REND. SEM. MAT. UNIV. PADOVA, Vol. 122 (2009)

Gruppi fattorizzati da sottogruppi ciclici

ENRICO JABARA (*)

Al professor Federico Menegazzo per il suo 65° compleanno

ABSTRACT - This paper is devoted to a study of groups defined by the presentation

$$G = \langle a, b, c \mid a^b = a^{1+r}, b^c = b^{1+s}, c^a = c^{1+t} \rangle \quad (r, s, t \in \mathbb{Z}).$$

It is proved that $G'' \leq Z(G)$ and that if r, s and t are all $\neq -2, 0$ then G is finite and its order divides $|(r,s)(s,t)(t,r)\rho\sigma\tau|$ where $\rho = (1+r)^{|s|} - 1$, $\sigma = (1+s)^{|t|} - 1$ and $\tau = (1+t)^{|r|} - 1$.

1. Introduzione.

Lo scopo che questo lavoro si prefigge è duplice. In primo luogo si continua lo studio, iniziato in [6], dei gruppi fattorizzati tramite tre (o più) sottogruppi abeliani. In secondo luogo si applicano alcuni dei risultati ottenuti allo studio della famiglia di gruppi definiti dalla seguente presentazione:

$$M(r,s,t) = \langle a, b, c \mid a^b = a^{1+r}, b^c = b^{1+s}, c^a = c^{1+t} \rangle; \qquad r, s, t \in \mathbb{Z}.$$

In [9] Mennicke ha studiato i gruppi $M(t,t,t)$ ed ha dimostrato che se $t \geq 1$ si tratta di gruppi finiti in cui il sottogruppo $\langle a^{t^3}, b^{t^3}, c^{t^3} \rangle$ è normale, abeliano e a quoziente nilpotente. Successivamente Schenkman in [13] ha dimostrato che il secondo derivato di $M(r,s,t)$ è nilpotente di classe al più 3 e che $M(r,s,t)$ è finito se r, s, t sono tutti maggiori di 0. In questo lavoro si dimostra il

(*) Indirizzo dell'A.: Dipartimento di Matematica Applicata, Università di Ca' Foscari, Dorsoduro 3825/e, 30123 Venezia, Italy.

E-mail: jabara@unive.it

2000 *Mathematical Subject Classification*: 20D40 (20F05,17B60).

TEOREMA 1. *Per ogni $r, s, t \in \mathbb{Z}$ il gruppo $G = M(r, s, t)$ è supersolubile e si ha $G'' \leq Z(G)$ e $\gamma_3(G) \leq Z(G')$. In particolare G' è nilpotente di classe al più 2. Inoltre se r, s, t sono tutti diversi da 0 e da -2 allora G è finito e il suo ordine divide*

$$|(r, s)(s, t)(t, r)\rho\sigma\tau|$$

ove $\rho = (1 + r)^{|s|} - 1$, $\sigma = (1 + s)^{|t|} - 1$, $\tau = (1 + t)^{|r|} - 1$ e (m, n) indica il massimo comun divisore tra i due numeri interi m e n.

La dimostrazione del Teorema 1 è ottenuta combinando alcuni risultati più generali riguardanti i gruppi fattorizzati con dei calcoli diretti sui commutatori. Si dimostrerà anche la seguente generalizzazione del Teorema 3 di [13].

PROPOSIZIONE 1. Sia G un gruppo generato da tre suoi sottogruppi A, B e C nilpotenti di classi rispettivamente k_A, k_B e k_C. Se $[A, B] \leq A$, $[B, C] \leq B$ e $[C, A] \leq C$ allora, posto $K = k_A + k_B + k_C$, si ha che il gruppo $\gamma_{K+1}(G)$ risulta nilpotente di classe al più K.

Dalla Proposizione 1 discende che se A, B e C sono sottogruppi abeliani di G allora $\gamma_4(\gamma_4(G)) = \{1\}$; sotto tali ipotesi si può ottenere un risultato più preciso.

PROPOSIZIONE 2. Sia G un gruppo generato da tre suoi sottogruppi abeliani A, B e C. Se $[A, B] \leq A$, $[B, C] \leq B$ e $[C, A] \leq C$ allora G' risulta nilpotente di classe al più 3.

È conveniente riformulare la prima parte del Teorema 1.

PROPOSIZIONE 3. Sia G un gruppo generato da tre suoi sottogruppi ciclici A, B e C. Se $[A, B] \leq A$, $[B, C] \leq B$ e $[C, A] \leq C$ allora G risulta supersolubile e si ha $G'' \leq Z(G)$ e $\gamma_3(G) \leq Z(G')$. In particolare G' risulta nilpotente di classe al più 2.

Le Proposizioni 1, 2 e 3 non si possono estendere al caso di quattro o più sottogruppi; infatti Higman in [4] ha dimostrato che il gruppo

$$\langle a, b, c, d \mid a^b = a^2,\ b^c = b^2,\ c^d = c^2,\ d^a = d^2 \rangle$$

è infinito e privo di sottogruppi di indice finito.

Nel §3 sarà dimostrato un analogo del Teorema 1 valido per gli anelli di Lie.

2. Dimostrazione delle Proposizioni 1 e 2.

DIMOSTRAZIONE DELLA PROPOSIZONE 1. Sia $G = \langle A, B, C\rangle$ con A, B e C soddisfacenti alle ipotesi dell'enunciato. Essendo $AB = BA$, $AC = CA$ e $BC = CB$ si deve avere $G = ABC$. Si ha poi $A^G = A^{ABC} = A^C \leq AC$ e, analogamente, $B^G \leq AB$ e $C^G \leq BC$. Poiché C è normalizzato da A e $\gamma_{k_A+1}(A) = \{1\}$ risulta $\gamma_{k_A+1}(A^G) \leq \gamma_{k_A+1}(AC) \leq C$. Siccome $A^G \trianglelefteq G$ e $\gamma_{k_A+1}(A^G)$ è caratteristico in A^G si ha $\gamma_{k_A+1}(A^G) \trianglelefteq G$ e quindi $\gamma_{k_A+1}(A^G) \leq C_G$. In maniera analoga si dimostra che $\gamma_{k_B+1}(B^G) \leq A_G$ e $\gamma_{k_C+1}(C^G) \leq B_G$.

I tre sottogruppi A_G, B_G e C_G sono normali in G e nilpotenti di classe che non supera rispettivamente k_A, k_B e k_C. Quindi il sottogruppo $L = A_G B_G C_G$ è normale in G e, per il teorema di Fitting (5.2.8 di [12]), nilpotente di classe al più $k_A + k_B + k_C = K$. Posto $\overline{G} = G/L$ in $\overline{G}$ si ha

$$\gamma_{k_A+1}(\overline{A}^{\overline{G}}) = \{1\}, \quad \gamma_{k_B+1}(\overline{B}^{\overline{G}}) = \{1\}, \quad \gamma_{k_C+1}(\overline{C}^{\overline{G}}) = \{1\}$$

e poiché $\overline{G} = \overline{A}\overline{B}\overline{C} = \overline{A}^{\overline{G}}\overline{B}^{\overline{G}}\overline{C}^{\overline{G}}$, ancora per il teorema di Fitting, si conclude che $\overline{G}$ è nilpotente e che la sua classe di nilpotenza non supera $k_A + k_B + k_C = K$. Dunque $\gamma_{K+1}(\gamma_{K+1}(G)) = \{1\}$. □

Per dimostrare la Proposizione 2 si utilizza il seguente risultato.

LEMMA 1. *Sia G un gruppo e A, B e C dei sottogruppi abeliani di G tali che $G = ABC$, $[A,B] \leq A$, $[B,C] \leq B$, $[C,A] \leq C$ e $A \cap B \cap C = \{1\}$. Allora $[G', G', G'] \leq Z(G)$.*

DIM. Sotto le ipotesi dell'enunciato risulta $A_G \cap B_G \leq Z(G)$; infatti essendo A e B abeliani essi sono centralizzati da $A_G \cap B_G$. Sia poi $x \in A_G \cap B_G$ e $y \in C$; poiché A normalizza C si ha $[x,y] \in C$, del resto $A_G \cap B_G \trianglelefteq G$ porge che $[x,y] \in A_G \cap B_G$ e allora $[x,y] \in A_G \cap B_G \cap C = \{1\}$. Quindi $A_G \cap B_G$ centralizza anche C e dunque $A_G \cap B_G \leq Z(G)$.

Ragionando come nella dimostrazione precedente e ricordando che A, B e C sono abeliani, si ottiene $(A^G)' \leq C_G$, $(B^G)' \leq A_G$ e $(C^G)' \leq B_G$.

Per dimostrare l'asserto si distinguono tre casi.

(a) Almeno due dei tre sottogruppi A_G, B_G e C_G risultano identici. Non è restrittivo supporre $A_G = \{1\}$ e $B_G = \{1\}$. Allora $(B^G)' = \{1\}$ e $(C^G)' = \{1\}$ e quindi il sottogruppo normale $N = B^G C^G$ risulta, per il teorema di Fitting, nilpotente di classe al più 2. Siccome G/N è isomorfo a un quoziente di A, che è

abeliano, si ha $G' \leq N$, da cui $[G', G', G'] = \{1\}$ e in questo caso l'asserto è dimostrato.

(b) Uno solo dei tre sottogruppi A_G, B_G e C_G risulta identico.
Non è restrittivo supporre che $C_G = \{1\}$ e dunque A^G è abeliano. In $\overline{G} = G/A_G$ anche $\overline{B}^{\overline{G}}$ è abeliano e quindi, ragionando come nel punto precedente, si ricava che $(G/A_G)'$ è nilpotente di classe al più 2 così come $(G/B_G)'$. Ma allora $[G', G', G'] \leq$ $\leq A_G \cap B_G \leq Z(G)$ e l'asserto è dimostrato.

(c) $A_G \neq \{1\}$, $B_G \neq \{1\}$ e $C_G \neq \{1\}$.
Allora siccome $A_G \cap B_G \cap C_G \leq A \cap B \cap C = \{1\}$, il gruppo G si immerge nel prodotto diretto $(G/A_G) \times (G/B_G) \times (G/C_G)$ e poiché ognuno dei tre fattori del prodotto diretto ricade nel caso considerato nel punto (b) se ne conclude che $[G', G', G'] \leq Z(G)$.

Quindi in ogni caso $[G', G', G'] \leq Z(G)$ e l'asserto è dimostrato. □

A questo punto la dimostrazione della Proposizione 2 è quasi immediata.

DIMOSTRAZIONE DELLA PROPOSIZIONE 2. Poiché A, B e C sono abeliani, risulta $A \cap B \cap C \leq Z(G)$. In $\widehat{G} = G/(A \cap B \cap C)$ si ha $\widehat{A} \cap \widehat{B} \cap \widehat{C} = \{1\}$ e quindi, per il Lemma 1, $[\widehat{G}', \widehat{G}', \widehat{G}'] \leq Z(\widehat{G})$ da cui $[G', G', G'] \leq Z_2(G)$. In ogni gruppo X si ha $[X', Z_2(X)] = \{1\}$, quindi $[G', G', G', G'] \leq$ $\leq [Z_2(G), G'] = \{1\}$ e G' risulta nilpotente di classe al più 3. □

OSSERVAZIONE 1. Con gli stessi medodi utilizzati nella dimostrazione della Proposizione 1 si può far vedere che se $G = \langle A, B, C\rangle$ con A, B e C risolubili di lunghezza derivata rispettivamente d_A, d_B e d_C e tali che $[A, B] \leq A$, $[B, C] \leq B$ e $[C, A] \leq C$, allora anche G è risolubile e la sua lunghezza derivata non supera $2(d_A + d_B + d_C)$. Inoltre, poiché $G = ABC$, se A, B e C sono policiclici, anche G risulta policiclico.

OSSERVAZIONE 2. Se G è un gruppo finito generato da tre sottogruppi ciclici A, B e C tali che $[A, B] \leq A$, $[B, C] \leq B$ e $[C, A] \leq C$, allora, ragionando come nella dimostrazione del Lemma 1 e della Proposizione 2 (e sfruttando il fatto che ogni sottogruppo di A è normalizzato da B, ogni sottogruppo di B è normalizzato da C e ogni sottogruppo di C è normalizzato da A) si può dimostrare che $G'' \leq Z_2(G)$ (e di conseguenza G' risulta nilpotente di classe al più 2). La dimostrazione che $G'' \leq Z(G)$ richiede, come sarà chiaro nel §4, maggiore attenzione.

3. Anelli di Lie.

Da una lettura delle dimostrazioni precedenti è facile convincersi che le Proposizioni 2 e 3 (in analogia a quanto avviene per il Teorema 2 di [13]) valgono anche per gli anelli di Lie (su $\mathbb{Z}$). Più precisamente se $\mathfrak{L}$ è un anello di Lie e $\mathfrak{A}$, $\mathfrak{B}$ e $\mathfrak{C}$ sono suoi sottanelli tali che $\mathfrak{L} = \mathfrak{A} + \mathfrak{B} + \mathfrak{C}$ e $[\mathfrak{A}, \mathfrak{B}] \leq \mathfrak{A}$, $[\mathfrak{B}, \mathfrak{C}] \leq \mathfrak{B}$ e $[\mathfrak{C}, \mathfrak{A}] \leq \mathfrak{C}$ allora

(i) se $\mathfrak{A}$, $\mathfrak{B}$ e $\mathfrak{C}$ sono nilpotenti di classe rispettivamente $k_{\mathfrak{A}}$, $k_{\mathfrak{B}}$ e $k_{\mathfrak{C}}$ allora, detto $K = k_{\mathfrak{A}} + k_{\mathfrak{B}} + k_{\mathfrak{C}}$, si ha $(\mathfrak{L}^{K+1})^{K+1} = \{0\}$;

(ii) se $\mathfrak{A}$, $\mathfrak{B}$ e $\mathfrak{C}$ sono abeliani allora $[\mathfrak{L}', \mathfrak{L}', \mathfrak{L}'] \leq Z_2(\mathfrak{L})$ e quindi, in particolare, $\mathfrak{L}'$ è nilpotente di classe al più 3.

Ove, come d'uso si pone $\mathfrak{L}^1 = \mathfrak{L}$, $\mathfrak{L}^n = [\mathfrak{L}^{n-1}, \mathfrak{L}]$, $\mathfrak{L}' = \mathfrak{L}^2$ e $\mathfrak{L}'' = [\mathfrak{L}', \mathfrak{L}']$.

Si supponga ora che $\mathfrak{A}$, $\mathfrak{B}$ e $\mathfrak{C}$ siano generati, come anelli, da $\mathfrak{a}$, $\mathfrak{b}$ e $\mathfrak{c}$ rispettivamente. Se si ha $[\mathfrak{a}, \mathfrak{b}] = r\mathfrak{a}$, $[\mathfrak{b}, \mathfrak{c}] = s\mathfrak{b}$, $[\mathfrak{c}, \mathfrak{a}] = t\mathfrak{a}$ con $r, s, t \in \mathbb{Z}$, l'anello di Lie generato da $\mathfrak{a}$, $\mathfrak{b}$ e $\mathfrak{c}$ sarà denotato con $L(r, s, t)$. Utilizzando l'identatà di Jacobi $[\mathfrak{a}, \mathfrak{b}, \mathfrak{c}] + [\mathfrak{b}, \mathfrak{c}, \mathfrak{a}] + [\mathfrak{c}, \mathfrak{a}, \mathfrak{b}] = 0$, si ricava

$$rs\mathfrak{a} + st\mathfrak{b} + rt\mathfrak{c} = 0. \tag{1}$$

da cui (commutando rispetto $\mathfrak{a}$, $\mathfrak{b}$ e $\mathfrak{c}$) si ottiene

$$rst\mathfrak{a} = rt^2\mathfrak{c}, \qquad rst\mathfrak{b} = r^2s\mathfrak{a}, \qquad rst\mathfrak{c} = s^2t\mathfrak{b}. \tag{2}$$

Commutando (2.b) tramite $\mathfrak{b}$ e $\mathfrak{a}$, (2.c) tramite $\mathfrak{c}$ e $\mathfrak{b}$ e (2.a) tramite $\mathfrak{a}$ e $\mathfrak{c}$, si ottiene

$$r^3s\mathfrak{a} = 0, \qquad s^3t\mathfrak{b} = 0, \qquad rt^3\mathfrak{c} = 0, \tag{3}$$

$$r^2st\mathfrak{a} = 0, \qquad rs^2t\mathfrak{b} = 0, \qquad rst^2\mathfrak{c} = 0. \tag{4}$$

Grazie alle (4) si ricava immediatamente che se $rst \neq 0$ allora $L(r, s, t)$ è finito e il suo ordine non supera $(rst)^4$.

Moltiplicando le relazioni (2) rispettivamente per t, r e s si ricava

$$rst^2\mathfrak{a} = 0, \qquad r^2st\mathfrak{b} = 0, \qquad rs^2t\mathfrak{c} = 0. \tag{5}$$

Da (2) applicando le (4) si ottiene

$$rs^2t\mathfrak{a} = 0, \qquad rst^2\mathfrak{b} = 0, \qquad r^2st\mathfrak{c} = 0. \tag{6}$$

Moltiplicando (1) rispettivamente per rs, rt e sr e tenendo conto delle (4) si ha anche

$$r^2s^2\mathfrak{a} = 0, \qquad s^2t^2\mathfrak{b} = 0, \qquad r^2t^2\mathfrak{c} = 0. \tag{7}$$

Si può quindi enunciare il

TEOREMA 2. *Se* $\mathfrak{L} = L(r,s,t)$ *allora si ha*

(a) $\mathfrak{L}'' \leq Z(\mathfrak{L})$;
(b) $[\mathfrak{L}^3, \mathfrak{L}^2] = \{0\}$.

Inoltre se $rst \neq 0$ *allora* $\mathfrak{L}$ *è finito e il suo ordine divide* $|(r,s,t)^3 r^2 s^2 t^2|$ *ove* (r,s,t) *denota il massimo comun divisore dei numeri interi r, s e t.*

DIM. Siccome $\mathfrak{L}'$ è generato da $r\mathfrak{a}$, $s\mathfrak{b}$ e $t\mathfrak{c}$ si ha che $\mathfrak{L}''$ è generato da $r^2 s\mathfrak{a}$, $s^2 t\mathfrak{b}$ e $rt^2\mathfrak{c}$. Sfruttando le uguaglianze (3) si ottiene

$$[r^2 s\mathfrak{a}, \mathfrak{b}] = r^3 s\mathfrak{a} = 0, \quad [s^2 t\mathfrak{b}, \mathfrak{c}] = s^3 t\mathfrak{b} = 0, \quad [rt^2\mathfrak{c}, \mathfrak{a}] = rt^3\mathfrak{c} = 0,$$

mentre dalle uguaglianze (5) si ricava

$$[r^2 s\mathfrak{a}, \mathfrak{c}] = -r^2 st\mathfrak{c} = 0, \quad [s^2 t\mathfrak{b}, \mathfrak{a}] = -rs^2 t\mathfrak{a} = 0, \quad [rt^2\mathfrak{c}, \mathfrak{b}] = -rst^2\mathfrak{b} = 0,$$

e l'asserto (a) è dimostrato.

Siccome $\mathfrak{L}^3$ è generato da $r^2\mathfrak{a}$, $s^2\mathfrak{b}$, $t^2\mathfrak{c}$, $rs\mathfrak{a}$, $st\mathfrak{b}$, $rt\mathfrak{c}$, ricordando (3), (4) e (7) si ottiene:

$$\begin{array}{lll}
[r^2\mathfrak{a}, s\mathfrak{b}] = r^3 s\mathfrak{a} = 0, & [s^2\mathfrak{b}, t\mathfrak{c}] = s^3 t\mathfrak{b} = 0, & [t^2\mathfrak{c}, r\mathfrak{a}] = rt^3\mathfrak{c} = 0, \\
[r^2\mathfrak{a}, t\mathfrak{c}] = -r^2 t^2\mathfrak{c} = 0, & [s^2\mathfrak{b}, r\mathfrak{a}] = -r^2 s^2\mathfrak{a} = 0, & [t^2\mathfrak{c}, s\mathfrak{b}] = -s^2 t^2\mathfrak{b} = 0, \\
[rs\mathfrak{a}, s\mathfrak{b}] = r^2 s^2\mathfrak{a} = 0, & [st\mathfrak{b}, t\mathfrak{c}] = s^2 t^2\mathfrak{b} = 0, & [rt\mathfrak{c}, r\mathfrak{a}] = r^2 t^2\mathfrak{c} = 0, \\
[rs\mathfrak{a}, t\mathfrak{c}] = -rst^2\mathfrak{c} = 0, & [st\mathfrak{b}, r\mathfrak{a}] = -r^2 st\mathfrak{a} = 0, & [rt\mathfrak{c}, s\mathfrak{b}] = -rs^2 t\mathfrak{b} = 0
\end{array}$$

e quindi anche l'asserto (b) è dimostrato.

Si supponga quindi $rst \neq 0$ e si consideri il sottoanello $\mathfrak{N}$ di $\mathfrak{L}$ generato dagli elementi $rs\mathfrak{a}$, $st\mathfrak{b}$ e $rt\mathfrak{c}$. Una semplice verifica mostra che $\mathfrak{N}$ è un ideale di $\mathfrak{L}$, che $\mathfrak{L}/\mathfrak{N}$ è finito e che il suo ordine divide $r^2 s^2 t^2$.

Per dimostrare l'asserto è quindi sufficiente dimostrare che $\mathfrak{N}$ è finito e che il suo ordine divide r^3, s^3 e t^3.

Siano

- $\mathfrak{T}_1$ il sottoanello di $\mathfrak{N}$ generato da $rst\mathfrak{c}$;
- $\mathfrak{T}_2$ il sottoanello di $\mathfrak{N}$ generato da $rst\mathfrak{a}$;
- $\mathfrak{T}_3$ il sottoanello di $\mathfrak{N}$ generato da $rst\mathfrak{b}$;

Utilizzando le relazioni (2) una verifica diretta porge che $\mathfrak{T}_1$, $\mathfrak{T}_2$ e $\mathfrak{T}_3$ sono ideali di $\mathfrak{N}$ (anzi di $\mathfrak{L}$).

Dalla relazione (1) si ottiene $rs\mathfrak{a} = -st\mathfrak{b} - rt\mathfrak{c}$ e quindi $\mathfrak{N}$ è generato come anello da $st\mathfrak{b}$ e $rt\mathfrak{c}$. Siccome $s(rt\mathfrak{c}) = rst\mathfrak{c} \in \mathfrak{T}_1$ e $s(st\mathfrak{b}) = s^2 t\mathfrak{b} = rst\mathfrak{c} \in \mathfrak{T}_1$ se ne deduce che $\mathfrak{N}/\mathfrak{T}_1$ è finito e che il suo ordine divide s^2. Dalla relazione (5.c) si ricava $s(rst)\mathfrak{c} = rs^2 t\mathfrak{c} = 0$ e quindi $\mathfrak{T}_1$ è finito e il suo ordine divide s. Dunque $|\mathfrak{N}|$ (è finito e) divide s^3.

Un ragionamento analogo applicato a $\mathfrak{T}_2$ (a $\mathfrak{T}_3$) mostra che $\mathfrak{N}$ è anche un divisore di t^3 (di r^3).

Il Teorema è quindi dimostrato. □

Se $r = s = t$ dalle relazioni (2) si ricava $t^3\mathfrak{a} = t^3\mathfrak{b} = t^3\mathfrak{c}$ e moltiplicando per t la (1) (che è diventata $t^2\mathfrak{a} + t^2\mathfrak{b} + t^2\mathfrak{c} = 0$) si ottiene

$$3t^3\mathfrak{a} = 3t^3\mathfrak{b} = 3t^3\mathfrak{c} = 0. \tag{8}$$

Tenendo conto che (3) porge $t^4\mathfrak{a} = t^4\mathfrak{b} = t^4\mathfrak{c} = 0$ si possono dare due casi

- 3 non divide t; allora $L(t,t,t)$ ha ordine t^8 ed è nilpotente di classe 3,
- 3 divide t; allora $L(t,t,t)$ ha ordine $3t^8$ ed è nilpotente di classe 4.

Si osservi che, in generale, $M(t,t,t)$ non è nemmeno nilpotente (infatti esso risulta finito e nilpotente se e solo se $t = 2$ o $t = -3$); si può però considerare il quoziente $RM(t,t,t)$ di $M(t,t,t)$ tramite il suo residuale nilpotente (ovvero l'ultimo termine della serie centrale discendente).

TABELLA 1.

	$L(t,t,t)$		$RM(t,t,t)$	
t	ordine	classe	ordine	classe
2	2^8	3	2^{11}	4
3^n	3^{8n+1}	4	3^{8n+1}	4
p^n, $p^n \neq 2$, $p \neq 3$	p^{8n}	3	p^{8n}	3
6	$2^8 \cdot 3^9$	4	$2^{14} \cdot 3^9$	5
12	$2^{16} \cdot 3^9$	4	$2^{16} \cdot 3^9$	4
10	$2^8 \cdot 5^8$	3	$2^{11} \cdot 5^8$	4
20	$2^{16} \cdot 5^8$	3	$2^{16} \cdot 5^8$	3
14	$2^8 \cdot 7^8$	3	$2^{17} \cdot 7^8$	6
28	$2^{16} \cdot 7^8$	3	$2^{16} \cdot 7^8$	3
30	$2^8 \cdot 3^9 \cdot 5^8$	4	$2^{20} \cdot 3^9 \cdot 5^8$	7
60	$2^{16} \cdot 3^9 \cdot 5^8$	4	$2^{16} \cdot 3^9 \cdot 5^8$	4
42	$2^8 \cdot 3^9 \cdot 7^8$	4	$2^{11} \cdot 3^9 \cdot 7^8$	4
510	$2^8 \cdot 3^9 \cdot 5^8 \cdot 17^8$	4	$2^{32} \cdot 3^9 \cdot 5^8 \cdot 17^8$	11

Utilizzando il software GAP e i calcoli svolti sopra si ottiene la Tabella 1. I dati riportati in tale tabella suggeriscono che (a parte il caso eccezionale in cui t è il doppio di un numero dispari) vi sia una buona corrispondenza tra i due tipi di struttura.

Per l'esatto ordine di $M(t,t,t)$ e $RM(t,t,t)$ si veda [9] e l'Osservazione 3.

4. Dimostrazione della Proposizione 3.

L'analogo nei gruppi dell'identità di Jacobi è l'identità Hall-Witt (si veda il Teorema 2.2.3.i di [3] o il 5.1.5.iv di [12])

$$[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x=1,$$

o, equivalentemente,

$$[x,y,z^x][z,x,y^z][y,z,x^y]=1.$$

Questa identità, anche se non è maneggevole come quella di Jacobi, costituisce uno strumento essenziale per lo studio dei gruppi $M(r,s,t)$ e dei loro quozienti. Infatti, posto $\rho=(1+r)^{|s|}-1$, $\sigma=(1+s)^{|t|}-1$ e $\tau=(1+t)^{|r|}-1$, si perviene al seguente risultato.

LEMMA 2. *Sia $G=\langle a,b,c\rangle$ un gruppo isomorfo a un quoziente di $M(r,s,t)$ con r,s,t numeri interi tutti maggiori di 0. Allora si ha:*

(1) $a^{(1+r)\rho}b^{(1+s)\sigma}c^{(1+t)\tau}=1$;
(2) $a^{r^2\rho}=1$, $b^{s^2\sigma}=1$, $c^{t^2\tau}=1$;
(3) $a^{st\rho}=1$, $b^{rt\sigma}=1$, $c^{rs\tau}=1$;
(4) $a^{r\rho}\in\langle b\rangle$, $b^{s\sigma}\in\langle c\rangle$, $c^{t\tau}\in\langle a\rangle$.

DIM. (1) si ottiene direttamente dall'identità di Hall-Witt mentre (2) e (3) si ottengono da (1) tramite alcuni calcoli sui commutatori (per i particolari si vedano i lavori [7] e [1] nonché la dimostrazione del Lemma 7).

Per dimostrare (4) si pone $x=a^\rho$, $y=b^\sigma$ e $z=c^\tau$. Per il punto (1) si ha $x^{1+r}z^{1+t}\in\langle b\rangle$ e quindi $x^{1+r}z^{1+t}=(x^{1+r}z^{1+t})^b$. Dal punto (2) discende che $x^{r^2}=1$, si può quindi scrivere $x^r=[x,b]=z^{1+t}(z^{-(1+t)})^b$ e siccome $z^{1+t}(z^{-(1+t)})^b=[z^{-(1+t)},b]\in B$ se ne conclude che $x^r\in\langle b\rangle$. In modo analogo si prova che $y^s\in\langle c\rangle$ e $z^t\in\langle a\rangle$. □

OSSERVAZIONE 3. Il Lemma 2 spiega in parte l'eccezionalità del caso $M(2,2,2)=RM(2,2,2)$. Infatti mentre in generale t^2 divide $\tau=(1+t)^{|t|}-1$ ma t^3 non lo divide, se $t=2$ si ha che $2^3=3^2-1$.

Inoltre in [9] Mennicke ha determinato l'esatto ordine di $M(t,t,t)$ (a parte un errore nel caso un cui t è pari). Si ha:

$$|M(t,t,t)| = \begin{cases} t^2\tau^3 & \text{se } (3,t)=1 \\ 3t^2\tau^3 & \text{se } (3,t)=3. \end{cases}$$

Da ciò si deduce facilmente che se $\tau = \tau_1\tau_2$ con $\pi(\tau_1) = \pi(t)$ e $(t,\tau_2)=1$ allora

$$|RM(t,t,t)| = \begin{cases} t^2\tau_1^3 & \text{se } (3,t)=1 \\ 3t^2\tau_1^3 & \text{se } (3,t)=3. \end{cases}$$

OSSERVAZIONE 4. Non è difficile dimostrare che

$$M(r,s,t) \simeq M(s,t,r) \simeq M(t,r,s)$$

ma, in generale, $M(r,s,t) \not\simeq M(r,t,s)$. Ad esempio $M(1,2,3)$ ha ordine 234 mentre $M(1,3,2)$ ha ordine 210.

Oltre all'Osservazione 4 e alcune identità sui commutatori enunciate nei Lemmi 2.2.2 e 2.2.4 di [3], che saranno adoperate senza un esplicito richiamo, nella dimostrazione della Proposizione 3 si utilizzano anche i seguenti lemmi.

LEMMA 3. *Sia G un gruppo generato da tre suoi sottogruppi ciclici A, B e C. Se $[A,B] \le A$, $[B,C] \le B$ e $[C,A] \le C$ allora $A\cap B$, $B\cap C$ e $C\cap A$ sono sottogruppi normali di G e si ha $[(A\cap B)(B\cap C)(C\cap A), G] \le A\cap B\cap C$. In particolare $A\cap B$, $B\cap C$ e $C\cap A$ sono contenuti in $Z_2(G)$ e se $A\cap B\cap C = \{1\}$ essi sono contenuti in $Z(G)$.*

DIM. Il sottogruppo $A\cap B$ è centralizzato da A e da B. Siccome C normalizza B e B è ciclico, ne segue che C normalizza $A\cap B$ e dunque $A\cap B \trianglelefteq G$. In maniera analoga si prova che $B\cap C \trianglelefteq G$ e $C\cap A \trianglelefteq G$.

Se $A\cap B\cap C = \{1\}$ allora, se si procede come nella prima parte della dimostrazione del Lemma 1, si prova che $[A\cap B, G] = \{1\}$, $[B\cap C, G] = \{1\}$ e $[C\cap A, G] = \{1\}$. Dunque $[(A\cap B)(B\cap C)(C\cap A), G] \le A\cap B\cap C$ e siccome $A\cap B\cap C \le Z(G)$ l'asserto è dimostrato. □

LEMMA 4. *Sia G un gruppo isomorfo a un quoziente di $M(r,s,t)$ con $r,s,t \in \mathbb{Z}$ tutti maggiori di 0. Se $Z(G) = \{1\}$ allora G è metabeliano.*

DIM. Il Lemma 3 ed il fatto che $Z(G) = \{1\}$ porgono che

$$A\cap B = B\cap C = C\cap A = \{1\}.$$

Quindi, per il punto (4) del Lemma 2, $a^{r\rho} = b^{s\sigma} = c^{t\tau} = 1$. Si conclude in quanto $G' = \langle a^r, b^s, c^t\rangle$ e $G'' = \langle a^{r\rho}, b^{s\sigma}, c^{t\tau}\rangle$. □

LEMMA 5. *Sia $P = \langle x \rangle$ un gruppo ciclico di ordine p^n e sia A un sottogruppo ciclico di* $\mathrm{Aut}(P)$ *di ordine p^k. Allora esiste un opportuno $\alpha \in A$ che genera A con $x^\alpha = x^\ell$ tale che*

(1) *se $p > 2$ allora $\ell = 1 + p^{n-k}$;*
(2) *se $p = 2$ allora si possono dare i seguenti casi*
   (i) $\ell = 1 + 2^{n-k-1}$,
   (ii) $\ell = -1 + 2^{n-k-1}$,
   (iii) $k = 1$ e $\ell = -1$.

DIM. L'asserto discende facilmente dal Lemma 5.4.1 di [3] e da semplici considerazioni aritmetiche. □

È conveniente dimostrare a parte che la Proposizione 3 è valida nel caso dei p-gruppi.

LEMMA 6. *Sia G un p-gruppo (finito) fattorizzato tramite tre sottogruppi ciclici A, B e C tali che $[A,B] \leq A$, $[B,C] \leq B$ e $[C,A] \leq C$. Allora $G'' \leq Z(G)$ e $\gamma_3(G) \leq Z(G')$.*

DIM. Sia $A = \langle a \rangle$, $B = \langle b \rangle$ e $C = \langle c \rangle$ con $a^b = a^{1+r}$, $b^c = b^{1+s}$ e $c^a = c^{1+t}$. Si osservi che, per ogni $i,j,k \in \mathbb{Z}$, si ha $(a^i)^b = (a^i)^{1+r}$, $(b^j)^c = (b^j)^{1+s}$ e $(c^k)^a = (c^k)^{1+t}$. Si può quindi supporre (rimpiazzando eventualmente a, b e c con opportune loro potenze) che gli automorfismi indotti per coniugio da a, b e c rispettivamente su C, A e B abbiano la forma descritta dal Lemma 5.

Se $K \in \mathbb{N}$ e $K = \pm p^n + Hp^{n+1}$ (con $H, n \in \mathbb{N}$) si scriverà $K = \pm p^n + \mathcal{O}(n)$ e, quando non vi sia possibilità di confusione, $K = \pm p^n + \mathcal{O}$.

Tenendo presente che

$$G' = \langle a^r, b^s, c^t \rangle, \qquad G'' = \langle a^{r\rho}, b^{s\sigma}, c^{t\tau} \rangle$$

e

$$[G,G,G] = \langle a^{r^2}, b^{s^2}, c^{t^2}, a^\rho, b^\sigma, c^\tau \rangle$$

si devono considerare vari casi.

I° Caso. $r = p^\alpha$, $s = p^\beta$ e $t = p^\gamma$ ($\alpha, \beta, \gamma \in \mathbb{N}$).

Si può supporre $\alpha \leq \beta \leq \gamma$ (il caso $\alpha \leq \gamma \leq \beta$ si tratta in maniera analoga).

Con le notazioni introdotte sopra si ha

$$\rho = p^{\alpha+\beta} + \mathcal{O}, \quad \sigma = p^{\beta+\gamma} + \mathcal{O} \quad \text{e} \quad \tau = p^{\alpha+\gamma} + \mathcal{O}.$$

Dalle relazioni (2) e (3) del Lemma 2 si ricava che l'ordine di a divide $p^{3\alpha+\beta}$, quello di b divide $p^{3\beta+\gamma}$ e $p^{\alpha+\beta+2\gamma}$ e quello di c divide $p^{2\alpha+\beta+\gamma}$.

Dal Lemma 2 discende $[a^{r\rho}, b] = [b^{s\sigma}, c] = [c^{t\tau}, a] = 1$.

Poi $[c, a^{r\rho}] = c^{(1+t)^{r\rho}-1}$ e siccome $(1+t)^{r\rho} - 1 = p^{2\alpha+\beta+\gamma} + \vartheta$ si ha $[c, a^{r\rho}] = 1$. Analogamente $(1+r)^{s\sigma} - 1 = p^{\alpha+2\beta+\gamma} + \vartheta$ e siccome per ipotesi $3\alpha + \beta \leq \alpha + 2\beta + \gamma$ si ha $[a, b^{s\sigma}] = 1$. Infine $(1+s)^{t\tau} - 1 = p^{\alpha+\beta+2\gamma} + \vartheta$ e $[b, c^{t\tau}] = 1$ porge che $G'' \leq Z(G)$.

Si ha $[a^{r^2}, b^s] = a^{r^2\rho} = 1$, $[b^{s^2}, c^t] = b^{s^2\sigma} = 1$ e $[c^{t^2}, a^r] = c^{t^2\tau} = 1$. Poi

- $[c^t, a^{r^2}] = c^{t\{(1+t)^{r^2}-1\}}$, si ha $t\{(1+t)^{r^2} - 1\} = p^{2\alpha+2\gamma} + \vartheta$ e siccome $2\alpha + \beta + \gamma \leq 2\alpha + 2\gamma$ risulta $[c^t, a^{r^2}] = 1$;
- $[a^r, b^{s^2}] = a^{r\{(1+r)^{s^2}-1\}}$, si ha $r\{(1+r)^{s^2} - 1\} = p^{2\alpha+2\beta} + \vartheta$ e siccome $3\alpha + \beta \leq 2\alpha + 2\beta$ risulta $[a^r, b^{s^2}] = 1$;
- $[b^s, c^{t^2}] = b^{s\{(1+s)^{t^2}-1\}}$, si ha $s\{(1+s)^{t^2} - 1\} = p^{2\beta+2\gamma} + \vartheta$ e siccome $\alpha + \beta + 2\gamma \leq 2\beta + 2\gamma$ risulta $[b^s, c^{t^2}] = 1$;
- $[a^\rho, b^s] = a^{\rho^2}$, $\rho^2 = p^{2\alpha+2\beta} + \vartheta$, $3\alpha + \beta \leq 2\alpha + 2\beta$ e quindi $[a^\rho, b^s] = 1$;
- $[c^t, a^\rho] = c^{t\{(1+t)^\rho-1\}}$, $t\{(1+t)^\rho - 1\} = p^{\alpha+\beta+2\gamma} + \vartheta$, $2\alpha + \beta + \gamma \leq \alpha + \beta + 2\gamma$ e quindi $[c^t, a^\rho] = 1$;
- $[b^\sigma, c^t] = b^{\sigma^2}$, $\sigma^2 = p^{2\alpha+2\beta} + \vartheta$, $\alpha + \beta + 2\gamma \leq 2\alpha + 2\beta$ e quindi $[b^\sigma, c^t] = 1$;
- $[a^r, b^\sigma] = a^{r\{(1+r)^\sigma-1\}}$, $r\{(1+r)^\sigma - 1\} = p^{2\alpha+\beta+\gamma} + \vartheta$, $3\alpha + \beta \leq 2\alpha + \beta + \gamma$ e quindi $[a^r, b^\sigma] = 1$;
- $[c^\tau, a^r] = c^{\tau^2}$, $\tau^2 = p^{2\alpha+2\gamma} + \vartheta$, $2\alpha + \beta + \gamma \leq 2\alpha + 2\gamma$ e quindi $[c^\tau, a^t] = 1$;
- la dimostrazione che $[b^s, c^\tau] = 1$ richiede un trattamento diverso. Dalla relazione (1) del Lemma 2 si ricava $c^{-\tau} = a^{(1+r)\rho} b^{(1+s)\sigma} c^{t\tau}$. Si ha $[b^s, a^\rho] = a^{-\rho^2} = 1$ (per quanto visto sopra) e $[b^s, c^{t\tau}] = 1$ perché $s\{(1+s)^{t\tau} - 1\} = p^{\alpha+2\beta+2\gamma} + \vartheta$ e $\alpha + \beta + 2\gamma \leq \alpha + 2\beta + 2\gamma$. Ovviamente b^s commuta con $b^{(1+s)\sigma}$ e quindi $[b^s, c^\tau] = 1$.

II° Caso. $p = 2$ e $1 + r = \pm 1 + 2^\alpha$, $1 + s = \pm 1 + 2^\beta$ e $1 + t = \pm 1 + 2^\gamma$ $(\alpha, \beta, \gamma \in \mathbb{N})$.

Questo caso comprende anche il caso (iii) del Lemma 5 (se, ad esempio, b induce l'inversione su A si può sempre scrivere $a^b = a^{-1+2^{|A|}}$).

Anche in questo caso si può supporre $\alpha \leq \beta \leq \gamma$ in quanto l'altra possibilità si tratta in maniera analoga. A titolo esemplificativo viene considerato solamente il caso

$$1 + r = -1 + 2^\alpha, \quad 1 + s = 1 + 2^\beta \quad \text{e} \quad 1 + t = 1 + 2^\gamma$$

in quanto gli altri casi sono del tutto simili.

Si ha

$$r = -2 + 2^{\alpha} = -2 + \vartheta, \quad s = 2^{\beta} \quad \text{e} \quad t = 2^{\gamma}$$

da cui

$$\rho = 2^{\beta+1} + \vartheta, \quad \sigma = 2^{\beta+\gamma} + \vartheta \quad \text{e} \quad \tau = 2^{\gamma+1} + \vartheta.$$

Dal Lemma 2 si ottiene che l'ordine di a divide $2^{\beta+3}$, quello di b divide $2^{3\beta+\gamma}$ e $2^{\beta+2\gamma+1}$ e quello di c divide $2^{\beta+\gamma+2}$. Da $(1+t)^{r\rho} - 1 = 2^{\beta+\gamma+2} + \vartheta$ si ha $[c, a^{r\rho}] = 1$. Da $(1+r)^{s\sigma} - 1 = -2^{\alpha+2\beta+\gamma} + \vartheta$ e $\beta + 3 \leq \alpha + 2\beta + \gamma$ si ha $[a, b^{s\sigma}] = 1$. Infine da $(1+s)^{t\tau} - 1 = 2^{\beta+\gamma+2} + \vartheta$ e $\beta + \gamma + 2 \leq \beta + 2\gamma + 1$ si ottiene $[b, c^{t\tau}] = 1$.

Questo prova che $G'' \leq Z(G)$; il fatto che $[G, G, G] \leq Z(G')$ si dimostra in maniera analoga. □

DIMOSTRAZIONE DELLA PROPOSIZIONE 3. Sia $A = \langle a \rangle$, $B = \langle b \rangle$ e $C = \langle c \rangle$.

Conviene iniziare dimostrando che G è supersolubile. Ragionando come nella dimostrazione della Proposizione 1 si ricava che se A_G, B_G e C_G sono tutti identici allora G è nilpotente e quindi (essendo finitamente generato) supersolubile. Esclusa tale possibilità, si devono distinguere quattro casi.

(a) I tre sottogruppi A, B e C sono finiti.

In questo caso si ragiona per induzione su $|A| + |B| + |C|$ (la base dell'induzione è triviale). Se $A_G \neq \{1\}$, l'ipotesi induttiva applicata a G/A_G ed il fatto che A_G è ciclico porgono la conclusione. Si ragiona in maniera analoga se $B_G \neq \{1\}$ o $C_G \neq \{1\}$.

(b) Uno solo tra i gruppi A, B e C è infinito.

Non è restrittivo supporre che sia C ad avere cardinalità infinita; in tal caso si ragiona per induzione su $|A| + |B|$. Se $A_G \neq \{1\}$ (o $B_G \neq \{1\}$) l'ipotesi induttiva applicata a G/A_G (ovvero a G/B_G) e il fatto che A_G (e B_G) è ciclico permettono di concludere. Se $C_G \neq \{1\}$ allora in $\overline{G} = G/C_G$ anche $\overline{C}$ risulta finito e si conclude per il punto precedente.

(c) Uno solo tra i sottogruppi A, B e C è finito.

Si supponga che sia A ad essere finito. In questo caso si ragiona per induzione su $|A|$. Se $A_G \neq \{1\}$ si conclude per l'ipotesi induttiva, se $B_G \neq \{1\}$ (oppure $C_G \neq \{1\}$) allora, considerando G/B_G (oppure G/C_G), si è ricondotti al caso (b).

(d) I tre sottogruppi A, B e C sono infiniti.

Allora quozientando G tramite A_G (ovvero B_G o C_G) si è ricondotti al caso precedente.

Per dimostrare che $G'' \leq Z(G)$ e $\gamma_3(G) \leq Z(G')$ si devono distinguere cinque casi (tenendo conto del fatto che gli unici automorfismi del gruppo ciclico infinito sono l'identità e l'inversione).

(1) $[a,b]=1$ (o $[b,c]=1$ o $[c,a]=1$).

In questo caso il gruppo AB è abeliano e G si fattorizza nel prodotto dei due sottogruppi abeliani AB e C. Per un noto risultato dovuto a Itô ([5]) G risulta metabeliano e in questo caso l'asserto è dimostrato.

(2) $a^b = a^{-1}$, $b^c = b^{-1}$ e $c^a = c^{-1}$.

In questo caso si ha $G' = \langle a^2, b^2, c^2 \rangle$ e si verifica facilmente che G' risulta abeliano.

(3) $a^b = a^{-1}$, $b^c = b^{-1}$, $c^a = c^{1+t}$, b ha ordine infinito e c ha ordine finito.

Dall'identità di Hall-Witt si ottiene $[a,b,c^a][c,a,b^c][b,c,a^b]=1$ da cui $[a^{-2},c]^a[c^t,b][b^{-2},a]^b = 1$ e $(c^{(1+t)^2-1})^{a^{-1}} = (b^{-1+(-1)^t})^c$. Siccome per ipotesi c ha ordine finito e b ha ordine infinito i due membri dell'ultima uguaglianza devono ridursi all'identità e quindi $[c,a^2]=1$ e $[b,c^t]=1$. Si ha ovviamente $[a,b^2]=1$ e quindi $G' = \langle a^2, b^2, c^t \rangle$ risulta abeliano.

(4) $a^b = a^{-1}$, $b^c = b^{1+s}$, $c^a = c^{1+t}$, b e c hanno ordine finito e a ha ordine infinito.

Siccome b e c hanno ordine finito si può supporre $s \geq 1$ e $t \geq 1$. Da $[a,b,c^a][c,a,b^c][b,c,a^b]=1$ segue $[a^{-2},c]^a[c^t,b]^c[b^s,a]^b = 1$ e $[a,b^s] \in BC$. Ma $[a,b^s] = a^{-1+(-1)^s}$ e a ha ordine infinito mentre BC è un sottogruppo finito di G, dunque $[a,b^s]=1$. Si ha poi $[c,a^2]^{a^{-1}} = (b^\sigma)^c$ (ove $\sigma = (1+s)^{|t|}-1$). Poiché $A \cap B \cap C = \{1\}$ il Lemma 3 porge $B \cap C \leq Z(G)$ e quindi $b^\sigma \in Z(G)$ e $[c,a^2] = c^{2t+t^2} \in Z(G)$. Si ha $b^\sigma = (b^\sigma)^c = b^{(1+s)\sigma}$ da cui $b^{s\sigma}=1$ e quindi $[b^s, c^t]=1$. Analogamente $c^{2t+t^2} = (c^{2t+t^2})^a = c^{(1+t)(2t+t^2)}$ porge $[c^t, a^2]=1$. Siccome $[a^2, b^s]=1$ ne risulta che $G' = \langle a^2, b^s, c^t \rangle$ è abeliano.

(5) $a^b = a^{1+r}$, $b^c = b^{1+s}$, $c^a = c^{1+t}$, con a, b e c di ordine finito.

Non è restrittivo supporre $r,s,t \geq 1$. Inoltre in questo caso G ha ordine finito; per provare l'asserto si ragiona per induzione su $|G|$ (la base dell'induzione essendo triviale).

Siano N_1 e N_2 due sottogruppi normali minimali distinti di G. Allora, posto $G_1 = G/N_1$ e $G_2 = G/N_2$, dall'ipotesi induttiva si ricava

$$[G_i'', G_i] = \{1\} = [[G_i, G_i, G_i], G_i'] \quad (i \in \{1,2\})$$

da cui $[G'', G] \leq N_1 \cap N_2 = \{1\}$, $[[G, G, G], G'] \leq N_1 \cap N_2 = \{1\}$ e in questo caso l'asserto è provato.

Quindi si può supporre che G ammetta un unico sottogruppo normale minimo N; tale N risulta essere un p-gruppo per qualche numero primo p. Ne discende che $F = F(G)$, il sottogruppo di Fitting di G, è un p-sottogruppo di G. Inoltre, essendo G supersolubile, si ha $G' \leq F$ (5.4.10 di [12]) e F è un p-sottogruppo di Sylow di G.

Si può scrivere $a = a_1 a_2$, $b = b_1 b_2$ e $c = c_1 c_2$ con a_1, b_1 e c_1 p-elementi di G (necessariamente contenuti in F) e a_2, b_2 e c_2 elementi di ordine coprimo con p. Si ha $F = \langle a_1, b_1, c_1 \rangle$ e posto $H = \langle a_2, b_2, c_2 \rangle$ si verifica (tenendo conto che b_2 normalizza $\langle a_2 \rangle$, c_2 normalizza $\langle b_2 \rangle$ e a_2 normalizza $\langle c_2 \rangle$) che H è un p'-sottogruppo di G; si ha quindi $G = FH$, $F \cap H = \{1\}$. Inoltre, poiché G/F è abeliano, anche H risulta abeliano.

Sia $c_2 \neq 1$. Si ha $[H, c_2] = \{1\}$ e $[c_1, c_2] = 1$, inoltre $[c_2, a_1] \in \in F \cap \langle c_2 \rangle = \{1\}$. Quindi $[G, c_2] = \langle [b_1, c_2] \rangle$ e siccome $\langle b_1 \rangle$ è un p-gruppo mentre c_2 induce un p'-automorfismo su $\langle b_1 \rangle$ si ha $[\langle [b_1, c_2] \rangle, c_2] = \langle [b_1, c_2] \rangle$.

Non si può avere $[b_1, c_2] = 1$ perché in tal caso $c_2 \in Z(G) \leq F$. Quindi $\langle [b_1, c_2] \rangle$ deve contenere N, l'unico sottogruppo minimale di G, e siccome $\langle [b_1, c_2] \rangle \cap Z(G) = \{1\}$ si deve avere $Z(G) = \{1\}$. Dal Lemma 4 discende che G è metabeliano e in questo caso l'asserto è dimostrato.

Si conclude allo stesso modo se $a_2 \neq 1$ o $b_2 \neq 1$. Infine, nel caso in cui $a_2 = b_2 = c_2 = 1$, $G = F$ è un p-gruppo (finito) e il Lemma 6 porge la conclusione. □

5. Dimostrazione del Teorema 1.

È conveniente enunciare la seguente generalizzazione del Lemma 2.

LEMMA 7. *Siano $r, s, t \in \mathbb{Z}$ tutti diversi da 0 e da -2 e sia $G = \langle a, b, c \rangle$ un quoziente di $M(r, s, t) = \langle a_*, b_*, c_* \mid a_*^{b_*} = a_*^{1+r}, b_*^{c_*} = b_*^{1+s}, c_*^{a_*} = c_*^{1+t} \rangle$, allora G è finito e risulta*

(1) $\langle a^\rho \rangle \leq \langle b^\sigma, c^\tau \rangle$, $\langle b^\sigma \rangle \leq \langle a^\rho, c^\tau \rangle$ e $\langle c^\tau \rangle \leq \langle a^\rho, b^\sigma \rangle$;
(2) $a^{r\rho} \in \langle b \rangle$, $b^{s\sigma} \in \langle c \rangle$, $c^{t\tau} \in \langle a \rangle$;
(3) $a^{r^2\rho} = 1$, $b^{s^2\sigma} = 1$, $c^{t^2\tau} = 1$;
(4) $a^{s\rho} \in \langle c \rangle$, $b^{t\sigma} \in \langle a \rangle$, $c^{r\tau} \in \langle b \rangle$;
(5) $a^{st\rho} = 1$, $b^{rt\sigma} = 1$, $c^{rs\tau} = 1$.

DIM. Utilizzando l'identità di Hall-Witt $[a, b, c^a][c, a, b^c][b, c, a^b] = 1$ si

perviene a

$$[a^r, c^a][c^t, b^c][b^s, a^b] = 1$$

da cui

$$[a, b^s]^b[b, c^t]^c[c, a^r]^a = 1.$$

Se $s > 0$ allora $[a, b^s] = a^\rho$; se invece $s < 0$ allora $[a, b^s] = [a, b^{-s}]^{-b^s} = (a^\rho)^{-b^s}$. Analogamente se $t > 0$ allora $[b, c^t] = b^\sigma$, se $t < 0$ allora $[b, c^t] = [b, c^{-t}]^{-c^t} = (b^\sigma)^{-c^t}$ e se $r > 0$ allora $[c, a^r] = c^\tau$ mentre se $r < 0$ allora $[c, a^r] = [c, a^{-r}]^{-a^r} = (c^\tau)^{-a^r}$. Sia $a^{-b^{1+s}} = a^i$, $b^{-c^{1+t}} = b^j$ e $c^{-a^{1+r}} = c^k$ allora, posto

$$\lambda = \begin{cases} 1+r & \text{se } s > 0 \\ i & \text{se } s < 0 \end{cases} \quad \mu = \begin{cases} 1+s & \text{se } t > 0 \\ j & \text{se } t < 0 \end{cases} \quad \nu = \begin{cases} 1+t & \text{se } r > 0 \\ k & \text{se } t < 0, \end{cases}$$

si ottiene

$$(\Xi) \qquad a^{\lambda\rho} b^{\mu\sigma} c^{\nu\tau} = 1.$$

Per dimostrare che G è finito si devono considerare due casi.

• Almeno uno tra a, b e c ha ordine finito.

Non è restrittivo supporre che sia a ad avere ordine finito; sia $|\langle a \rangle| = m$. Allora $c = c^{a^m} = c^{(1+t)^m}$ e quindi (siccome $1 + t \neq \pm 1$), c ha ordine finito che divide $(1+t)^m - 1$. Se $|\langle c \rangle| = n$, ragionando in maniera analoga, si prova che b ha ordine finito che divide $(1+s)^n - 1$. Siccome ogni elemento di G si può scrivere nella forma $a^i b^j c^k$ (con $i, j, k \in \mathbb{Z}$ opportuni) si può concludere che, in questo caso, G ha ordine finito.

• I tre elementi a, b e c hanno tutti ordine infinito.

Ragionando per assurdo si dimostra che questo caso non si può dare. Posto $a_1 = a^{\lambda\rho}$, $b_1 = b^{\mu\sigma}$ e $c_1 = c^{\nu\tau}$ si ha $a_1 \neq 1$, $b_1 \neq 1$, $c_1 \neq 1$ e, per (Ξ), $a_1 b_1 c_1 = 1$. Si osservi che non è restrittivo supporre $\lambda\rho > 0$ (in caso contrario, in luogo di a_1, b_1 e c_1, si considerano i rispettivi inversi). Si ottiene quindi

$$b_1^{-1} a_1^{-1} = c_1 = c_1^c = (b_1^{-1} a_1^{-1})^c = b_1^{-1-s} a_1^{-c}$$

e $[a_1, c] = b_1^{-s}$. Siccome $a_1 = a^{\lambda\rho}$ risulta $[a_1, c] = c^{1-(1+t)^{\lambda\rho}} \in \langle c \rangle$ e dunque l'elemento $b_2 = b_1^s$ appartiene a $\langle b \rangle \cap \langle c \rangle$. Ma allora

$$b_2 = b_2^c = b_2^{(1+s)}$$

e b dovrebbe avere ordine finito, contraddicendo le ipotesi.

Tenendo presente che a, b e c hanno ordine finito si ottiene

$$\langle a^{\lambda\rho}\rangle = \langle a^{\rho}\rangle, \quad \langle b^{\mu\sigma}\rangle = \langle b^{\sigma}\rangle \quad \text{e} \quad \langle c^{\nu\tau}\rangle = \langle c^{\tau}\rangle;$$

utilizzando tali uguaglianze si dimostra facilmente (1).

Il punto (2) si ricava ragionando come nella dimostrazione del punto (4) del Lemma 2.

Dal punto (2) si ottiene

$$1 = [a^{r\rho}, b] = a^{r^2\rho}, \ 1 = [b^{s\sigma}, c] = b^{s^2\sigma} \ \text{ e } \ 1 = [c^{t\tau}, a] = c^{t^2\tau},$$

il che prova il punto (3).

Tenendo conto che G è finito, la Proposizione 3 porge che a^{ρ}, b^{σ} e c^{τ} commutano tra loro. Per (1) si può scrivere $a^{\rho} = b^{i\sigma}c^{j\tau}$ ($i, j \in \mathbb{Z}$ opportuni) e quindi $a^{s\rho} = (b^{i\sigma}c^{j\tau})^s = b^{is\sigma}c^{js\tau}$. Poiché, per (2), $b^{s\sigma} \in \langle c\rangle$ si può concludere che $a^{s\rho} \in \langle c\rangle$. In maniera del tutto analoga si prova che $b^{t\sigma} \in \langle a\rangle$ e $c^{r\tau} \in \langle b\rangle$.

Infine, per dimostrare (5), si può scrivere $a^{s\rho} = c^k$ ($k \in \mathbb{Z}$ opportuno) da cui $a^{s\rho} = (c^k)^a = c^{k(1+t)} = a^{(1+s)t\rho}$ e $a^{st\rho} = 1$. Allo stesso modo si verifica che $b^{rt\sigma} = 1$ e $c^{rs\tau} = 1$. □

Dimostrazione del Teorema 1. Sia G un quoziente di $M(r, s, t)$ con $r, s, t \in \mathbb{Z}$. Il fatto che, se $r \neq 0, -2$, $s \neq 0, -2$ e $t \neq 0, -2$, G è finito discende dal Lemma 7 (la dimostrazione fornita in [7], dove viene esplicitato solo il caso $r, s, t \in \mathbb{N}$, non è molto chiara). I fatti che G è supersolubile, che $G'' \leq Z(G)$ e che $\gamma_3(G) \leq Z(G')$ discendono direttamente dalla Proposizione 3. Per dimostrare che, sotto tali ipotesi, l'ordine di G divide $|(r, s)(s, t)(t, r)\rho\sigma\tau|$ si ragiona per induzione su $|G|$ (la base dell'induzione essendo triviale).

Il gruppo $L = \langle a^{\rho}, b^{\sigma}, c^{\tau}\rangle$ è un sottogruppo di G contenuto in $\gamma_3(G)$, in particolare L è abeliano. Inoltre $L \trianglelefteq G$ infatti $[a^{\rho}, b] = a^{r\rho} \in L$ poi, siccome r divide ρ, si può scrivere $\rho = rk$ e poiché $[c, a^r] = c^{\tau}$ e c^{τ} commuta con c e con a^r (in quanto $a^r \in G'$) si ha $[a^{\rho}, c] = [c, a^{rk}]^{-1} = [c, a^r]^{-k} = c^{-k\tau} \in L$. In maniera analoga si prova che $[b^{\sigma}, a], [b^{\sigma}, c], [c^{\tau}, a], [c^{\tau}, b] \in L$.

Se $L = \{1\}$ allora l'ordine di G divide $|\rho\sigma\tau|$ e l'asserto è dimostrato. Si può quindi assumere che $L \neq \{1\}$. Sia p un divisore primo dell'ordine di L. Se L non è un p-gruppo si può scrivere $L = L_1 \times L_2$ con L_1 p-sottogruppo non banale e L_2 p'-sottogruppo non banale. Per l'ipotesi induttiva gli ordini dei due gruppi G/L_1 e G/L_2 dividono entrambi $|(r, s)(s, t)(t, r)\rho\sigma\tau|$ e siccome $(|L_1|, |L_2|) = 1$ anche l'ordine di G deve dividere tale numero.

Si supponga quindi che L sia un p-gruppo. Poiché G/L ha ordine che divide $|\rho\sigma\tau|$ per dimostrare l'asserto è sufficiente far vedere che l'ordine di L divide $(r, s)(s, t)(t, r)$; per far questo si sfrutta il fatto che il reticolo dei sottogruppi di un p-gruppo ciclico è totalmente ordinato.

Sia $r = p^\alpha r'$, $s = p^\beta s'$, $t = p^\gamma t'$ con $(r's't', p) = 1$; si può supporre (eventualmente rinominando gli elementi a, b e c) che $\alpha \leq \beta \leq \gamma$ oppure che $\alpha \leq \gamma \leq \beta$. Si può inoltre considerare solamente il caso $\alpha \leq \beta \leq \gamma$ in quanto l'altro caso è del tutto simile. Siccome $(r, s) = p^\alpha(r', s')$, $(s, t) = p^\beta(s', t')$ e $(t, r) = p^\alpha(t', r')$ sarà sufficiente dimostrare che $|L|$ divide $p^{2\alpha+\beta}$.

Dal Lemma 7 si ottiene $L = \langle a^\rho, b^\sigma \rangle$.

Ancora dal Lemma 7 si ottiene $a^{p^{2\alpha}\rho} = 1$ da cui $a^{p^{\alpha+\beta}\rho} = 1$ e $a^{rs\rho} = 1$; poiché $c^{rs\tau} = 1$ risulta anche $b^{rs\sigma} = 1$.

Sempre per il Lemma 7 si ha $a^{r\rho} \in A \cap B$; a questo punto si possono dare due casi

- $\langle a^{r\rho} \rangle \leq \langle b^{s\sigma} \rangle$.
  Siccome $a^{r\rho}, b^{s\sigma} \in \langle b^{s\sigma} \rangle$ l'ordine di $L/\langle b^{s\sigma} \rangle$ divide $p^{\alpha+\beta}$ e poiché $b^{rs\sigma} = 1$ l'ordine di L divide $p^{2\alpha+\beta}$.
- $\langle a^{r\rho} \rangle \geq \langle b^{s\sigma} \rangle$.
  Siccome $a^{r\rho}, b^{s\sigma} \in \langle a^{r\rho} \rangle$ l'ordine di $L/\langle a^{r\rho} \rangle$ divide $p^{\alpha+\beta}$ e poiché $a^{r^2\sigma} = 1$ l'ordine di L divide $p^{2\alpha+\beta}$.

Dunque in ogni caso $|L|$ divide $(r, s)(s, t)(t, r)$ e l'asserto è dimostrato. □

OSSERVAZIONE 5. Sia $G = M(r, s, t)$ e si supponga che G sia finito. Se p è il più piccolo divisore primo di $|G|$, siccome G è supersolubile esso ammette un p-complemento normale (si veda 5.4.8 di [12]). In particolare essendo

$$G/G' \simeq C_r \times C_s \times C_t$$

se $r = p^\alpha$, $s = p^\beta$ e $t = p^\gamma$ allora $RM(r, s, t)$ (il quoziente di G tramite il suo residuale nilpotente) è un p-gruppo isomorfo a un p-sottogruppo di Sylow di G. Inoltre il residuale nilpotente N di G è abeliano e non è difficile dimostrare che il suo ordine è $|\rho\sigma\tau|_{p'}$ (se $n \in \mathbb{N}$ con $n_{p'}$ si indica la p'-parte di n cioè quel numero n' tale che $n = p^\lambda n'$ con $(n', p) = 1$ mentre con $n_p = p^\lambda$ si indica la p-parte di n).

L'esatta determinazione dell'ordine $\omega = \omega_p(\alpha, \beta, \gamma)$ di $RM(p^\alpha, p^\beta, p^\gamma)$ sembra però abbastanza difficile. Numerosi esperimenti condotti col software GAP portano a congetturare che ω divida sempre il numero

$$\Omega = \Omega_p(\alpha, \beta, \gamma) = \begin{cases} (p^\alpha, p^\beta)(p^\beta, p^\gamma)(p^\gamma, p^\alpha)[\rho\sigma\tau]_p/(p^\alpha, p^\beta, p^\gamma) & \text{se } p \neq 3 \\ 3(3^\alpha, 3^\beta)(3^\beta, 3^\gamma)(3^\gamma, 3^\alpha)[\rho\sigma\tau]_3/(3^\alpha, 3^\beta, 3^\gamma) & \text{se } p = 3 \end{cases}$$

Per l'Osservazione 3 si ha $\omega_p(\gamma, \gamma, \gamma) = \Omega_p(\gamma, \gamma, \gamma)$ ma, in generale, può accadere che $\omega \neq \Omega$ come mostrano i risultati riportati nella Tabella 2. Si osservi che in tutti i casi considerati si ha $\omega_p(\alpha, \beta, \gamma) = \omega_p(\alpha, \gamma, \beta)$; risulta però (ad esempio) $|M(2, 4, 8)| = 2^{16} \cdot 3 \cdot 13 \cdot 313$ mentre $|M(2, 8, 4)| = 2^{16} \cdot 3 \cdot 5^2 \cdot 41^2$.

Un altro problema che sembra di non facile soluzione è la determinazione dell'esatta classe di nilpotenza di $RM(r,s,t)$.

TABELLA 2.

			$p=2$			$p=3$			$p=5$		
α	β	γ	ω	Ω/ω	classe	ω	Ω/ω	classe	ω	Ω/ω	classe
1	1	1	2^{11}	1	4	3^9	1	5	5^8	1	3
1	1	2	2^{12}	1	5	3^{11}	1	5	5^{10}	1	4
1	2	2	2^{14}	1	6	3^{13}	3	5	5^{13}	1	5
2	2	2	2^{16}	1	3	3^{17}	1	4	5^{16}	1	3
1	2	3	2^{16}	1	6	3^{15}	3	5	5^{15}	1	5
1	3	2	2^{16}	1	7	3^{15}	1	6	5^{15}	1	6
2	2	3	2^{18}	1	4	3^{19}	1	4	5^{18}	1	4
2	2	4	2^{20}	1	4	3^{21}	1	5	5^{20}	1	4
1	3	5	2^{22}	2	7	3^{21}	9	6	5^{21}	5	6
1	5	3	2^{22}	2	9	3^{21}	9	8	5^{21}	5	8
3	3	3	2^{24}	1	3	3^{25}	1	4	5^{24}	1	3
1	4	6	2^{26}	4	8	3^{25}	27	7	5^{25}	25	7
1	6	4	2^{26}	4	10	3^{25}	27	9	5^{25}	25	9
2	4	5	2^{28}	1	5	3^{28}	1	5	5^{28}	1	5
2	4	6	2^{30}	1	5	3^{30}	3	5	5^{30}	1	5

OSSERVAZIONE 6. Non è difficile dimostrare che se $p \neq 2$ o se p^α, p^β e p^γ sono tutti maggiori di 4 allora $RM(p^\alpha, p^\beta, p^\gamma)$ è un p-gruppo *powerful* nel senso della definizione data in [8]. Ne segue che se $M(r,s,t)$ è finito allora un suo p-sottogruppo di Sylow è un p-gruppo *powerful* per ogni numero primo dispari p (si rammenti che $M(r,s,t)$ è supersolubile e si veda 5.4.8 di [12]).

OSSERVAZIONE 7. Vi è un altro caso in cui $M(r,s,t)$ risulta finito. Si supponga infatti $r = -2$ e sia $s = 2s_1 + 1$ dispari; allora $\rho = (1+r)^{|s|} - 1 = -2$, $\sigma = (1+s)^{|t|} - 1$ e $\tau = (1+t)^2 - 1$. Condizione necessaria e sufficiente affinché $M(-2, 2s_1+1, t)$ sia finito è che ρ, σ e τ siano tutti diversi da 0, il che accade se e solo se $t \notin \{-2, 0\}$. In questo caso si può dimostrare che

$$|M(-2, 2s_1+1, t)| = |\rho\sigma\tau|.$$

OSSERVAZIONE 8. Mentre questo lavoro era in fase di revisione è apparsa la pubblicazione [2] in cui vengono studiati i gruppi $G(a,b;c,d;e,f)$ definiti dalla presentazione

$$\langle x,y,z \mid (x^a)^y = x^b, (y^c)^z = y^d, (z^e)^x = z^f \rangle; \quad a,b,c,d,e,f \in \mathbb{Z}.$$

Si ha ovviamente $M(r,s,t) = G(1,1+r;1,1+s;1,1+t)$ e quindi i gruppi $G(a,b;c,d;e,f)$ costituiscono una generalizzazione di quelli considerati nel presente lavoro. Il Teorema 2 di [2] stabilisce che, se $(a,b) = (c,d) = (e,f) = 1$ e se nessuna delle tre coppie di parametri è uguale a $(\pm 1, \pm 1)$, allora $G(a,b;c,d;e,f)$ ammette un quoziente *universale* $Q = Q(a,b;c,d;e,f)$ tra quelli in cui x, y e z hanno ordine finito, Q è finito e risolubile e Q' è nilpotente di classe al più due.

Non è difficile vedere come, utilizzando con poche modifiche la dimostrazione del Teorema 1, sia possibile affermare che risulta $Q'' \leq Z(Q)$ (si veda l'Osservazione 2).

Si osservi anche che in [11] è dimostrato che, se $1 \leq a < b$, $1 \leq c < d$ e $(a,b) = (c,d) = 1$, allora $G(a,b;c,d;1,f)$ ha ordine finito (si veda anche il Lemma 6 di [2]). D'altro canto è facile dimostrare che $Q(n,n+1;n,n+1;n,n+1) = \{1\}$ per ogni $n \in \mathbb{Z}$; tenendo conto di alcuni risultati ottenuti in [2] appare ragionevole formulare la seguente

CONGETTURA. Il gruppo $G(n,n+1;n,n+1;n,n+1)$ risulta infinito per ogni $n \in \mathbb{Z} \setminus \{-2,-1,0,1\}$.

In [10] Neumann afferma che se $2 \leq a \leq |b|$, $2 \leq c \leq |d|$ e $2 \leq e \leq |f|$ allora $G(a,b;c,d;e,f)$ è un gruppo infinito; purtroppo la dimostrazione da lui fornita non è corretta.

Ringraziamenti. L'autore esprime la sua gratitudine all'anonimo referee per l'attenta e puntigliosa lettura del testo, grazie alla quale alcuni errori e parecchie inesattezze hanno potuto essere eliminati dalla versione finale di questo lavoro.

BIBLIOGRAFIA

[1] M. A. ALBAR - A. A. AL-SHUAIBI, *On Mennicke groups of deficiency zero. II.* Canad. Math. Bull., **34**, no. 3 (1991), pp. 289–293.

[2] D. ALLCOCK, *Triangles of Baumslag-Solitar groups.* arXiv:0808.0934v1 ([v1] Wed, 6 Aug 2008; http://arxiv.org/abs/0808.0934v1).

[3] D. GORENSTEIN, *Finite groups.* Second edition. Chelsea Publishing Co., New York, 1980.

[4] G. Higman, *A finitely generated infinite simple group.* J. London Math. Soc. **26**, (1951). 61–64.
[5] N. Itô. *Über das Produkt von zwei abelschen Gruppen.* Math. Z. **62** (1955), 400–401.
[6] E. Jabara, *Gruppi fattorizzati da sottogruppi abeliani.* Rend. Sem. Mat. Univ. Padova. [In corso di pubblicazione]
[7] D. L. Johnson, E. F. Robertson, *Finite groups of deficiency zero.* Homological group theory (Proc. Sympos., Durham, 1977), pp. 275–289, London Math. Soc. Lecture Note Ser., **36**, Cambridge Univ. Press, Cambridge-New York, 1979.
[8] A. Lubotzky, A. Mann, *Powerful p-groups. I. Finite groups.* J. Algebra **105** (1987), no. 2, 484–505.
[9] J. Mennicke, *Einige endliche Gruppen mit drei Erzeugenden und drei Relationen.* Arch. Math. **10** (1959) 409–418.
[10] B. H. Neumann, *Some group presentations.* Canad. J. Math. **30** (1978), no. 4, 838–850.
[11] M. Post. *Finite three-generator groups with zero deficiency.* Comm. Algebra **6** (1978), no. 13, 1289–1296.
[12] D. J. S. Robinson, *A course in the theory of groups.* Graduate Texts in Mathematics, **80**. Springer-Verlag, New York-Berlin, 1982.
[13] E. Schenkman, *A factorization theorem for groups and Lie algebras.* Proc. Amer. Math. Soc. **68** (1978), no. 2, 149–152.

Manoscritto pervenuto in redazione il 4 luglio 2008