Sia G un p-gruppo e il reticolo $L(G)$ dei sottogruppi di G sia modulare. Allora, se G non è hamiltoniano, esiste un gruppo abeliano A tale che $L(G)$ è isomorfo al reticolo $L(A)$ dei sottogruppi di A.*

Proposizione 8. *Sia G un gruppo appartenente ad $S(2^n)$ di esponente 2^m $(n \leqslant m)$ di tipo generale. Se $n \geqslant 3$, G è generabile mediante due soli elementi a, b, e si ha*

$$G = \langle a, b \mid a^{2^n} = b^{2^m} = 1, a^{-1} ba^{1+2^{m-1}} \rangle .$$

Dimostrazione. Siano $c, d \in G$. Se $\langle c, d \rangle$ è abeliano o hamiltoniano $\langle c \rangle$ e $\langle d \rangle$ sono permutabili. In caso contrario $\langle c, d \rangle \in S(2^n)$, ed avrà un esponente 2^s con $n \leqslant s \leqslant m$. Dalla Proposizione 5 segue

$$\langle c, d \rangle = \langle e, f \mid e^{2^n} = f^{2^s} = 1, e^{-1} fe = f^{1+2^{s-1}} \rangle .$$

In base alla Proposizione 6 si ha che i sottogruppi di $\langle c, d \rangle$ sono a due a due permutabili, quindi anche $\langle c \rangle$ e $\langle d \rangle$ lo sono. Ne segue che tutti i sottogruppi di G sono a due a due permutabili, onde in base alla Proposizione 6 il reticolo $L(G)$ dei sottogruppi di G è modulare. In base alla Proposizione 7, esiste un gruppo abeliano A tale che $L(G)$ è isomorfo ad $L(A)$. Supponiamo che G non sia generabile con due soli elementi.

Allora nemmeno A è generabile mediante due soli elementi, cioè in un sistema di generatori di A vi sono almeno tre elementi indipendenti. Di conseguenza, anche nel sottogruppo M generato dagli elementi d'ordine 2 di A vi sono almeno tre elementi indipendenti, onde l'ordine di M è $\geqslant 8$. Ma allora anche l'ordine del sottogruppo degli elementi di ordine 2 di G è $\geqslant 8$, contro la Proposizione 3. Pertanto G è generabile mediante due soli elementi, onde, in base alla Proposizione 5

$$G = \langle a, b \mid a^{2^n} = b^{2^m} = 1, a^{-1}ba = b^{1+2^{m-1}} \rangle$$

con $n \leqslant m$.

Caratterizzazione dei gruppi di esponente 2^m $(m \geqslant 3)$ appartenenti ad $S(4)$ di tipo generale

Proposizione 9. *Sia G un gruppo di esponente 2^m $(m \geqslant 3)$ appartenente ad $S(4)$, di tipo generale, e sia K il sottogruppo generato dagli elementi di G di ordine $\leqslant 4$. Se G ha almeno tre generatori indipendenti, $K \in S(4)$ ed è della forma*

$$K = Q \times \langle c \rangle$$

con Q gruppo dei quaternioni e c elemento d'ordine 4.

Dimostrazione. Dal Corollario 1 discende che K è costituito da tutti e soli gli elementi di G di ordine $\leqslant 4$. Inoltre, per la Proposizione 5, è $H \leqslant \phi(G)$. Supponiamo che G abbia almeno tre generatori indipendenti. Allora altrettanto avviene per $\dfrac{\overline{G}}{\phi(\overline{G})} = \dfrac{G/H}{\phi(G)/H}$ e quindi anche per $\dfrac{G}{H}$. Ma, in base alla Proposizione 4, $\dfrac{G}{H}$ è abeliano, quindi anche $\dfrac{K}{H}$ ha almeno tre generatori indipendenti. Poiché $H \leqslant \phi(K)$, anche K ha tre generatori indipendenti.

K non può essere abeliano perché in tale caso anche H avrebbe tre generatori indipendenti, contro la Proposizione 3. Non può nemmeno essere hamiltoniano, altrimenti sarebbe prodotto diretto di un gruppo dei quaternioni Q per un 2-gruppo abeliano elementare, e l'elemento d'ordine 2 di Q sarebbe il solo elemento di G d'ordine 2 che sia potenza di elementi di G di ordine $\geqslant 4$, contro la Proposizione 5.

Pertanto $K \in S(4)$.

Sia d un elemento di G di ordine 2^m. Allora $d^{2^{m-2}}$ ha ordine 4 e quindi è in K. Ma essendo $m \geqslant 3$, si ha $2^{m-2} \geqslant 2$, onde $d^{2^{m-2}}$ è nel centro di G. Pertanto in K c'è un elemento d'ordine 4 appartenente al centro. I gruppi di esponente 4 appartenenti a $S(4)$ con almeno tre generatori sono quelli indicati coi nn. 2), 3), 4) nel Teorema 4 di [3]; di essi solo quello indicato col n. 2 ha elementi d'ordine 4 appartenenti al centro. Quindi

$$K = \langle a, b, c \mid a^4 = c^4 = 1, b^2 = a^2, a^{-1}ba = b^{-1}, ac = ca, bc = cb \rangle.$$

Tale gruppo è prodotto diretto di $Q = \langle a, b \rangle$, che è un gruppo dei quaternioni, per $\langle c \rangle$. Il centro di K è $\langle c, H \rangle$, quindi $d^{2^{m-2}} = cx$ con x in H.

Proposizione 10. *Ogni gruppo di esponente 2^m $(m \geqslant 3)$ appartenente ad $S(4)$, di tipo generale è della forma*

$$G = \langle a, b \,|\, a^4 = b^{2^m} = 1, a^{-1}ba = b^{1+2^{m-1}} \rangle .$$

Dimostrazione. Se G non possiede tre generatori indipendenti, è della forma richiesta, in base alla Proposizione 5. Basterà quindi dimostrare che G non può avere tre generatori indipendenti.

Supponiamo che, al contrario, G abbia almeno tre generatori indipendenti. Allora, in base alla Proposizione 8, G contiene il sottogruppo $K = \langle a, b, c \,|\, a^4 = b^4 = 1, b^2 = a^2, a^{-1}ba = b^{-1}, ac = ca, bc = cb \rangle$. Inoltre G contiene un elemento d di ordine 2^m tale che $d^{2^{m-2}}$ sia un elemento d'ordine 4 del centro di K. Sarà allora $d^{2^{m-2}} = ch$ con $h \in H$. Possiamo ridurci al caso $d^{2^{m-2}} = c$. Inoltre $\langle d \rangle$ è normale, onde $a^{-1}da = d$ oppure $a^{-1}da = d^{1+2^{m-1}}$, e analogamente $b^{-1}db = d$ oppure $b^{-1}db = d^{1+2^{m-1}}$. Scambiando eventualmente tra loro gli elementi a, b, ab ci si può ridurre ai due casi seguenti:

1) $a^{-1}da = b^{-1}db = d$,

2) $a^{-1}da = d,\ b^{-1}db = d^{1+2^{m-1}}$;

Si avrà anche $(ad)^4 = a^4d^4 = d^4$, onde $\langle ad \rangle$ ha ordine 2^n, e pertanto è normale. Ma nel caso 1) si ha $[ad, b] = a^2$, e nel caso 2) si ha $[ad, b] = a^2d^{2^{m-1}}$. Ma sia a^2 che $a^2d^{2^{m-1}}$ non appartengono ad $\langle ad \rangle$, quindi $\langle ad \rangle$ non è normale, contraddizione. Pertanto G è generabile con due soli elementi e, in base alla Proposizione 5, è del tipo richiesto.

Conclusioni

Dalle Proposizioni 1, 8 e 10 discende il

Teorema 1. *Le seguenti affermazioni sono equivalenti*:

1) *G è un 2-gruppo di esponente 2^m, appartenente ad $S(2^n)$ con $2 \leqslant n$, $3 \leqslant m$.*

2) *G è uno dei gruppi seguenti*:

a) $G = \langle a, b \,|\, a^4 = 1, b^4 = a^2, a^{-1}ba = b^{-1} \rangle$;

b) $G = \langle a, b \,|\, a^{2^n} = b^{2^m} = 1, a^{-1}ba = b^{1+2^{m-1}} \rangle$ $(2 \leqslant n, 3 \leqslant m, n \leqslant m)$.

Dai Teoremi 1, 2, 3, 4 della *Nota* [3] e dal Teorema 1 di questo lavoro discende il seguente risultato conclusivo:

Teorema 2. *Le seguenti affermazioni sono equivalenti*:

I) *G è un p-gruppo appartenente ad $S(p^n)$*;

II) *G è uno dei gruppi seguenti*:

1) $G = \langle a, b \,|\, a^{p^n} = b^{p^m} = 1, a^{-1}ba = b^{1+p^{m-1}} \rangle$ (*p qualunque*, $n \geqslant 1$, $m \geqslant 2$, $n \leqslant m$);

2) $G = \langle a, b \,|\, a^4 = 1, b^4 = a^2, a^{-1}ba = b^{-1} \rangle$, $(p = 2, n = 2)$;

3) $G = \langle a, b, c \,|\, a^p = b^p = c^p = 1, b^{-1}ab = ac, ac = ca, bc = cb \rangle$, $(p > 2, n = 1)$;

4) $G = \langle a, b, c \mid a^p = b^p = c^{p^m} = 1,\ b^{-1}ab = ac^{p^{m-1}},\ ac = ca,\ bc = cb \rangle$, $(p > 2, n = 1, m > 1)$;

5) $G = \langle a, b, c \mid a^2 = b^4 = 1,\ c^{2^{m-1}} = b^2,\ a^{-1}ba = b^{-1},\ ac = ca,\ bc = cb \rangle$, $(p = 2, n = 1, m > 1)$;

6) $G = \langle a, b, c \mid a^4 = c^4 = 1,\ b^2 = a^2,\ a^{-1}ba = b^{-1},\ ac = ca,\ bc = cb \rangle$, $(p = 2, n = 2)$;

7) $G = \langle a, b, c \mid a^4 = b^4 = 1, c^2 = b^2, a^{-1}ba = b^{-1}, ac = ca, c^{-1}bc = ba^2 \rangle$, $(p = 2, n = 2)$;

8) $G = \langle a, b, c, d \mid a^4 = b^2 = 1, c^2 = d^2 = a^2, b^{-1}ab = a^3, c^{-1}dc = d^3, ac = ca, ad = da, bc = cb, bd = db \rangle$, $(p = 2, n = 1)$;

9) $G = \langle a, b, c, d \mid a^4 = b^4 = 1,\ c^2 = b^2,\ d^2 = a^2,\ a^{-1}ba = b^{-1},\ ac = ca, b^{-1}cb = ca^2,\ a^{-1}da = da^2b^2,\ bd = db,\ c^{-1}dc = db^2 \rangle$, $(p = 2, n = 2)$.

NOTA. Il gruppo n. 4) del suddetto Teorema 2 coincide col gruppo n. 3) del Teorema 1 di [3], salvo il cambiamento del sistema di generatori.

BIBLIOGRAFIA

[1] B. HUPPERT, *Endliche Gruppen I*. Die Grundlehren der mathematischen Wissenschaften, 134, Springer-Verlag, Berlin-Heidelberg-New York 1967.

[2] R. SCHMIDT, *Subgroup Lattices of Groups*. De Gruyter exposition in mathematics, 14, Walter de Gruyter, Berlin, New York 1994.

[3] G. ZAPPA, *Sui gruppi finiti i cui sottogruppi non normali hanno tutti lo stesso ordine*. Rend. Mat. Acc. Lincei, s. 9, v. 13, 2002, 5-16.

Pervenuta il 20 dicembre 2002,
in forma definitiva il 27 gennaio 2003.

Dipartimento di Matematica «U. Dini»
Università degli Studi di Firenze
Viale Morgagni, 67 A - 50134 FIRENZE