

RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

FEDERICO MENEGAZZO

**Un problema sul gruppo degli automorfismi
di un p -gruppo finito**

Rendiconti del Seminario Matematico della Università di Padova,
tome 69 (1983), p. 1-6

http://www.numdam.org/item?id=RSMUP_1983__69__1_0

© Rendiconti del Seminario Matematico della Università di Padova, 1983, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*
<http://www.numdam.org/>

Un problema sul gruppo degli automorfismi di un p -gruppo finito.

FEDERICO MENEGAZZO (*)

Un teorema di O. Müller [2] asserisce che ogni p -gruppo finito G , che non sia abeliano elementare o extraspeciale, possiede automorfismi esterni che inducono l'identità sul quoziente modulo il sottogruppo di Frattini $\Phi(G)$. Il problema dell'esistenza di automorfismi esterni che inducono l'identità, oltre che sul quoziente $G/\Phi(G)$, anche sul sottogruppo $\Phi(G)$ è stato studiato da P. Schmid in [4]. Per i gruppi G tali che $C_G(\Phi(G)) \leq \Phi(G)$ tale problema ammette la seguente formulazione equivalente in termini coomologici: $H^1(G/\Phi(G), Z(\Phi(G))) \neq 1$? In [4] si dimostra appunto che, se G è un p -gruppo regolare, allora $H^1(G/\Phi(G), Z(\Phi(G))) \neq 1$, e si chiede se un tale risultato vale in generale.

In questo lavoro si costruisce una famiglia di p -gruppi finiti per ognuno dei quali $C_G(\Phi(G)) \leq \Phi(G)$ e $H^1(G/\Phi(G), Z(\Phi(G))) = 1$; ciò permette di rispondere negativamente alla domanda posta in [4]. I gruppi in questione vengono esibiti come sottogruppi di opportuni prodotti intrecciati; si vede dalla costruzione stessa che possono venire scelti ad arbitrio il centro del gruppo e il numero di generatori, e che la classe di nilpotenza e la lunghezza di risolubilità possono essere arbitrariamente alte.

1. Alcuni risultati preliminari.

DEFINIZIONE. Siano H un p -gruppo abeliano elementare, A un p -gruppo abeliano, entrambi finiti e non identici. Il sottogruppo

(*) Indirizzo dell'A.: Seminario Matematico, Università di Padova, via Belzoni, 7 - 35100 Padova (Italia).

« base » B del prodotto intrecciato standard $AwrH$ è, in modo ovvio, un H -modulo. Ogni H -modulo M isomorfo a B verrà chiamato H -modulo intrecciato su A .

Se in particolare A è omociclico di esponente p^n e dimensione m , ogni H -modulo intrecciato su A è isomorfo a $(\mathbb{Z}/p^n\mathbb{Z}[H])^m$ sul quale H opera moltiplicando a destra.

La proposizione seguente è probabilmente ben nota.

LEMMA 1.1. *Siano H un p -gruppo abeliano elementare, A un p -gruppo abeliano, entrambi finiti e non identici; se M è un H -modulo intrecciato su A , allora $H^1(H, M) = 1$.*

DIMOSTRAZIONE. Induzione su $d = \dim H$; possiamo supporre che M sia proprio B , il sottogruppo « base » del prodotto intrecciato standard $AwrH$. Se $d = 1$ e t è un generatore di H , risulta $H^1(H, B) = \{b \in B | b^{1+t+\dots+t^{p-1}} = 1\} / \{[b, t] | b \in B\}$ ([1], I, 16.10); è noto che $\{b \in B | b^{1+t+\dots+t^{p-1}} = 1\}$ consiste esattamente delle funzioni $b: H \rightarrow A$ tali che $\prod_{i=0}^{p-1} b(t^i) = 1$, e di conseguenza ha ordine $|A|^{p-1}$; d'altra parte $C_B(H) = Z(AwrH) \cong A$, da cui $|\{[b, t] | b \in B\}| = |B|/|A| = |A|^{p-1}$. Supponiamo ora $d > 1$, spezziamo H in prodotto diretto $H = K \times \langle t \rangle$ con $t \neq 1$, e dimostriamo che ogni automorfismo di $W = AwrH$ che induca l'identità su B e su W/B è interno (vedi [1], I, 17.1). Sia α un tale automorfismo. $(BK)^\alpha = BK$, $BK \cong A^{(t)}wrK$ e per l'ipotesi induttiva $\alpha|_{BK}$ è interno, indotto da un certo $g \in B$. Se \bar{g} indica l'automorfismo interno di W indotto da g , $\beta = \alpha\bar{g}^{-1}$ induce l'identità su BK e su W/B , e in particolare $t^\beta = tf$ con $f \in C_B(K)$, da cui $(C_B(K)\langle t \rangle)^\beta = C_B(K)\langle t \rangle$. $C_B(K)\langle t \rangle$ è a sua volta (isomorfo ad) un prodotto intrecciato standard $Awr\langle t \rangle$, con sottogruppo « base » $C_B(K)$, e $\beta|_{C_B(K)\langle t \rangle}$ induce l'identità su $C_B(K)$ e su $C_B(K)\langle t \rangle/C_B(K)$. Ne segue che $\beta|_{C_B(K)\langle t \rangle}$ è interno, indotto da un certo $g^* \in C_B(K)$. Se con \bar{g}^* si indica l'automorfismo interno di W indotto da g^* , è subito visto che $\beta\bar{g}^{*-1} = \alpha\bar{g}^{-1}\bar{g}^{*-1} = 1$, cioè α è interno, come si voleva.

LEMMA 1.2. *Per ogni p -gruppo finito abeliano non identico A esiste un p -gruppo finito G , con due generatori, tale che $A \cong Z(G) \triangleleft G'$.*

(La costruzione che segue, non pubblicata, è dovuta a R. E. Phillips; ringrazio vivamente il prof. Phillips per avermi cortesemente permesso di includerla).

DIMOSTRAZIONE. Sia C un gruppo ciclico di ordine $p^n = \exp A$; è noto che nel gruppo $V = AwrC$ si ha $A \cong Z(V) \triangleleft V'$. Sia ora $T = \langle t \rangle$

un gruppo ciclico di ordine p^m , dove m è sufficientemente grande da garantire l'esistenza di un sottoinsieme S di T tale che $|S| = |V|$, $|S \cap Su| \leq 1$ per ogni $u \in T$, $u \neq 1$. Ad esempio, una scelta soddisfacente le condizioni dette è $p^m > 2^{|V|+1}$, $S = \{t, t^2, t^4, \dots, t^{2^{|V|+1}}\}$ [3]. Il gruppo G cercato sarà un sottogruppo di $W = VwrT$. Sia φ una biiezione di S su V ; la posizione $f(s) = \varphi(s)$ per ogni $s \in S$, $f(x) = 1$ se $x \in T \setminus S$ definisce un elemento f del sottogruppo « base » di W . Poniamo ora $G = \langle f, t \rangle$; G è un p -gruppo finito con 2 generatori. Per ogni coppia v_1, v_2 di elementi di V risulta $v_1 = \varphi(s_1)$, $v_2 = \varphi(s_2)$ con $s_i \in S$, $Ss_1^{-1} \cap Ss_2^{-1} = \{1\}$, il supporto di $f^{s_i^{-1}}$ è esattamente Ss_i^{-1} e dunque il commutatore $g = [f^{s_1^{-1}}, f^{s_2^{-1}}]$ è una funzione di supporto $\{1\}$ e tale che $g(1) = [f^{s_1^{-1}}(1), f^{s_2^{-1}}(1)] = [f(s_1), f(s_2)] = [v_1, v_2]$. Questa osservazione permette di concludere, utilizzando il fatto ovvio che G' è T -invariante, che il derivato F' del sottogruppo base F di W , costituito da tutte le funzioni di T in V la cui immagine è contenuta in V' , è contenuto in G' ; ne segue da un lato che $Z(W) \leq G'$, da cui $Z(W) \leq Z(G)$, dall'altro $Z(G) \leq C_W(F') \wedge C_W(T) \leq F \wedge Z(W)T = Z(W)$, e dunque $G' \geq Z(G) = Z(W) \cong Z(V) \cong A$.

COROLLARIO 1.3. *Per ogni p -gruppo finito abeliano non identico A e per ogni intero $d \geq 2$ esiste un p -gruppo finito G_d con d generatori, tale che $A \cong Z(G_d) \leq G'_d$.*

DIMOSTRAZIONE. G_2 è stato costruito nel lemma precedente; supponiamo $d > 2$ e di aver costruito G_2, \dots, G_{d-1} ; basta definire $G_d = G_{d-1}wrT_{d-1}$ dove T_{d-1} è ciclico di ordine p . La verifica che G_d soddisfi le condizioni richieste è immediata.

2. La costruzione.

TEOREMA 2.1. *Siano H un p -gruppo abeliano elementare non ciclico, A un p -gruppo abeliano non identico entrambi finiti, M un H -modulo intrecciato su A . Esiste un p -gruppo finito G tale che $G/\Phi(G) \cong H$ e $C_G(\Phi(G)) = Z(\Phi(G)) \cong M$, dove il secondo isomorfismo è un isomorfismo di H -moduli.*

DIMOSTRAZIONE. Sia $H = \langle h_1 \rangle \times \dots \times \langle h_d \rangle$ una decomposizione di H in fattori diretti di ordine p ; $d \geq 2$ per ipotesi. Sia L un p -gruppo finito con d generatori l_1, \dots, l_d tale che $A \cong Z(L) \leq L'$ (per esempio, L potrebbe essere il gruppo G_d del corollario 1.3). Nel sottogruppo « base »

F del prodotto intrecciato standard $W = LwrH$ si considerino gli elementi f_i ($i = 1, \dots, d$) così definiti: $f_i(1) = l_i$, $f_i(x_j) = 1$ per ogni $x \in H \setminus \{1\}$; si ponga $G = \langle f_1 h_1, \dots, f_d h_d \rangle$. G è un p -gruppo finito con al più d generatori; da $H \cong W/F = FG/F \cong G/F \wedge G$ segue che G ha precisamente d generatori e che $F \wedge G = \Phi(G)$. $(f_i h_i)^p = \prod_{r=0}^{p-1} f_i^{h_i^{-r}}$ è una funzione di H in L con supporto $\langle h_i \rangle$ e tale che $(f_i h_i)^p(1) = \prod_{r=0}^{p-1} f_i(h_i^r) = f_i(1) = l_i$; ne segue che $u_{ij} = [(f_i h_i)^p, (f_j h_j)^p]$ è una funzione di supporto $\{1\}$ e tale che $u_{ij}(1) = [l_i, l_j]$. Questo è il primo passo nella dimostrazione per induzione che se $c = [x_1, x_2, \dots, x_k]$ è un commutatore di peso $k \geq 2$ con entrate $x_i \in \{l_1, l_2, \dots, l_d\}$, la funzione $u_c: H \rightarrow L$ con supporto $\{1\}$ e tale che $u_c(1) = c$ appartiene a $\Phi(G)$; infatti, supposto $k > 2$ e posto $c' = [x_1, \dots, x_{k-1}]$, $x_k = l_r$, $u_{c'} \in \Phi(G)$ per ipotesi induttiva e $u_c = [u_{c'}, (f_r h_r)^p] \in \Phi(G)$. Ma allora tutte le funzioni con supporto $\{1\}$ e immagine in L' appartengono a $\Phi(G)$, e anzi (il trasporto dal supporto $\{1\}$ al supporto $\{h\}$, dove $h = \prod_{i=1}^d h_i^{r_i}$, può essere realizzato coniugando con $\prod_{i=1}^d (f_i h_i)^{r_i} = f^* h \in G$, con f^* opportuno elemento di F) tutto il derivato F' di F è contenuto in $\Phi(G)$. In particolare $Z(F) = \{f: H \rightarrow L \mid \text{Im } f \subseteq Z(L)\} \leq F' = \{f: H \rightarrow L \mid \text{Im } f \subseteq L'\} \leq \Phi(G)$, da cui $Z(F) \leq Z(\Phi(G))$. Inoltre $C_G(\Phi(G)) \leq C_W(Z(F)) \wedge G = F \wedge G = \Phi(G)$. Sia ora $f \in Z(\Phi(G)) = Z(F \wedge G)$; poichè $F' \leq \Phi(G)$ risulta $\Phi(G) \triangleleft W$, $Z(\Phi(G)) \triangleleft W$ e quindi, per ogni $h \in H$, $f^{h^{-1}} \in Z(\Phi(G))$. Perciò $[f^{h^{-1}}, (f_i h_i)^p](1) = [f(h), l_i] = 1$ per $i = 1, \dots, d$, cioè $\text{Im } f \subseteq Z(L)$, $f \in Z(F)$; ne segue che $Z(\Phi(G)) = C_G(\Phi(G)) = Z(F)$. Osservando poi che $Z(F)H$ è isomorfo ad $AwrH$ con sottogruppo « base » $Z(F)$, si conclude che M è isomorfo a $Z(\Phi(G))$ come H -modulo, e la dimostrazione è terminata.

OSSERVAZIONE. Risulta immediatamente dalla dimostrazione che $Z(G) = C_{Z(F)}(H) = Z(W) \cong A$.

Combinando il teorema 2.1 con il lemma 1.1 si ottiene una famiglia di p -gruppi finiti con la proprietà che per ognuno di essi $C_G(\Phi(G)) = Z(\Phi(G))$ e $H^1(G/\Phi(G), Z(\Phi(G))) = 1$ (o, se si preferisce, tali che ogni automorfismo che induca l'identità su $\Phi(G)$ e su $G/\Phi(G)$ risulta interno), rispondendo così negativamente alla domanda posta in [4]. Rimane ovviamente aperto il problema di quali coppie (H, M) dove H, M sono p -gruppi abeliani finiti, H è elementare non ciclico, M è un H -modulo non identico tale che $H^1(H, M) = 1$, sono ottenibili in

questo modo; per quali coppie del tipo suddetto cioè esista un p -gruppo finito G con $G/\Phi(G) \cong H$ e $Z(\Phi(G)) \cong M$ come H -moduli. Un primo risultato in questa direzione è la proposizione seguente.

PROPOSIZIONE 2.2. *Siano H un p -gruppo abeliano elementare, M un H -modulo tale che $H^1(H, M) = 1$ (H, M entrambi finiti e non identici); se M è un p -gruppo abeliano elementare, allora esiste un p -gruppo abeliano A tale che M è un H -modulo intrecciato su A .*

DIMOSTRAZIONE. Sia A un complemento (gruppale) di $[M, H]$ in M . Dimosteremo che M è un H -modulo intrecciato su A ; poichè se X è un H -sottomodulo di M tale che $M = X[M, H]$ allora $X = M$, si tratta di verificare che $M = \langle A^h | h \in H \rangle = \bigtimes_{h \in H} A^h$. Faremo induzione su $d = \dim H$. Se $d = 1$, $H = \langle t \rangle$, sia B un sottogruppo di A tale che $B^{\langle t \rangle} = B \times B^t \times \dots \times B^{t^{p-1}}$, massimale rispetto a questa proprietà.

Supponiamo che B sia diverso da A , e sia $a \in A \setminus B \cdot \langle a \rangle^{\langle t \rangle}$ ha ordine p , perchè altrimenti sarebbe $a^{f(t)} = 1$ con $f \in \mathbb{Z}/p\mathbb{Z}[x]$ di grado minore di p , e il polinomio minimo di t su $\langle a \rangle^{\langle t \rangle}$, che è del tipo $(x-1)^r$, avrebbe grado minore di p e quindi dividerebbe $(x-1)^{p-1}$; ma allora sarebbe $a^{1+t+\dots+t^{p-1}} = 1$, cioè $a \in [M, t]$, una contraddizione. Supponiamo ora $\langle a \rangle^{\langle t \rangle} \wedge B^{\langle t \rangle} \neq 1$; allora $1 \neq a^{(t-1)^{p-1}} \in B^{\langle t \rangle}$, anzi $a^{(t-1)^{p-1}} \in C_{B^{\langle t \rangle}}(t)$; ma $B^{\langle t \rangle}$ è un $\langle t \rangle$ -modulo intrecciato su B , e quindi $H^1(\langle t \rangle, B) = 1$, e $C_{B^{\langle t \rangle}}(t) = \{b^{1+t+\dots+t^{p-1}} | b \in B\}$, da cui $a^{(t-1)^{p-1}} = b^{(t-1)^{p-1}}$ per qualche $b \in B$, $(a^{-1}b)^{1+t+\dots+t^{p-1}} = 1$, $a^{-1}b \in [M, t] \wedge A = 1$, $a = b \in B$, contraddizione. Questo significa che $(\langle a \rangle \times B)^{\langle t \rangle}$ ha ordine $p^2 |B|^p =$
 $= |\langle a \rangle \times B|^p$, cioè $(\langle a \rangle \times B)^{\langle t \rangle} = \bigtimes_{i=0}^{p-1} (\langle a \rangle \times B)^{t^i}$, contro la massimalità

di B : abbiamo visto che $B = A$, cioè la tesi (se $d = 1$). Sia ora $d > 1$, $H = K \times \langle l \rangle$ con $l \neq 1$; $H^1(\langle l \rangle, M) = 1$ dà, per quanto visto sopra, $|M| = |M/[M, l]|^p = |C_M(l)|^p \cdot C_M(l)$ è un K -sottomodulo di M ed è subito visto che $H^1(K, C_M(l)) = 1$. Per l'ipotesi induttiva allora, se U è un sottogruppo di $C_M(l)$ tale che $C_M(l) = U \times [C_M(l), K]$, risulta $|C_M(l)| = |U|^{[K]}$. Ora, un tale U è $A^{1+l+\dots+l^{p-1}}$; infatti $C_M(l) = M^{1+l+\dots+l^{p-1}} = A^{1+l+\dots+l^{p-1}} \times [M, H]^{1+l+\dots+l^{p-1}}$ perchè $\text{Ker}(1+l+\dots+l^{p-1}) = [M, l] \leq [M, H]$ e

$$[M, H]^{1+l+\dots+l^{p-1}} = [M^{1+l+\dots+l^{p-1}}, K] = [C_M(l), K];$$

inoltre $|A^{1+l+\dots+l^{p-1}}| = |A|$. In conclusione $|M| = |C_M(l)|^p = |A|^{[K]^p} = |A|^{[H]}$, come volevasi.

La proposizione precedente risponde al problema posto per le coppie (H, M) con M di esponente p ; è d'altra parte facile costruire esempi di H -moduli M con $|H| = p^2$, $\exp M = p^2$, $H^1(H, M) = 1$ che non sono intrecciati, ai quali dunque la proposizione precedente e la costruzione del teorema 2.1 non si applicano.

BIBLIOGRAFIA

- [1] B. HUPPERT, *Endliche Gruppen I*, Berlin - Heidelberg - New York (1967).
- [2] O. MÜLLER, *On p -automorphisms of finite p -groups*, Arch. Math., **32** (1979), pp. 533-538.
- [3] R. E. PHILLIPS, *Embedding methods for periodic groups*, Proc. London Math. Soc., (3) **35** (1977), pp. 238-256.
- [4] P. SCHMID, *A cohomological property of regular p -groups*, Math. Z., **175** (1980), pp. 1-3.

Manoscritto pervenuto in redazione il 29 novembre 1981.