Rendiconti *del* Seminario Matematico *della* Università di Padova

Giovanni Zacher

Sugli elementi modulari in un *p*-gruppo

Rendiconti del Seminario Matematico della Università di Padova, tome 24 (1955), p. 165-182

<http://www.numdam.org/item?id=RSMUP_1955__24__165_0>

SUGLI ELEMENTI MODULARI IN UN p-GRUPPO

Memoria (*) *di* GIOVANNI ZACHER (*a Padova*)

Il presente lavoro contiene un primo studio della classe costituita dagli elementi modulare di un reticolo $\mathfrak{L}$ [1]). La nozione di elemento modulare di un reticolo è dovuta allo Zappa: Se $\mathfrak{L}$ è un reticolo, un suo elemento m si dirà un elemento modulare, qualora, preso comunque un sottoreticolo modulare $\mathfrak{R}$ di $\mathfrak{L}$, il reticolo $\{m, \mathfrak{R}\}$ generato da m ed $\mathfrak{R}$ risulta ancora un sottoreticolo modulare di $\mathfrak{L}$. Lo studio degli elementi modulari nel reticolo $\mathfrak{L}(G)$ dei sottogruppi di un gruppo G ha interesse perchè permette di caratterizzare completamente in certi casi, la struttura del reticolo $\mathfrak{L}(G)$.

La presente memoria è stata suddivisa in 6 numeri. Nel n. 2 si mettono in evidenza alcune proprietà generali di cui godono gli elementi modulari di un reticolo qualunque. Si stabilisce, fra l'altro, che gli elementi del centro e gli elementi neutri di un reticolo sono sempre elementi modulari. Si assegnano inoltre alcuni teoremi di «riduzione» che permettono di limitare lo studio degli elementi modulari ai reticoli sem-

---

(*) Pervenuta in Redazione il 28 marzo 1955.
Indirizzo dell'A.: Seminario matematico, Università, Padova.

1) I risultati esposti in questa Memoria sono tratti in parte da un mio lavoro, premiato dalla Accademia delle Scienze Fisiche e Matematiche in Napoli, e deposto negli archivi di quella Accademia. Prescindo naturalmente da differenze formali di esposizione. Gli altri risultati di quel lavoro saranno esposti insieme con delle proposizioni ulteriori, in una Memoria che redigerò prossimamente.

plici, e si rivelano particolarmente utili nello studio degli elementi modulari del reticolo $\mathfrak{L}(G)$.

Nel n. 3 si assegna una condizione necessaria perchè un sottogruppo di un p-gruppo d'ordine finito, sia un elemento modulare. Nel n. 4 si passa allo studio degli elementi modulari nel reticolo $\mathfrak{L}(G)$ di un p-gruppo finito d'esponente p. Il teorema fondamentale ivi raggiunto è il seguente: Il reticolo $\mathfrak{L}(G)$ di un p-gruppo finito d'esponente p contiene elementi modulari diversi da 1 e G, se, e solo se, il reticolo $\mathfrak{L}(G)$ è modulare. Il n. 5 contiene un'applicazione di questo teorema.

Il teorema del n. 3 non può essere esteso in generale nemmeno ai p-gruppi regolari [2] [2]) qualora l'esponente superi p; la cosa è dimostrata nel n. 6 adducendo un esempio nel quale l'esponente del gruppo è p^2.

1. - Notazioni: Un reticolo sarà indicato sempre con una lettera maiuscola in corsivo, come per es. $\mathfrak{L}$, mentre gli elementi di un reticolo verranno indicati in generale con lettere minuscole in corsivo. I e 0 rappresenteranno il massimo e minimo assoluto di un reticolo. (a) l'ideale principale generato da a ed $(\breve{a})$ l'ideale duale principale generato da a. $\{M\}$ il reticolo generato dagli elementi dell'insieme M. $\mathfrak{L}\,\mathfrak{H}$ il reticolo prodotto cardinale di $\mathfrak{L}$ e $\mathfrak{H}$.

Un gruppo si indicherà sempre con una lettera maiuscola in stampatello, come per es. G, mentre gli elementi di un gruppo verranno indicati con lettere minuscole in stampatello. $\mathfrak{L}(G)$ è il reticolo dei sottogruppi del gruppo G. $o(G)$ ordine del gruppo G, $[G:H]$ indice del sottogruppo H in G. S_{p^α} sottogruppo di Sylow d'ordine p^α; ${}_pH$ sottogruppo il cui indice è p^α.

$N(H)$ normalizzante di H in G; $C(H)$ centralizzante di H in G; $\Phi(G)$ sottogruppo di Frattini di G.

2. - Sia $\mathfrak{L}$ un reticolo qualunque; allora, secondo Zappa, un elemento m di $\mathfrak{L}$ chiameremo un elemento domulare di $\mathfrak{L}$ se

---

[2]) I numeri tra parentesi quadre si riferiscono alla bibliografia riportata in fondo alla Memoria.

soddisfa alla seguente condizione: se $\mathfrak{R}$ è un arbitrario sottoreticolo modulare di $\mathfrak{L}$, il sottoreticolo $\{m, \mathfrak{R}\}$ risulta ancora modulare.

In questo numero esporremo diverse proprietà degli elementi modulari di un reticolo $\mathfrak{L}$.

I. - Se m è un elemento modulare di un reticolo $\mathfrak{L}$, m è un elemento modulare di ogni sottoreticolo di $\mathfrak{L}$ cui appartiene.

II. - Se tra 2 reticoli $\mathfrak{L}$, $\mathfrak{L}'$ esiste un isomorfismo τ, se m è un elemento modulare di $\mathfrak{L}$, l'elemento corrispondente $m' = \tau(m)$ ad m nell'isomorfismo τ, è un elemento modulare di $\mathfrak{L}'$. Infatti un isomorfismo tra reticoli trasforma un sottoreticolo modulare di $\mathfrak{L}$ in un sottoreticolo modulare di $\mathfrak{L}'$ e viceversa.

III. - Gli elementi I e 0 di un reticolo $\mathfrak{L}$ sono elementi modulari di $\mathfrak{L}$.

Infatti se $\mathfrak{R}$ è un sottoreticolo di $\mathfrak{L}$, il reticolo $\{I, \mathfrak{R}\}$ differisce da $\mathfrak{R}$ al massimo per l'elemento I. Se quindi $\mathfrak{R}$ è un sottoreticolo modulare di $\mathfrak{L}$, se x, y, z sono tre elementi qualunque di $\{I, \mathfrak{R}\}$, con $x \leq z$, sarà ancora.

$$x \cup (y \cap z) = (x \cup y) \cap z \tag{1}$$

in quanto se x, y, z sono tutti diversi di I essi stanno in $\mathfrak{R}$ che per ipotesi è modulare; se poi qualcuno di essi coincide con I la (1) è ancora vera dato il significato I.

Con ragionamento duale si prova che pur 0 è un elemento modulare di $\mathfrak{L}$.

Poichè I e 0 sono elementi modulari in qualunque reticolo che li contiene li chiameremo nel seguito elementi modulari banali di un reticolo.

IV. - Gli elementi modulari di un reticolo $\mathfrak{L}$ costituiscono un sottoreticolo modulare $\mathfrak{L}'$ di $\mathfrak{L}$.

Infatti siano m_1, m_2 due arbitrari elementi modulari di un reticolo $\mathfrak{L}$. Basterà allora dimostrare che sia $m_1 \cup m_2$ sia $m_1 \cap m_2$ sono elementi modulari di $\mathfrak{L}$.

Sia $\mathfrak{R}$ un qualunque sottoreticolo modulare di $\mathfrak{L}$. Poichè

$$\{m_1 \cup m_2, \mathfrak{R}\} \subseteq \{m_1, m_2, \mathfrak{R}\}$$

si conclude che il reticolo $\{ m_1 \cup m_2, \mathfrak{R} \}$ è modulare essendo tale $\{m_1, m_2, \mathfrak{R}\} = \{ m_1, \{ m_2, \mathfrak{R} \}\}$.

Lo stesso si può ripetere per $\{ m_1 \cap m_2, \mathfrak{R} \}$.

Che poi $\mathfrak{L}'$ sia modulare segue dal fatto che presi tre elementi m_1, m_2. m_3 di $\mathfrak{L}'$ con $m_1 \leq m_3$, sussiste la (1) perchè il reticolo $\{ m_1, \{m_2, m_3\}\}$ risulta modulare.

V. - Sia $\mathfrak{L}$ un reticolo in cui ogni sottoreticolo modulare $\mathfrak{R}$ di $\mathfrak{L}$ è contenuto in un sottoreticolo modulare massimo; allora gli elementi modulari di $\mathfrak{L}$ sono tutti e soli gli elementi comuni a tutti i sottoreticoli modulari massimi di $\mathfrak{L}$.

Infatti se m è un elemento modulare ed $\mathfrak{M}$ un sottoreticolo modulare massima di $\mathfrak{L}$, poichè $\{ m, \mathfrak{M} \}$ è ancora un reticolo modulare di $\mathfrak{L}$, dovrà essere $\{ m, \mathfrak{M} \} = \mathfrak{M}$, ossia m è contenuto in $\mathfrak{M}$. Viceversa sia m un elemento comune a tutti i sottoreticoli modulari massimi di $\mathfrak{L}$. Sia $\mathfrak{R}$ un sottoreticolo modulare di $\mathfrak{L}$. $\mathfrak{R}$ sarà contenuto in un sottoreticolo modulare massimo $\mathfrak{M}$ di $\mathfrak{L}$. Ne segue $\{ m, \mathfrak{R} \} \subseteq$ $\subseteq \{ m, \mathfrak{M} \} = \mathfrak{M}$. ossia $\{ m, \mathfrak{R} \}$ è un reticolo modulare.

VI. - Gli elementi del centro di un reticolo $\mathfrak{L}$ sono elementi modulari.

Sia $\mathfrak{R}$ un sottoreticolo di $\mathfrak{L}$. Se $\bar{\mathfrak{H}}$ e $\bar{\bar{\mathfrak{K}}}$ sono gli insiemi rispettiv. delle prime e seconde componenti degli elementi di $\mathfrak{R}$, $\bar{\mathfrak{H}}$ e $\bar{\bar{\mathfrak{K}}}$ sono 2 sottoreticoli rispettivamente di $\mathfrak{H}$ e di $\mathfrak{K}$ e risulta

$$\mathfrak{R} \subseteq \bar{\mathfrak{H}} \bar{\bar{\mathfrak{K}}}$$

ossia $\mathfrak{R}$ è un sottoreticolo, in generale proprio, del prodotto cardinale $\bar{\mathfrak{H}} \bar{\bar{\mathfrak{K}}}$.

Sussiste la proposizione: Il reticolo $\mathfrak{R}$ è modulare se e solo se tali sono $\bar{\mathfrak{H}}$ e $\bar{\bar{\mathfrak{K}}}$.

La sufficienza della condizione consegue immediatamente dal fatto che se $\bar{\mathfrak{H}}$ e $\bar{\bar{\mathfrak{K}}}$ sono modulari, tale è pure il reticolo $\bar{\mathfrak{H}} \bar{\bar{\mathfrak{K}}}$.

Per dimostrare la necessità della condizione faremo vedere che se $\bar{\mathfrak{H}}$ o $\bar{\bar{\mathfrak{K}}}$ non è modulare, tale non può essere neppure $\mathfrak{R}$.

Supponiamo, per fissare le idee, che $\bar{\mathfrak{H}}$ sia non modulare. Esistono allora 3 elementi h_1, h_2, h_3 di $\bar{\mathfrak{H}}$ con $h_1 < h_3$ tali che

$$h_1 \cup (h_2 \cap h_3) \neq (h_1 \cup h_2) \cap h_3 \tag{2}$$

Siano r_1, r_2, r_3 tre elementi di $\mathfrak{R}$ che hanno rispettivamente h_1, h_2, h_3 per prime componenti: $r_1 = [h_1, k_1]$, $r_2 = [h_2, k_2]$, $r_3 = [h_3, k_3]$.

Ora $r_1 \cup r_3 = [h_1 \cup h_3, k_1 \cup k_3] = [h_3, k_1 \cup k_3]$. Posto $r_1 \cup r_3 = \bar{r}_3$ si avrà dunque $r_1 < \bar{r}_3$ e per la modularità di $\mathfrak{R}$ risulterà

$$r_1 \cup (r_2 \cap \bar{r}_3) = (r_1 \cup r_2) \cap \bar{r}_3$$

il che implica

$$h_1 \cup (h_2 \cap h_3) = (h_1 \cup h_2) \cap h_3$$

in contrasto con la (2).

Visto dunque che $\overline{\mathfrak{H}}$, $\overline{\mathfrak{K}}$ sono reticoli modulari, consideriamo un elemento del centro di $\mathfrak{L}$, ad es. $[0, I]$: il reticolo $\{[0, I], \overline{\mathfrak{H}}\,\overline{\mathfrak{K}}\}$ non è altro che il prodotto cardinale $\{0, \overline{\mathfrak{H}}\}$ $\{I, \overline{\mathfrak{K}}\}$ di $\{0, \overline{\mathfrak{H}}\}$ ed $\{I, \overline{\mathfrak{K}}\}$. Ora ricordiamo che 0, I sono elementi modulari e modulari sono i reticoli $\overline{\mathfrak{H}}$, $\overline{\mathfrak{K}}$; quindi tali saranno i reticoli $\{0, \overline{\mathfrak{H}}\}$, $\{I, \overline{\mathfrak{K}}\}$ e di conseguenza

$$\{[0, I], \overline{\mathfrak{H}}\,\overline{\mathfrak{K}}\} = \{0, \overline{\mathfrak{H}}\}\{I, \overline{\mathfrak{K}}\}.$$

Ma $\mathfrak{R} \subseteq \overline{\mathfrak{H}}\,\overline{\mathfrak{K}}$ quindi $\{\mathfrak{R}, [0, I]\} \subseteq \{[0, I], \overline{\mathfrak{H}}\,\overline{\mathfrak{K}}\}$, ossia $\{\mathfrak{R}, [0, I]\}$ è modulare. c. v. d.

VII. - **Ogni elemento neutro di un reticolo $\mathfrak{L}$ è un elemento modulare.**

Infatti per un noto teorema di BIRKHOFF[3]), se a è un elemento neutro di un reticolo $\mathfrak{L}$, la corrispondenza τ che associa ad ogni elemento x di $\mathfrak{L}$ la coppia ordinata $[x \cap a, x \cap a]$ definisce un isomorfismo tra $\mathfrak{L}$ ed un sottoreticolo $\mathfrak{B}$ del reticolo $\mathfrak{A}\mathfrak{B}$ prodotto cardinale di 2 reticoli dove $\mathfrak{A} = (a)$, $\mathfrak{B} = (\breve{a})$

L'isomorfismo τ porta l'elemento neutro a nell'elemento $[a, a]$ che è un elemento del centro di $\mathfrak{A}\,\mathfrak{B}$ essendo $a = I$ in $\mathfrak{A}$ ed $a = 0$ in $\mathfrak{B}$.

3) [1] pag. 28.

L'elemento $[a, a]$ per VI è un elemento modulare di $\mathfrak{A}\,\mathfrak{B}$ e quindi pure di $\mathfrak{R}$. Dato ora l'isomorfismo tra $\mathfrak{L}$ ed $\mathfrak{A}$ in cui ad a corrisponde l'elemento modulare $[a, a]$ di $\mathfrak{R}$, per II concludiamo che a è un elemento modulare di $\mathfrak{L}$.

VIII. - Sia $\mathfrak{L}$ un reticolo ed m un suo elemento modulare. Detto b un elemento qualunque di $\mathfrak{L}$, consideriamo l'ideale principale (b) generato da b; ebbene l'elemento $b \cap m$ è un elemento modulare del reticolo (b).

Sia invero $\mathfrak{R}$ un sottoreticolo modulare qualunque di (b). Il reticolo $\mathfrak{R}$ sarà quindi un sottoreticolo modulare pure di $\mathfrak{L}$.

Per provare il teorema, basterà far veder che $\{m \cap b, \mathfrak{R}\}$ è un reticolo modulare. Ora abbiamo le seguenti relazioni

$$\begin{aligned}(3) \qquad \{m \cap b, \mathfrak{R}\} \subseteq \{b \cap m, \mathfrak{R}, b\} = \{b \cap m, \{b, \mathfrak{R}\}\} \subseteq \\ \subseteq \{b, m, \{b, \mathfrak{R}\}\} = \{m, \{\mathfrak{R}, b\}\}.\end{aligned}$$

Posto $\mathfrak{S} = \{\mathfrak{R}, b\}$, $\mathfrak{S}$ è un reticolo modulare. Infatti b è il massimo assoluto di $\mathfrak{S}$, quindi è un elemento modulare di $\mathfrak{S}$ ma allora, essendo $\mathfrak{R}$ un sottoreticolo modulare di $\mathfrak{S}$, $\{b, \mathfrak{R}\} = \mathfrak{S}$ è modulare. Dato che per ipotesi m è un elemento modulare di $\mathfrak{L}$, il reticolo $\{m, \{\mathfrak{R}, b\}\}$ risulta pure modulare. Ne segue dalla (3) che il reticolo $\{m \cap b, \mathfrak{R}\}$ è pure modulare c. v. d.

Con ragionamento duale si perviene alla proposizione

IX. - Sia $\mathfrak{L}$ un reticolo ed m un suo elemento modulare. Detto b un elemento qualunque di $\mathfrak{L}$, considerimo l'ideale principale duale $(\breve{b})$ generato da b; ebbene l'elemento $b \cup m$ è un elemento modulare di $(\breve{b})$.

X. - Se $\mathfrak{H}$ e $\mathfrak{K}$ sono due reticoli dotati di 0, (I) se m è un elemento modulare di $\mathfrak{H}$, m è pure un elemento modulare del prodotto cardinale $\mathfrak{H}\,\mathfrak{K}$.

Infatti se $\mathfrak{R}$ è un reticolo modulare, se $\overline{\mathfrak{H}}$, $\overline{\mathfrak{K}}$ hanno il significato loro attribuito in VII, risulta

$$(4) \qquad \{[m, 0], \mathfrak{R}\} \subseteq \{[m, 0], \overline{\mathfrak{H}}\,\overline{\mathfrak{K}}\} = \{m, \overline{\mathfrak{H}}\}\{0, \overline{\mathfrak{K}}\}.$$

Ora $\overline{\mathfrak{H}}$, $\overline{\mathfrak{K}}$ sono reticoli modulari (VI) e quindi pure $\{m, \overline{\mathfrak{H}}\}$, $\{0, \overline{\mathfrak{K}}\}$, sicchè la (4) prova il nostro teorema.

XII. - Se m è un elemento modulare di un reticolo $\mathfrak{L}$ dotato di 0, se b è un qualunque elemento di $\mathfrak{L}$ con $m \cap b = 0$ allora se l è un elemento dell'ideale (m), l è un elemento modulare nell'ideale $(l \cup b)$ generato da $l \cup b$.

Infatti abbiamo

$$l = l \cup (b \cap m) = (l \cup b) \cap m \tag{5}$$

essendo m modulare ed $l \leq m$.

La (5) ci dice, in virtù della VIII, che l è un elemento modulare di $(l \cup b)$. c. v. d.

Dualmente:

XII. - Se m è un elemento modulare di un reticolo $\mathfrak{L}$ dotato di I, se b è un qualunque elemento di $\mathfrak{L}$ con $m \cup b = I$ allora se l è un elemento dell'ideale duale $(\breve{m})$, l è un elemento modulare nell'ideale duale $(l \breve{\cap} b)$ generato da $l \cap b$.

3. - Sia G un gruppo ed H, K due suoi sottogruppi. Ricordiamo che i due sottogruppi H, K di G diconsi tra loro permutabili se il sistema degli elementi HK coincide con quello KH di G. Un sottogruppo H di G che sia un elemento modulare di $\mathfrak{L}(G)$ si dirà semplicemente un sottogruppo modulare di G.

Teorema: *Se G è un p-gruppo d'ordine p^{α}, i sottogruppi modulari di G sono permutabili con ogni sottogruppo di G.*

Il teorema è ovvio se l'ordine di G è p; useremo quindi induzione sull'ordine del gruppo G. Sia M un sottogruppo modulare di G. Se M è un elemento modulare banale di $\mathfrak{L}(G)$, il teorema è vero perchè allora M coincide o con G o col sottogruppo identico 1 di G. Possiamo inoltre supporre che M non sia un sottogruppo massimo di G perchè in un p-gruppo tali gruppi sono normali e quindi permutabili con ogni sottogruppo di G. Esclusi questi casi, supponiamo che M, pur essendo un sottogruppo modulare, non sia permutabile con ogni sottogruppo di G. Esisterà allora un sottogruppo ciclico $\{a\}$ di G non permutabile con M. Sia N un sottogruppo massimo di G contenente (propriamente) M. Consideriamo il gruppo unione $\{a\} \cup M$. Per le ipotesi d'induzione, dovrà essere $\{a\} \cup M = G$.

Poniamo

$$M \cap \{a\} = \{b\}, \qquad N \cap \{a\} = \{b_1\}.$$

Sarà $\{b_1\}$ contenuta propriamente in $\{a\}$, $\{b_1\} \subset \{a\}$, altrimenti sarebbe $\{a\} \cup M \subseteq \{a\} \cup N = N \subset G$, contro ipotesi.

Inoltre non può essere $\{b_1\} = \{b\}$. Infatti in tal caso il reticolo $\{M, N, \{a\}\}$ non potrebbe essere modulare avendo esso un diagramma di Hasse quale indicato in fig. 1.

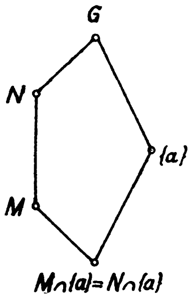

Figura 1

Sarà quindi

$$\{b_1\} \supset \{b\}$$

Ora valgono le relazioni

$$(6) \quad \begin{aligned} M \cap \{b_1\} &= M \cap \{N \cap \{a\}\} = M \cap \{a\} = \{b\} \\ M \cup \{b_1\} &= M \cup \{N \cap \{a\}\} = \{M \cup \{a\}\} \cap N = G \cap N = N. \end{aligned}$$

Dalla (6), per le ipotesi d'induzione, segue che $\{b_1\}$ è permutabile con M, sicchè

$$(7) \qquad M \cup \{b_1\} = M\{b_1\}.$$

Inoltre N è permutabile con $\{a\}$ sicchè un elemento g di G si può mettere sotto la forma $g = n\bar{a}$ con n ed $\bar{a}$ elementi convenienti di N ed $\{a\}$. Ma $n = m\bar{b}$ per la (6) e (7), ($\bar{b}$ elemento conv. di $\{b_1\}$).

Dunque

$$(8) \qquad g = n\bar{a} = (m\bar{b})\bar{a} \doteq m(\bar{b}\bar{a}) = m\bar{\bar{a}}$$

dove $\bar{\bar{a}}$ è un elemento di $\{a\}$, avendosi $\{b_1\} \subset \{a\}$.

La (8) ci dice che il sistema $M\ \{a\}$ coincide con G, ossia il sistema $H\ \{a\}$ è un gruppo il che implica la permutabilità di M con $\{a\}$.

L'assurdo cui siamo pervenuti prova il teorema.

Osservazione: Chiamando con Zappa quasi abeliano un gruppo in cui due suoi qualunque sottogruppi sono tra loro permutabili, dal teorema segue come corollario la ben nota proposizione: La classe dei p-gruppi G d'ordine finito in cui $\mathfrak{L}\ (G)$ è un reticolo modulare coincide con la classe dei p-gruppi quasi abeliani.

Invero se $\mathfrak{L}\ (G)$ è un reticolo modulare, ogni sottogruppo di G è un sottogruppo modulare, per cui ogni sottogruppo di G è permutabile con ogni sottogruppo di G.

4. - In questo numero con G indicheremo sempre un p-gruppo d'ordine finito p^α, con $\alpha \geq 1$, in cui tutti gli elementi abbiano ordine p, ossia G sia d'esponente p.

Sia P un sottogruppo modulare di G d'ordine p. Il gruppo P, in virtù del teorema del n.ro precedente, risulta permutabile con ogni sottogruppo di G. Siano H, K due sottogruppi di G d'ordine p. Consideriamo il reticolo $\{H, K, P\}$ e supponiamo che risulti $H \cup K \supset P$. Dimostriamo allora che il reticolo $\{H, K, P\}$ è modulare se e solo se H è permutabile con K.

La sufficienza è ovvia in quanto il gruppo $H \cup K \cup P$ risulta abeliano. Per la necessità, supposto H non permutabile con K, osserviamo che

$$H \cup [K \cap (H \cup P)] = H \tag{9}$$

essendo $(H \cup P) \cap K = 1$, perchè $H \cup P$ è abeliano e non può quindi contenere K.

Inoltre

$$(H \cup K) \cap (H \cup P) = H \cup P \tag{10}$$

essendo $H \cup K \supset P$, $H \cup K \supset H$.

La (9) confrontata con la (10) ci dice pertanto che $\{H, K, P\}$ non può essere modulare, se H non è permutabile con K.

I. - **Il gruppo G può contenere sottogruppi modulari d'ordine p se e solo se G è abeliano elementare.**

Sia P un sottogruppo modulare d'ordine p ed H, K due sottogruppi d'ordine p non permutabili tra loro. Poichè P sta nel centro di G, per quanto dimostrato, dovrà essere $P \cap \cap (H \cup K) = 1$, e quindi il gruppo $P \cup H \cup K$ risulta il prodotto diretto di P per $H \cup K$.

Posto $P = \{a\}$, e $\{b\}$ un sottogruppo del centro di $H \cup K$, consideriamo il sottogruppo $\{a\,b\}$. Esso non è contenuto in $H \cup K$ ma sta in $C(H \cup K)$. Pertanto risulta

$$\{ab\} \times (H \cup K) = \{a\} \times (H \cup K)$$

Ora la corrispondenza $a^{\sigma} n \rightarrow a^{\sigma} b^{\sigma} n$ con n in $H \cup K$ è un automorfismo di $P \times (H \cup K)$. Infatti presi 2 elementi g_1, g_2 di $P \times (H \cup K)$ si ha

$$\begin{array}{lll} g_1 = a^{\sigma_1} n_1, & g_2 = a^{\sigma_2} n_2, & g_1 g_2 = a^{\sigma_1 + \sigma_2} n_1 n_2 \\ \downarrow & \downarrow & \downarrow \\ g_1' = a^{\sigma_1} b^{\sigma_1} n_1, & g_2' = a^{\sigma_2} b^{\sigma_2} n_2, & (g_1 g_2)' = a^{\sigma_1 + \sigma_2} b^{\sigma_1 + \sigma_2} n_1 n_2 \end{array}$$

da cui $g'_1\, g'_2 = (g_1\, g_2)'$.

In tale automorfismo il gruppo P va nel gruppo $T = \{a\,b\}$. Quindi T è pure un sottogruppo modulare di $P \times (H \cup K)$ (II del n. 1).

Il reticolo $\{T, H, K\}$ è pertanto modulare e quindi pure il reticolo $\{P, T, H, K\}$.

Si hanno le relazioni seguenti

$H \cup K \supset (H \cup T \cup P) \cap (H \cup K)$ perchè $H \cup K$ non contiene P e l'ordine di $H \cup T \cup P$ non può superare p^3. Inoltre $M = (H \cup T \cup P) \cap (H \cup K)$ contiene H. Invero $[H \cup (T \cup P)] \cap \cap (H \cup K) = H \cup [(T \cup P) \cap (H \cup K)]$ ed $(T \cup P) \cap (H \cup K)$ contiene $\{b\}$, che è diverso da H. Quindi $H \cup K \supset M \supset H \supset 1$. Inoltre $M \cup K = H \cup K$ perchè $H \cup K \supset M \supset H$. $M \supset K = 1$, perchè se K fosse contenuto in M, sarebbe $M \supseteq H \cup K$. Si ha pertanto il seguente diagramma (fig. 2)

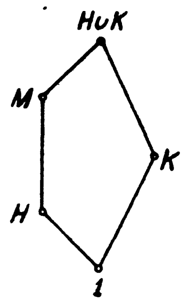

Figura 2

ossia il reticolo $\{P, T, H, K\}$ non è modulare.

L'assurdo cui siamo pervenuti prova la nostra proposizione.

II. - Se G non è abeliano, nessun sottogruppo massimo di G può essere un sottogruppo modulare.

Infatti sia N un tale sottogruppo. Ci sarà allora un sottogruppo $P = \{b\}$ per cui $N \cap P = 1$, $N \cup P = G$.

Sia P non un sottogruppo normale in G. Esisterà allora un sottogruppo $H = \{h\}$ di N non permutabile con P.

Risulta allora

$$H \cup (N \cap P) \neq (H \cup P) \cap N$$

vale a dire il reticolo $\{H, P, N\}$ non è modulare.

Infatti il primo membro coincide con H, mentre il secondo contiene propriamente H; invero si hanno le relazioni

$$\{b\} = H \subset N; \qquad \{aha^{-1}\} \neq H; \qquad \{aha^{-1}\} \subset N.$$

Quindi

$$H \subset \{aha^{-1}\} \cup \{h\} \subseteq N.$$

D'altra parte $P \cup H \supseteq \{a\} \cup \{aha^{-1}\}$, per cui $N \cap [P \cup H] \supset H$.

Resta il caso da esaminare in cui il gruppo P risulta normale in G, per cui $G = N \times P$.

Per ipotesi d'induzione possiamo supporre che ogni sottogruppo proprio di G che contiene un sottogruppo modulare non banale sia abeliano. Sia N_1 un sottogruppo d'indice p in N. $\{c\}$ un sottogruppo di N non contenuto in N_1. Avremo $N = N_1 \{c\}$.

Posto $N = N_1\{ac\}$, risulta $N_1 \cap \{ac\} = 1$. Infatti se ac fosse in N_1, ac starebbe in N e poichè N contiene c, N conterrebbe anche a, contro ipotesi. Analogamente $\overline{N} \cap \{a\} = 1$, sicchè

$$N \cong \frac{N \times \{a\}}{\{a\}} = \frac{G}{\{a\}} = \frac{\overline{N} \times \{a\}}{\{a\}} \cong \overline{N}.$$

Essendo dunque $N \cong \overline{N}$, $N \times \{a\} = \overline{N} \times \{a\}$, esiste un automorfismo di G che muta N in $\overline{N}$. $\overline{N}$ è quindi un sottogruppo modulare di G; ma allora tale è pure il gruppo non identico $N \cap \overline{N} \subset N$, sicchè N è abeliano e quindi pure $G = N \times \{a\}$.

Siamo ora in grado di dimostrare

III. - Se G è un p-gruppo d'ordine finito e d'esponente p, condizione necessaria e sufficiente affinchè G contenga un sottogruppo modulare diverso da G e da 1 è che G sia abeliano.

La sufficienza è ovvia. Resta da dimostrare la necessità della condizione. Sia H un sottogruppo modulare proprio non identico. Possiamo supporre per quanto precede che H sia nè un sottogruppo massimo nè minimo di G. Siano P, Q due sottogruppi minimi di G non permutabili tra loro. Si presentano 2 casi:

$$\alpha)\ P \cup Q = G, \qquad \beta)\ P \cup Q \subset G.$$

Esaminiamo il primo caso. Il gruppo H non può contenere nè P nè Q perchè altrimenti risulterebbe $H \cup P = G$ oppure $H \cup Q = G$ il che è impossibile essendo H non massimo e permutabile con ogni sottogruppo di G. Consideriamo il reticolo $\{H, P, Q\}$. E' $P \cap Q = 1$, $(H \cup P) \cap Q = 1$, Essendo $H \cup P \subset G$. Inoltre è $P \subset H \cup P$, $(H \cup P) \cup Q = G$. Quindi il diagramma di $\{H, P, Q\}$ è quello della fig. 3

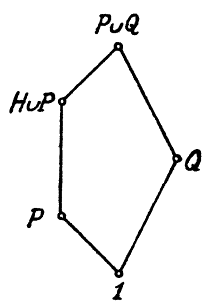

Figura 3

ossia $\{H, P, Q\}$ non è un reticolo modulare.

Passiamo al secondo caso. Possiamo supporre $H \not\subset Q \cup P$, perchè altrimenti per ipotesi d'induzione è $Q \cup P$ un gruppo abeliano, e quindi Q permutabile con P.

Sarà quindi $(Q \cup P) \cap H \subset H$ Sia s un elemento di H non contenuto in $H \cap (Q \cup P)$. Il gruppo $\{s\}$ è normale in G. Infatti per la II, H sta nel centro di G essendo $H \cup P$ un gruppo abeliano se P è un sottogruppo minimo qualunque di G. Consideriamo il gruppo $\frac{G}{\{s\}}$; ivi il gruppo $\frac{H}{\{s\}}$ è un sottogruppo modulare proprio non identico.

Per induzione sull'ordine di G, il gruppo $\frac{G}{\{s\}}$ sarà abeliano elementare. Ora $P \cup Q \simeq \frac{(P \cup Q) \times \{s\}}{\{s\}}$; ma $\frac{Q \cup P \times \{s\}}{\{s\}} \subset \subset \frac{G}{\{s\}}$, quindi $\frac{G}{\{s\}}$ è abeliano. Ma allora lo è pure $P \cup Q$.

5. - Come applicazione della conclusione raggiunta nel n. 3, diamo qui il seguente teorema: Se G è un p-gruppo d'ordine finito, se M è un sottogruppo modulare proprio non contenuto in $V(G)$, ove $V(G)$ è il sottogruppo di G generato dalle potenze p-esime degli elementi di G, allora il gruppo $V(G)$ coincide con Φ G).

Infatti consideriamo il gruppo $T = V(G) \cup M$. Tale gruppo è un sottogruppo proprio di G, perchè $V(G)$ come sottogruppo del gruppo di FRATTINI $\Phi(G)$ non ha complementi in G. Il gruppo T contiene propriamente $V(G)$ avendo supposto M non contenuto in $V(G)$, sicchè il gruppo $\frac{M \cup V(G)}{V(G)}$ è un sottogruppo modulare proprio non identico di $\frac{G}{V(G)}$ (IX).

Ora l'esponente del p-gruppo $\frac{G}{V(G)}$ è p.

Pertanto per la III del n. 3, il gruppo $\frac{G}{V(G)}$ è abeliano (elementare).

Sia $a_1, a_2, \ldots a_d$ una base minima di G. Sarà allora $a_1 \mid V(G) \mid, a_2 \mid V(G) \mid, \ldots a_d \mid V(G) \mid$ una base di $\frac{G}{V(G)}$ per cui l'indice di $V(G)$ in G non può essere minore di p^d. D'altra parte $\Phi(G) \supseteq V(G)$, $[\Phi : (G)] = p^d$, quindi come volevasi

$$\Phi(G) = V(G).$$

Corollario: Se G è un p-gruppo d'ordine finito con $p \neq 2$, generato da due elementi, il gruppo G ha il reticolo $\mathfrak{L}(G)$ modulare se contiene un sottogruppo modulare proprio non contenuto in $V(G)$.

Infatti pel teorema precedente risulta $\Phi(G) = V(G)$; inoltre è $d = 2$, $p \neq 2$, il che, per un risultato di HUPPERT [3], basta per concludere che G sia un gruppo quasi abeliano.

6. - Diamo in questo numero l'esempio di un p-gruppo G, che pur non avendo il suo reticolo $\mathfrak{L}(G)$ modulare, contiene un elemento modulare. Consideriamo a tal fine il seguente gruppo d'ordine p^4 con p numero primo dispari, generato da tre elementi, a, b, c soddisfacenti alle seguenti relazioni:

$$a^{p^2} = 1, \; b^p = 1, \; c^p = 1, \; b^{-1}ab = a^{p+1}, \; c^{-1}ac = ab, \; c^{-1}bc = b.$$

Questo gruppo non è a reticolo modulare.

Infatti gli elementi a e c generano da soli tutto il gruppo, perchè dalla relazione $c^{-1}ac = ab$ segue che il gruppo $\{c, a\}$ contiene anche l'elemento b per cui

$$\{a, c\} = \{a, b, c\} = G.$$

Ora se $\mathfrak{L}(G)$ fosse modulare, G, essendo un p-gruppo, dovrebbe essere pure quasi abeliano il che non può essere perchè i due gruppi $\{a\}$, $\{c\}$ non sono permutabili essendo il sistema $\{a\}\{c\}$ d'ordine p^3, mentre l'ordine del gruppo G è p^4. Ci proponiamo di far vedere che questo gruppo G contiene uno ed un solo sottogruppo modulare non banale costituito dal sottogruppo $\{a^p\}$. L'unicità segue dalle seguenti considerazioni. Poichè G è un p-gruppo con p dispari generato da due elementi, a reticolo non modulare, per quanto si è visto nel numero precedente, un eventuale sottogruppo modulare non banale deve essere contenuto nel gruppo $V(G)$.

D'altra parte $V(G)$ è nel nostro caso d'indice p^3 in G al più perchè non può coincidere con $\Phi(G)$ in quanto ciò comporterebbe la quasi abelianità di G. Quindi $V(G) = \{a^p\}$, e l'unico sottogruppo non identico contenuto in $V(G)$ risulta $V(G)$ stesso.

Per dimostrare che $\{a^p\}$ è un sottogruppo modulare, dobbiamo premettere diverse considerazioni sul gruppo G. Notiamo anzitutto che tutti i sottogruppi massimi di G sono quasi abeliani e precisamente di due tipi

α) abeliano elementare

β) generato da due elementi r, s soddisfacenti alle relazioni

$$r^{p^2} = s^p = 1, \quad s^{-1}rs = r^{p+1}$$

quindi quasi abeliano, ma non abeliano.

Un'altra proprietà del gruppo G che conviene mettere in evidenza è data dalla seguente proposizione: Se H è un sottogruppo ciclico d'ordine p^2 di G, e K un sottogruppo non ciclico d'ordine p^2, per cui $H \cup K = G$, il gruppo K contiene al più un sottogruppo d'ordine p permutabile con H.

Infatti supponiamo che ciò non sia vero. Consideriamo il gruppo $\dfrac{G}{\{a^p\}}$ tale gruppo non è abeliano perchè il derivato di G è d'ordine p^2 dato da $\{a^p\}\{b\}$. Se due sottgruppi S_1, S_2 d'ordine p di K sono permutabili con H, il gruppo $\dfrac{H \cup K}{\{a^p\}}$ è abeliano perchè si ha

$$\frac{H \cup K}{\{a^p\}} = \frac{H \cup (S_1 \cup S_2)}{\{a^p\}} = \frac{H \cup S_1}{\{a^p\}} \cup \frac{H \cup S_2}{\{a^p\}}.$$

Ma $\dfrac{H \cup S_i}{\{a^p\}}$ $(i = 1, 2)$ è abeliano e così pure $S_1 \cup S_2$.

Premesso ciò, sia $\mathfrak{R}$ un sottoreticolo modulare di $\mathfrak{L}(G)$. Se $\mathfrak{R}$ è contenuto in un reticolo $\mathfrak{L}(M)$ con M sottogruppo massimo di G, $\{\{a^p\}, \mathfrak{R}\}$ è pure modulare tenuto conto che $\mathfrak{L}(M)$ lo è e che $a^p\}$ è un sottogruppo di M. Modulare è pure il reticolo $\{a^p\}, \mathfrak{R}, G\}$ essendo G un sottogruppo modulare. Il caso che ci resta da esaminare è pertanto quello in cui $\mathfrak{R}$ non contenga $\{a^p\}$, ma contenga almeno due sottogruppi propri H, K di G, per cui

$$H \cup K = G \tag{11}$$

Da qui segue tenendo conto della struttura del gruppo G, che uno dei due gruppi H, K, ad es. H deve essere di uno dei due tipi

α) ciclico d'ordine p^2

β) non abeliano d'ordine p^3.

Esaminiamo anzitutto il caso in cui H sia ciclico d'ordine p^2.

Poichè nessun sottogruppo $\{b\}$ di G ciclico d'ordine p^2 può avere intersezione identica col gruppo $V(G) = \{a^p\}$,

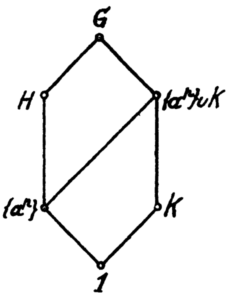

Figura 4

e poichè dovrà essere per ogni elemento L di $\mathfrak{R}$, $L \cap H = 1$, altrimenti in $\mathfrak{R}$ ci starebbe $\{a^p\}$, L può avere ordine al massimo p^2 e deve essere abeliano elementare. Se $\mathfrak{R}$ contiene solo G, 1, H, K, il reticolo $\{\{a^p\}, \mathfrak{R}\}$ è modulare come si vede osservando il suo diagramma in fig. 4. Supponiamo che oltre H, K, il reticolo $\mathfrak{R}$ contenga ancora un sottogruppo L e sia $L \cap H = 1$. Il gruppo L sarà pertanto abeliano elementare ed $L \cup K$ deve essere d'ordine p^2, perchè altrimenti $\mathfrak{R}$ conterrebbe $\{a^p\}$ Ma L e K non possono essere tutti e due solo d'ordine p, altrimenti il reticolo $\{H, K, L\}$ non è modulare, dovendo essere $H \cap (K \cup L) = 1$ Sarà quindi $L \subset K$ dato che il viceversa comporterebbe la non modularità di $\mathfrak{R}$. Pertanto possiamo dire che nelle nostre ipotesi se $\mathfrak{R}$ oltre H, K, 1, G contiene un altro elemento L, esso è contenuto in K. Ora il reticolo $\{\{a^p\}, L, H, K\}$ è modulare in quanto il suo diagramma è quello di fig. 5.

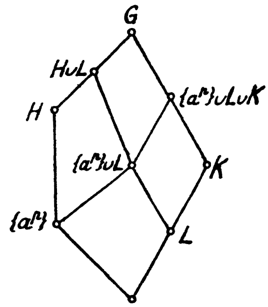

Figura 5

Se oltre L, in $\mathfrak{R}$ ci sta un altro sottogruppo L_1, sarà $L_1 \subset K$, $K = L \cup L_1$.

Ma per la proposizione precedente, L_1 non può essere permutabile con H, quindi il reticolo $\{L, L_1, H, K\}$ non risulta modulare avendosi un diagramma quale quello di fig. 6.

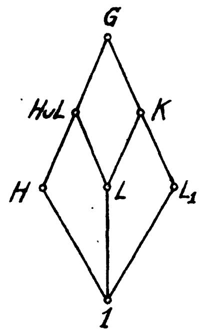

Figura 6

Passiamo al secondo caso in cui H sia d'ordine p^3 non abeliano. Allora nessun elemento non contenuto in H può essere ciclico d'ordine p^2, perchè altrimenti in $\mathfrak{R}$ ci starebbe $\{a^p\}$ Sia poi L un sottogruppo ciclico d'ordine p^2 contenuto in $\mathfrak{R}$ ed in H. Deve essere $L \cup K = G$; infatti dovendo essere

$L \cap K = 1$, se l'ordine di K non è inferiore a p^2 la cosa è evidente; se K ha ordine p, e fosse K permutabile con L, avendosi $H = L \cup S$, con S opportuno sottogruppo d'ordine p di H, il gruppo d'ordine $p^2 : S \times K$ conterebbe 2 sottogruppi permutabili con L, il che è impossibile per la proposizione dimostrata. Essendo dunque $L \cup K = G$, con L ciclico d'ordine p^2, si cade nel caso precedente. Possiamo supporre così che in $\mathfrak{R}$ non stanno sottogruppi ciclici d'ordine p^2. Se allora aggiungiamo ad $\mathfrak{R}$ l'elemento $\{a^p\}$, il reticolo $\{\{a^p\}, \mathfrak{R}\}$ resta ancora privo di sottogruppi ciclici d'ordine p^2. Ma allora $\{\{a^p\}, \mathfrak{R}\}$ è modulare perchè ogni sottoreticolo non modulare di $\mathfrak{L}(G)$ contiene come elemento almeno un sottogruppo ciclico d'ordine p^2.

BIBLIOGRAFIA

[1] G. BIRKHOFF, *Lattice Theory*. Publ. by the American Math. Soc., 1948.

[2] P. HALL, *A contribution to the theory of groups of prime power order*. Pr. London, Math. Soc., vol. 36.

[3] B. HUPPERT, *Über das Produkt von paarweise vertauschbaren zyklischen Gruppen*. Math. Zeitschr., vol. 58.

[4] G. ZAPPA, *Reticoli e Geometrie finite*. Libreria Editrice Liguori, (1952).

[5] — — *Gruppi quasi-abeliani*. Acta Pont. Acad. Sc., vol. 6, n. 29.

[6] — — *Caratterizzazione dei gruppi di Dedekind finiti*. Comm. Pont. Acad. Sc., vol. 8, n. 15.

[7] H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*. Liepzig, Teubner, 1937.