RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ANDREA LUCCHINI

Sui gruppi il cui gruppo delle autoproiettività è transitivo sugli atomi

Rendiconti del Seminario Matematico della Università di Padova, tome 75 (1986), p. 275-294

<http://www.numdam.org/item?id=RSMUP_1986__75__275_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 75 (1986)

Sui gruppi il cui gruppo delle autoproiettività è transitivo sugli atomi.

ANDREA LUCCHINI

Negli anni passati sono stati studiati i gruppi finiti con il gruppo degli automorfismi che agisce in maniera transitiva sui sottogruppi minimi: è stato dimostrato che si tratta di p-gruppi i quali, per p dispari, risultano abeliani (vedi [5]).

Lo scopo di questo lavoro è affrontare un problema che traduce quello appena esposto in termini di proprietà del reticolo dei sottogruppi: ci si occupa infatti dei gruppi finiti con il gruppo delle autoproiettività transitivo sugli atomi del reticolo dei sottogruppi.

Poichè ogni automorfismo induce un'autoproiettività tutti i gruppi il cui gruppo degli automorfismi è transitivo sugli atomi godono della proprietà reticolare richiesta; non vale il viceversa: ad esempio, mentre un gruppo il cui gruppo degli automorfismi è transitivo sugli atomi è necessariamente un p-gruppo, questo non succede per le autoproiettività. Il primo risultato ottenuto in questo lavoro è per l'appunto la completa descrizione dei gruppi finiti che soddisfano alla proprietà in questione ma il cui ordine è divisibile per almeno due primi distinti.

Il secondo risultato riguarda invece i p-gruppi e rivela che, per $p \neq 2$, i p-gruppi con un sottogruppo ciclico del gruppo delle autoproiettività transitivo sugli atomi sono modulari e dunque sono tutti e soli i p-gruppi proiettivi a gruppi con un sottogruppo ciclico del gruppo degli automorfismi transitivo sugli atomi (cfr. [4]).

Tale risultato è falso per $p = 2$ così come non valgono per $p = 2$ i risultati generali ottenuti nel caso degli automorfismi: l'eccezione-

Indirizzo dell'A.: Istituto di Algebra e Geometria, via Belzoni 7, 35131 Padova.

lità dei 2-gruppi è legata all'esistenza di 2-gruppi non ciclici ma con un unico sottogruppo minimo.

Le notazioni scelte sono quelle solitamente usate.

1. Vale il seguente risultato:

TEOREMA A: *Sia G un gruppo finito con l'ordine divisibile per almeno due primi distinti e con il gruppo delle autoproiettività transitivo sugli atomi del reticolo dei sottogruppi di G: G è ciclico con le componenti primarie della stessa altezza oppure è P-gruppo.* (Un p-gruppo ciclico di ordine p^k è detto di altezza k, per la definizione di P-gruppo vedi [1] pag. 11).

DIMOSTRAZIONE. Sia G un S-gruppo, cioè sia $G = P \times H$ con P un P-gruppo non ciclico e con gli ordini di H e P coprimi: supponiamo per assurdo $H \neq \langle 1 \rangle$: sia C_r un sottogruppo di H d'ordine r con r un primo che non divide $|P|$. Sia P abeliano elementare d'ordine p^{n+1} e sia C_p un suo sottogruppo d'ordine p. È $C_r = C_p^\sigma$ per un'opportuna autoproiettività σ. Poichè $L(G) = L(P) \times L(H)$ è anche $L(G) = L(G^\sigma) = L(P^\sigma) \times L(H^\sigma)$. In base al teorema 4 dimostrato a pag. 5 di [1] P^σ e H^σ devono avere ordini coprimi ma P^σ è P-gruppo d'ordine $p^n r$ e p divide $|H^\sigma|$: assurdo. Sia invece $|P| = p^n q$ $(p > q)$ e sia C_q un q-Sylow di P; sia σ autoproiettività tale che $C_r = C_q^\sigma$: $G = P^\sigma \times H^\sigma$ e $|P^\sigma| = p^n r$ quindi i q-Sylow di G centralizzano il p-Sylow di G essendo tutti contenuti in H^σ ma questo nega che P sia P-gruppo: di nuovo un assurdo. Dunque se G è S-gruppo è necessariamente P-gruppo.

G non sia S-gruppo e sia π l'insieme dei primi che dividono $|G|$: poichè le autoproiettività agiscono transitivamente sugli atomi per ogni $p_i \in \pi$ esiste una autoproiettività di G singolare in p_i: per la proposizione 2.9 a pag. 44 in [1] le singolarità sono tutte di prima specie (vedi per la def. [1] pag. 42) e dunque ([1] prop. 2.8 pag. 43) G contiene, per ogni $p_i \in \pi$, un p_i Sylow complemento normale Q_i. $\bigcap_{i \neq j} Q_i$ è un p_j-Sylow ed è normale perchè intersezione di normali: dunque G è prodotto diretto dei suoi sottogruppi di Sylow. Sia S_i il p_i-sottogruppo di Sylow di G: per ogni $p_j \in \pi$, $i \neq j$, esiste una autoproiettività φ che manda un sottogruppo di S d'ordine p_i in un sottogruppo di G d'ordine p_j: S^φ è il p_j-Sylow di G (vedi [1] th. 12 pag. 47); da [1] th. 12 pag. 12 segue che S è ciclico d'ordine p_i^n e S^φ è ciclico d'ordine p_j^n. Quindi se G non è S-gruppo è ciclico con le componenti primarie della stessa altezza.

2. Lo scopo del lavoro successivo è la dimostrazione del seguente risultato:

TEOREMA B: *Sia G un p-gruppo finito, $p \neq 2$, con un sottogruppo ciclico, $\langle\sigma\rangle$, del gruppo delle autoproiettività transitivo sugli atomi: G è modulare.*

Dimostriamo prima alcune proprietà generali dei p-gruppi con la proprietà reticolare richiesta.

In tutto questo paragrafo con G si intende un p-gruppo con p dispari, di esponente p^m e con il gruppo delle autoproiettività transitivo sugli atomi.

Valgono per G i seguenti risultati:

PROPOSIZIONE 2.1:

i) *Sia $a \in G$ con $|a| = p$: $a \in N_G(H)$ per ogni $H \leqslant G$;*

ii) $\Omega_1(G) = \{a: a \in G \text{ e } a^p = 1\}$ è un sottogruppo abeliano di G;

iii) $\Omega_1(G) = \mathfrak{O}_{m-1}(G)$.

DIMOSTRAZIONE DI (i). $Z(G) \neq \langle 1\rangle$ poichè G è p-gruppo: sia $\langle z\rangle \leqslant \leqslant Z(G)$ d'ordine p: $\langle z\rangle$ è di Dedekind e dunque lo è $\langle a\rangle$ essendo l'immagine di $\langle z\rangle$ tramite un'autoproiettività ma i sottogruppi di Dedekind di un gruppo nilpotente sono quasi normali: H contiene $\langle a\rangle$ oppure è massimo, e dunque normale, in $\langle H, a\rangle = H\langle a\rangle$.

(ii) è ovvia conseguenza di (i).

DIMOSTRAZIONE DI (iii). $\Omega_{m-1}(G) \leqslant \Omega_1(G)$ è ovvio. Viceversa: G contiene un sottogruppo ciclico $\langle a\rangle$ d'ordine p^m: sia $g \in \Omega_1(G)$: esiste un'autoproiettività σ con $\langle g\rangle = \langle a^{p^{m-1}}\rangle^\sigma$: $\langle a\rangle^\sigma$ è ciclico d'ordine p^m e contiene $\langle g\rangle$.

PROPOSIZIONE 2.2. *Siano g_1 e g_2 appartenenti a G con $|g_1| = |g_2| = p^2$ e $\langle g_1^p\rangle = \langle g_2^p\rangle$:* è $\langle g_1\rangle\, \Omega_1(G) = \langle g_2\rangle\, \Omega_1(G)$.

DIMOSTRAZIONE. Sia $a\Omega_1(G) \in Z(G/\Omega_1(G))$ con $|a| = p^2$ e sia $b \in G$ con $a^p = b^p$; se $\langle a\rangle = \langle b\rangle$ è ovviamente $\langle a\rangle\, \Omega_1(G) = \langle b\rangle\, \Omega_1(G)$. Sia $\langle a\rangle \neq \langle b\rangle$: $[a, b] = g \in \Omega_1(G)$. Se $g \in \langle a^p\rangle$ è $|\langle a, b\rangle| = p^3$: $\langle a, b\rangle$ contiene almeno due sottogruppi minimi distinti poichè $p \neq 2$ e $\langle a, b\rangle$ non è ciclico: esiste dunque $h \in \langle a, b\rangle$ d'ordine p con $h \notin \langle a\rangle$; è $\langle a, h\rangle = \langle a, b\rangle$ da cui $b \in \langle a, h\rangle \leqslant \langle a\rangle\, \Omega_1(G)$; analogamente $a \in \langle b\rangle \Omega_1(G)$

e dunque $\langle a\rangle\,\Omega_1(G) = \langle b\rangle\,\Omega_1(G)$. Se invece $g \notin \langle a^p\rangle$ segue da 2.1 (i) che $\langle a^p, g\rangle = \Omega_1\langle a, b\rangle$. Consideriamo un'autoproiettività σ che mandi $\langle g\rangle$ in $\langle z\rangle$ con $z \in Z(G)$: esistono a_1 e b_1 tali che $\langle a\rangle^\sigma = \langle a_1\rangle$, $\langle b\rangle^\sigma = \langle b_1\rangle$ e $a_1^p = b_1^p$. $[a_1, b_1] \in \Omega_1\langle a_1, b_1\rangle = \Omega_1(\langle a, b\rangle^\sigma) = (\Omega_1\langle a, b\rangle)^\sigma =$ $= \langle a^p, g\rangle^\sigma = \langle a_1^p, z\rangle \leqslant Z\langle a_1, b_1\rangle$: $\langle a_1, b_1\rangle$ è nilpotente di classe al più due e quindi $(a_1 b_1^{-1})^p = 1 : a_1 b_1^{-1} \in \Omega_1(G)$ implica $\langle a\rangle\,\Omega_1(G) = (\langle a_1\rangle\,\Omega_1(G))^{\sigma^{-1}} =$ $= (\langle b_1\rangle\,\Omega_1(G))^{\sigma^{-1}} = \langle b\rangle\Omega_1(G)$. Se poi è $\langle b_1^p\rangle = \langle b_2^p\rangle = \langle a^p\rangle$ risulta $\langle b_1\rangle\,\Omega_1(G) = \langle a\rangle\,\Omega_1(G) = \langle b_2\rangle\,\Omega_1(G)$. Siano infine $\langle g_1\rangle$ e $\langle g_2\rangle$ due sottogruppi d'ordine p^2 con $\langle g_1^p\rangle = \langle g_2^p\rangle$: è $\langle g_1\rangle\,\Omega_1(G) = \langle g_2\rangle\,\Omega_1(G)$: se così non fosse, se σ è un'autoproiettività che manda $\langle g_1^p\rangle$ in $\langle a^p\rangle$, sarebbe $(\langle g_1\rangle\,\Omega_1(G))^\sigma \neq (\langle g_2\rangle\,\Omega_1(G))^\sigma$ cioè $\langle b_1\rangle\,\Omega_1(G) \neq \langle b_2\rangle\,\Omega_1(G)$ per b_1 e b_2 tali che $\langle g_1\rangle^\sigma = \langle b_1\rangle$ e $\langle g_2\rangle^\sigma = \langle b_2\rangle$ e quindi tali che $\langle b_1^p\rangle =$ $= \langle b_2^p\rangle = \langle a^p\rangle$ in contrasto con quanto appena dimostrato.

$\Omega_1(G)^\sigma = \Omega_1(G)$ per ogni σ autoproiettività di G e dunque ogni autoproiettività di G induce un'autoproiettività su $G/\Omega_1(G)$: vale a questo proposito il seguente risultato:

PROPOSIZIONE 2.3. *Se T è un sottogruppo del gruppo delle autoproiettività di G transitivo sugli atomi del reticolo di G allora il gruppo delle autoproiettività indotto da T su $G/\Omega_1(G)$ è transitivo sugli atomi di $G/\Omega_1(G)$.*

DIMOSTRAZIONE. Siano $H/\Omega_1(G)$ e $K/\Omega_1(G)$ due atomi del reticolo di $G/\Omega_1(G)$: è $H = \langle a\rangle\,\Omega_1(G)$, $K = \langle b\rangle\,\Omega_1(G)$ con $|a| = |b| = p^2$: sia $\sigma \in T$ con $\langle a^p\rangle^\sigma = \langle b^p\rangle$: $\langle a\rangle^\sigma = \langle b_1\rangle$ con $\langle b_1^p\rangle = \langle b^p\rangle$: $(\langle a\rangle\,\Omega_1(G))^\sigma =$ $= \langle b_1\rangle\,\Omega_1(G) = \langle b\rangle\,\Omega_1(G)$ in base alla proposizione precedente e dunque l'autoproiettività indotta da σ su $G/\Omega_1(G)$ fa corrispondere $K/\Omega_1(G)$ a $H/\Omega_1(G)$. Valgono infine le seguenti proprietà:

PROPOSIZIONE 2.4.

i) *per ogni k, $1 \leqslant k \leqslant m-1$, il gruppo delle autoproiettività di $G/\Omega_k(G)$ è transitivo sugli atomi*;

ii) $\Omega_k(G) = \{x : x \in G \text{ e } x^{p^k} = 1\}$;

iii) $1 \leqslant \Omega_1(G) \leqslant \ldots \leqslant \Omega_{m-1}(G) \leqslant G$ *è serie abeliana di G*;

iv) *ogni elemento di G è contenuto in un sottogruppo ciclico d'ordine p^m*;

v) $\Omega_1(G) \leqslant Z(G)$.

Le prime quattro proprietà si dimostrano per induzione tenendo

conto dei risultati precedenti e osservando che

$$\Omega_i(G/\Omega_1(G)) = \Omega_{i+1}(G)/\Omega_1(G)\,.$$

Dimostriamo (v) per induzione sull'esponente di G: sia $x \in \Omega_1(G)$: in base a 2.1 (iii) è $x = a^{p^{m-1}}$; $a^{p^{m-2}}\Omega_1(G) \in \Omega_1(G/\Omega_1(G)) \leqslant Z(G/\Omega_1(G))$ per ipotesi induttiva: per ogni $b \in G$ $b^{-1}a^{p^{m-2}}b = a^{p^{m-2}}g(b)$ con $g(b)$ un elemento di $\Omega_1(G)$ dipendente da b; $[a^{p^{m-2}}, g(b)] \in \langle a^{p^{m-1}}\rangle$ poichè $g(b)$ normalizza a ed ha ordine al più p: $[a^{p^{m-2}}, g(b)] \in Z\langle a^{p^{m-2}}, g(b)\rangle$ ma allora $\langle a^{p^{m-2}}, g(b)\rangle$ è nilpotente di classe al più 2 e $(a^{p^{m-2}}g(b))^p = a^{p^{m-1}}g(b)^p = a^{p^{m-1}}$. Quindi

$$b^{-1}xb = b^{-1}a^{p^{m-1}}b = (b^{-1}a^{p^{m-2}}b)^p = (a^{p^{m-2}}g(b))^p = a^{p^{m-1}}\,.$$

3. Iniziamo la dimostrazione del teorema B: se G ha esponente p da 2.1 (ii) segue che G è abeliano elementare. Se G ha esponente p^m con $m \underset{\neq}{>} 1$ in base a 2.3 si può procedere per induzione e supporre che $G/\Omega_1(G)$ sia un gruppo modulare di esponente p^{m-1}: in tale situazione si dimostra il seguente risultato:

LEMMA 3.1. *Esiste un p-gruppo A proiettivo a G tale che $G/\Omega_1(A)$ è abeliano.*

La dimostrazione di tale lemma viene condotta per passi successivi:

i) In base al teorema di Iwasawa sulla struttura dei p-gruppi modulari (vedi [1] th. 14 pag. 13) esistono in G un sottogruppo normale N e un elemento g di ordine p^m con $G = \langle g, N\rangle$, $N/\Omega_1(G)$ abeliano e $(x\Omega_1(G))^{g\Omega_1(G)} = x^{1+p^s}\Omega_1(G)$ per ogni $x \in N$: se poi N è scelto massimale rispetto alle proprietà a cui deve soddisfare vale $n + s + 1 = m$ se $p^n = |G/N|$. Si può supporre $s \neq 0$ altrimenti $G/\Omega_1(G)$ sarebbe abeliano e non ci sarebbe altro da dimostrare.

ii) Esiste un sottogruppo M di N con $\Omega_1(G) \leqslant M$, $M \lhd G$ e G/M ciclico d'ordine p^{n+1}.

DIMOSTRAZIONE. $G/\Omega_1(G)$, essendo modulare e in base a 2.4 (iv), ammette una base del tipo $g\Omega_1(G)$, $v_1\Omega_1(G)$, ..., $v_k\Omega_1(G)$ con $|g\Omega_1(G)| = |v_i\Omega_1(G)| = p^{m-1}$ per ogni i $1 \leqslant i \leqslant k$; essendo $G = \langle g, N\rangle$ non è restrittivo supporre $v_i \in N$; $\langle g\Omega_1(G)\rangle \cap N/\Omega_1(G) = \langle g^{p^n}\Omega_1(G)\rangle \neq \Omega_1(G)$ poichè $m - 1 \underset{\neq}{>} n$: $M = \langle g^{p^{n+1}}, v_1, \ldots, v_k\rangle$ soddisfa alle proprietà richieste.

iii) $(1+p^s)$ ha ordine p^{n+1} mod p^m poichè $s+n+1=m$ dunque $((1+p^s)^{p^{n+1}}-1)/p^s = e^*p^{n+1}$ con $(e^*, p)=1$: $g^{p^{n+1}} = u = v^{e^*}$ con u e v appartenenti ad M.

iv) L'applicazione di M in M che manda x in x^{1+p^s} è automorfismo: infatti poichè $M' \leqslant \Omega_1(G) \leqslant Z(G)$

$$(ab)^{1+p^s} = a^{1+p^s}b^{1+p^s}[b,a]^{(1+p^s)p^s/2} = a^{1+p^s}b^{1+p^s}.$$

v) Per ogni $a \in M$ è $a^g = a^{1+p^s}\delta(a)$ con $\delta(a)$ un elemento di $\Omega_1(G)$ dipendente da a; definisco una applicazione ξ di M in sè nel modo seguente:

$a^\xi = a\delta(a)$:

$$a^{1+p^s}\delta(a)b^{1+p^s}\delta(b) = a^g b^g = (ab)^g = (ab)^{1+p^s}\delta(ab) = a^{1+p^s}b^{1+p^s}\delta(ab)$$

quindi

$$(ab)^\xi = ab\delta(ab) = ab\delta(a)\delta(b) = a\delta(a)b\delta(b) = a^\xi b^\xi;$$

inoltre $a\delta(a)=1$ implica $a \in \Omega_1(G)$: $a^g = a$ e $\delta(a) = a = 1$; ξ è un automorfismo. Poichè $a^{\xi^i} = a\delta(a)^i$ $\xi^p = 1$.

Sia $\langle t \rangle$ un gruppo ciclico d'ordine p^m: consideriamo $A = M\langle t \rangle$, prodotto semidiretto parziale di M e $\langle t \rangle$ con $t^{p^{n+1}} = v$ e $x^t = x^\xi$ per ogni $x \in M$ (poichè ξ è automorfismo con $\xi^p = 1$ e, essendo $\Omega_{m-1}(M) \leqslant \leqslant Z(G)$, $v^\xi = v$ le condizioni perchè A esista — vedi [2] pag. 25-27 — sono soddisfatte): A ha esponente p^m, A/M ha ordine p^{n+1}, $A/\Omega_1(A)$ è abeliano e $\Omega_1(A) \leqslant Z(A)$; si osserva inoltre che $\Omega_{m-1}(A) \leqslant Z(A)$.

vi) Ogni x appartenente ad A si scrive nella forma $x = a^{i(x)}$ con $a \in M$: la scrittura non è unica ma è individuata (mod p^m) $i(x)p^s$. Poichè A è nilpotente di classe al più due e A' ha esponente p l'applicazione $\tau(x)$ di A in sè che manda ogni $y \in A$ in $y^{1+i(x)p^s}$ è un automorfismo; così è definita una applicazione τ da A in $P(\mathrm{Aut}\, A)$, l'insieme degli automorfismi potenza di A. È $\tau(x) = 1$ per ogni x appartenente ad M e $y^{\tau(t)} = y^{1+p^s}$ per ogni $y \in A$.

vii) $\tau(x)\tau(y) = \tau(x^{\tau(y)}y)$ essendo x e y arbitrari elementi di A.

Dimostrazione. Sia $x = at^{i(x)}$ e $y = bt^{i(y)}$; per ogni $z \in A$ è

$$z^{\tau(x)\tau(y)} = z^{(1+i(x)p^s)(1+i(y)p^s)} = z^{1+(i(x)+i(y)+i(x)i(y)p^s)p^s};$$

$$x^{\tau(y)}y = \left(at^{i(x)}\right)^{1+i(y)p^s}bt^{i(y)} = a^{1+i(y)p^s}t^{i(x)(1+i(y)p^s)}bt^{i(y)} = a^*b^*t^{i(x)+i(x)i(y)p^s+i(y)}$$

con a^* e b^* opportuni elementi di M: dunque

$$z^{\tau(x^{\tau(y)}y)} = z^{1+(i(x)+i(x)i(y)p^s+i(y))p^s}.$$

viii) Da vii) segue che l'identità di A in sè è un τ-automorfismo incrociato (cfr. [3]); è noto che in tale situazione se su A definisco una nuova operazione « $\circ$ » ponendo $x \circ y = x^{\tau(y)}y$ $(A, \circ)$ è ancora un gruppo che nel nostro caso indicheremo con G_1.

ix) L'identità è una biezione da A in G_1 che induce una proiettività tra questi due gruppi.

DIMOSTRAZIONE. È sufficiente verificare che per x e y appartenenti ad A valgono le relazioni:

a) $x \circ y \in \langle x, y\rangle_A$

b) $xy \in \langle x, y\rangle_{G_1}$:

$x \circ y = x^{\tau(y)}y \in \langle x\rangle_A y \subseteq \langle x, y\rangle_A$ poichè $\tau(y)$ è automorfismo potenza. È anche $\langle x^{\tau(y)}\rangle_A = \langle x\rangle_A$ quindi $x = x^{\lambda\tau(y)}$ e $xy = x^{\lambda\tau(y)}y = x^{\lambda} \circ y$: dunque per verificare (b) basta vedere che $x^{\lambda} \in \langle x\rangle_{G_1}$; ma questo è vero perchè $|x|_A = |x|_{G_1}$: infatti vale $(x^r)_{G_1} = x^{1+\tau(x)+\ldots+\tau(x)^{r-1}}$ e allora sia $p^k = |x|_A$ e $r = |x|_{G_1}$: $1 = (x^r)_{G_1} = x^{1+\tau(x)+\ldots+\tau(x)^{r-1}}$: $x^{\tau(x)} = x^{1+p^s\nu}$ pertanto $1 + (1 + \nu p^s) + \ldots + (1 + \nu p^s)^{r-1} \equiv 0 \mod p^k$ e quindi $(1 + \nu p^s)^r - 1 = \mu p^k \nu p^s$ e questo implica che p^k divide r; ovviamente $r \leqslant p^k$ poichè $\langle x\rangle_{G_1} \leqslant \langle x\rangle_A$ e quindi si conclude $r = p^k$.

x) G_1 e G sono isomorfi.

DIMOSTRAZIONE. È $G = \langle M, g\rangle$ e $G_1 = \langle M, t\rangle$ con M che eredita da G, da A e da G_1 la stessa operazione. Sia $\hat{t}$ l'inverso di t in G_1 (è $\hat{t} = (t^{-1})^{\tau(t)^{-1}}$) e sia $a \in M$: $\hat{t} \circ a \circ t = (\hat{t} \circ a)^{\tau(t)}t = (\hat{t}a)^{\tau(t)}t = \hat{t}^{\tau(t)}a^{\tau(t)}t = t^{-1}a^{1+p^s}t = a^{1+p^s}\delta(a) = g^{-1}ag$; inoltre

$$(t^{p^{n+1}})_{G_1} = t^{1+\tau(t)+\ldots+\tau(t)^{p^{n+1}-1}} = t^{1+(1+p^s)+\ldots+(1+p^s)^{p^{n+1}-1}} =$$

$$= t^{(1+p^s)^{p^{n+1}}-1/p^s} = t^{e^*p^{n+1}} = v^{e^*} = u = g^{p^{n+1}}.$$

Le relazioni appena evidenziate permettono di dimostrare che l'applicazione ϱ da G a G_1 che fa corrispondere at^i all'elemento ag^i è ben definita ed è un isomorfismo: infatti sia $ag^i = bg^j$: $b^{-1}a = g^{j-i} \in \langle g\rangle \wedge M =$

$= \langle g^{p^{n+1}} \rangle$: $b^{-1}a = g^{j-i} = t^{j-i}$ e quindi $at^i = bt^j$; inoltre

$$(ag^ibg^j)^\varrho = (ab^{g^{-i}}g^{i+j})^\varrho = (ab^{g^{-i}})t^{i+j} = ab^{t^{-i}}t^{i+j} = at^ibt^j = (ag^i)^\varrho\,(bg^j)^\varrho\,.$$

Questo conclude la dimostrazione del lemma 3.1: in base a tale lemma si potrà considerare dimostrata la tesi del teorema B se e solo se la dimostreremo per il gruppo A: infatti G è modulare se e solo se lo è A visto che A e G sono proiettivi. All'autoproiettività che opera transitivamente sugli atomi di G corrisponde un'autoproiettività che opera transitivamente sugli atomi di A.

Con tecniche simili a quelle usate per la dimostrazione del lemma 3.1 si ottiene il seguente risultato, che sarà utile nell'ultima parte della dimostrazione del teorema B.

LEMMA 3.2. *Sia N un sottogruppo massimale di A, $g \in A \setminus N$ con $|g| = \exp(A) = p^m$, $r \in \mathbb{Z}$ con $(r,p) = 1$: si può cambiare l'operazione su A ottenendo un gruppo A_1 proiettivo ad A e tale che, se con $[x,y]_A$ e $[x,y]_{A_1}$ indico il commutatore di x e y calcolato, rispettivamente, in A e A_1, valgono le relazioni*:

i) $[x,y]_A = [x,y]_{A_1}$ per ogni x e y appartenenti a N,

ii) $[x,g]_{A_1} = [x,g]_A x^{rp^{m-1}}$ per ogni $x \in N$.

DIMOSTRAZIONE. Ogni $a \in A$ si scrive nella forma $a = yg^{i(a)}$ con $y \in N$; tenendo conto che $|A/N| = p$ e procedendo come nel passo (vi) della dimostrazione del lemma 3.1 si definisce una corrispondenza τ da A a P (Aut A) ponendo $x^{\tau(a)} = x^{1+i(a)rp^{m-1}}$: valgono anche in questo caso le proprietà:

i) $\tau(y)$ è l'identità per ogni $y \in N$,

ii) $a^{\tau(a)} = a^{1+rp^{m-1}}$ per ogni $a \in A$,

iii) $\tau(x)\tau(y) = \tau\big(x^{\tau(y)}y\big)$.

Dunque su A si può definire una nuova operazione « $\circ$ » ponendo $x \circ y = x^{\tau(y)}y$ e $A_1 = (A, \circ)$ risulta essere un gruppo proiettivo ad A. Poichè il cambiamento di operazione lascia inalterata l'operazione indotta su N, se x e y sono elementi di N è $[x,y]_A = [x,y]_{A_1}$. Sia $x \in N$, $\hat{x}$ e $\hat{g}$ gli inversi, rispettivamente, di x e g in A_1: $\hat{x} = x^{-1}$ e $\hat{g} = (g^{-1})^{\tau(g)^{-1}}$;

$$\hat{g} \circ x \circ g = \big(\hat{g}^{\tau(x)}x\big)^{\tau(g)}g = (\hat{g}x)^{\tau(g)}g =$$

$$= \big((g^{-1})^{\tau(g)^{-1}}x\big)^{\tau(g)}g = g^{-1}x^{\tau(g)}g = g^{-1}x^{1+rp^{m-1}}g = g^{-1}xgx^{rp^{m-1}};$$

dunque

$$[x, g]_{A_1} = \hat{x} \circ \hat{g} \circ x \circ g = x^{-1} \circ (g^{-1} x g x^{p^{m-1}}) =$$
$$= (x^{-1})^{\tau(g^{-1} x g x^{rp^{m-1}})} g^{-1} x g x^{rp^{m-1}} = x^{-1} g^{-1} x g x^{rp^{m-1}} = [x, g]_A x^{rp^{m-1}} .$$

4. Se A è generato da due elementi, tenendo presente che, fissati ad arbitrio due elementi a, b, risulta $\Omega_1\langle a, b\rangle \leqslant \langle a^{p^{m-1}}, b^{p^{m-1}}, [a, b]\rangle$ e che in base a 2.4 (iv) anche $\Omega_1(A)$ è generato da due elementi, si deduce che per ogni coppia (a, b) di elementi di A vale $\langle a, b\rangle = \langle a\rangle\langle b\rangle$: dunque in tale ipotesi A è quasi-Hamiltoniano e quindi modulare. Pertanto nel seguito della dimostrazione si può supporre $\Omega_1(A)$ generato da almeno tre elementi indipendenti. $\Omega_1(A)$ è abeliano elementare e dunque lo si può pensare come spazio vettoriale sul corpo $K = GF(p)$; lo stesso si può dire di $A/\Omega_{m-1}(A)$: l'applicazione π da $A/\Omega_{m-1}(A)$ in $\Omega_1(A)$ definita ponendo $(a\Omega_{m-1}(A))^\pi = a^{p^{m-1}}$ è in tal senso un K-isomorfismo. Poichè si sta assumendo che la K-dimensione di $\Omega_1(A)$ è almeno 3 posso supporre che l'autoproiettività σ transitiva sugli atomi di A sia indotta su $\Omega_1(A)$ e $A/\Omega_{m-1}(A)$ da due K-isomorfismi, α e α_1 rispettivamente, scelti tali che sia $\alpha_1\pi = \pi\alpha$. α opera transitivamente sui sottospazi 1-dimensionali di $\Omega_1(A)$: questo comporta l'esistenza di un K-isomorfismo ϱ di $\Omega_1(A)$ sul gruppo additivo di una estensione finita $K(\lambda)$ di K tale che $(v)^{\alpha\varrho} = \lambda(v^\varrho)$ per ogni $v \in \Omega_1(A)$ (cfr. [7] pag. 80).

Poichè $A' \leqslant \Omega_1(A) \leqslant Z(A)$ è ben definita una applicazione K-bilineare γ da $\Omega_1(A) \times \Omega_1(A)$ in $\Omega_1(A)$ tramite la posizione $\gamma(x, y) = [a, b]$ essendo a e b scelti tali che $x = (a\Omega_{m-1}(A))^\pi$ e $y = (b\Omega_{m-1}(A))^\pi$: dunque $\Omega_1(A)$ si può atteggiare a K-algebra; tale struttura di algebra la trasporto su $K(\beta)$ mediante ϱ ponendo $\beta(l, m) = \gamma(l^{\varrho^{-1}}, m^{\varrho^{-1}})^\varrho$ per ogni coppia (l, m) di elementi in $K(\beta)$.

LEMMA 4.1. *Per ogni a, b appartenenti a $K(\lambda)$ risulta $\beta(\lambda a, \lambda b) = k_1(a, b)\lambda\beta(a, b) + k_2(a, b)\lambda a + k_3(a, b)\lambda b$ con $k_1(a, b)$, $k_2(a, b)$ e $k_3(a, b)$ elementi di K dipendenti da a e b.*

DIMOSTRAZIONE. Sia $a = (x\Omega_{m-1}(A))^{\pi\varrho}$ e $b = (y\Omega_{m-1}(A))^{\pi\varrho}$:

$$\beta(\lambda a, \lambda b) = \beta\big(\lambda(x\Omega_{m-1}(A))^{\pi\varrho}, \lambda(y\Omega_{m-1}(A))^{\pi\varrho}\big) =$$
$$= \beta\big((x\Omega_{m-1}(A))^{\pi\alpha\varrho}, (y\Omega_{m-1}(A))^{\pi\alpha\varrho}\big) =$$
$$= \gamma\big((x\Omega_{m-1}(A))^{\pi\alpha}, (y\Omega_{m-1}(A))^{\pi\alpha}\big)^\varrho =$$
$$= \gamma\big((x\Omega_{m-1}(A))^{\alpha_1\pi}, (y\Omega_{m-1}(A))^{\alpha_1\pi}\big)^\varrho = [\hat{x}, \hat{y}]^\varrho$$

essendo

$$\hat{x}\Omega_{m-1}(A) = (x\Omega_{m-1}(A))^{\alpha_1} \text{ e } \hat{y}\Omega_{m-1}(A) = (y\Omega_{m-1}(A))^{\alpha_1}.$$

Ma

$$[\hat{x}, \hat{y}] \in \Omega_1\langle \hat{x}, \hat{y}\rangle = \Omega_1(\langle x, y\rangle^\sigma) = (\Omega_1\langle x, y\rangle)^\sigma =$$
$$= (\Omega_1\langle x, y\rangle)^\alpha = \langle x^{p^{m-1}}, y^{p^{m-1}}, [x, y]\rangle^\alpha =$$
$$= \langle (x\Omega_{m-1}(A))^\pi, (y\Omega_{m-1}(A))^\pi, \gamma\big((x\Omega_{m-1}(A))^\pi, (y\Omega_{m-1}(A))\big)^\pi\rangle^\alpha$$

e dunque

$$\beta(\lambda a, \lambda b) = [\hat{x}, \hat{y}]^\varrho = k_1 x\Omega_{m-1}(A)^{\pi\alpha\varrho} + k_2 y\Omega_{m-1}(A)^{\pi\alpha\varrho} +$$
$$+ k_3\gamma(x\Omega_{m-1}(A)^\pi,\ \gamma\Omega_{m-1}(A)^\pi)^{\alpha\varrho} =$$
$$= k_1\lambda(x\Omega_{m-1}(A))^{\pi\varrho} + k_2\lambda(y\Omega_{m-1}(A))^{\pi\varrho} +$$
$$+ k_3\lambda\gamma\big((x\Omega_{m-1}(A))^\pi,\ (y\Omega_{m-1}(A))^\pi\big)^\varrho =$$
$$= k_1\lambda a + k_2\lambda b + k_3\lambda\gamma(a^{\varrho^{-1}}, b^{\varrho^{-1}})^\varrho = k_1\lambda a + k_2\lambda b + k_3\lambda\beta(a, b)$$

essendo k_1, k_2 e k_3 opportuni elementi di K.

Il teorema B sarà dimostrato se e solo se si dimostrerà che per ogni a e b in $K(\lambda)$ $\beta(a, b) \in \langle a, b\rangle$: infatti è noto che un p-gruppo finito è modulare se e solo se è quasi-Hamiltoniano: d'altra parte poichè $\Omega_{m-1}(A) \leqslant Z(A)$ A è un gruppo quasi-Hamiltoniano se e solo se per ogni coppia di elementi x, y appartenenti ad A, indipendenti e di ordine massimo, risulta $\langle x, y\rangle = \langle x\rangle\langle y\rangle$: poichè $\langle x, y\rangle/\Omega_1\langle x, y\rangle$ è abeliano e $\Omega_1\langle x, y\rangle = \langle x^{p^{m-1}}, y^{p^{m-1}}, [x, y]\rangle$ $\langle x, y\rangle = \langle x\rangle\langle y\rangle$ è equivalente a $[x, y] \in \in \langle x^{p^{m-1}}, y^{p^{m-1}}\rangle$.

Osserviamo a questo punto che per ogni $a \in K(\lambda)$ si può definire un elemento di $\mathrm{End}_K K(\lambda)$, a^*, ponendo, per ogni $b \in K(\lambda)$, $b^{a^*} = \beta(a, b)$. Sia $a_1, \ldots, a_n$ una base di $K(\lambda)$ come K-spazio vettoriale: se $a = \sum_{i=1}^{n} s_i a_i$ con $s_i \in K$ la matrice $n \times n$ ad elementi in K che rappresenta a^* rispetto a tale base ha polinomio caratteristico della forma:

$$x^n + x^{n-1} f_1(s_1, \ldots, s_n) + \ldots + x f_{n-1}(s_1, \ldots, s_n) + f_n(s_1, \ldots, s_n)$$

dove f_i è un polinomio omogeneo di grado i a coefficienti in K nelle indeterminate $s_1, \ldots, s_n$; d'altra parte poichè $a^{a^*} = a$ risulta $f_n = 0$.

Un noto teorema di Chevalley (vedi [6]) afferma che se f è un polinomio omogeneo in $K[x_1, \ldots, x_n]$ di grado minore di n (il numero delle variabili) e $f(0, \ldots, 0) = 0$ allora esiste una n-upla $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ con $a_i \in K$ e $f(a_1, \ldots, a_n) = 0$. Applico questo risultato a f_{n-1}: esiste una n-upla $(t_1, \ldots, t_n)$ con $t_i \in K$ e $f_{n-1}(t_1, \ldots, t_n) = 0$. Sia $h_1 = \sum_{i=1}^{n} t_i a_i$: il polinomio caratteristico di h_1^* è divisibile per x^2 e questo implica l'esistenza di un elemento $h_2 \in K(\lambda)$ tale che $\beta(h_1, h_2) = h_2^{h_1^*} \in \langle h_1 \rangle$.

Quanto osservato finora servirà in particolare per dimostrare che il teorema B vale per i gruppi generati da 3 elementi; prima di vedere questo è però opportuno verificare il seguente risultato:

LEMMA 4.2. *Sia n la dimensione di $K(\lambda)$ come K spazio vettoriale, X e Y gli insiemi, rispettivamene, dei sottospazi 1 e $n-1$ dimensionali di $K(\lambda)$: l'applicazione χ che ad $\langle a \rangle$ fa corrispondere $\langle a\lambda^{-1}, \ldots, a\lambda^{-(n-1)} \rangle$ è una biezione di X in Y: pertanto la moltiplicazine per λ opera transitivamente anche su Y.*

DIMOSTRAZIONE. Poichè il polinomio minimo di λ^{-1} in $K(\lambda)$ ha grado n $\lambda^{-1}, \ldots, \lambda^{-(n-1)}$ sono linearmente indipendenti e quindi lo sono, per ogni $a \in K(\lambda)$ con $a \neq 0$, $a\lambda^{-1}, \ldots, a\lambda^{-(n-1)}$: dunque il codominio di χ è effettivamente contenuto in Y; per verificare che χ è biettiva basta vedere che è iniettiva poichè $|X| = |Y| = p^n - 1/p - 1$; sia dunque $\langle a\lambda^{-1}, \ldots, a\lambda^{-(n-1)} \rangle = \langle b\lambda^{-1}, \ldots, b\lambda^{-(n-1)} \rangle = W$; è $b = af(\lambda^{-1})$ con $f(\lambda^{-1}) = \sum_{i=0}^{r} a_i \lambda^{-i}$ dove $a_i \in K$, $a_r \neq 0$ e $r \leqslant n-1$: sia per assurdo $r \neq 0$: $b\lambda^{-(n-r)} \in W$ ma $b\lambda^{-(n-r)} = a \sum_{i=0}^{r} a_i \lambda^{-(n-r+i)}$ e quindi $aa_r\lambda^{-n} \in W$: questo implica $W = \langle a\lambda^{-1}, \ldots, a\lambda^{-(n-1)}, a\lambda^{-n} \rangle = K(\lambda)$ assurdo: dunque $r = 0$, $f(\lambda^{-1}) \in K$ e $\langle b \rangle = \langle a \rangle$.

LEMMA 4.3. *Vale il teorema B se G è generato da al più tre elementi.*

DIMOSTRAZIONE. Sia $K(\lambda)$ spazio vettoriale di dimensione 3 su K: in base alle osservazioni fatte in precedenza esiste un sottospazio 2-dimensionale $\langle a_1, a_2 \rangle$ tale che $\beta(a_1, a_2) \in \langle a_1, a_2 \rangle$; vale $\beta(b_1, b_2) \in \in \langle b_1, b_2 \rangle$ per ogni coppia di elementi indipendenti: infatti in base al lemma precedente è $\langle b_1, b_2 \rangle = \lambda^i \langle a_1, a_2 \rangle$ e allora $\beta(b_1, b_2) \in \langle \beta(\lambda^i a_1, \lambda^i a_2) \rangle \leqslant$ $\leqslant$ (in base al lemma 4.1) $\leqslant \lambda^i \langle a_1, a_2, \beta(a_1, a_2) \rangle \leqslant \lambda^i \langle a_1, a_2 \rangle = \langle b_1, b_2 \rangle$.

5. Se $n = \dim(K(\lambda)) \underset{\neq}{\geqslant} 3$ continuiamo la dimostrazione del teorema B ragionando per assurdo, supponendo che esistano elementi

a, b in $K(\lambda)$ con $\beta(a,b) \notin \langle a, b\rangle$. Sotto tale ipotesi dimostriamo per passi successivi che $\beta(\lambda a, \lambda b)$ si può scrivere nella forma $k_1 \lambda\beta(a,b) + k_2(a,b)\lambda a + k_3(a,b)\lambda b$ con k_1 che non dipende nè da a nè da b. Per le coppie tali che $\beta(a,b) \in \langle a, b\rangle$ non c'è alcun conto da fare poichè in tal caso, essendo a, b e $\beta(a,b)$ linermente dipendenti, il coefficiente di $\lambda\beta(a,b)$ nella scrittura di $\beta(\lambda a, \lambda b)$ si può scegliere ad arbitrio: quello che invece va dimostrato è che $k_1(a,b)$ non dipende dai due particolari elementi a, b scelti fra tutti quelli tali che $\beta(a,b) \notin \langle a, b\rangle$.

Passo (a):siano a, b, c elementi di $K(\lambda)$ tali che:

i) $\beta(a,b) \notin \langle a, b\rangle$;

ii) $\beta(a,c) \notin \langle a, c\rangle$;

iii) $a, b, c, \beta(a,b)$ sono linearmente indipendenti:

è $k_1(a,b) = k_1(a,c)$.

DIMOSTRAZIONE. Se $\beta(a,c) \in \langle a, b, c\rangle$ sostituisco c con $c' = c + rb$ con $r \neq 0$ e tale che $\beta(a,c') \notin \langle a, c'\rangle$ (poichè $p \neq 2$ un tale r esiste altrimenti esisterebbero in K m_1, m_2 con $m_1 \neq m_2$ $m_i \neq 0$ e $\beta(a, c + m_i b) \in \in \langle a, c + m_i b\rangle$ per $i = 1$ e 2 da cui seguirebbe $\beta(a, (m_1 - m_2)b) \in \in \langle a, b, c\rangle$ in contrasto con (iii)).

a, b e c' soddisfano (i), (ii), (iii) e (iv): $\beta(a,c') \notin \langle a, c', b\rangle$ infatti $\beta(a, c + rb) \in \langle a, b, c'\rangle = \langle a, b, c\rangle$ implica $\beta(a,b) \in \langle a, b, c\rangle$ in contraddizione con (iii); se già a, c soddisfano (iv) posso scrivere $c = c'$. Per ogni $s \in K$ vale la relazione:

$$(*)\quad \beta(\lambda a, \lambda(c' + sb)) = k_1(a, c' + sb)\lambda\beta(a, c' + sb) + k_2(a, c' + sb)\lambda a + k_3(a, c' + sb)\lambda(c' + sb) = k_1(a, c' + sb)\lambda\beta(a, c') + sk_1(a, c' + sb)\lambda\beta(a, b) + k_2(a, c' + sb)\lambda a + k_3(a, c' + sb)\lambda c' + sk_3(a, c' + sb)\lambda b .$$

Ma vale anche:

$$(**)\quad \beta(\lambda a, \lambda(c' + sb)) = \beta(\lambda a, \lambda c') + s\beta(\lambda a, \lambda b) = = k_1(a, c')\lambda\beta(a, c') + k_2(a, c')\lambda a + k_3(a, c')\lambda c' + sk_1(a, b)\lambda\beta(a, b) + sk_2(a, b)\lambda a + sk_3(a, b)\lambda b .$$

Sottraendo (**) da (*) e dividendo per λ ottengo:

$$\beta(a, c')\big(k_1(a, c') - k_1(a, c' + sb)\big) + \beta(a, b)s\big(k_1(a, b) -$$
$$- k_1(a, c' + sb)\big) = a\big(k_2(a, c' + sb) - k_2(a, c') - sk_2(a, b)\big) +$$
$$+ b\big(sk_3(a, c' + sb) - sk_3(a, b)\big) + c'\big(k_3(a, c' + sb) - k_3(a, c')\big).$$

Se $k_1(a, c') = k_1(a, c' + sb)$ per qualche $s \neq 0$ deve essere anche $k_1(a, b) = k_1(a, c' + sb)$ altrimenti risulterebbe $\beta(a, b) \in \langle a, b, c' \rangle$ in contrasto con (iii). Supponiamo per assurdo che non valga $k_1(a, c') = k_1(a, c' + sb)$ per alcun $s \neq 0$: poichè $\beta(a, b)$, a, b, c' sono linearmente indipendenti $\beta(a, c')$ si scrive in modo unico come loro combinazione: pertanto per ogni $s \neq 0$ vale

$$(***) \qquad \frac{s\big(k_1(a, c' + sb) - k_1(a, b)\big)}{k_1(a, c') - k_1(a, c' + sb)} = \frac{k_1(a, c' + b) - k_1(a, b)}{k_1(a, c') - k_1(a, c' + b)}.$$

Pongo $s = \big(k_1(a, b) - k_1(a, c' + b)\big)/\big(k_1(a, c') - k_1(a, c' + b)$: è $s \neq 0$ poichè $k_1(a, c' + b) = k_1(a, b)$ implica $k_1(a, c' + b) = k_1(a, c')$ contro l'ipotesi fatta oppure $\beta(a, c') \in \langle a, b, c' \rangle$ in contrasto con (iv). Da (***), dividendo entrambi i membri per s, ottengo $k_1(a, b) = k_1(a, c')$. Se infine pongo $s = \big(k_1(a, c' + b) - k_1(a, b)\big)/\big(k_1(a, c') - k_1(a, c' - b)\big)$, divido per s entrambi i membri di (***) e sostituisco $k_1(a, b)$ a $k_1(a, c')$ trovo $k_1(a, c') = k_1(a, c' + sb)$ in contraddizione con l'ipotesi di partenza: dunque esiste $s \in K$, $s \neq 0$, tale che $k_1(a, c' + sb) = k_1(a, b) = k_1(a, c') = k_1$. Si deduce da quanto scritto finora:

$$\beta\big(\lambda a, \lambda(sb + c')\big) = k_1\lambda\beta(a, sb + c') + k_2(a, sb + c')\lambda a +$$
$$+ k_3(a, sb + c')\lambda(sb + c') = \beta(\lambda a, \lambda sb) + \beta(\lambda a, \lambda c') =$$
$$= sk_1\lambda\beta(a, b) + sk_2(a, b)\lambda a + sk_3(a, b)\lambda b +$$
$$+ k_1\lambda\beta(a, c') + k_2(a, c')\lambda a + k_3(a, c')\lambda c'$$

da cui segue:

$$\big(k_3(a, b) - k_3(a, sb + c')\big)s\lambda b + \big(k_3(a, c') - k_3(a, sb + c')\big)\lambda c' =$$
$$\big(k_2(a, sb + c') - k_2(a, b)s - k_2(a, c')\big)\lambda a.$$

Poichè a, b e c' sono linearmente indipendenti è $k_3(a, c') = k_3(a, sb + c') = k_3(a, b) = k_3$: ma allora per ogni d_1 e d_2 appartenenti a K

$$\beta(\lambda a, \lambda(d_1 b + d_2 c')) = d_1\beta(\lambda a, \lambda b) + d_2\beta(\lambda a, \lambda c') = k_1 d_1 \lambda\beta(a, b) +$$
$$+ k_3 d_1 \lambda b + k_2(a, b) d_1 \lambda a + k_1 d_2 \lambda\beta(a, c') + k_3 d_2 \lambda c' + k_2(a, c') d_2 \lambda a =$$
$$= k_1 \lambda\beta(a, d_1 b + d_2 c') + k_3 \lambda(d_1 b + d_2 c') +$$
$$+ (k_2(a, b) d_1 + k_2(a, c') d_2)\lambda a:$$

se

$$\beta(a, d_1 b + d_2 c') \notin \langle a, d_1 b + d_2 c' \rangle$$

è

$$k_1(a, d_1 b + d_2 c') = k_1 = k_1(a, b):$$

se ne deduce finalmente $k_1(a, b) = k_1(a, c)$ essendo in ogni caso c combinazione lineare di b e c'.

Passo (b): fissato a risulta $k_1(a, b) = k_1(a, c)$ per ogni coppia di elementi b e c tali che $\beta(a, b) \notin \langle a, b \rangle$ e $\beta(a, c) \notin \langle a, c \rangle$.

Dimostrazione. Se $c \in \langle a, b \rangle$ nessun problema: infatti dati r e s in K $\beta(\lambda a, \lambda(ra + sb)) = s\beta(\lambda a, \lambda b) \equiv k_1(a, b) s\lambda\beta(a, b) \mod \langle \lambda a, \lambda b \rangle \equiv$ $\equiv k_1(a, b)\lambda\beta(a, ra + sb) \mod \langle \lambda a, \lambda b \rangle$.

Sia $c \notin \langle a, b \rangle$: se $c \notin \langle a, b, \beta(a, b) \rangle$ oppure $b \notin \langle a, c, \beta(a, c) \rangle$ la conclusione segue dal passo (a). Altrimenti risulta

$$\langle a, b, c \rangle = \langle a, b, \beta(a, b) \rangle = \langle a, c, \beta(a, c) \rangle .$$

Sia $h \notin \langle a, b, c \rangle$: se $\beta(a, h) \notin \langle a, h \rangle$ in base ad (a) è $k_1(a, b) = k_1(a, h) =$ $= k_1(a, c)$; sia invece $\beta(a, h) \in \langle a, h \rangle$: $a, b, c, b + h$ sono indipendenti e $\beta(a, b + h) \notin \langle a, b + h \rangle$ poichè $\beta(a, b + h)$ è una combinazione lineare di a, b, c, h con il coefficiente di c non banale (infatti $\beta(a, b) \in$ $\in \langle a, b, c \rangle \setminus \langle a, b \rangle$) e $c \notin \langle a, b, h \rangle$: ripeto allora il ragionamento precedente con $h' = b + h$ al posto di h.

Abbiamo quindi dimostrato che si può scrivere

$$\beta(\lambda a, \lambda b) = k_a \lambda\beta(a, b) + k_2(a, b)\lambda a + k_3(a, b)\lambda b$$

con k_a non dipendente da b.

Passo (c): assegnati ad arbitrio a e b appartenenti a $K(\lambda)$ risulta $k_a = k_b$.

DIMOSTRAZIONE. Se a e b sono linearmente dipendenti il risultato è ovvia conseguenza della bilinearità di β. Dunque posso supporre a e b indipendenti.

Se $\beta(a, b) \notin \langle a, b\rangle$ $\beta(\lambda a, \lambda b)$ si scrive in maniera unica come combinazione di $\lambda\beta(a, b)$, λa, λb ma $\beta(\lambda a, \lambda b) \equiv k_a \lambda\beta(a, b) \mod \langle \lambda a, \lambda b\rangle$ e $\beta(\lambda b, \lambda a) \equiv k_b \lambda\beta(b, a) \mod \langle \lambda a, \lambda b\rangle$: ne segue $k_a = k_b$. Sia invece $\beta(a, b) = ra + sb$ con r e s appartenenti a K; se esiste h tale che $\beta(a, h) \notin \langle a, h\rangle$ e $\beta(b, h) \notin \langle b, h\rangle$ ripetendo il ragionamento appena fatto si ottiene $k_a = k_h = k_b$. Se è invece $\beta(a, h) \in \langle a, h\rangle$ oppure $\beta(b, h) \in \langle b, h\rangle$ per ogni $h \in K(\lambda)$ costruisco due sottoinsiemi di $K(\lambda)$, X_a e X_b, in base alle seguenti modalità: per ogni $h \in K(\lambda) \setminus \langle a, b\rangle$: $h \in X_b$ se e solo se vale (i) $\beta(a, h) \notin \langle a, h\rangle$ oppure (ii) $\beta(a, h) \in \langle a, h\rangle$, $\beta(b, h) \in \langle b, h\rangle$ e $\beta(b, a + h) \in \langle b, a + h\rangle$; $h \in X_a$ se e solo se vale (iii) $\beta(b, h) \notin \langle b, h\rangle$ oppure (iv) $\beta(a, h) \in \langle a, h\rangle$, $\beta(b, h) \in \langle b, h\rangle$ e $\beta(a, b + h) \in \langle a, h + b\rangle$. $K(\lambda) \setminus \langle a, b\rangle \subseteq X_a \cup X_b$: infatti se h non soddisfa nè a (i) nè a (iii) essendo $\beta(a, a + h + b) \in \langle a, a + h + b\rangle$ (da cui segue $\beta(a, h + b) \in \langle a, h + b\rangle$) oppure $\beta(b, a + h + b) \in \langle b, a + h + b\rangle$ (da cui $\beta(b, h + a) \in \langle b, h + a\rangle$) h soddisfa a (ii) oppure a (iv).

Sia $H_a = \langle a, b, X_a\rangle$, $H_b = \langle a, b, X_b\rangle$: $H_a \cup H_b = K(\lambda)$ e quindi $K(\lambda) = H_a$ oppure $K(\lambda) = H_b$. Non è restrittivo proseguire supponendo $H_a = K(\lambda)$: per ogni $h \in X_a$ risulta $\beta(a, h) = t(h)a + sh$ con $t(h) \in K$: infatti se h soddisfa a (iii) è $\beta(a, h) = t(h)a + s(h)h$: poichè

$$\beta(b, h + b) = \beta(b, h) \notin \langle b, h\rangle = \langle b, h + b\rangle$$

è necessariamente $\beta(a, h + b) \in \langle a, h + b\rangle$ cioè $t(h)a + s(h)h + ra + sb = c_1 a + c_2 h + c_2 b$ essendo c_1 e c_2 opportuni elementi di K: poichè a, b e h sono linearmente indipendenti risulta $s(h) = c_2 = s$; alla medesima conclusione si arriva se h soddisfa a (iv).

Sia dunque c un generico elemento di $K(\lambda)$: $c = k_1 a + k_2 b + \sum_{i=3}^{n} k_i h_i$ con $h_i \in X_a$ e $k_i \in K$:

$$\beta(a, c) = \beta\Big(a, k_1 a + k_2 b + \sum_{i=3}^{n} k_i h_i\Big) = \Big(k_2 r + \sum_{i=3}^{n} k_i t(h_i)\Big)a +$$

$$+ s\Big(k_2 b + \sum_{i=3}^{n} k_i h_i\Big) = \Big(k_2 r - k_1 s + \sum_{i=3}^{n} k_i t(h_i)\Big)a + sc \in \langle a, c\rangle:$$

poichè la moltiplicazione per λ opera transitivamente sui sottospazi 1-dimensionali di $K(\lambda)$, ragionando come nella dimostrazione del lemma 4.3, si deduce $\beta(a_1, a_2) \in \langle a_1, a_2 \rangle$ per ogni coppia (a_1, a_2) di elementi di $K(\lambda)$ in contraddizione con l'ipotesi fatta all'inizio di questo paragrafo.

Si è così provato che

$$\beta(\lambda a, \lambda b) = k_1 \lambda \beta(a, b) + k_2(a, b)\lambda a + k_3(a, b)\lambda b .$$

Sia $\mu = k_1^{-1}\lambda$: $K(\lambda) = K(\mu)$ e la moltiplicazione per μ risulta, come quella per λ, transitiva sui sottospazi 1-dimensionali di $K(\mu)$: inoltre

$$\begin{aligned}\beta(\mu a, \mu b) = \beta(k_1^{-1}\lambda a, k_1^{-1}\lambda b) = k_1^{-2}\beta(\lambda a, \lambda b) = \\ = k_1^{-1}\lambda\beta(a, b) + k_1^{-2}k_2(a, b)\lambda a + k_1^{-2}k_3(a, b)\lambda b = \\ = \mu\beta(a, b) + k_1^{-1}k_2(a, b)\mu a + k_1^{-1}k_3(a, b)\mu b:\end{aligned}$$

vale cioè $(\beta(\mu a, \mu b) - \mu\beta(a, b))/\mu \in \langle a, b \rangle$.

L'applicazione δ da $K(\mu) \times K(\mu)$ in $K(\mu)$ definita ponendo $\delta(a, b) = (\beta(\mu a, \mu b) - \mu\beta(a, b))/\mu$ è bilineare alternante e per ogni coppia (a, b) di elementi di $K(\mu)$ risulta $\delta(a, b) \in \langle a, b \rangle$.

LEMMA 5.1. *Sia V un K-spazio vettoriale di dimensione n e sia δ una applicazione bilineare alternante da $V \times V$ in V tale che per ogni x, y appartenenti a V sia $\delta(x, y) \in \langle x, y \rangle$: se δ non è banale esiste un sottospazio $n-1$ dimensionale di V, W, e un elemento v tali che $\langle v \rangle \oplus W = V$, $\delta(v, w) = w$ per ogni $w \in W$ e $\delta(w_1, w_2) = 0$ per ogni coppia (w_1, w_2) di elementi in W.*

DIMOSTRAZIONE. Poichè δ è non banale esistono $\hat{v}$ e $\hat{w}$ con $\delta(\hat{v}, \hat{w}) \neq 0$: posso supporre $\delta(\hat{v}, \hat{w}) = r\hat{v} + s\hat{w}$ con $s \neq 0$:

$$\delta(s^{-1}\hat{v}, rs^{-1}\hat{v} + \hat{w}) = rs^{-1}\hat{v} + \hat{w}:$$

pongo $v = s^{-1}\hat{v}$ e $w_1 = rs^{-1}\hat{v} + \hat{w}$ e ottengo $\delta(v, w_1) = w_1$; sia $v, w_1, \hat{w}_2, \ldots, \hat{w}_{n-1}$ una base per V: $\delta(v, \hat{w}_i) = c_1(i)v + c_2(i)\hat{w}_i$ per $2 \leqslant i \leqslant n-1$; $\delta(v, w_1 + \hat{w}_i) = c_1(i)v + w_1 + c_2(i)\hat{w}_i$ deve appartenere a $\langle v, w_1 + \hat{w}_i \rangle$ e questo comporta $c_2(i) = 1$: pongo $w_i = c_1(i)v + \hat{w}_i$ e ottengo per V una base $v, w_1, \ldots, w_{n-1}$ tale che $\delta(v, w_i) = w_i$ per $1 \leqslant i \leqslant n-1$.

Sia $\delta(w_i, w_j) = k_1 w_i + k_2 w_j$ con k_1 e k_2 in K: $\delta(w_i + v, w_j) =$

$= k_1 w_i + k_2 w_j + w_j \in \langle w_i + v, w_j \rangle$: ne segue $k_1 = 0$: analogamente si deduce $k_2 = 0$ e dunque $\delta(w_i, w_j) = 0$ per ogni $i, j, 1 \leqslant i, j \leqslant n-1$. In relazione al nostro problema possiamo affermare che se non è $\beta(\mu x, \mu y) = \mu\beta(x, y)$ per ogni x e y in $K(\mu)$ allora esiste $a \in K(\mu)$ e H_1 sottospazio $n-1$ dimensionale di $K(\mu)$ con

$$K(\mu) = \langle a \rangle \oplus H_1,$$

$$\beta(\mu h_1, \mu h_2) = \mu\beta(h_1, h_2) \text{ per ogni } h_1, h_2 \in H_1$$

e $\beta(\mu a, \mu h) = \mu\beta(a, h) + \mu h$ per ogni $h \in H_1$.

In base al lemma 4.3 è $H_1 = \langle \hat{b}\mu^{-1}, \ldots, \hat{b}\mu^{-(n-1)} \rangle$ per $\hat{b}$ un opportuno elemento di $K(\mu)$: poichè $\hat{b} \notin H_1$ è $\hat{b} = ka + h$ con $k \neq 0$ e $h \in H_1$: considero $b = k^{-1}(ka + h) = a + k^{-1}h$:

$$H_1 = \langle b\mu^{-1}, \ldots, b\mu^{-(n-1)} \rangle, \ \langle b \rangle \oplus H_1 = K(\mu) \quad \text{e}$$

$\delta(b, h) = h$ per ogni $h \in H_1$:

Considero $H_2 = \langle b(1-\mu^{-1}), \ldots, b(1-\mu^{-(n-1)}) \rangle$: poichè μ^{-1} è algebrico di grado n su K H_2 ha dimensione $n-1$; inoltre $b \notin H_2$ altrimenti sarebbe $H_2 = \langle b, b\mu^{-1}, \ldots, b\mu^{-(n-1)} \rangle = K(\mu)$: risulta pertanto

$$\langle b \rangle \oplus H_2 = K(\mu).$$

LEMMA 5.2. $(1-\mu) \notin \langle 1-\mu^{-1}, \ldots, 1-\mu^{-(n-1)} \rangle$.

DIMOSTRAZIONE per assurdo. Pongo $\nu = \mu^{-1}$: $(1-\mu) \in \langle 1-\mu^{-1}, \ldots, 1-\mu^{-(n-1)} \rangle$ se e solo se $(1-\nu) \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu$: se è vera l'ultima relazione mostro per induzione che $1-\nu^i \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu$ per ogni i, $1 \leqslant i \leqslant n$: chiaramente $1-\nu \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu$. Per ipotesi induttiva, dato $i \leqslant n$, è

$$1-\nu^{i-1} \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu$$

inoltre

$$\nu(\nu^{i-2} - \nu^{i-1}) \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu ;$$

e quindi

$$1-\nu^{i-1} + \nu(\nu^{i-2} - \nu^{i-1}) = 1-\nu^i \in \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu:$$

dunque $K(\mu) = \langle 1-\nu, \ldots, 1-\nu^n \rangle \leqslant \langle 1-\nu, \ldots, 1-\nu^{n-1} \rangle \nu$ e questo è assurdo.

Da questo lemma segue che è $\mu b = sb + h_2$ con $s \neq 1$ e $h_2 \in H_2$: infatti da $s = 1$ seguirebbe $\mu b - b \in H_2$ e quindi $\mu - 1 \in \langle 1 - \mu^{-1}, \ldots, 1 - \mu^{-(n-1)} \rangle$.

A questo punto della dimostrazione introduco un nuovo gruppo A_1 così definito: se δ è banale $A_1 = A$; se δ non è banale valgono le osservazioni appena fatte e quindi pongo A_1 uguale al gruppo ottenuto cambiando l'operazione su A come descritto nel lemma 3.2, scegliendo come g un elemento tale che $(g^{p^{m-1}})^\varrho = b$, come N un sottogruppo massimo di A tale che $(\mathcal{O}_{m-1}(N))^\varrho = H_2$ e ponendo $r = 1/(1-s)$. A_1 è proiettivo ad A: σ è un'autoproiettività anche per A_1, indotta su $\Omega_1(A_1) = \Omega_1(A)$ dallo stesso K-automorfismo α e vale ancora l'identificazione di $\Omega_1(A_1)$ con $K(\mu)$: è diversa invece la struttura di algebra indotta su $K(\mu)$ da A_1: più precisamente se β_1 è l'applicazione bilineare che A_1 induce su $K(\mu)$ risulta $\beta|H_2 \times H_2 = \beta_1|H_2 \times H_2$ e $\beta_1(b, h_2) = \beta(b, h_2) + rh_2$ per ogni $h_2 \in H_2$. Si osserva infine che, poichè per ogni a, b elementi di $K(\mu)$ $\beta_1(a, b) - \beta(a, b) \in \langle a, b \rangle$, anche per β_1 vale una relazione del tipo $(\beta_1(\mu a, \mu b) - \mu\beta_1(a, b))/\mu = \delta_1(a, b)$ dove δ_1 soddisfa alle ipotesi del lemma 5.1.

LEMMA 5.3. *δ_1 è banale.*

DIMOSTRAZIONE. Sia $h = (\mu^{-1} - \mu^{-2})b$: $h \neq 0$, $h \in H_2 \cap H_2^{\mu^{-1}} \cap H_1$; per ogni i con $1 \leqslant i \leqslant n-1$ valgono le seguenti relazioni:

$$\beta_1(b\mu^{-i}, h) = \beta_1(b + b(\mu^{-i} - 1), h) = \beta_1(b, h) + \beta_1(b(\mu^{-i} - 1), h) =$$

(tenendo presente che h e $b(1 - \mu^{-i}) \in H_2$) =

$$= \beta(b, h) + rh + \beta(b(\mu^{-i} - 1), h) = \beta(b\mu^{-i}, h) + rh.$$

$$\beta_1(b\mu^{-i}\mu, h\mu) = \beta_1(b + b(\mu^{-i+1} - 1), h\mu) =$$

$$= \beta_1(b, h\mu) + \beta_1(b(1 - \mu^{-i+1}), h\mu) =$$

(tenendo presente che anche $h\mu \in H_2$ e così pure $b(\mu^{-i+1} - 1)$, il quale tutt'al più è 0 per $i = 1$)

$$= \beta(b, h\mu) + rh\mu + \beta(b(\mu^{-i+1} - 1, h\mu)) = \beta(b\mu^{-i}\mu, h\mu) + rh\mu\,.$$

Inoltre poichè $b\mu^{-i}$ e h appartengono a H_1 è $\delta(b\mu^{-i}, h) = 0$ e dunque

$\beta(\mu b\mu^{-i}, \mu h) - \mu\beta(b\mu^{-i}, h) = 0$ da cui

$$\beta_1(\mu b\mu^{-i}, \mu h) - r\mu h - \mu\beta_1(b\mu^{-i}, h) + r\mu h = 0$$

quindi $\beta_1(\mu b\mu^{-i}, \mu h) - \mu\beta_1(b\mu^{-i}, h) = 0$ cioè per ogni i con $1 \leqslant i \leqslant n-1$ è $\delta_1(b\mu^{-i}, h) = 0$.

È inoltre $\beta_1(b, h) = \beta(b, h) + rh$ poichè $h \in H_2$ e

$$\beta_1(\mu b, \mu h) = \beta_1(sb + h_2, \mu h) = \beta_1(sb, \mu h) +$$

$$+ \beta_1(h_2, \mu h) = \beta(sb, \mu h) + rs\mu h + \beta(h_2, \mu h)$$

(poichè h_2 e $\mu h \in H_2$) e quindi $\beta_1(\mu b, \mu h) = \beta(\mu b, \mu h) + rs\mu h$: essendo $h \in H_1$ $\delta(b, h) = h$ cioè $\beta(\mu b, \mu h) - \mu\beta(b, h) = \mu h$ e quindi

$\beta_1(\mu b, \mu h) - rs\mu h - \mu\beta_1(b, h) + r\mu h = \mu h$:

$$\beta_1(\mu b, \mu h) - \mu\beta_1(b, h) = \mu h(1 + rs - r) = 0$$

vale cioè $\delta_1(b, h) = 0$: ma allora

$$\delta_1(\langle b, \mu^{-1}b, \ldots, \mu^{-(n-1)}b\rangle, h) = \delta_1(K(\mu), h) = 0\ .$$

Sia per assurdo $\delta_1 \neq 0$: esistono l e M con $M \oplus \langle l\rangle = K(\mu)$, $\delta_1(M, M) = 0$, $\delta_1(l, m) = m$ per ogni $m \in M$: sia $h = cl + \overline{m}$ con $c \in K$ e $\overline{m} \in M$: $0 = \delta_1(l, h) = \delta_1(l, \overline{m}) = \overline{m}$ e quindi $h = cl$ ma $0 = \delta_1(h, m) = cm$ per ogni $m \in M$ e dunque $c = 0$ e questo è assurdo perchè h è stato scelto diverso da 0. Dal lemma 5.3 segue che la moltiplicazione per μ è un automorfismo d'algebra per la struttura d'algebra indotta su $K(\mu)$ da A_1 che permuta transitivamente i sottospazi 1-dimensionali di $K(\mu)$: è stato dimostrato, ed è uno dei punti fondamentali nello studio dei p-gruppi con il gruppo degli automorfismi transitivo sui sottogruppi minimi, che algebre di questo tipo sono banali, cioè il prodotto di due elementi è sempre zero (cfr. [4], [5] e [7] pag. 82-85): ma β_1 banale equivale ad A_1 abeliano: A_1 abeliano implica A modulare poichè A e A_1 sono proiettivi e A modulare implica $\beta(a, b) \in \langle a, b\rangle$ per ogni coppia (a, b) di elementi di $K(\mu)$ e questo contraddice l'ipotesi di partenza della dimostrazione per assurdo condotta in questo ultimo paragrafo.

A questo punto il teorema B è completamente dimostrato.

BIBLIOGRAFIA

[1] M. SUZUKI, *Structure of a group and the structure of its lattice of subgroups*, Springer-Verlag, Berlin (1956).
[2] D. GORENSTEIN, *Finite groups*, Harper and Row, New York (1968).
[3] R. BAER, *Crossed isomorphism*, Amer. Journal of Math., **66** (1944), pp. 341-404.
[4] G. HIGMAN, *Suzuki 2-groups*, Illinois J. Math., **7** (1963), pp. 73-96.
[5] E. SHULT, *On finite automorphic algebras*, Illinois J. Math., **13** (1969), pp. 625-653.
[6] C. CHEVALLEY, *Demonstration d'une hypothese de M. Artin*, Abh. Math. Sem. Univ. Hamburg, **11** (1936), p. 73.
[7] N. BLACKBURN, *Metodi di Lie nei gruppi*, Quaderni dei gruppi di ricerca matematica del consiglio nazionale delle ricerche (1973).

Manoscritto pervenuto in redazione il 29 giugno 1985.