REND. SEM. MAT. UNIV. PADOVA, Vol. 129 (2013)
DOI 10.4171/RSMUP/129-1

Automorfismi involutori di *p*-gruppi finiti

EGLE BETTIO (*) - GIORGIO BUSETTO (**) - ENRICO JABARA (***)

ABSTRACT - Let p be a fixed odd prime number. In this note we study the class of finite p-groups G admitting an automorphism φ of order 2 such that $G = \langle g^{-1}g^{\varphi} \mid g \in G \rangle$ and $(g^{-1}g^{\varphi})^p = 1$ for all $g \in G$. In this paper we prove that if the derived length of G is d and $C_G(\varphi)$ is nilpotent of class c, then the nilpotency class of G is bounded by a function depending only on d, c and p. We prove also that if $p = 3$ and $C_G(\varphi)$ is nilpotent of class c, then G is nilpotent of class at most $2c + 1$.

MATHEMATICS SUBJECT CLASSIFICATION (2010). 20F18, 20F45, 05B07.

KEYWORDS. Finite p-groups, involutive automorphisms, Brick loops.

1. Introduzione

Sia G un gruppo finito di ordine dispari e φ un suo automorfismo di ordine 2. Se si considera il sottogruppo $F = C_G(\varphi)$ e l'insieme I degli elementi di G invertiti da φ, allora G si fattorizza come $G = FI$ (cioè ogni elemento di G si può scrivere in maniera unica come prodotto di un elemento di F e uno di I).

Da un lavoro di Fischer ([6]) segue che se $G = \langle I \rangle$ e ogni elemento di I ha ordine una potenza di un numero primo $p \neq 2$, allora G è un p-gruppo e, sotto tali ipotesi, l'insieme delle involuzioni del prodotto semidiretto $G\langle \varphi \rangle$

(*) Indirizzo dell'A.: Liceo Scientifico G. B. Benedetti, Castello 2835, 30122, Venezia.
E-mail: egle.bettio@istruzione.it
(**) Indirizzo dell'A.: Dipartimento di Informatica, Università di Ca' Foscari, Via Torino 153, 30172, Mestre (Venezia).
E-mail: gbusetto@unive.it
(***) Indirizzo dell'A.: Dipartimento di Filosofia e Beni Culturali, Università di Ca' Foscari, Dorsoduro 3484/D, 30123 Venezia.
E-mail: jabara@unive.it

si può atteggiare a quasigruppo distributivo. Anche nell'insieme I si possono introdurre operazioni non necessariamente associative e le strutture che si ottengono in tal modo sono state indagate nel caso generale da Glauberman ([7], in particolare l'Esempio 2 a p. 379; si veda anche [5], p.120). Il caso in cui I ha esponente 3 è di particolare interesse ed è stato considerato, tra gli altri, da M. Hall ([10]) per caratterizzare alcune configurazioni geometriche, da Manin ([12], capitolo I) per lo studio di alcune questioni riguardanti le forme cubiche, da Beneteau ([1], [2]), Smith ([17], [18]) e altri autori in connessione con un problema posto da Bruck ([4] e tutto il capitolo 8 di [5]).

In [16] sono stati studiati i gruppi che soddisfano alla condizione di Fischer ed è stata esibita una costruzione che fornisce p-gruppi generati da I aventi lunghezza derivata arbitrariamente elevata. Scopo di questo lavoro è di approfondire lo studio di tali gruppi quando l'ordine di ogni elemento non banale di I è un numero primo dispari p. Dimostreremo che se F è nilpotente di classe c allora la classe di nilpotenza di G è limitata in funzione di c, di p e di d, la lunghezza derivata di G. Nel caso in cui sia $p = 3$ dimostreremo che se F ha classe di nilpotenza c allora la classe di nilpotenza di G non supera $2c + 1$; da questo fatto discende che se F ha esponente 3, allora G è nilpotente di classe al più 7 ed ha esponente al più 9.

2. Notazioni e risultati preliminari

In quanto segue G denoterà sempre un gruppo finito di ordine dispari, φ un automorfismo di ordine 2 di G, $F = C_G(\varphi)$ il sottogruppo degli elementi centralizzati da φ e $I = I_G(\varphi)$ il sottoinsieme di G costituito dagli elementi invertiti da φ. L'esponente di I è il minimo comune multiplo tra gli ordini degli elementi di I. Infine con p denoteremo un numero primo dispari fissato.

Definizione 2.1. Diremo che G è un p-gruppo di Fischer se G è dotato di un automorfismo involutorio φ e sono soddisfatte le due condizioni seguenti:

(a) G è generato da I,
(b) ogni elemento di I ha ordine una potenza di p.

Dal citato risultato di Fischer ([6]) discende che un p-gruppo di Fischer è un p-gruppo nel senso usuale del termine.

Definizione 2.2. Diremo che G è un $\mathscr{F}(p)$-gruppo, ovvero un p-gruppo di Fischer in senso stretto, se alla condizione (b) della Definizione 2.1 viene sostituita la più restrittiva

(b′) ogni elemento non banale di I ha ordine p.

La precedente nomenclatura non è standard; in particolare la classe dei gruppi in $\mathscr{F}(p)$ non coincide con quella dei p-gruppi che ammettono un automorfismo I-speciale (secondo la definizione data in [16]).

Scriveremo $[a,b]$ per il commutatore $a^{-1}b^{-1}ab$ di due elementi a e b appartenenti ad un gruppo G, se poi $c \in G$ scriveremo $[a,b,c]$ in luogo $[[a,b],c]$. Se A e B sono sottogruppi di G con $[A,B]$ denotiamo il sottogruppo di G generato dai commutatori $[a,b]$ con $a \in A$ e $b \in B$; poniamo poi, per induzione, $[A,_{(1)}B] = [A,B]$ e, se $t \in \mathbb{N}$ con $t > 0$, $[A,_{(t+1)}B] = [[A,_{(t)}B],B]$. Per il resto le notazioni usate saranno quelle usuali (come in [15] o in [8]).

Il Lemma 10.4.1 di [8] riassume le informazioni essenziali sui gruppi finiti dotati di un automorfismo involutorio. Ne riportiamo l'enunciato con piccole modifiche.

Lemma 2.3. *Sia G un gruppo di ordine dispari e sia φ un suo automorfismo di ordine 2. Allora:*

(a) $G = FI = IF$, $F \cap I = \{1\}$ *e* $|I| = |G : F|$.

(b) *Se G è abeliano allora I è un sottogruppo di G e si ha $G = F \times I$.*

(c) *Se S è un sottoinsieme di F e $S^x = S$ per qualche $x \in I$ allora* $[S,x] = 1$.

(d) *Se H è un sottogruppo di G contenuto in I allora H risulta abeliano e φ-invariante.* □

Osserviamo inoltre che se $x \in I$ e $f \in F$ allora $(x^f)^\varphi = (x^{-1})^f = (x^f)^{-1}$ e dunque l'insieme I è normalizzato da F. Utilizzeremo spesso, senza richiamarli esplicitamente, l'osservazione precedente ed il seguente semplice risultato.

Lemma 2.4. $I = \{g^{-1}g^\varphi \mid g \in G\}$.

Dim. (Si veda anche il Lemma 2.1 di [16]). Se $x = g^{-1}g^\varphi$ allora $x^\varphi = g^{-\varphi}g = x^{-1}$ e $x \in I$. Sia $x \in I$ e sia k un numero naturale tale che $2k \equiv 1$ mod. $|x|$ (tale k esiste perché $|G|$ è dispari); posto $g = x^{-k}$ si ha $g^{-1}g^\varphi = x^{2k} = x$. □

Il prossimo lemma si dimostra con una verifica diretta.

LEMMA 2.5. *Sia H un sottogruppo normale e φ-invariante di G e sia $\overline{\varphi}$ l'automorfismo indotto in maniera naturale da φ su $\overline{G} = G/H$. Risulta allora $C_{\overline{G}}(\overline{\varphi}) = FH/H$ e $I_{\overline{G}}(\overline{\varphi}) = IH/H$.* □

LEMMA 2.6. *Se $G = \langle I \rangle$ e N è un sottogruppo normale di G contenuto in F o in I, allora $N \leq Z(G)$.*

DIM. Dalle ipotesi segue che N è un sottogruppo φ-invariante di G.

Se $N \leq F$ allora dal Lemma 2.3.c segue $[N, I] = 1$ e quindi $[N, G] = 1$.

Se $N \subseteq I$, $h \in N$ e $x \in I$ allora si ha $(h^{-1})^x = (h^x)^{-1} = (h^x)^\varphi = (h^{-1})^{x^{-1}}$ da cui $[h, x^2] = 1$. Poiché $|x|$ è dispari si conclude che $[h, x] = 1$. □

Se $k \in \mathbb{N}$ con $\gamma_k(G)$ denotiamo il k-esimo termine della serie centrale discendente di G.

LEMMA 2.7. *Se $G = \langle I \rangle$ allora per ogni numero naturale $t > 0$ si ha che*

(a) *φ induce l'inversione su $\gamma_{2t-1}(G)/\gamma_{2t}(G)$;*
(b) *φ induce l'identità su $\gamma_{2t}(G)/\gamma_{2t+1}(G)$.*

DIM. Per ogni numero naturale $k > 0$ e per ogni $x_1, x_2, \ldots, x_k \in I$ si ha

$$[x_1, x_2, \ldots, x_k]^\varphi \equiv [x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}] \equiv [x_1, x_2, \ldots, x_k]^{(-1)^k} \mod \gamma_{k+1}(G),$$

e quindi, ricordando che G è generato da I, φ agisce su $\gamma_k(G)/\gamma_{k+1}(G)$ come l'identità o come l'inversione a seconda che k sia pari o dispari. □

3. Proprietà dei $\mathscr{F}(p)$-gruppi

Se G è un $\mathscr{F}(p)$-gruppo allora G/G', essendo generato da elementi di ordine p, risulta essere un p-gruppo abeliano elementare. Da questo fatto discende (si veda, ad esempio, 5.2.6 di [15]) che per ogni $k \in \mathbb{N}$ il quoziente $\gamma_k(G)/\gamma_{k+1}(G)$ è un p-gruppo abeliano elementare; nel seguito utilizzeremo questo fatto senza richiamarlo specificatamente.

LEMMA 3.1. *Se G è un $\mathscr{F}(p)$-gruppo allora per ogni $x, y \in I$ si ha $(xy)^p = 1$.*

DIM. Poiché $p \neq 2$ esiste un numero naturale r tale che $2r \equiv 1$ mod. p. Se $y \in I$ anche $y^r \in I$ e, come è facile verificare, $y^r x y^r \in I$. Dunque $(y^r x y^r)^p = 1$; sviluppando il prodotto si ottiene $y^r (xy)^{p-1} x y^r = 1$ e quindi $(xy)^p = 1$. □

PROPOSIZIONE 3.2. *Se G è un $\mathscr{F}(p)$-gruppo metabeliano allora G ha esponente p e classe di nilpotenza al più p.*

DIM. Sia $N = G'$. Poiché su G/N l'automorfismo φ induce l'inversione, dal Lemma 2.5 segue $F \leq N$. Un elemento $g \in G$ si può scrivere (Lemma 2.3.a) come $g = fx^{-1}$ con $f \in F$ e $x \in I$ opportuni. Allora

$$g^p = (fx^{-1})^p = ff^x \dots f^{x^{p-1}} x^{-p} = ff^x \dots f^{x^{p-1}}$$

in quanto, per ipotesi, $x^p = 1$. Siccome f appartiene a N, che è normale e abeliano, si ha $[f^{x^i}, f^{x^j}] = 1$ per ogni coppia di numeri interi i, j da cui

$$(g^p)^\varphi = ff^{x^{-1}} \dots f^{x^{-p+1}} = ff^x \dots f^{x^{p-1}} = g^p.$$

Dunque $G^p \leq F$ e, per il Lemma 2.6, si ha $G^p \leq Z(G)$. Il gruppo $G/Z(G)$ è un gruppo metabeliano di esponente p e quindi ha classe di nilpotenza al più p per un classico risultato di Meier-Wunderli ([13], si veda anche il Teorema 7.18 di [14]). Ne consegue che G deve avere classe di nilpotenza al più $p+1$.

Siano $x, y \in I$ e sia $H = \langle x, y \rangle$, ricordando che un gruppo metabeliano di esponente p con 2 generatori ha classe di nilpotenza al più $p-1$ ([13]) e ripercorrendo i passaggi svolti sopra si ottiene che H ha clase al più p e che $H^p \leq F$. Ma allora $\gamma_p(H) \leq F$ mentre il Lemma 2.7 porge $\gamma_p(H) \leq I$: dunque $\gamma_p(H) = 1$. Ne consegue che ogni sottogruppo di G generato da due elementi di I ha esponente p e classe di nilpotenza al più $p-1$. In particolare per ogni $x, y \in I$ si ha $[x, y]^p = 1$ e $[x,_{(p-1)} y] = 1$. Poiché $N = \langle [x, y] \mid x, y \in I \rangle^G$ è abeliano e $[x, y]$ ha ordine al più p ne segue che N è un p-gruppo abeliano elementare.

Dimostriamo ora che per ogni $g \in N$ e ogni $x \in I$ si ha $[g,_{(p-1)} x] = 1$. Non è restrittivo supporre che g sia prodotto di elementi della forma $[a, b]$ con $a, b \in I$ in quanto $[a, b, c,_{(p-1)} x] = 1$ perché G ha classe di nilpotenza al più $p+1$. Quindi è sufficiente dimostrare che $[a, b,_{(p-1)} x] = 1$ per ogni $a, b, x \in I$. Ricordando che $[a, b,_{(p-1)} x] \in Z(G)$ e che in ogni gruppo metabeliano M si ha $[u, v, z] = [v, z, u]^{-1}[z, u, v]^{-1}$ per ogni $u, v, z \in M$ e $[u, v, z] = [u, z, v]$ per ogni $u \in M'$ e ogni $v, z \in M$ si ottiene:

$$[a, b,_{(p-1)} x] = [b, x, a,_{(p-2)} x]^{-1}[x, a,_{(p-2)} x, b]^{-1} = [b,_{(p-1)} x, a]^{-1}[a,_{(p-1)} x, b]$$

che è uguale a 1 essendo $[a,_{(p-1)} x] = 1 = [b,_{(p-1)} x]$.

Preso $g \in G$ si ha $g = fx$ con $f \in F$ e $x \in I$ opportuni (Lemma 2.3.a); inoltre $x^p = 1$ per ipotesi e $f^p = 1$ perché $f \in N$. Nel gruppo $K = \langle g, g^\varphi \rangle = \langle f, x \rangle$ si ha $[f,_{(p-1)} x] = 1$. Siccome $f \in N$ il gruppo $\langle f \rangle^K$ è abeliano e dunque K ha classe di nilpotenza al più $p-1$; quindi K, essendo generato da elementi di ordine p, ha esponente p.

Possiamo quindi concludere che G ha esponente p e, essendo metabeliano, classe di nilpotenza al più p. $\square$

Generalizziamo l'identità $[x, y, z][y, z, x][z, x, y] = 1$, valida in ogni gruppo metabeliano, nel seguente modo.

LEMMA 3.3. *Sia X un sottogruppo normale di un gruppo G e supponiamo che si abbia $[X, G, G'] = 1$. Allora*

$$[x, g, h][g, h, x][h, x, g] = 1$$

per ogni $x \in X$ e ogni $g, h \in G$.

DIM. Si tratta di una verifica diretta sui commutatori. $\square$

LEMMA 3.4. *Sia G un $\mathscr{F}(p)$-gruppo e sia N un sottogruppo normale e φ-invariante di G tale che $N = \langle N \cap I, [N, G] \rangle$. Allora*

(a) $[N,_{(p-1)} G] \leq N'[N, G']$ *e quindi se* $N \leq G'$ *allora* $[N,_{(p-1)} G] \leq [N, G']$.

(b) $[N,_{(p)} G] \leq [N, G, G']$.

DIM. Nella dimostrazione sia di (a) che di (b) ci serviamo del seguente risultato: se $N \trianglelefteq G$ e se $[N, G]$ è abeliano allora

$$(\dagger) \qquad [x,_{(p-1)} g] = 1 \quad \forall x \in N \cap I \quad \forall g \in I.$$

L'identità ($\dagger$) è un'immediata conseguenza del teorema di Meier-Wunderli applicato all'$\mathscr{F}(p)$-gruppo metabeliano $\langle x, g \rangle$ che, per la Proposizione 3.2, ha esponente p.

Per dimostrare (a) possiamo supporre $N'[N, G'][N,_{(p)} G] = 1$ e dimostrare che per ogni $x \in N$ e ogni $g \in I$ si ha $[x,_{(p-1)} g] = 1$. Siano $a, b \in N$, ricordando che N è abeliano si ottiene $[ab,_{(p-1)} g] = [a,_{(p-1)} g][b,_{(p-1)} g]$, dunque se $a \in N$ e $b \in [N, G]$ si ha

$$[ab,_{(p-1)} g] = [a,_{(p-1)} g],$$

in quanto $[N,_{(p)} G] = 1$. Per ipotesi è $N = \langle N \cap I, [N, G] \rangle$; si può quindi supporre $x \in I$ e ($\dagger$) fornisce la conclusione cercata.

Siccome $G' \leq C_G(N)$ si ha $G = C_G(N)I$ e il gruppo $\Xi = G/C_G(N)$ risulta abeliano e agisce in maniera naturale su N. Ogni elemento $\xi \in \Xi$ ha una controimmagine in I e quindi per ($\dagger$) risulta $[x,_{(p-1)} \xi] = 1$ per ogni $x \in N$ e ogni $\xi \in \Xi$. In End(N) si ha quindi $(\xi - 1)^{p-1} = 0$ per ogni $\xi \in \Xi$ e ricordando che N è un p-gruppo abeliano elementare si ottiene che

$$\xi^{p-1} + \xi^{p-2} + \ldots + \xi + 1 = (\xi - 1)^{p-1} = 0 \quad \forall \xi \in \Xi.$$

Siamo dunque nelle condizioni di applicare il Lemma 7.19 di [14] e ottenere

$$[N,_{(p-1)} \Xi] = [N,_{(p)} \Xi];$$

dalle ipotesi segue che $[N,_{(p-1)} G] = [N,_{(p)} G] = 1$.

Per dimostrare (b) possiamo supporre che $[N, G, G'][N_{(p+1)}G] = 1$; in particolare $[N, G]$ risulta abeliano. Come nella dimostrazione di (a) è sufficiente far vedere che $[z,_{(p-1)} g] = 1$ per ogni $z \in [N, G]$ e ogni $g \in I$. Essendo per ipotesi $N = \langle N \cap I, [N, G] \rangle$ e $G = \langle I \rangle$ si verifica facilmente che non è restrittivo supporre $z = [x, h]$ con $x \in N \cap I$ e $h \in I$. Quindi, ricordando che $[N, G, G'] = 1$, dal Lemma 3.3 si ottiene

$$[x, h,_{(p-1)} g] = [h,_{(p-1)} g, x]^{-1}[x,_{(p-1)} g, h].$$

Essendo $\langle g, h \rangle$ un $\mathscr{F}(p)$-gruppo con due generatori risulta $[h,_{(p-1)} g] \in G''$ e quindi

$$[h,_{(p-1)} g, x] \in [G'', N] \leq [N, G', G'] = 1.$$

D'altra parte, per (†), si ha $[x,_{(p-1)} g, h] = 1$. Quindi $[x, h,_{(p-1)} g] = 1$, come richiesto. □

Osservazione 3.5. La condizione $N = \langle N \cap I, [N, G] \rangle$ è equivalente a $N = \langle N \cap I \rangle^G$, in quanto G è un p-gruppo finito. Abbiamo preferito la prima formulazione in quanto è più comoda da utilizzare (come si può constatare nella dimostrazione dei prossimi risultati). □

Lemma 3.6. *Se G è un $\mathscr{F}(p)$-gruppo, allora $\gamma_{k+p-1}(G) \leq [\gamma_k(G), G']$ per ogni $k \geq 2$.*

Dim. Sia ℓ un numero naturale dispari. Poiché $G = \langle I \rangle$ dai Lemmi 2.5 e 2.7.a segue che $\gamma_\ell(G) = \langle \gamma_\ell(G) \cap I, \gamma_{\ell+1}(G) \rangle$ e quindi per il Lemma 3.4.a si ha che

$$\gamma_{\ell+p-1}(G) = [\gamma_\ell(G),_{(p-1)} G] \leq [\gamma_\ell(G), G']$$

se $\ell > 1$, e, per il Lemma 3.4.b,

$$\gamma_{\ell+p}(G) = [\gamma_\ell(G),_{(p)} G] \leq [\gamma_\ell(G), G, G'] = [\gamma_{\ell+1}(G), G']$$

per ogni ℓ. Questo prova che $\gamma_{k+p-1}(G) \leq [\gamma_k(G), G']$ per ogni $k \geq 2$. □

PROPOSIZIONE 3.7. *Sia G un $\mathscr{F}(p)$-gruppo. Allora per ogni numero intero t si ha $\gamma_{(p-1)t+2}(G) \leq \gamma_{t+1}(G')$. In particolare se G' è nilpotente di classe t allora G ha classe di nilpotenza al più $(p-1)t+1$.*

DIM. Procediamo per induzione su t. L'asserto è ovvio se $t=0$; se invece $t>0$ dal Lemma 3.6 e dall'ipotesi induttiva segue che

$$\gamma_{(p-1)t+2}(G) \leq [\gamma_{(p-1)(t-1)+2}(G), G'] \leq [\gamma_t(G'), G'] = \gamma_{t+1}(G')$$

e l'asserto è dimostrato. □

LEMMA 3.8. *Sia G un $\mathscr{F}(p)$-gruppo e sia N un sottogruppo abeliano, normale e φ-invariante di G. Supponiamo che $\gamma_{k+1}(G) \leq C_G(N)$ per qualche $k \in \mathbb{N}$ e che F sia nilpotente di classe c. Allora, posto $m = \max\{p, c+1\}$ risulta $[N,_{(m)} \gamma_k(G)] = 1$. Inoltre esiste una funzione $g(k) = g(k,c,p)$ dipendente solamente da k, c e p tale che $[N,_{(g(k))} G] = 1$; si ha $g(k) \leq m^k$.*

DIM. Siccome N è abeliano dal Lemma 2.3.b segue $N = (N \cap F) \times (N \cap I)$. Quindi, se si pone $T = C_G(N)\gamma_k(G)$, ancora dal fatto che N è abeliano, discende che $N \leq C_G(N) \leq T$.

Dimostriamo che $[N,_{(m)} T] = 1$ distinguendo due casi.

- k è pari.

Allora φ induce l'identità su $\gamma_k(G)/\gamma_{k+1}(G)$ e dunque $T = (T \cap F)C_G(N)$. Risulta quindi $N \cap IT$ e in $\overline{T} = T/(N \cap I)$ si ha $[\overline{N},_{(c)} \overline{T}] = 1$ perché, per ipotesi, F ha classe di nilpotenza c. Dunque il sottogruppo normale $[N,_{(c)} T]$ di G è contenuto in I e per il Lemma 2.6 si ha $[N,_{(c)} T] \leq Z(G)$ e quindi

$$[N,_{(m)} T] \leq [N,_{(c+1)} T] = 1.$$

- k è dispari.

Allora φ induce l'inversione su $T/C_G(N)$. Il sottogruppo $L = \langle T \cap I \rangle$ è un sottogruppo normale e φ-invariante di T, inoltre L risulta essere un $\mathscr{F}(p)$-gruppo e si ha $T = LC_G(N)$. Dal Lemma 3.4 e dall'Osservazione 3.5, posto $R = \langle N \cap I \rangle^L$, si ottiene $[R,_{(p-1)} L] = 1$ e quindi anche $[N \cap I,_{(p-1)} T] = 1$; in particolare si ha $N \cap I \leq Z_{p-1}(T)$.

In $\overline{G} = G/Z_{p-1}(T)$ si ha quindi $\overline{N} \leq C_{\overline{G}}(\varphi)$ e perciò $\overline{N} \leq Z(\overline{G})$ da cui

$$[N,_{(m)} T] \leq [N,_{(p)} T] = 1.$$

Per dimostrare che $[N,_{(g(k))} G] = 1$ ragioniamo per induzione su k.

Se $k = 1$ allora $G/C_G(N)$ è abeliano; applicando il Lemma 3.4 e tenendo conto dell'Osservazione 3.5 si ottiene che

$$\langle N \cap I \rangle^G \leq Z_{p-1}(G).$$

In $\overline{G} = G/Z_{p-1}(G)$ risulta $\overline{N} \leq C_{\overline{G}}(\varphi)$ e quindi, per il Lemma 2.3.c, si ha $\overline{N} \leq Z(\overline{G})$. Dunque $[N,_{(p)} G] = 1$ e si può porre $g(1) = p$; per come è stato definito m risulta certamente $g(1) \leq m$.

Sia $k > 1$. Consideriamo i quozienti $\overline{G}_i = G/[N,_{(i)} \gamma_k(G)]$ per $i = 1, 2, \ldots, m$; in $\overline{G}_i$ il sottogruppo $[\overline{N},_{(i-1)} \gamma_k(\overline{G}_i)]$ centralizza $\gamma_k(\overline{G})$ e l'ipotesi induttiva porge $[\overline{N},_{(i-1)} \gamma_k(\overline{G}_i),_{(g(k-1))} \overline{G}_i] = 1$ da cui

$$[N,_{(m \cdot g(k-1))} G] \leq [N,_{(m)} \gamma_k(G)] = 1.$$

Dunque $[N,_{(g(k))} G] = 1$ con $g(k) \leq m \cdot g(k-1) \leq m \cdot m^{k-1} = m^k$. □

TEOREMA 3.9. *Sia G un $\mathscr{F}(p)$-gruppo di lunghezza derivata d. Se F è nilpotente di classe c allora la classe di nilpotenza di G è limitata da una funzione f dipendente solamente da d, c e p.*

DIM. La dimostrazione procede per induzione su d, la lunghezza derivata del gruppo G.

Se $d = 1$ allora si può porre $f(1, c, p) = f(1, 0, p) = 1$ e in questo caso l'asserto è dimostrato.

Sia $d > 1$ e sia $N = G^{(d-1)}$. Allora N è un sottogruppo abeliano, normale e φ-invariante di G. Se k è la classe di nilpotenza di G/N, l'ipotesi induttiva porge che $k \leq f(d-1, c, p)$ e risulta $\gamma_{k+1}(G) \leq N \leq C_G(N)$. Dunque, per il Lemma 3.8 si ha, $[N,_{(g(k))} G] = 1$, quindi $N \leq Z_{g(k)}(G)$ e G ha classe di nilpotenza limitata da

$$k + g(k) \leq f(d-1, c, p) + g(f(d-1, c, p), c, p)$$

(ove g è la funzione definita nel Lemma 3.8). Quindi ponendo

$$f(d, c, p) = f(d-1, c, p) + g(f(d-1, c, p), c, p)$$

si ottiene la definizione induttiva della funzione f cercata. □

COROLLARIO 3.10. *Sia G un $\mathscr{F}(p)$-gruppo di lunghezza derivata d in cui F ha esponente p. Allora G ha classe di nilpotenza limitata da una funzione h dipendente solamente da d e da p.*

DIM. Essendo $F \leq G'$ si ha $F^{(d-1)} = 1$. Poiché F ha esponente p e lunghezza derivata (al più) $d-1$, il Teorema 7.18 di [14] porge che se c è la classe di nilpotenza di F risulta $c \le \dfrac{(p-1)^{d-1}-1}{p-2}$. Quindi se poniamo

$$h(d,p) = f\left(d, \frac{(p-1)^{d-1}-1}{p-2}, p\right)$$

dal Teorema 3.9 segue che la classe di nilpotenza di G è limitata da $h(d,p)$. $\square$

Per un ulteriore risultato sui $\mathscr{F}(p)$-gruppi si veda la Proposizione 4.14 del prossimo paragrafo.

4. Il caso $p = 3$

LEMMA 4.1. *Sia G un $\mathscr{F}(3)$-gruppo. Allora per ogni $x, y \in I$ il gruppo $\langle x, y\rangle$ ha esponente 3 e quindi classe di nilpotenza al più 2 e ordine al più 27. In particolare si ha $[x, y] \in F$ e $[x, y]^3 = 1$.*

DIM. È sufficiente dimostrare che se $x, y \in I$ allora il gruppo $\langle x, y\rangle$ ha classe di nilpotenza al più 2, infatti un gruppo di classe di nilpotenza al più 2 generato da elementi di ordine 3 ha esponente 3. Per il Lemma 3.1 si ha $(yx^{-1})^3 = 1$ da cui $yx^{-1}y = xy^{-1}x$ e quindi

$$[x, y] = (yx)^{-1}xy = yxyxxy = yxyx^{-1}y = yxxy^{-1}x = [y^{-1}, x] = [x, y]^{y^{-1}}$$

da cui $[x, y, y] = 1$. In maniera analoga si prova che $[y, x, x] = 1$ e quindi $[x, y] \in Z(\langle x, y\rangle)$ e $\gamma_3(\langle x, y\rangle) = 1$.

Da $[x, y] \in Z(\langle x, y\rangle)$ segue $[x, y]^\varphi = [x^{-1}, y^{-1}] = [x, y] \in F$. $\square$

Denotiamo con $\mathsf{B}(3, k)$ il gruppo con k generatori nella varietà dei gruppi di esponente 3. È noto che $|\mathsf{B}(3, 2)| = 3^3$, $|\mathsf{B}(3, 3)| = 3^7$, $|\mathsf{B}(3, 4)| = 3^{14}$ e, in generale, $|\mathsf{B}(3, k)| = 3^r$ con

$$r = k + \binom{k}{2} + \binom{k}{3}.$$

Inoltre se $k \ge 3$ allora $\mathsf{B}(3, k)$ ha classe di nilpotenza 3 (si vedano i Teoremi 14.2.3, 12.3.5 e 12.3.6 di [15]).

ESEMPIO 4.2. Sia $H = \langle a, b, c\rangle$ un 3-gruppo tale che $\langle a, b\rangle$, $\langle a, c\rangle$ e $\langle b, c\rangle$ siano tutti isomorfi a $\mathsf{B}(3, 2)$. Se definiamo l'automorfismo φ di H ponendo $a^\varphi = a^{-1}$, $b^\varphi = b^{-1}$, $c^\varphi = c^{-1}$, e poniamo $N = \langle (g^{-1}g^\varphi)^3 \mid g \in H\rangle$ allora N

risulta un sottogruppo normale e φ-invariante di H. Posto $G = H/N$ si può verificare che

(a) G è un 3-gruppo di ordine 3^{10} ed esponente 9;
(b) G ha lunghezza derivata 3 e classe di nilpotenza 4;
(c) risulta $G'' = \gamma_4(G) = Z(G)$ e si ha $|G''| = 3^3$;
(d) G è un $\mathscr{F}(3)$-gruppo in cui F ha esponente 3, classe di nilpotenza 2 ed ordine 3^6;
(e) $F' = G''$ e G/G'' risulta isomorfo a $\mathsf{B}(3,3)$.

PROPOSIZIONE 4.3. *Sia G un $\mathscr{F}(3)$-gruppo. Allora per ogni numero naturale t si ha $\gamma_{2t+2}(G) = \gamma_{t+1}(G')$. In particolare se G' ha classe di nilpotenza t allora la classe di nilpotenza di G non supera $2t+1$.*

DIM. Applicando la Proposizione 3.7 con $p = 3$ si ottiene che per ogni $t \in \mathbb{N}$ si ha $\gamma_{2t+2}(G) \leq \gamma_{t+1}(G')$. Del resto in ogni gruppo Γ si ha $[\gamma_i(\Gamma), \gamma_j(\Gamma)] \leq \gamma_{i+j}(\Gamma)$ e quindi $\gamma_{t+1}(G') \leq \gamma_{2t+2}(G)$. □

PROPOSIZIONE 4.4. *Se G è un $\mathscr{F}(3)$-gruppo, allora G' ha la stessa classe di nilpotenza di F.*

DIM. Sia c la classe di nilpotenza di F. Allora, ricordando che $G' = F\gamma_3(G)$, si ha

$$\gamma_{c+1}(G') \leq \gamma_{c+1}(F) \prod_{i=1}^{c+1} [\underbrace{G', \ldots, G'}_{i-1}, \gamma_3(G), \underbrace{G', \ldots, G'}_{c-i+1}] \leq \gamma_{2c+3}(G).$$

Poiché $\gamma_{c+1}(G') = \gamma_{2c+2}(G)$ e G è nilpotente, l'inclusione precedente porge che $\gamma_{c+1}(G') = 1$. Del resto la classe di nilpotenza di G' e maggiore o uguale a quella di F perché $F \leq G'$ e questo dimostra l'asserto. □

Per ottenere la Proposizione 4.4 è essenziale che G sia un $\mathscr{F}(3)$-gruppo, come mostrano i seguenti due esempi.

ESEMPIO 4.5. Sia $G = \langle g_1, g_2 \rangle$ e, posto

$$[g_1, g_2] = g_3, \ [g_1, g_3] = g_4, \ [g_2, g_3] = g_5, \ [g_2, g_4] = g_6, \ [g_1, g_6] = g_7,$$

supponiamo che in G siano soddisfatte le seguenti relazioni:

$$g_1^3 = 1, \ g_2^3 = 1, \ g_3^3 = 1, \ g_4^3 = 1, \ g_5^3 = 1, \ g_6^3 = 1, \ g_7^3 = 1,$$
$$[g_3, g_6] = 1, \ [g_4, g_5] = 1, \ [g_4, g_6] = 1$$

e che inoltre $Z(G) = \langle g_7 \rangle$. Si può verificare che G è un 3-gruppo di ordine 3^7, esponente 9, lunghezza derivata 3 e classe di nilpotenza 5. Ponendo $g_1^{\varphi} = g_1^{-1}$ e $g_2^{\varphi} = g_2^{-1}$ si definisce un automorfismo involutorio di G. Il centralizzante F di φ in G è un gruppo abeliano elementare di ordine 9 mentre G' non è abeliano. L'insieme I (che ha ordine 3^5) genera G ma contiene elementi di ordine 9 e quindi G non è un $\mathscr{F}(3)$-gruppo nel senso della Definizione 2.2.

ESEMPIO 4.6. Sia $G = \langle x, y \rangle$ il gruppo con due generatori nella varietà dei gruppi di esponente 5 e classe di nilpotenza 5. Si può verificare che $|G| = 5^{10}$, e che $G'' = \gamma_5(G) = Z(G)$ ha ordine 25. Il gruppo G ammette un automorfismo φ che inverte i generatori ed è quindi certamente un $\mathscr{F}(5)$-gruppo. Poiché $G'' = \gamma_5(G)$ è invertito da φ, posto $\overline{G} = G/G''$ si ha $F \simeq \overline{F}$ ed essendo $\overline{F} \leq \overline{G}'$ se ne ricava che $\overline{F}$, e quindi F stesso, è abeliano. Per costruzione G' non è abeliano e quindi non ha la stessa classe di nilpotenza di F.

TEOREMA 4.7. Sia G un $\mathscr{F}(3)$-gruppo in cui F ha classe di nilpotenza c. Se κ è la classe di nilpotenza di G risulta:

$$2c \leq \kappa \leq 2c + 1.$$

DIM. Immediata, in vista della Proposizioni 4.3 e 4.4. $\square$

PROPOSIZIONE 4.8. *Sia G un $\mathscr{F}(3)$-gruppo. Se F ha esponente 3 allora G ha classe di nilpotenza al più 7, lunghezza derivata al più 3 ed esponente al più 9.*

DIM. Ogni gruppo di esponente 3 ha classe di nilpotenza al più 3 (12.3.5 e 12.3.6 di [15]) e quindi, per il Teorema 4.7, G ha classe di nilpotenza al più 7. Siccome G' ha classe di nilpotenza al più 3 (come F) si ha

$$[G'', G''] = [\gamma_2(G'), \gamma_2(G')] \leq \gamma_4(G') = 1,$$

quindi G'' è abeliano e, per il Lemma 2.3.b, esso risulta prodotto diretto di un fattore contenuto in F e di uno contenuto in I. Per ipotesi entrambi tali fattori hanno esponente 3, dunque G'' ha esponente 3 e G ha esponente al più 9. $\square$

OSSERVAZIONE 4.9. Smith in [18] ha costruito, per ogni numero naturale $n \geq 2$, dei $\mathscr{F}(3)$-gruppi generati da n elementi di I aventi classe di nilpotenza (almeno) $2n - 3$. Dalla Proposizione 4.8 segue allora che esistono $\mathscr{F}(3)$-gruppi in cui l'esponente di F è almeno 9 (si veda anche l'Osservazione 4.13). Costruzioni equivalenti sono state ottenute da Malbos in [11] e Beneteau in [1] utilizzando in luogo dei gruppi altri tipi di strutture algebriche. $\square$

OSSERVAZIONE 4.10. Alcune delle computazioni effettuate in [10], da cui abbiamo tratto spunto per la costruzione dell'Esempio 4.2, sono tratte dal lavoro [9] in cui M. Hall fornisce una soluzione positiva per il problema di Burnside relativo all'esponente 6. In effetti il gruppo che viene costruito nel corso della dimostrazione del Teorema 2.2 di [9] permette di ottenere l'Esempio 4.11, una versione più elaborata dell'Esempio 4.2. $\square$

ESEMPIO 4.11. Consideriamo il 3-gruppo $G = \langle a, b, c, d\rangle$ tale che i quattro sottogruppi $\langle a, b, c\rangle$, $\langle a, b, d\rangle$, $\langle a, c, d\rangle$ e $\langle b, c, d\rangle$ siano tutti isomorfi a $\mathsf{B}(3,3)$. Definiamo un automorfismo φ di G ponendo $a^\varphi = a^{-1}$, $b^\varphi = b^{-1}$, $c^\varphi = c^{-1}$, $d^\varphi = d^{-1}$; si può verificare che

(a) G è un 3-gruppo di lunghezza derivata 3, di ordine 3^{17} ed esponente 9;
(b) G è un $\mathscr{F}(3)$-gruppo in cui F ha esponente 3;
(c) G ha classe di nilpotenza 4, $G'' = Z(G)$ e $G/Z(G)$ è isomorfo a $\mathsf{B}(3,4)$.

OSSERVAZIONE 4.12. Fissato $k \in \mathbb{N}$, $k > 0$, sia F_{k+1} il gruppo libero generato da $\xi_1, \xi_2, \ldots, \xi_k, \phi$ e sia

$$N = \langle \xi_i^3, \phi^2, (\xi_i\phi)^2, [g, \phi]^3 \mid g \in F_{k+1}, i = 1, 2, \ldots, k\rangle^{F_{k+1}}.$$

Nel gruppo $\Gamma = F_{k+1}/N = \langle x_1, x_2, \ldots, x_k, \varphi\rangle$, ove si è posto

$$x_i = \xi_i N \quad i = 1, 2, \ldots, k \quad \text{e} \quad \varphi = \phi N,$$

il sottogruppo $\mathsf{F}(3,k) = \langle x_1, x_2, \ldots, x_k\rangle$ è normale, ha indice 2 e su di esso φ induce un automorfismo involutorio che inverte i generatori.

Con abuso di linguaggio diremo che $\mathsf{F}(3,k)$ è il gruppo libero con k generatori nella classe dei $\mathscr{F}(3)$-gruppi (tale classe non è una varietà in quanto non è vero che un sottogruppo di un $\mathscr{F}(3)$-gruppo è ancora un $\mathscr{F}(3)$-gruppo). Un risultato generale asserisce che $\mathsf{F}(3,k)$ è finito per ogni $k \in \mathbb{N}$ (si veda [3]).

Per il Lemma 4.1 si ha $\mathsf{F}(3,2) = \mathsf{B}(3,2)$. L'Esempio 4.2 fornisce una dimostrazione diretta che $\mathsf{F}(3,3)$ è finito, in quanto è facile verificare che il gruppo costruito in tale esempio è effettivamente isomorfo a $\mathsf{F}(3,3)$. $\square$

OSSERVAZIONE 4.13. Utilizzando il software GAP ([GAP]) si può verificare che il gruppo $G = \mathsf{F}(3,4)$ ha classe di nilpotenza 6, esponente 9 e ordine 3^{49}. Risulta inoltre $|I| = 3^{12}$, $|F| = 3^{37}$ e $|\gamma_6(G)| = 3^{16}$ e $Z(G) = \gamma_6(G)$. Va anche detto che F ha classe di nilpotenza 3 ed esponente 9. $\square$

Il seguente risultato fornisce una limitazione all'ordine di un $\mathscr{F}(p)$-gruppo in funzione di $|I|$ (questo risultato migliora quello ottenuto in [3] nel caso particolare $p = 3$).

Proposizione 4.14. *Sia G un $\mathscr{F}(p)$-gruppo e sia $|I| = p^k$ allora $|G| \leq p^n$ con $n = \dfrac{1}{2}k(k+1)$. Tale limitazione è la migliore possibile.*

Dim. Sia c la classe di nilpotenza di G. Poiché G è generato da elementi di ordine p, per ogni $i \in \{1, 2, \dots, c\}$ il gruppo $\gamma_i(G)/\gamma_{i+1}(G)$ è abeliano elementare. Sia quindi $|I| = p^k$ e $n = k(k+1)/2$.

Dimostriamo l'asserto ragionando per induzione su c.

Se $c = 1$ allora $G = I$ e l'enunciato è ovvio.

Se $c = 2$ allora $G' \leq F$ e $G' \leq Z(G)$ è abeliano elementare ed è generato da al più $k(k-1)/2$ elementi e quindi $|G| \leq p^n$. Per ogni numero primo $p > 2$ sia $\mathsf{B}_2(p,k)$ il gruppo libero con k generatori nella varietà dei gruppi di classe di nilpotenza 2 ed esponente p. Tale gruppo ammette un automorfismo φ di ordine 2 che inverte tutti i generatori e si verifica facilmente che $|I| = p^k$ e $|\mathsf{B}_2(p,k)| = p^n$. Questo fatto mostra che la limitazione determinata è la migliore possibile.

Sia $c > 2$.

Se c è dispari allora $\gamma_c(G) \subseteq I$ e in questo caso l'asserto è ovvio.

Se c è pari allora $\gamma_c(G) \leq F$. Sia p^i l'ordine di $\gamma_{c-1}(G)/\gamma_c(G)$ e sia $\overline{G} = G/\gamma_{c-1}(G)$. In $\overline{G}$ si ha $|\overline{I}| = p^{k-i}$ e quindi, per l'ipotesi induttiva, $|\overline{G}| \leq p^{\overline{n}}$ con $\overline{n} = (k-i)(k-i+1)/2$. Siccome $G/G' \leq IG'/G'$ risulta $|G/G'| \leq |\overline{I}| = p^{k-i}$ e perciò si ha

$$|\gamma_c(G)| \leq p^{(k-i)i}.$$

Quindi

$$|G| = |G/\gamma_{c-1}(G)| \cdot |\gamma_{c-1}(G)/\gamma_c(G)| \cdot |\gamma_c(G)| \leq p^{(k-i)(k-i+1)/2} \cdot p^i \cdot p^{(k-i)i}$$

e poiché risulta

$$\frac{(k-i)(k-i+1) + 2i + 2(k-i)i}{2} = \frac{k(k+1)}{2} - \frac{i(i-1)}{2} \leq n,$$

l'asserto è dimostrato. □

Osservazione 4.15. La limitazione ottenuta nella Proposizione 4.14 può essere raggiunta anche nel caso di $\mathscr{F}(p)$-gruppi la cui classe di nilpotenza sia maggiore di 2. Infatti il gruppo $G = \mathsf{F}(3,3)$ costruito nell'Esempio 4.2 è un $\mathscr{F}(3)$-gruppo di ordine 3^{10} e classe di nilpotenza 4 in cui $|I| = 3^4$. □

Ringraziamenti. Gli autori desiderano esprimere la loro gratitudine al referee che, con numerosi suggerimenti, ha contribuito in maniera determinante a migliorare la struttura generale del lavoro e a raffinare alcuni risultati.

REFERENCES

[1] L. Beneteau, *Les groupes de Fischer au sens restreint: dimension et classe de nilpotence du dérivé.* C. R. Acad, Sc. Paris **285** (1977), pp. 693–695.

[2] L. Beneteau, *Free commutative Moufang loops on anticommutative graded rings.* J. Algebra **67** (1980), pp. 1–35.

[3] T. S. Bolis, *Every finitely generated Fischer group is finite.* Proc. Amer. Math. Soc. **42** (1974), pp. 387–389.

[4] R. H. Bruck, *An open question concerning Moufang loops.* Arch. Math. **10** (1959), pp. 419–421.

[5] R. H. Bruck, *A survey of binary sistems.* Springer - Verlag, New York - Heidelberg - Berlin II ed. (1968).

[6] B. Fischer, *Distributive quasigruppen endlicher ordnung.* Math. Z. **83** (1964), pp. 267–303.

[7] G. Glauberman, *On loops of odd order.* J. Algebra **1** (1964), pp. 374–396.

[8] D. Gorenstein, *Finite groups.* Harper & Row, New York (1968).

[9] M. Hall jr., *Solution of the Burnside problem for exponent six.* Illinois J. Math. **2** (1958), pp. 764–786.

[10] M. Hall jr., *Automorphisms of Steiner triple systems.* Proc. Symp. Pure Math. **VI** Amer. Math. Soc. Providence R. I. (1962), pp. 47–66.

[11] J. P. Malbos, *Sur la classe de nilpotence des boucles commutatives de Moufang et des espaces médiaux.* C. R. Acad. Sci. Paris Sér. A-B **287** (1978), pp. A691–A693.

[12] Yu. I. Manin, *Cubic forms: algebra, geometry, arithmetic.* North-Holland, Amsterdam - London - New York (1968).

[13] H. Meier-Wunderli, *Metabelsche Gruppen.* Comm. Math. Helvetici **25** (1951), pp. 1–10.

[14] D. J. S. Robinson, *Finiteness conditions and generalized soluble groups.* Springer - Verlag, New York - Heidelberg - Berlin (1972).

[15] D. J. S. Robinson, *A course in the theory of groups.* Springer - Verlag, New York - Heidelberg - Berlin (1982).

[16] R. Scapellato, *Sur les groupes engendrés par une classe de p-involutions.* Arch. Mat. (Basel) **56** (1991), pp. 5–12.

[17] J. H. D. Smith, *Finite distributive quasigroups.* Math. Proc. Camb. Phil. Soc. **80** (1976), pp. 37–41.

[18] J. H. D. Smith, *On the nilpotence class of commutative Moufang loops.* Math. Proc. Camb. Phil. Soc. **84** (1978), pp. 387–404.

[GAP] The GAP Group, GAP – Groups, Algorithms and Programming. Version 4.4.12 (2008).

Manoscritto pervenuto in redazione il 15 Febbraio 2011.