RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

FRANCO NAPOLITANI

Gruppi finiti minimali non modulari

Rendiconti del Seminario Matematico della Università di Padova, tome 45 (1971), p. 229-248

<http://www.numdam.org/item?id=RSMUP_1971__45__229_0>

GRUPPI FINITI MINIMALI NON MODULARI

FRANCO NAPOLITANI *)

Sia $\mathfrak{F}$ una proprietà gruppale. Si dice che un gruppo G è un gruppo minimale non $\mathfrak{F}$-gruppo se ogni sottogruppo proprio di G, ma non G, ha la proprietà $\mathfrak{F}$. Gruppi minimali non $\mathfrak{F}$-gruppi sono stati studiati da vari autori. Ricordiamo i lavori di Miller-Moreno [12] e Redei [14] sui gruppi finiti minimali non abeliani; di Iwasawa [10], Schmidt [16] e Redei [15] sui gruppi finiti minimali non nilpotenti; di Huppert [6] e Doerk [4] sui gruppi finiti minimali non supersolubili.

In questa nota vengono studiati i gruppi finiti minimali non modulari (un gruppo *modulare* o *M-gruppo* è un gruppo avente il reticolo dei sottogruppi modulare). La struttura degli M-gruppi finiti è ben nota (vedi § 1) ed è dovuta ad Iwasawa [9], [13], [17].

Spesso nel seguito chiameremo M_1-gruppo un gruppo minimale non modulare; un M_1-p-gruppo è un p-gruppo che è un M_1-gruppo.

Tutti i gruppi considerati in questa nota sono finiti. Le notazioni e le definizioni sono quelle usuali della teoria dei gruppi; la maggior parte di quelle che incontreremo sono date sotto.

Se G è un gruppo, G_i indica l'i-esimo termine della sua serie centrale discendente, $G_2=G'$ il suo gruppo derivato, $Z(G)$ il centro, $\Phi(G)$ il sottogruppo di Frattini e $|G|$ il suo ordine. Se $x, y \in G$, allora $[x, y]= =xyx^{-1}y^{-1}$, $x^y=yxy^{-1}$; $|x|$ è l'ordine di x. $\subseteq$, $\subset$ e $\lhd$ denotano rispettivamente sottogruppo, sottogruppo proprio e sottogruppo normale. Se T è un sottoinsieme di G, $\langle T \rangle$ è il sottogruppo generato da T e $C_G(T)$ il centralizzante di T in G. C_n denota il gruppo ciclico di ordine n; $A \leftthreetimes B$

---

*) Indirizzo dell'A.: Seminario Matematico dell'Università di Padova.
Lavoro eseguito nell'ambito dei gruppi di ricerca matematica del C.N.R.

il prodotto semi-diretto di A mediante B. Se G è un p-gruppo, allora

$$\Omega_i(G)=\langle x\in G \mid x^{p^i}=1\rangle \text{ ed } \mathfrak{V}_i(G)=\langle x\in G \mid x=y^{p^i} \text{ per qualche } y\in G\rangle;$$

$\mu=\mu(G)$ è il più piccolo intero tale che $g^{p^\mu}=1$ per ogni $g\in G$. D_8 denota il gruppo diedrale di ordine 8 e Q_8 il gruppo dei quaternioni di ordine 8. Siano p e q numeri primi distinti e sia l il più piccolo intero positivo per cui $p^l\equiv 1 \pmod q$. Sia $K(p^l)$ il corpo con p^l elementi e ω sia un elemento fissato di $K(p^l)$ il cui ordine moltiplicativo sia q. Il gruppo

$$G=\langle a_\alpha,\ b \mid a_\alpha{}^p=b^{q^n}=1;\ a_\alpha a_\beta=a_{\alpha+\beta},\ a_\alpha{}^b=a_{\omega\alpha},\ (\alpha,\ \beta\in K(p^l))\rangle$$

lo indicheremo con $G(p, q, n)$.

Come è dimostrato nel lavoro [9] un gruppo G di ordine composto è minimale non abeliano se e solo se è del tipo $G(p, q, n)$. Un P^*_0-gruppo è un gruppo del tipo $G=P\leftthreetimes C_q{}^n$ con P p-gruppo abeliano elementare e $C_q{}^n$ inducente su P automorfismi non identici del tipo $a\to a^r$ per ogni $a\in P$ ed r indipendente da a e soddisfacente alle $r\not\equiv 1$, $r^q\equiv 1 \pmod p$.

I principali risultati di questa nota sono i seguenti:

TEOREMA A. *Un p-gruppo G, $p\neq 2$, è minimale non modulare se e solo se*:

1) *$G/\mathfrak{V}_1(G)$ è non abeliano di ordine p^3;*
2) *esiste in G un elemento c di ordine p, $c\notin\mathfrak{V}_1(G)$, che induce su G un automorfismo potenza.*

Il teorema A è la naturale estensione di un risultato di Huppert sui p-gruppi di ordine dispari metaciclici (o, ciò che è lo stesso, p-gruppi modulari con due generatori). L'ipotesi che c abbia ordine p è essenziale, come dimostra l'esistenza del seguente gruppo:

$$G=\langle a,\ b \mid a^{p^2}=b^{p^2}=c^{p^2}=1,\ [a,\ b]=c,\ [c,\ a]=[c,\ b]=1\rangle.$$

TEOREMA B. *Un gruppo G è un p-gruppo finito minimale non modulare se e solo se è del tipo di uno dei seguenti*:

(i) $G=\langle a,\ b \mid a^2=b^{2^n}=c^2=1,\ [a,\ b]=c,\ [c,\ a]=[c,\ b]=1,\ n>1\rangle$

(ii) $G=\langle a,\ b \mid a^2=b^{2^n}=c^2=1,\ [a,\ b]=c,\ [c,\ a]=1,\ [c,\ b]=b^{2^{n-1}},\ n\geq 4\rangle$;

(iii) $G=\langle a,\ b \mid a^{2^n}=b^4=1,\ b^a=b^3\rangle$;

(iv) $G=\langle a,\ b \mid a^{2^n}=1,\ b^4=a^{2^{n-1}},\ b^a=b^{-1},\ n>2\rangle$;

(v) $G=\langle a,\ b \mid a^{2^n}=1,\ b^4=a^{2^{n-1}},\ b^a=b^3,\ n>2\rangle$;

(vi) *il gruppo generalizzato dei quaternioni* Q_{16} ;

(vii) $G=\langle a,\ b \mid a^4=c^2=1,\ b^4=a^2,\ [a,\ b]=c,\ [c,\ a]=1,\ [c,\ b]=b^4\rangle$;

(viii) $\Gamma_2=\langle a,\ b \mid a^8=1,\ a^4=b^4=c^2,\ [a,\ b]=c,\ [c,\ a]=[c,\ b]=1\rangle$;

(ix) $\Gamma_3=\langle a,\ b \mid a^8=1,\ a^4=b^4=c^2,\ [a,\ b]=c,\ [c,\ a]=[c,\ b]=a^4\rangle$;

(x) $\Gamma_1=\langle a,\ b \mid b^9=c^3=1,\ b^3=a^3,\ [a,\ b]=c,\ [c,\ a]=1,\ [c,\ b]=b^3\rangle$;

(xi) *Immagine omomorfa* $\varphi(G(n))$ *di un gruppo del tipo:* $G(n)=\langle a,\ b \mid a^{p^n}=b^{p^n}=1,\ [a,\ b]=c,\ c^p=b^{p^{s+1}},\ s\geq 2$ *per* $p=2,\ n\geq 3$ *per* $p=3,\ n\geq 4$ *per* $p=2,\ b^{-p^s}c=t,\ b^t=b^{1+p^{n-1}},\ a^t=a^{1+p^{n-1}}\rangle$ *con* Kern $\varphi\subseteq\mathfrak{U}_1(G(n))$ *per* $p\geq 3$, Kern $\varphi\subseteq\mathfrak{U}_2(G(n))$ *per* $p=2$.

I gruppi da (i) a (vii) sono 2-gruppi fattorizzabili, esprimibili cioè come prodotto di due sottogruppi ciclici; da (iii) a (vi) sono metaciclici; (vi) e (vii) contengono Q_8 . Γ_1 , Γ_2 , Γ_3 sono i soli p-gruppi minimali non modulari e non fattorizzabili che non siano generabili con elementi indipendenti. Dal teorema B si deduce che i p-gruppi minimali non modulari per $p\geq 5$ sono regolari nel senso di P. Hall.

TEOREMA C. *Sia H un p-gruppo minimale non modulare. Se H non è metaciclico, non contiene Q_8 e non è isomorfo a Γ_1 , Γ_2 , Γ_3 , allora H è reticolarmente isomorfo ad un p-gruppo minimale non abeliano.*

Baer [1] e Jones [11] hanno provato che un p-gruppo modulare non Hamiltoniano è reticolarmente isomorfo ad un p-gruppo abeliano. Il teorema C dà la misura di come una analoga proprietà valga per gli M_1-p-gruppi.

TEOREMA D. *Un gruppo G di ordine composto è minimale non modulare se e solo se è uno dei seguenti:*

(1) $G=G(p,\ q,\ n)$ *con* $p\not\equiv 1 \pmod q$;

(2) *il prodotto non diretto* $Q_8\leftthreetimes C_3^n$;

(3) $G=C_p \leftthreetimes Q$, *ove* $Q=C_q{}^n \times C_q$, $n \neq 0$, *e* $C_p C_q{}^n$ *è un* P^*_0*-gruppo*;

(4) $G=C_p \leftthreetimes Q$, *ove* $Q=C_q{}^n \leftthreetimes C_q$, $n>2$ *per* $p=2$, $|Q'|=q$ *e* $C_p C_q{}^u$ *è un* P^*_0*-gruppo*;

(5) *il prodotto non diretto* $C_p \leftthreetimes Q_8$;

(6) $G=C_{p^2} \leftthreetimes C_q{}^n$ *con* $|Z(G)|=q^{n-1}$;

(7) $G=C_p \leftthreetimes C_q{}^n$, $n \geq 2$, $|Z(G)|=q^{n-2}$;

(8) $G=P \leftthreetimes Q$ *con* $P=\langle a_1, a_2 \rangle$ *p-gruppo abeliano elementare,* $Q=\langle b \rangle$ *q-gruppo ed* $a_1{}^b=a_1^{r_1}$, $a_2{}^b=a_2^{r_2}$, $r_1 \not\equiv 1$, $r_1 \not\equiv r_2$, $r_1{}^q \equiv r_2{}^q \equiv 1 \pmod p$;

(9) $G=P \leftthreetimes Q$ *con* $P=\langle a_1, a_2, \ldots, a_i, \ldots, a_q \rangle$ *p-gruppo abeliano elementare,* $Q=\langle b \rangle$ *q-gruppo di ordine* q^n, $n \geq 2$, $q^2 \nmid p-1$ *ed* $a_i{}^b = a_{i+1}$ *per* $i \neq q$, $a_q{}^b=a_1{}^r$, $r \not\equiv 1$, $r^q \equiv 1 \pmod p$;

(10) $G=(C_p \times C_q) \leftthreetimes C_t{}^n$, *t, p, q primi distinti, con* $|Z(G)|=t^{n-1}$;

(11) $G=C_p \leftthreetimes (C_q{}^n \times C_t{}^m)$, *t, p, q primi distinti, con* $|Z(G)|=q^{n-1}t^{m-1}$.

Un gruppo si dice quasi-Hamiltoniano se ha i sottogruppi a due a due permutabili. I gruppi quasi-Hamiltoniani sono gli M-gruppi nilpotenti [9]. Immediata conseguenza del teorema D è allora il seguente:

TEOREMA E. *Un gruppo è minimale non quasi-Hamiltoniano se e solo se è un* M_1*-p-gruppo o un gruppo del tipo* $G(p, q, n)$ *o infine il prodotto non diretto* $Q_8 \leftthreetimes C_3{}^n$.

1. Risultati preliminari.

Sia G un p-gruppo modulare non-Hamiltoniano. Allora:

1.1. $\Omega_i(G)=\{x \in G \mid x^{p^i}=1\}$;

1.2. l'applicazione $G \ni g \to g^{p^{\mu-1}}$, $\mu=\mu(G)$, è un endomorfismo di G;

1.3. ogni sottogruppo ed ogni quoziente di G è un p-gruppo modulare non-Hamiltoniano.

Le 1.1, 1.2, 1.3 sono dimostrate in [9] e [17]. Esse sono peraltro deducibili dal seguente fondamentale teorema:

TEOREMA 1.1. (K. Iwasawa [9], [13], [17]). *Un p-gruppo finito non-Hamiltoniano G è modulare se e solo se esiste un sottogruppo nor-*

male abeliano A di G ed un elemento t in G tale che $G=\langle A, t\rangle$ e per un fissato intero s, con $s\geq 2$ se $p=2$, $a^t=a^{1+p^s}$ per ogni $a\in A$.

TEOREMA 1.2. (K. Iwasawa [9], [17]). *Un gruppo finito G è modulare se e solo se è prodotto diretto di gruppi a due a due coprimi ciascuno dei quali è un P^*_0-gruppo oppure un p-gruppo modulare.*

LEMMA 1.1. *Sia G un p-gruppo per il quale l'applicazione $\varphi : g \to g^{p^{\mu-1}}$, $\mu=\mu(G)$, sia un endomorfismo. Se $\mu>1$, φ è un endomorfismo centrale, cioè $\varphi(G)=\mho_{\mu-1}(G)\subseteq Z(G)$.*

DIM. Se $x, y\in G$, allora $xy^{p^{\mu-1}}x^{-1}=(xyx^{-1})^{p^{\mu-1}}=x^{p^{\mu-1}}y^{p^{\mu-1}}x^{-p^{\mu-1}}$, cioè $[x^{p^{\mu-1}}, y^{p^{\mu-1}}]=1$. Poichè $\mu>1$, si ha $\langle x\rangle=\langle x^{p^{\mu-1}}\rangle$ e così $y^{p^{\mu-1}}\in Z(G)$.

LEMMA 1.2. *Sia G un p-gruppo tale che per ogni $H\subseteq G$, l'applicazione $h\to h^{p^{\mu-1}}$, $\mu=\mu(H)$, sia un endomorfismo di H. Allora ogni automorfismo-potenza Θ di G di ordine p, che nel caso in cui $p=2$ e $\mu(G)>2$, fissi almeno un elemento di ordine 4, è un automorfismo universale* [1].

DIM. Se G ha esponente p, Θ è l'identità. Sia $\mu>1$. Se G è un 2-gruppo, $\Omega_2(G)$ ha esponente p^2 ed è abeliano essendo l'applicazione $\Omega_2(G)\ni h\to h^2$ un endomorfismo. Allora Θ è universale su $\Omega_2(G)$ e così il lemma è provato per i 2-gruppi G con $\mu(G)=2$, mentre per $\mu(G)>2$, essendo Θ l'identità su $\Omega_2(G)$, si ha $g^\Theta=g$ oppure $g^\Theta=g^{1+\frac{|g|}{2}}$ per ogni $g\in G$. Così in tutta generalità e qualunque sia il primo p, si ha $g^\Theta=g^{1+\frac{\alpha(g)|g|}{p}}$ con $1\leq\alpha(g)\leq p$. Se Θ non fosse universale dovrebbero esistere due elementi a e b, $|a|=|b|=p^\nu$, di G per cui $\alpha=\alpha(a)\neq\alpha(b)=\beta$ e tali che ν sia minimo. Ma per il lemma 1.1, l'applicazione $-1+\Theta$: $g\to g^{-1}g^\Theta$ è un endomorfismo [2]) di $\langle a, b\rangle$. Così $a^{\alpha p^{\nu-1}}b^{\beta p^{\nu-1}}=a^{-1+\Theta}b^{-1+\Theta}=(ab)^{-1+\Theta}=(ab)^{\gamma p^{k-1}}$ dove $p^k=|ab|$, $\gamma=\alpha(ab)$. Se $\langle a\rangle\cap\langle b\rangle\neq 1$ scelti a e b in modo che $a^{p^{\nu-1}}=b^{-p^{\nu-1}}$, l'ipotesi su G comporta $\nu-1\geq k$ e

---

[1]) Un automorfismo potenza si dice universale se è del tipo: $g\to g^n$ con n indipendente da g.

[2]) Cooper [3] ha provato che se Θ è un automorfismo potenza di un gruppo, $-1+\Theta$ è un endomorfismo centrale. Si è preferito dedurre ciò dal lemma 1.1 per ragioni di semplicità.

così, per la minimalità di ν, $(ab)^{-1+\Theta}=1$; cioè $\alpha=\beta$. Dunque $\langle a\rangle \cap \cap \langle b\rangle=1$ e $k=\nu$. Ma allora

$$a^{\alpha p^{\nu-1}}b^{\beta^{\nu-1}}=a^{\gamma p^{\nu-1}}b^{\gamma p^{\nu-1}};$$

una contraddizione poichè quest'ultima relazione è vera solo se $\alpha=\beta=\gamma$.

OSSERVAZIONE 1.1. L'ipotesi che Θ lasci fermo almeno un elemento di ordine 4 quando $p=2$ e $\mu(G)>2$ non è superflua. Nel gruppo modulare $G=\langle a, b \mid a^{2^n}=b^{2^n}=1,\ b^a=b^{1+2^{n-1}},\ n\geq 3\rangle$ l'applicazione φ definita canonicamente ponendo $\varphi(a)=a^{-1}$ e $\varphi(b)=b^{-1+2^{n-1}}$ è un automorfismo potenza non universale.

LEMMA 1.3. *Sia G un p-gruppo esprimibile nella forma $G=H\langle c\rangle$ con $H \lhd G$ modulare non-Hamiltoniano e c di ordine p. Se l'elemento c induce su H un automorfismo potenza Θ che fissa almeno un elemento di ordine 4 se $p=2$ e $\mu(H)\geq 2$, G è modulare (non-Hamiltoniano).*

DIM. Poichè per ogni $T\subseteq H$ l'applicazione $T\ni t\to t^{p^{\mu-1}}$, $\mu=\mu(T)$, è un endomorfismo di T, Θ è un automorfismo potenza universale su H. Senza ledere la generalità, si può supporre che Θ sia l'identità oppure Θ sia l'automorfismo $H\ni h\to h^{1+p^{\mu-1}}$, $\mu=\mu(H)$. Se $\Theta=1$ il lemma segue immediatamente dal teorema 1.1. Se $\Theta\neq 1$, siano $X=\langle hc^{\alpha}\rangle$ e $Y=\langle kc^{\beta}\rangle$, $h, k\in H$, arbitrari sottogruppi ciclici di G. Posto $T=\langle h, k, c\rangle$, allora T contiene un sottogruppo normale abeliano N ed un elemento t tali che $T=\langle N, t\rangle$ e, per un fissato intero s non inferiore a 2 se $p=2$, si abbia $n^t=n^{1+p^s}$ per ogni $n\in N$. Infatti $\langle h, k\rangle=TH$ è generabile con due elementi a e b tali che $a^b=a^{1+p^s}$, $s\geq 2$ se $p=2$. Allora se $s>\mu-1$, basta scegliere $N=T\cap H$ e $t=c$. Se $s=\mu-1$, si scelga $N=\langle bc^{-1}, a\rangle$ e $t=b$ quando $|a|=p^{\mu}$; ed invece $N=T\cap H$ e $t=c$ quando $|a|<p^{\mu}$. Infine se $s<\mu-1$, si ponga $N=\langle c^{-1}b^{p^{\mu-1-s}}, a\rangle$ e $t=b$. T è quindi modulare e pertanto X e Y contenuti in T sono permutabili. Ciò assicura che G è un M-gruppo.

2. *p*-gruppi minimali non modulari.

Sia G un M_1-p-gruppo. G è un gruppo con due generatori altrimenti i sottogruppi ciclici di G sarebbero a due a due permutabili e G sa-

rebbe modulare. Se a e b generano G, poniamo $T=\langle a^p, b^p\rangle$. T, normale sia in $\langle a^p, b\rangle$ che in $\langle a, b^p\rangle$, è sottogruppo normale di G.

LEMMA 2.1. *Sia* $G=\langle a, b\rangle$ *un* M_1*-p-gruppo. Allora*:

1) *se* $p\geq 3$, $\langle a^p, b^p\rangle=\mho_1(G)$ *e* $G/\mho_1(G)$ *è non abeliano di ordine* p^3;

2) *se* $p=2$ *e* $Q_8\trianglelefteq G$, $\langle a^4, b^4\rangle=\mho_2(G)$ *e* $G/\mho_2(G)$ *è un* M_1*-gruppo con tutti i sottogruppi propri abeliani.*

DIM. 1) se $p\geq 3$, G/T, con $T=\langle a^p, b^p\rangle$, è il gruppo non abeliano di esponente p ed ordine p^3, altrimenti G sarebbe generato da due sottogruppi ciclici permutabili e quindi sarebbe modulare [5]. $T\subseteq\mho_1(G)$ e G/T di esponente p implicano $T=\mho_1(G)$.

2) $N=\langle a^4, b^4\rangle$ è normale in G essendo $N=\mho_1(T=\langle a^2, b^2\rangle)$. Allora poichè $Q_8\trianglelefteq G$, G/N ha esponente 4 e così $\mho_2(G)\subseteq N$. D'altra parte $N\subseteq\mho_2(G)$ onde $N=\mho_2(G)$. $G/\mho_2(G)$, essendo G omomorfo a D_8, è non modulare: i suoi sottogruppi propri sono abeliani poichè $\mu(G/\mho_2(G))\leq 2$.

Dal lemma 2.1 discende che un M_1-p-gruppo per $p\geq 3$ non è fattorizzabile nel prodotto di due sottogruppi ciclici. Esistono invece M_1-2-gruppi fattorizzabili. I lemmi seguenti classificano questi gruppi.

LEMMA 2.2. *Sia* G *un* M_1*-2-gruppo fattorizzabile. Se* Q_8 *non è contenuto in* G, *allora* G *è uno dei gruppi da* (i) *a* (v) *del teorema* B.

DIM. α) G non è metaciclico. Per un teorema di Ito-Ohara [8] G/G' ha invarianti $(2^\gamma, 2)$ con $\gamma>1$. Da ciò, per un risultato di Blackburn [2], segue che esiste $H\lhd G$ tale che G modulo H abbia relazioni di definizione: $[a, b]=c$, $a^4=b^2=c^2=1$, $[a, c]=[b, c]=1$ in termini di due generatori a, b. $\mu(G/H)=2$ implica $H\supseteq\mho_2(G)$; ma $G/\mho_2(G)$ ha ordine non superiore a 16 onde $H=\mho_2(G)$. Allora $\langle a^2, b^4\rangle=\langle a^4, b^4\rangle$ e così $a^2=b^{4h}$, h intero. Da ciò, per l'ipotesi $Q_8\trianglelefteq G$, segue che $\langle a, b^2\rangle$ si spezza su $\langle b^2\rangle\lhd G$ e pertanto possiamo assumere $a^2=1$. Da ciò segue immediatamente che G è del tipo (i) o (ii). La limitazione $n\geq 4$ in (ii) è conseguenza della relazione $ab^2a^{-1}=(cb)^2=[b, c]b^2$.

β) G è metaciclico. Per la definizione esiste $N\lhd G$ tale che N e G/N siano entrambi ciclici. Sia A un sottogruppo ciclico tale che $G=AN$.

Poichè D_8 è immagine omomorfa di G, $G'=N^2$; d'altra parte, essendo modulari i sottogruppi propri di G e di $G/A\cap N$, deve risultare $G_3\subseteq N^8$ modulo $A\cap N$. Quanto detto comporta $|N:A\cap N|=4$ e conseguentemente $|A\cap N|=2$. Da ciò discende che G è del tipo (iii)-(v).

LEMMA 2.3. *Sia G un M_1-2-gruppo. Se $G\supset Q_8$, allora G è il gruppo* (vi) *o* (vii) *del teorema* B.

DIM. Ogni sottogruppo massimo di G ha non più di tre generatori, essendo generato (indicati con a e b opportuni generatori di G) da a, b^2, $[a, b]$. Segue che M massimo in G, se Hamiltoniano, ha ordine non superiore a 2^4. Così $|G|\leq 2^5$ e $\mu(G)\leq 3$. Se $G^4=1$, $\Phi(G)$ è abeliano elementare e $G\natural Q_8$. Dunque $G^4\neq 1$. Siano a e b generatori di G e sia $|b|=2^3$. Se $\langle b\rangle\lhd G$, G è Q_{16}. Se $\langle b\rangle$ non è normale in G, il quoziente $G/\langle b^4\rangle$ ha ordine 16 ed è fattorizzabile ma non metaciclico. Identificando a con un elemento di G avente ordine 2 modulo $\langle b^4\rangle$ e che insieme con b generi G, si ottiene il gruppo (vii).

OSSERVAZIONE 2.1. Il lemma 2.3 comporta che un M_1-2-gruppo non fattorizzabile non contiene Q_8 come sottogruppo. Allora, per il lemma 2.1 un M_1-2-gruppo G è non fattorizzabile se e solo se $G/\mho_2(G)$ è non fattorizzabile. In un M_1-2-gruppo non fattorizzabile $G/\mho_2(G)$ è pertanto il gruppo di ordine 32 avente relazioni di definizione: $a^4=$ $=b^4=c^2=1$, $[a, b]=c$, $[c, a]=[c, b]=1$. In particolare G/G' ha invarianti 2^α, 2^β con $\alpha, \beta\geq 2$.

LEMMA 2.4. *Sia G un p-gruppo, $p\geq 3$, di esponente non superiore a p^2. Se è un M_1-gruppo, G è il gruppo Γ_1 oppure*:

(j) $G=\langle a, b \mid a^{p^n}=b^{p^m}=c^p=1,\ [a, b]=c,\ [c, a]=[c, b]=1,$ $1\leq n, m\leq 2\rangle$;

(jj) $G=\langle a, b \mid a^p=b^{p^2}=c^p=1,\ [a, b]=c,\ [c, a]=1,\ [c, b]=b^p,$ $p>3\rangle$;

(jjj) $G=\langle a, b \mid a^{p^2}=b^{p^2}=c^p=1,\ [a, b]=c,\ [c, a]=a^p,\ [c, b]=b^p,$ $p>3\rangle$.

DIM. Sia $G=\langle a, b\rangle$ un M_1-p-gruppo, $p\geq 3$, di esponente $\leq p^2$. Se $|G'|=p$ è evidente che G è del tipo (j). Supposto $|G'|>p$, $\mho_1(G)=$ $=\langle a^p, b^p\rangle$ è ciclico di ordine p oppure abeliano elementare di ordine

p^2. Se $|\mho_1(G)|=p$, allora $|G'|=p^2$, G ha classe 3 e $C_G(G')$ ha indice p in G. Senza ledere la generalità si può scegliere $a\in C_G(G')$ e $b\notin C_G(G')$. Allora per $p>3$, G contiene un generatore di ordine p che, poichè G è un M_1-p-gruppo, appartiene a $C_G(G')$ e così G è il gruppo (jj). Per $p=3$, le eventuali relazioni di definizione di G potrebbero essere: $b^9=c^3=1$, $a^3=b^{3\alpha}$, $[a, b]=c$, $[c, b]=b^3$, $[c, a]=1$, con $\alpha=0, 1, -1$. Ma se $\alpha=0$, ba^{-1} è di ordine p e non permutabile con c; se $\alpha=1$, ab è di ordine p e non permutabile con c. Pertanto $\alpha=-1$ e $G=\Gamma_1$. Infine se $|\mho_1(G)|=p^2$, G ha ordine p^5 ed è generabile con elementi entrambi di ordine p^2 ed indipendenti, (come segue dal lemma 2.1). Ciò implica $(G')^p=1$ e conseguentemente $\mho_1(G)\subseteq Z(G)$. Se $p=3$, $G/\langle a^3\rangle$ e $G/\langle b^3\rangle$ risultano del tipo (j) e di conseguenza $|G'|=p$. Per $p>3$, il commutatore $[a, b]$ trasforma a e b in uguali potenze altrimenti $\langle [a, b], ab\rangle$ non sarebbe modulare e così G è del tipo (jjj).

LEMMA 2.5. *Sia G un M_1-2-gruppo non fattorizzabile. Se $\mu(G)\leq 3$, o G coincide con Γ_2, Γ_3 oppure è del tipo:*

(j) $G=\langle a, b \mid a^{2^n}=b^{2^m}=c^2=1,\ [a, b]=c,\ [c, a]=[c, b]=1,\ 2\leq n,\ m\leq 3\rangle$.

DIM. Se $\mu(G)=2$ l'asserto è evidente. Sia $\mu(G)=3$, $G=\langle a, b\rangle$, $c=[a, b]$. Se $|a|=4$, allora $|c|=2$. Infatti, se così non fosse, si avrebbe $b^4=c^2$ e $b^c=b^5$; e da queste le relazioni contraddittorie $(ab)^c=ab^5$, $(ab)^4=1$. Dopodichè dalla relazione $b^2=(b^2)^a=(cb)^2=[b, c]c^2b^2$ segue $[b, c]=1$ e così, quando $|a|=4$, G è del tipo (j). Supponiamo adesso $|a|=|b|=2^3$. Se $\langle a\rangle\cap\langle b\rangle=1$, G è ancora del tipo (j), tali risultando $G/\langle a^4\rangle$ e $G/\langle b^4\rangle$. Infine sia $\langle a\rangle\cap\langle b\rangle\neq 1$. Per l'osservazione 2.1, è necessariamente $|\langle a\rangle\cap\langle b\rangle|=2$. Formali verifiche provano che non si è ricondotti ad uno dei casi appena trattati soltanto se G è Γ_2 oppure Γ_3.

LEMMA 2.6. *Γ_1, Γ_2, Γ_3 non sono immagini omomorfe proprie di un M_1-p-gruppo.*

DIM. *a)* $p=3$. Se supponiamo falso l'asserto, dovrà esistere un M_1-gruppo $G=\langle a, b\rangle$, $|G|=3^5$, contenente un sottogruppo normale N di ordine p tale che $G/N\cong\Gamma_1$. Per il lemma 2.4, G ha esponente p^3, e quindi $(\langle a\rangle\cap\langle b\rangle)\supset N$. Ma $[a, b]=c$ ha ordine p modulo N. L'essere

G un M_1-gruppo implica così che $[c, a]$ e $[c, b]$ appartengono entrambi ad N in contraddizione con $G/N \cong \Gamma_1$.

b) $p=2$. Procedimento dimostrativo analogo a quello seguito in *a*).

LEMMA 2.7. *Sia G un p-gruppo minimale non modulare differente da Γ_1 per $p=3$ ed avente esponente non inferiore a 16 per $p=2$. Allora*:

a) *l'applicazione $G \ni g \to g^{p^{\mu-1}} (\mu = \mu(G))$ è un endomorfismo di G;*

b) *ogni elemento c di ordine p appartenente a $\Phi(G)$ induce su G un automorfismo potenza universale della forma $g \to g^{1+\alpha p^{\mu-1}}$ con $\mu = \mu(G)$ ed $1 \leq \alpha \leq p$. Per $p=3$ e $\mu(G) \leq 2$, si ha $\alpha = p$.*

DIM. *a*) Sia $p \geq 3$. Se $\mu(G) \leq 2$ una semplice verifica prova la a) (G ha classe minore di p). Se $\mu(G) > 2$, per ogni coppia di elementi u, v di G, si ha $(uv)^p = u^p v^p t$ con u^p, v^p in $\mho_1(G)$ e $t \in \mho_2(G)$, e ciò poichè $G/\mho_2(G)$ è un M_1-p-gruppo di esponente p^2 non isomorfo a Γ_1 (lemma 2.6). E così, essendo $\mho_1(G)$ modulare di esponente $p^{\mu-1}$, la 1.2 implica $(uv)^{p^{\mu-1}} = (u^p v^p t)^{p^{\mu-2}} = u^{p^{\mu-1}} v^{p^{\mu-1}}$. Per $p=2$ la prova viene effettuata in modo simile operando modulo $\mho_3(G)$.

b) Segue immediatamente dalla a) e dal lemma 1.2. La limitazione $\alpha = p$ per $p=3$ e $\mu(G) \leq 2$ è giustificata dal fatto che, ad eccezione di Γ_1, gli M_1-3-gruppi di esponente 3^2 hanno i sottogruppi propri abeliani.

LEMMA 2.8. Sia G un *M_1-p-gruppo non fattorizzabile e differente da Γ_2 e Γ_3 per $p=2$. Allora*:

a) *se $p \neq 2$, $\Phi(G) = G'\mho_1(G)$ si spezza su $\mho_1(G)$;*

b) *se $p=2$, $G'\mho_2(G)$ si spezza su $\mho_2(G)$.*

DIM. a) Se $\mu(G) \leq 2$, la a) è vera per il lemma 2.4. Supposto $\mu(G) > 2$, procediamo per induzione su $|G|$. Sia $G = \langle a, b \rangle$ ed $|a| \geq |b|$. Per il lemma 2.7 $|a| = p^\mu \geq p^3$ e, per il lemma 1.1, $a^{p^{\mu-1}} \in Z(G)$. Poichè la a) può supporsi vera in $G/\langle a^{p^{\mu-1}} \rangle$, segue che esiste in G un elemento c, $|c| \leq p^2$, $c \in \Phi(G)$, $c \notin \mho_1(G)$. Se $|c| = p^2$, allora $\langle a^{p^{\mu-2}}, c \rangle = \langle a^{p^{\mu-2}}, t \rangle$ con t di ordine p e non in $\mho_1(G)$ perchè altrimenti anche c apparterrebbe ad $\mho_1(G)$. La a) è così provata.

LEMMA 2.9. *Se G è un M_1-p-gruppo, G' è abeliano del tipo (p^m, p^r, p^s) con $m \neq 0$ ed $r, s \leq 1$.*

DIM. Se G è fattorizzabile oppure è un 2-gruppo di esponente non inferiore a 16, il lemma è vero per i lemmi 2.2, 2.3 e 2.5. Altresì è vero se G ha esponente p o se $G = \Gamma_1$. Esclusi questi casi, $\Omega_1(G)$ è abeliano elementare di ordine p^3 e contiene l'elemento di ordine p la cui esistenza è stabilita dal lemma 2.8. Allora per il lemma 2.1, $G/\Omega_1(G)$ è ciclico oppure è generato da due sottogruppi ciclici permutabili. Se $G/\Omega_1(G)$ è ciclico, $\Omega_1(G) \supseteq G'$ e tutto è provato. Nella seconda eventualità, $G/\Omega_1(G)$ è metaciclico. Ciò per un teorema di Huppert [5] per $p \geq 3$ e per il già citato risultato di Ito-Ohara [8] per $p = 2$, essendo gli invarianti di G/G' entrambi maggiori di 1. Così G' è contenuto in un gruppo modulare $T = \langle x, y, z \rangle$, con $x^{p^m} = 1$, $y^p = 1$, $z^p = 1$, $x \in \mathfrak{V}_1(G)$ ed $y, z \in \Phi(G)$. Allora per la b) del lemma 2.7 T è abeliano e di conseguenza lo è anche G'.

DIM. DEL TEOREMA A. I lemmi 2.1, 2.7 e 2.8 provano che le 1) e 2) sussistono in un M_1-p-gruppo di ordine dispari.

Viceversa un p-gruppo con le proprietà 1) e 2) è un gruppo non modulare con due generatori. Allora se le 1) e 2) non implicassero l'appartenenza alla classe degli M_1-gruppi, dovrebbe esistere un p-gruppo G, $p \geq 3$, di ordine minimo con le proprietà 1) e 2) e con un sottogruppo proprio non modulare. L'elemento $c \notin \mathfrak{V}_1(G)$ di ordine p, la cui esistenza è stabilita dalla 2) appartiene a $\Phi(G)$ poichè $| G/\mathfrak{V}_1(G) | > p^2$. Sia $N \lhd G$, $| N | = p$, un sottogruppo di $\mathfrak{V}_1(G) = T$. Per la minimalità di G, G/N è un M_1-gruppo. Allora, per il lemma 2.1, per ogni sistema di generatori a, b di G si ha

$$\langle a, T \rangle / N = \langle aN, \mathfrak{V}_1(G/N) \rangle = \langle aN, b^p N \rangle.$$

Quindi ogni sottogruppo massimo di G è del tipo $\langle M, c \rangle$ con $M \supset T$ ed M/N metaciclico. L'essere M/N metaciclico implica $| M/N / \Omega_1(M/N) | \leq p^2$. Se $N \subseteq \mathfrak{V}_1(T)$ allora $\mathfrak{V}_1(M) \supset N$ e così $| M/\mathfrak{V}_1(M) | \leq p^2$. Da ciò: M è modulare e quindi anche $\langle M, c \rangle$ è modulare (lemma 1.3). Pertanto T ha esponente p. Sia g tale che $g^p \neq 1$. L'avere $\langle g, T \rangle / N$ un sottogruppo ciclico di indice p implica $\mathfrak{V}_1(\langle g, T \rangle) = \langle g^p \rangle$ e così, per l'ipotesi su c, è anche $\mathfrak{V}_1(\langle g, T, c \rangle) = \langle g^p \rangle$. Segue $T \subseteq Z(G)$. Ma allora

M è abeliano e quindi $\langle M, c\rangle$ è modulare. Questo assurdo completa la dimostrazione.

DIM DEL TEOREMA B. Per quanto precede è sufficiente provare che un p-gruppo non fattorizzabile e non isomorfo a Γ_1, Γ_2, Γ_3 è minimale non modulare se e solo se è del tipo (xi).

a) *Necessità.*

Se G è un 2-gruppo e $\mu(G)$ è minore o uguale a 3, G è, per il lemma 2.5, immagine omomorfa di $G(4)$. Supporremo pertanto che se $p=2$ $\mu(G)>3$. $(G')^p$ è ciclico (lemma 2.9) ed è contenuto in $\mho_3(G)$ per $p=2$. Allora, per ogni $H\subseteq G/(G')^{p^2}$, l'applicazione $h\to h^{p^{\mu-1}}$, $\mu=\mu(H)$, è un endomorfismo di H. Esistono così due elementi a e b tali che $G=\langle a, b\rangle$ e $\langle b\rangle\supset(G')^p$ con $[\langle b\rangle:(G')^p]\geq 2^3$ per $p=2$. Posto $[a, b]=c$, allora $\langle c^p\rangle=(G')^p$, e, essendo $\langle b, c\rangle$ modulare, $[b, c]\in\langle b\rangle$ ed è in $Z(\langle b, c\rangle)$. Dalla (1) $ab^pa^{-1}=(cb)^p=[b, c]^{\binom{p}{2}}c^pb^p$ segue $\langle b^p\rangle\lhd\langle a, b^p\rangle$ e quindi, essendo $[\langle b^p\rangle:\langle c^p\rangle]>2$ per $p=2$, è lecito supporre $ab^pa^{-1}=$ $=(b^p)^{1+p^s}$, $s\geq 2$ per $p=2$. Così: (2) $[b, c]^{\binom{p}{2}}c^p=b^{p^{s+1}}$. Se $[b, c]^{\binom{p}{2}}=1$, in particolare se $p\geq 3$, allora $c^p=b^{p^{s+1}}$. Proviamo che anche per $p=2$ si possono assumere a e b tali che $c^p=b^{p^{s+1}}$ con s opportuno. Sia infatti $p=2$ e $[b, c]=[b, c]^{\binom{p}{2}}\neq 1$. È necessariamente $|b|=2^\mu$. $\mu=\mu(G)$, in quanto esiste in $\Phi(G)$ un elemento di ordine 2 che agisce come c su $\langle b\rangle$, e così $[b, c]=b^{2^{\mu-1}}$. La (2) dà $c^2=b^{2^{\mu-2}}$, per $s\geq\mu-1$, e $c^2=1$, per $s=\mu-2$. Sia $s<\mu-2$. Poichè $1+p^s$ ha ordine moltiplicativo $p^{\mu-1-s}$ modulo $p^{\mu-1}$, l'elemento $a^{p^{\mu-2-s}}$ coniuga b^p in $b^{p+p^{\mu-1}}$. Posto $a^*=a^{1+p^{\mu-2-s}}$ $c^*=[a^*, b]$ è uguale a ct con $t\in C_G(\langle b\rangle)$ in quanto $\langle a^{p^{\mu-2-s}}, b\rangle'\subseteq$ $\subseteq(G')^p\mho_{\mu-1}(G)$. Allora la $b^{p^{s+1}}b^{p^{\mu-1}}=[b, c^*]^{\binom{p}{2}}(c^*)^p$ implica $(c^*)^p=b^{p^{s+1}}$; e, così, anche per $p=2$ G è generabile con elementi a e b tali che $c^p=b^{p^{s+1}}$, $s\geq 2$ per $p=2$. Per il lemma 2.7, $b^{-p^s}c$ induce su G un automorfismo del tipo $g\to g^{1+\alpha p^{\mu-1}}$ con $1\leq\alpha\leq p$. Se $\alpha\neq p$, $\alpha\neq 1$, sia γ tale che $\gamma\alpha\equiv 1$ (mod. p). Posto $\overline{b}=b^\gamma$ e $\overline{c}=[b, c]^{\binom{\gamma}{2}}c^\gamma$ si ha $\langle a, \overline{b}\rangle=\overline{c}$ e $(\overline{c})^p=(\overline{b})^{p^{s+1}}$ con $(\overline{b})^{-p^s}\overline{C}$ che induce su G l'automorfismo $g\to g^{1+p^{\mu-1}}$ Pertanto G è generabile con due elementi a e b tali che $c^p=b^{p^{s+1}}$, $c=$ $=[a, b]$, $s\geq 2$ per $p=2$, e, posto $t=b^{-p^s}c$, si ha $a^t=a$, $b^t=b$ oppure

$a^t=a^{1+p^{\mu-1}}$, $b^t=b^{1+p^{\mu-1}}$ con $\mu=\max\{|a|, |b|\}$ [3]). Da ciò è immediato che G è isomorfo ad un gruppo del tipo $G(n)/K$, $K\subseteq \mho_1(G(n))$ per $p>2$, $K\subseteq \mho_2(G(n))$ per $p=2$. Le limitazioni su n discendono dai lemmi 2.4 e 2.5.

b) *Sufficienza.*

Basta verificare che $G(n)$ è un gruppo minimale non modulare. $G(n)$ ha esponente $p^n=|a|=|b|$ ed in $G(n)$ l'applicazione $G(n)\ni g\to g^{p^{n-1}}$ è un endomorfismo. Così t induce su $G(n)$ un automorfismo potenza. Allora, se $p\geq 3$, $G(n)$ è minimale non modulare per il teorema A. Se $p=2$, $G(n)$ è non modulare poichè D_8 è una sua immagine omomorfa. I sottogruppi massimi di $G(n)$ hanno forma $\langle H, t\rangle$ ove H è metaciclico ed H/H' ha invarianti entrambi maggiori di 2. H è quindi modulare [8] ed infine per il lemma 1.3 anche $\langle H, t\rangle$ è modulare.

DIM. DEL TEOREMA C. Per un fissato intero positivo n ($n\geq 3$ per $p=3$, $n\geq 4$ per $p=2$), siano:

$$G^*=\langle a, b \mid a^{p^n}=b^{p^n}=1,\ [a, b]=c,\ c^p=b^{p^{s+1}},\ s\geq 2 \text{ per } p=2,\ t=b^{-p^s}c,\ b^t=b,\ a^t=a\rangle$$

$$G=\langle a, b \mid a^{p^n}=b^{p^n}=1,\ [a, b]=c,\ c^p=1,\ b^c=b,\ a^c=a\rangle.$$

G^* e G sono p-gruppi minimali non modulari.

I) $\mathfrak{L}(G^*)\cong\mathfrak{L}(G)$. Il metodo che usiamo per stabilire l'esistenza di questo isomorfismo è essenzialmente quello seguito da Baer nel provare che ogni gruppo modulare non-Hamiltoniano è isomorfo ad un gruppo abeliano [1], [11]. Diamo ora schematicamente la dimostrazione.

Sia $e=1+p^s$, $\sigma(k)=1+e+\ldots+e^{k-1}$, $p^m=p^{n-s}$, e^* il resto di $\sigma(p^m)/p^m$ modulo p^n: e^* è primo con p. Inoltre siano D il sottogruppo di G^* generato da $\{a^{p^m}, b, t\}$, V il gruppo ottenuto aggiungendo a D un elemento w tale che $w^{p^m e^*}=a^{p^m}$, $[w, b]=t$, $[t, w]=1$. Ogni elemento v di V è esprimibile in un unico modo nella forma da^i, $i=i(d)$, con $d\in D$ e $0<i\leq p^m$. Poichè l'ordine moltiplicativo di e modulo p^n è p^m, segue che $i=j$ è condizione necessaria e sufficiente perchè $\sigma(i)\equiv\sigma(j)$

[3]) Applicando il teorema di Holder [18] sulle estensioni metacicliche le relazioni date possono essere completate in relazioni di definizione per G.

(mod. p^m) e $0<i,\ j\leq p^m$. Resta così definito per ogni v di V un unico intero $j(v)$ tale che $0<j(v)\leq p^m$ e $i(v)\equiv\sigma(j(v))$ (mod. p^m). Poichè $|V'|=p$ ed s è non inferiore a 2 per $p=2$, si ha che $v^{f(x)}=v^{e^{j(x)}}$ definisce un automorfismo di V. Si può vedere che $f(xy^{f(x)})=f(x)f(y)$ per ogni coppia di elementi $x,\ y\in V$. Se in V definiamo una nuova moltiplicazione $\circ$ ponendo $x\circ y=xy^{f(x)}$, V, per la precedente formula, è un gruppo rispetto ad $\circ$. Chiamiamo $C=\langle w,\ D\rangle$ questo gruppo. Sia w' l'inverso di w in C. Si ha

$$c=w\circ b\circ w'\circ b^{-1}=w\circ(bw')\circ b^{-1}=(wb^cw'^e)\circ b^{-1}=$$

$$=(wb^ew^{-1})\circ b^{-1}=b^{p^s}t=b^{t^s}\circ t,\ c^p=(b^{p^s}\circ t)^p=(b^{p^s}t)^p=b^{p^{s+1}}.$$

$$(a)^t=a,\ (b)^t=b,\ (w)^{p^m}=w^{\sigma(p^m)}=w^{t^me^*}=a^{p^m}.$$

Quindi C è isomorfo a G^* mediante l'applicazione $d\to d$ $(d\in D)$ e $w\to a$. L'applicazione identica τ di V su C soddisfa l'identità $\tau(x)\tau(y)=$ $=\tau(xy^{f(x)})$ dove f è un automorfismo di V tale che $f(xy^{f(x)})=f(x)f(y)$. Quindi τ è un « crossed » automorfismo. Esso induce un isomorfismo di $\mathfrak{L}(G^*)$ su $\mathfrak{L}(V)$. Poichè $V\cong G$, la I) è provata.

II) $\mathfrak{L}(G^*)\cong\mathfrak{L}(G(n))$. Si fissi per ogni sottogruppo ciclico U di ordine massimo di $G^*/\Omega_1(G^*)$ un rappresentante u di un generatore. L'elemento u ha ordine p^n. Fissato un complemento H_u di $\langle u^{p^{n-1}}\rangle$ in $\Omega_1(G^*)$, si considerino tutti i prodotti uh, $h\in H_u$. Sia $\mathfrak{M}^*$ l'insieme ottenuto operando nel modo anzidetto. Ad ogni sottogruppo ciclico A^*, $|A^*|=p^n$, di G^* resta associato un unico generatore dato da $A^*\cap\mathfrak{M}^*$. Sia $\mathfrak{A}^*$ la riunione, nel senso della teoria degli insiemi, di $\mathfrak{M}^*$ e $\Phi(G^*)$. Gli elementi di G^* e di $G(n)$ sono esprimibili in un unico modo nella forma

$$1)\qquad b^\beta a^\alpha t^\gamma,\ 0\leq\beta,\ \alpha<p^n,\ 0\leq\gamma<p.$$

Sia ρ l'applicatzione di G^* su $G(n)$ che pone in corrispondenza elementi aventi uguale espressione formale 1) e siano $\mathfrak{A}=\rho(\mathfrak{A}^*)$, $\mathfrak{M}=\rho(\mathfrak{M}^*)$. È evidente che $\rho(\Phi(G^*))=\Phi(G(n))$ e con ciò, $\mathfrak{A}=\{\mathfrak{M},\Phi(G(n))\}$. Inoltre ad ogni sottogruppo ciclico A di ordine massimo di $G(n)$ viene associato uno ed un solo generatore dato da $\mathfrak{M}\cap A$. Sia φ l'applicazione di

$\mathfrak{A}^*$ su $\mathfrak{A}$ definita ponendo

$$\varphi : \mathfrak{A}^* \to \mathfrak{A} \begin{cases} \varphi(x)=\rho(x) \text{ se } x\in\mathfrak{M}^* \\ \varphi(x)=\rho(x) \text{ se } x\in\Phi(G^*) \text{ e } p>3 \\ \varphi(x)=\rho(x)(a^{-\beta\alpha^2}b^{\beta^2\alpha})^{p^{n-1}} \text{ per } p=3 \\ \varphi(x)=\rho(x)(a^{-\beta\binom{\alpha}{2}}b^{\alpha\left[\binom{\beta}{2}+\beta^2\right]})^{p^{n-1}} \text{ per } p=2, \text{ se } x=b^{\beta p}a^{\alpha p}t^{\gamma}. \end{cases}$$

Proviamo che

$$2) \qquad \langle \varphi(K^*\cap\mathfrak{A}^*)\rangle\cap\mathfrak{A}=\varphi(K^*\cap\mathfrak{A}^*)$$

per ogni sottogruppo K^* di G^*. Se $K^*\supseteq\mathfrak{V}_{n-1}(G^*)$ oppure $K^*\subseteq\Phi(G^*)$ la 2) sussiste poichè nel primo caso φ si prolunga canonicamente in un isomorfismo di $G^*/\mathfrak{V}_{n-1}(G^*)$ su $G(n)/\mathfrak{V}_{n-1}(G(n))$, nel secondo la restrizione di φ a $\Phi(G^*)$ è un'applicazione di $\Phi(G^*)$ su $\Phi(G(n))$ che conserva i sottogruppi. Sia $K^*\not\subseteq\Phi(G^*)$, $K^*\not\supseteq\mathfrak{V}_{n-1}(G^*)$. Allora K^* è un gruppo ciclico di ordine p^n oppure un gruppo di ordine p^{n+1} con un sottogruppo massimo ciclico. Se K^* è ciclico, si ha

$$K^*\cap\mathfrak{A}^*=\{\Phi(K^*),\ K^*\cap\mathfrak{M}^*=b^{\beta}a^{\alpha}t^{\gamma}\}.$$

Indichiamo con t^* e t le espressioni formali 1) di $(b^{\beta}a^{\alpha}t^{\gamma})^p$ rispettivamente in G^* e $G(n)$. Si ha:

$$t=t^* \text{ per } p>3$$

$$t=t^*(a^{-\beta\alpha^2}b^{\beta^2\alpha})^{p^{n-1}} \text{per } p=3$$

$$t=t^*(a^{-\beta\binom{\alpha}{2}}b^{\alpha\left[\binom{\beta}{2}+\beta^2\right]})^{p^{n-1}}(a^{\alpha\gamma}b^{\beta\gamma})^{p^{n-1}} \text{per } p=2.$$

Da ciò, poichè $(a^{\alpha\gamma}b^{\beta\gamma})^{p^{n-1}}\in\Phi(K^*)$ (lemma 2.7), segue la 2).

Infine se $K^*=\langle b^{\beta}a^{\alpha}t^{\gamma},\ d\rangle$ con d, $|d|=p$, non in $\mathfrak{V}_{n-1}(G^*)$, posto $b^{\beta}a^{\alpha}t^{\gamma}=l$ si ha

$$K^*\cap\mathfrak{A}^*=\{l,\ ldk_1,\ ld^2k_2,\ \ldots,\ ld^{p-1}k_{p-1},\ \langle l^p,\ d\rangle\} \text{ con } k_i\in\langle l^{p^{n-1}}\rangle$$

e da ciò di nuovo per le 1') la validità della 2). La 2) e la 2'):

$$\langle\varphi^{-1}(K\cap\mathfrak{A})\rangle\cap\mathfrak{A}^*=\varphi^{-1}(K\cap\mathfrak{A}),$$

per ogni $K \subseteq G(n)$, assicurano che l'applicazione

$$\mathfrak{L}(G^*) \ni K^* \to \langle \varphi(K^* \cap \mathfrak{A}^*) \rangle$$

è un isomorfismo di $\mathfrak{L}(G^*)$ su $\mathfrak{L}(G(n))$. Dalle I) e II) segue che esiste un isomorfismo Ψ di $\mathfrak{L}(G(n))$ su $\mathfrak{L}(G)$. Ogni M_1-p-gruppo B non metaciclico, non isomorfo a Γ_1, Γ_2, Γ_3 e non avente Q_8 come sottogruppo è della forma $G(n)/T$. Poichè G è minimale non abeliano e $\Psi(T) \lhd G$ il teorema è provato.

3-1. M_1-gruppi di ordine composto.

Premettiamo i seguenti lemmi alla dimostrazione del teorema D:

LEMMA 3.1. *Se G è un gruppo con tutti i sottogruppi propri modulari, allora*

(1) *G è risolubile,*

(2) *se $|G|$ è divisibile per più di due numeri primi distinti, G è supersolubile,*

(3) *Se $|G|$ è divisibile per più di tre primi distinti, G è modulare.*

DIM. (1) Si osservi che ogni sottogruppo proprio di G è supersolubile (teorema 1.2) e si applichi un noto risultato [6].

(2) Il gruppo G, avendo tutti i sottogruppi propri supersolubili ed avendo ordine divisibile per più di due fattori primi distinti, ammette la fattorizzazione:

(*) $G = PK$, con $P \lhd G$ p-sottogruppo di Sylow relativo al massimo divisore primo di $|G|$ e $P \cap K = 1$. Sia $N \lhd P$, $|N| = p$. Poichè, per ogni primo $q \mid |K|$ e per ogni q-elemento k di K, $\langle k, N \rangle \subseteq \subseteq P\langle k \rangle \subset G$ è supersolubile, il sottogruppo N è normale in G. Osservando che se $N = P$, $G/N \cong K$ è supersolubile, la (2) segue per induzione su $|G|$.

(3) Per la (*), se P è un fattore diretto di G, l'asserto è evidente. Supposto $G \neq P \times K$, sia $Q \subset K$, $Q \not\subseteq C_G(P)$, un q-sottogruppo di Sylow di G. Q è un fattore diretto di K ed ogni t-sottogruppo di K, $t \neq q$ primo, è contenuto in $C_G(P)$, altrimenti G conterrebbe un sottogruppo proprio non modulare. Segue $G = PQ \times K_1$ e quindi G è modulare.

LEMMA 3.2. *Sia G un gruppo minimale non nilpotente. Se i sottogruppi di Sylow di G sono modulari, allora*:

(1) *se $Q_8 \not\subset G$, G è minimale non abeliano;*

(2) *se $Q_8 \subset G$, $G = Q_8 \leftthreetimes C_{3^n}$, con C_{3^n} inducente su Q_8 un automorfismo di ordine 3.*

DIM. Si ricorda che se H è un gruppo minimale non nilpotente, $H = PQ$, $|P| = p^m$, $|Q| = q^n$, con $P \lhd H$ e Q ciclico.

(1) Se la (1) fosse falsa dovrebbe esistere un gruppo $G \supset Q_8$ minimale non nilpotente, ma non minimale non abeliano, di ordine minimo rispetto a questa proprietà. Se $P^p = 1$, G sarebbe minimale non abeliano. Pertanto $\Omega_1(P) \neq G$ è contenuto in $C_G(Q)$. Sia $Z \lhd P$, $|Z| = p$. G/Z è minimale non abeliano per la minimalità di G. Dunque P/Z ha esponente p e, poichè Q centralizza Z, è $|P/Z| \geq p^2$. Questa diseguaglianza comporta, essendo $Q_8 \not\subset P$, che $\Omega_1(P) \supset Z$. Ma ciò è assurdo poichè P/Z è normale minimo in G/Z.

(2) Proviamo soltanto che $P = Q_8$. Ed infatti se $P = Q_8 \times P^*$ con P^* 2-gruppo abeliano elementare, $Z(G)$ conterrebbe P^* e così $G = QQ_8 \times P^*$ risulterebbe nilpotente.

LEMMA 3.3. *Sia G un gruppo con tutti i sottogruppi propri modulari e sia $|G| = p^\alpha q^\beta$ con $p > q$. Se un sottogruppo proprio di G è non nilpotente, allora $G = P \leftthreetimes Q$, $|P| = p^\alpha$, $|Q| = q^\beta$, con P ciclico di ordine p^2 oppure abeliano elementare e Q modulare con un sottogruppo massimo ciclico.*

DIM. Sia G un controesempio con p^α minimo. Poichè ogni sottogruppo proprio di G è q-nilpotente e G non è minimale non nilpotente, G è esso stesso q-nilpotente [8] e pertanto $G = P \leftthreetimes Q$, $|P| = p^\alpha$, $|Q| = q^\beta$. Se Q non è ciclico deve contenere un sottogruppo massimo $\overline{Q}$ tale che $\overline{Q}P$ non sia nilpotente. Essendo $\overline{Q}P$ un gruppo modulare divisibile per due soli primi, $\overline{Q}P$ è un P^*_0-gruppo e da ciò discende immediatamente una contraddizione sulla scelta di G. Pertanto Q è ciclico con $Q^q \subseteq Z(G)$. Se $\Phi(P)\,\Omega_1(P)$ coincidesse con P, dalle ipotesi seguirebbe che P è di esponente p. Dunque $P \supset \Phi(P)\Omega_1(P)$, e l'esistenza in G di un sottogruppo modulare non nilpotente implica che $Q\Phi(P)\Omega_1(P)$ è un P^*_0-gruppo. In particolare segue da ciò che P ha esponente p^2. Sia $N \lhd P$

un sottogruppo di ordine p contenuto in $\Phi(P)$. Se $|P/N|=p$, P sarebbe ciclico di ordine p^2. Quindi $|P/N|\geq p^2$ e poichè, essendo $p\neq 2$, $\Omega_1(P)\supset N$, G/N ha sottogruppi modulari non nilpotenti. Ciò comporta, data la minimalità di p^α, che P/N è ciclico di ordine p^2 oppure abeliano elementare. P/N ciclico implica $N\not\subseteq\Phi(P)$. Quindi P/N è abeliano elementare ed $N=\Phi(P)$. Dal teorema di Maschke segue allora che G contiene un sottogruppo normale T tale che $P/N=\Omega_1(P)/N\times T/N$. TQ è modulare non nilpotente tale essendo QN: ma ciò è assurdo poichè T è ciclico di ordine p^2. Questa contraddizione prova l'asserto.

I p-gruppi modulari non ciclici con un sottogruppo massimo ciclico sono: Q_8, i gruppi abeliani di tipo (p^n, p) e

$$G=\langle b, c \mid b^{p^n}=c^p=1,\ cbc^{-1}=b^{1+p^{n-1}},\ n>1,\ n>2 \text{ per } p=2\rangle.$$

Dal lemma precedente segue subito il

COROLLARIO 3.1. *Sia G un gruppo con tutti i sottogruppi propri modulari e sia $|G|=p^\alpha q^\beta$, $p>q$. Se un sottogruppo proprio di G è non nilpotente e i q-sottogruppi non sono ciclici, G è uno dei gruppi da* (3) *a* (5) *del teorema* D.

DIM. DEL TEOREMA D. I) $|G|=p^\alpha q^\beta$. Se G è minimale non nilpotente, esso, per il lemma 3.2, è del tipo (1) o (2). Supponiamo che un sottogruppo proprio di G sia non nilpotente. Allora $p>q$ e $G=P\times Q$ con P e Q come descritti dal lemma 3.3. Il caso in cui Q non è ciclico è stato già esaminato (corollario 3.1). Sia Q ciclico e tale sia anche P. Se $|P|=p^2$, allora P^pQ è un P^*_0-gruppo e G è il gruppo (6), mentre se $|P|=p$, PQ^p è un P^*_0-gruppo e G è (7). Rimane da esaminare il caso in cui Q è ciclico e P è abeliano elementare non ciclico. Sia $Q=\langle b\rangle$ e sia f l'automorfismo che b induce su P. Se P non è normale minimo in G, si vede che $|P|=p^2$ e, indicata con $\{a_1, a_2\}$ una base opportuna di P, f è definito da

$$a_1^f=a_1^{r_1},\ a_2^f=a_2^{r_2},\ \text{con } r_1\neq 1,\ r_1\neq r_2,\ r_1^q\equiv r_2^q\equiv 1 \pmod{p}.$$

Infine sia P normale minimo in G. Poichè PQ^q è un P^*_0-gruppo, si ha $f^q=r$ con $r\neq 1$, $r^q\equiv 1 \pmod{p}$. Considerato P come spazio vettoriale su $\boldsymbol{Z}_p$, il polinomio minimo $m(x)$ di f divide x^q-r. Se $q^2\mid p-1$, il polino-

mio $x^q - r$ è completamente riducibile su $\boldsymbol{Z}_p$ e P non è normale minimo in G. Dunque $q^2 \nmid p-1$. In questo caso $x^q - r$ è irriducibile [4]) su $\boldsymbol{Z}_p$ e pertanto coincide con $m(x)$. Poichè $m(x)$ divide il polinomio caratteristico, dim $P \geq q$ e così la minimalità di P implica $|P| = p^q$. Da ciò segue subito che G è del tipo (9).

II) $|G| = p^\alpha q^\beta t^\gamma$, con $p > q > t$. G, supersolubile per il lemma 3.1, è esprimibile nella forma $(PQ)T$ con P e PQ normali in G e P, Q, T sottogruppi di Sylow relativi rispettivamente a p, q, t. I sottogruppi PQ, PT, e QT sono modulari e due di essi sono P^*_0-gruppi altrimenti G sarebbe riducibile e quindi modulare. Da ciò segue che P, Q, T sono ciclici e $|P| = p$. Se $C_G(P)$ ha indice primo in G, allora PQ è ciclico di ordine pq e gli automorfismi non identici che T induce su PQ hanno ordine t e non fissano alcun elemento di PQ; di conseguenza G è il gruppo (10). Se invece $|G : C_G(P)| = qt$, QT è ciclico e G è del tipo (11).

BIBLIOGRAFIA

[1] Baer, R.: *Crossed isomorphisms*, Amer. J. of Math., 66 (1944) 341-404.

[2] Blackburn, N.: *On prime power groups with two generetors*, Proc. Cambridge Phil. Soc., 54, 327-337 (1958).

[3] Cooper, C. D. H.: *Power automorphisms of a group*, Math. Z., 107, 335-356 1968.

[4] Doerk, K.: *Minimal nicht uberauflosbare, endliche Gruppen*, Math. Z., 91, 198-205 (1966).

[5] Huppert, B.: *Uber das Produkt von paarweise vertauschbaren zyklischen Gruppen*, Math. Z., 58, 243-264 (1953).

[6] Huppert, B.: *Normalteiler und maximale Untergruppen endlicher Gruppen*, Math. Z., 60, 409-434 (1954).

[7] Ito, N., Ohara, A.: *Sur les groupes factorisables par deux-2-groupes cycliques*, I-II, Proc. of the Japan Academy, XXXII, 731-740 (1956).

[8] Ito, N.: *Note on (LM)-groups of finite orders*, Kodai Math. Sem. Rep., 1951, 1-6.

---

[4]) Sia α uno zero di $x^q - r$ e sia $[\boldsymbol{Z}_p(\alpha) : \boldsymbol{Z}_p] = d \leq q$. Allora $q^2 \mid p^d - 1$ e, poichè $q^2 \nmid p-1$, $p = 1 + kq$ con $(k, q) = 1$. Dalla $p^d = (1 + kq)^d$ segue $q^2 \mid dkq$ cioè q/d ed infine $q = d$.

[9] IWASAWA, K.: *Über die endlichen Gruppen und die Verbände ihrer Untergruppen*, J. Univ., Tokyo, 4, 171-199 (1941).

[10] IWASAWA, K.: *Über die Struktur der endlichen Gruppen, deren echte Untergruppen samtlich nilpotent sind*, Proc. Phys. Math, Soc. Jap., (3), 23, 1-4 (1941).

[11] JONES, A. W.: *The lattice isomorphisms of certain finite groups*, Duke Math. Journal, 12 (1945) 541-560.

[12] MILLER, G. A., MORENO, H.: *Nonabelian groups in which every subgroup is abelian*, Trans. Am. Math. Soc., 4, 398-404 (1903).

[13] NAPOLITANI, F.: *Sui p-gruppi modulari finiti*, Rend. Sem. Mat. Univ. Padova, XXXIX, 296-303 (1967).

[14] REDEI, L.: *Das schiefe Produkt in der Gruppentheorie*, Com. Math. Helvet., 20, 225-267 (1947).

[15] REDEI, L.: *Die endlichen einstufig nichtnilpotenten Gruppen*, Publ. Math. Debrecen, 4, 303-324 (1956).

[16] SCHMIDT, O. J.: *Sui gruppi finiti ogni sottogruppo proprio dei quali è nilpotente*, (in russo) Math. Sbornik, 31, 366-372.

[17] SUZUKI, M.: *Structure of a group and the structure of its lattice of subgroups*, Erg. Math., 10, Berlin, Springer 1956.

[18] ZASSENHAUS, H.: *The theory of groups*, New York, Chelsea, 1958.

Manoscritto pervenuto in redazione il 1° dicembre 1970.