RENDICONTI
*del*
SEMINARIO MATEMATICO
*della*
UNIVERSITÀ DI PADOVA

GIOVANNI ZACHER

# Sugli elementi modulari di un gruppo finito

*Rendiconti del Seminario Matematico della Università di Padova*, tome 26 (1956), p. 70-84

<http://www.numdam.org/item?id=RSMUP_1956__26__70_0>

# SUGLI ELEMENTI MODULARI DI UN GRUPPO FINITO

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

Nella presente Nota [1]) caratterizzo i sottogruppi di Hall di un gruppo finito $G$ che sono elementi modulari.

Un sottogruppo $H$ di un gruppo finito $G$ dicesi un sottogruppo di Hall se l'ordine di $H$ è primo col suo indice in $G$, e un sottogruppo $M$ di $G$ dicesi un elemento modulare di $G$, se, detto $\mathfrak{R}$ un qualunque sottoreticolo modulare di $\mathfrak{L}(G)$, il reticolo $\{M, \mathfrak{R}\}$ generato da $M$ ed $\mathfrak{R}$ è ancora modulare. Ciò ricordato, ecco la caratterizzazione cui pervengo:

*Se un sottogruppo di Hall, $M$, del gruppo (finito) $G$ è anche un elemento modulare, o:*

*α) $G$ è il prodotto diretto di $M$ per un altro sottogruppo $H$ di $G$;*

*oppure*

*β) detto $S$ un sottogruppo di Sylow di $M$ non direttamente permutabile con un sottogruppo di Sylow $S_1$ di $G$ d'ordine primo con $M$, il reticolo $\mathfrak{L}(S \cup S_1)$ è modulare, e $G$ è il prodotto diretto di $S \cup S_1$ per il suo complemento $T$ in $G$* [2]);

*viceversa, tanto la α) quanto la β) implicano che $M$ è elemento modulare per $G$, se per $G$ esso è un sottogruppo di Hall.*

---

(*) Pervenuta in Redazione il 10 luglio 1956.

Indirizzo dell'A.: Seminario matematico, Università, Padova.

1) Che si collega alla Memoria mia: Sugli elementi modulari in un $p$-gruppo, pubblicata in Rend. Sem. Matem. Univ. di Padova, vol. 24, (1955).

2) Il gruppo $M$ è evidentemente il prodotto diretto di $S$ ed $M \cap T$.

Determino altresì gli elementi modulari in un gruppo finito a sottogruppi di Sylow ciclici.

**1.** - Ricordiamo alcune convenzioni, ormai usuali, da conservare in tutto questo lavoro.

Lettere maiuscole stampatello, quali $G$, $H$, $K$, $L$, ... indicano gruppi, che sono sempre supposti d'ordine finito; $S_{p^\alpha}$ indica un sottogruppo di Sylow d'ordine $p^\alpha$; $\mathbf{1}$ è il sottogruppo identico, oppure l'elemento identico.

Le prime lettere minuscole $a$, $b$, $c$, ... dell'alfabeto indicano elementi di un gruppo; $m$, $n$, $l$, $t$, $r$ numeri interi non negativi; $p$, $q$ numeri primi distinti; $(m, n)$ ed $[m, n]$ il massimo comun divisore ed il minimo comune multiplo di $m$, $n$. Inoltre $N(H)$ è il normalizzante di $H$ in $G$; $C_G(H)$ il centralizzante di $H$ in $G$; $(G : H)$ è l'indice di $H$ in $G$. Ed ancora $\{a, b, c, \ldots\}$ è il sottogruppo generato da $a$, $b$, ...; $\mathfrak{L}(G)$ è il reticolo dei sottogruppi di $G$; $\{H, K, L, \ldots\}$ è il reticolo generato dai sottogruppi $H$, $K$, $L$, ...; $[H, K]$ è il sottogruppo generato dagli elementi $hkh^{-1}k^{-1}$ con $h \in H$, $k \in K$. Un gruppo, si dirà come di consueto riducibile se è il prodotto diretto di due suoi sottogruppi propri non identici; in caso contrario, irriducibile. Due gruppi $H_1$, $H_2$ si dicono direttamente permutabili se ogni elemento di $H_1$ è permutabile con ogni elemento di $H_2$. L'unione di due gruppi permutabili si indicherà pure con $H_1H_2$. La notazione $H \subset G$ significa che $H$ è contenuto propriamente in $G$.

**2.** - Premettiamo qualche considerazione sui gruppi (finiti) a sottogruppi di Sylow ciclici.

È noto [7] che un gruppo $G$ a sottogruppi di Sylow ciclici è generabile mediante due elementi $a$ e $b$ legati dalle relazioni:

$$a^m = b^n = \mathbf{1}; \quad bab^{-1} = a^r \tag{1}$$

con $m \geq 1$, $n \geq 1$, $(G : 1) = mn$, $((r-1)n, m) = 1$, $r^n \equiv 1$ mod. $m$; nel qual caso $\{a\}$ è il derivato di $G$. Il gruppo $G$ è supersolubile. Se $G$ è riducibile, con $G = K_1 \times K_2$, risulta $((K_1 : \mathbf{1}), (K_2 : \mathbf{1})) = 1$.

Mostriamo ora che:

1,2): Se $N$ è un sottogruppo normale di $G$, se i sottogruppi di Sylow di $G$ sono ciclici e nessuno di essi appartiene ad $N$, $\frac{G}{N}$ è riducibile se e soltanto se tale è $G$.

Infatti se i sottogruppi $S_{p^\alpha}$ ed $S_{q^\beta}(p > q)$ sono di Sylow per $G$, permutabili, e danno luogo nell'omomorfismo canonico di $G$ su $\frac{G}{N}$ a due sottogruppi di Sylow $S'_{p^{\alpha'}}$ e $S'_{q^{\beta'}}$ di $\frac{G}{N}$ direttamente permutabili, risulta $[S_{p^\alpha}, S_{q^\beta}] \subset N$. Il che è possibile se e solo se $S_{p^\alpha} \cup S_{q^\beta} = S_{p^\alpha} \times S_{q^\beta}$ in quanto o è $[S_{p^\alpha}, S_{q^\beta}] = S_{p^\alpha}$ oppure $[S_{p^\alpha}, S_{q^\beta}] = \mathbf{1}$.

Consideriamo in $G$ i tre sottogruppi $H_1 = \{b\}$, $H_2 = \{a^r b\}$, $H_3 = \{a^{r-1} b\}$. Essi hanno come ordine $n$ e se $G$ non è ciclico, sono sottogruppi propri di $G$ distinti a due a due. Infatti $a^{r-1}b = a^{-1}ba$; $(a^r b)^n = a^{r^n + \ldots + r} b^n = a^{r^n + \ldots + r + 1 - 1}$. Ora $r^n - 1 = km$, $r^{n-1} + \ldots + r + 1 = (r^n - 1) : (r - 1) = km : (r - 1)$; ma $((r-1), m) = 1$, quindi $k = k_1(r-1)$, sicchè $r^{n-1} + \ldots + r + 1 = k_1(r-1)m$; per cui $r^n - 1 + r^{n-1} + \ldots + r + 1 = \bar{k}m$; epperò $(a^r b)^n = a^{\bar{k}m} = \mathbf{1}$. Inoltre $H_1 \cup H_2 = H_1 \cup H_3 = H_2 \cup H_3 = G$, perchè $|a^{r-1}| = |a^r| = |a|$, essendo $(r-1, m) = (r, m) = 1$. Ne segue pure $H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3$ normale in $G$. In definitiva:

2,2): Se $G$ è un gruppo non ciclico, a sottogruppi di Silow ciclici, generato da due elementi $a$, $b$ legati dalle relazioni (1), $G$ contiene sempre almeno tre sottogruppi d'ordine $n$ che a due a due danno per unione $G$ e che si intersecano a due a due secondo uno stesso sottogruppo di $G$.

Inoltre:

3,2): Nelle stesse ipotesi della proposizione 2,2, il centro ha intersezione identica col derivato di $G$.

Infatti sia $c$ un elemento comune al centro ed al derivato, $\{a\}$, di $G$. Possiamo supporre che sia $c = a^t$ con $t$ un divisore conveniente di $m$. Nelle nostre ipotesi risulta $ba^t b^{-1} = a^t$. D'altra parte $ba^t b^{-1} = (bab^{-1})^t = a^r$ ; quindi $t(r-1) \equiv 0 \bmod m$; ciò implica $t \equiv m$, essendo $((r-1), m) = 1$; in conclusione $c = \mathbf{1}$.

**3.** - Ricordiamo alcune proposizioni che ci saranno utili nel seguito; la prima delle quali si trova dimostrata in [1] ed in [5], le altre in [3] ed in [4]:

1,3): Se l'ordine del gruppo irriducibile $G$ possiede due fattori primi diversi $p$ e $q$, con $p > q$, il reticolo $\mathfrak{L}(G)$ è modulare se e solo se $G$ è generato da un $p$-gruppo abeliano elementare $S$ e da un elemento $b$ d'ordine $q^\beta$, tali che per ogni elemento $x$ di $S$ si abbia $b^{-1}xb = x^n$ con $n^q \equiv 1$ mod. $p$, $n$ non dipendendo da $x$;

2,3): Gli elementi modulari di un gruppo $G$ formano un sottoreticolo di $\mathfrak{L}(G)$ che comprende $G$ ed **1** (elementi modulari banali). Ogni automorfismo reticolare di $\mathfrak{L}(G)$ muta elementi modulari in elementi modulari;

3,3): Se $M$ è un elemento modulare del gruppo $G$, se $N$ è un sottogruppo di $G$, $M \cap N$ è un elemento modulare di $N$. Se $N$ è normale in $G$, $M \cup N$ è un elemento modulare di $G/N$;

4,3): Se $G = H_1 \times H_2$, con $H_i$ sottogruppo di Hall, se $M$ è un elemento modulare di $H_1$ o $H_2$, $M$ è un elemento modulare di $G$;

5,3): Se $M$ è un elemento modulare del gruppo $G$, i sottogruppi ciclici di $M$ sono permutabili con tutti quei sottogruppi ciclici di $G$ che hanno l'ordine primo con quello di $M$;

6,3): In ogni reticolo $\mathfrak{L}$, gli elementi neutri sono modulari.

**4.** - In questo n. esponiamo alcune proprietà degli elementi modulari in un gruppo $G$, irriducibile, a sottogruppi di Sylow ciclici. I simboli sono quelli del n. 2. Incominciamo col dimostrare la propos.:

1,4): Se il derivato $\{a\}$ di $G$ è d'ordine $p$, $\{a\}$ è un elemento modulare se e solo se il reticolo $\mathfrak{L}(G)$ è modulare.

Siano $L_1$, $L_2$ ed $L_3$ tre sottogruppi d'ordine $n$ di $G$, distinti a due a due e siffatti da aversi [3])

$$(2) \quad L_1 \cup L_2 = L_1 \cup L_3 = L_2 \cup L_3 = G. \quad L_1 \cap L_2 = L_1 \cap L_3 = L_2 \cap L_3.$$

---

[3]) Nelle ipotesi attuali le (2) seguono dalle altre condizioni imposte ad $L_1$, $L_2$ e $L_3$; e per la leggittimità di queste ultime non c'è nemmeno bisogno della 2,2) sempre nel caso attuale.

Se $\{a\}$ è modulare, l'intersezione $L_1 \cap L_2$ è massima in $L_1$. Nel fatto sia $K_1$, per assurdo, un sottogruppo proprio di $L_1$ contenente propriamente $L_1 \cap L_2$:

$$L_1 \cap L_2 \subset K_1 \subset L_1,$$

e, se $L_2 = a^v L_1 a^{-v}$, con $v$ intero conveniente, si ponga $K_2 = a^v K_1 a^{-v}$.

Allora il reticolo $\{L_1, L_2, L_3\}$ è modulare, mentre $\{\{a\}, L_1, L_2, L_3\}$ non lo è, perchè $(\{a\}K_1) \cap L_2 = K_2$, e quindi $L_1 \cup L_2 = K_2 \cup L_1 = G$, $L_1 \cap L_2 = K_2 \cap L_1$.

Ciò premesso, attesa la irriducibilità di $G$, $L_1$ copre $L_1 \cap L_2$ se e soltanto se l'ordine $n$ di $L_1$ è $q^\beta$. D'altra parte $\mathfrak{L}(G)$ è un reticolo modulare, se $(G:\mathbf{1}) = pq^\beta$ e se $L_1$ copre $L_1 \cap L_2$, a norma della 1,3. Donde la conclusione.

Passiamo ora alla:

2,4): Se nel gruppo $G$ il derivato $\{a\}$ ha ordine $p^\alpha$ con $\alpha > 1$, il sottogruppo $\{a^{p^{\alpha-1}}\}$ non può essere un elemento modulare.

Basterà supporre $\alpha = 2$, perchè ci si può sempre ricondurre a questo caso considerando il fattoriale di $G$ rispetto a $\{a^{p^{\alpha-2}}\}$. Siano allora $H_1$, $H_2$ due sottogruppi quali quelli della 2,2). Sia $(\{a^p\}H_1) \cap H_2 = Q \supset H_1 \cap H_2$. Allora $H_1$ ammette in $\{a^p\}H_1$ un tal coniugato $H'_1$ da aversi $H'_1 \cap H_2 = Q$. Ora $H'_1 \cup H_2 \supset \{a^p\}$, in quanto $H'_1 \neq H_2$. Quindi $H_1 \cup H_2 \supset H_1$, ossia $H'_1 \cup H_2 = G$. Pertanto $Q$ è normale in $G$ e risulta $H_1 \cap H_2 \supseteq Q$, cioè $H_1 \cap H_2 \supset H_1 \cap H_2$. L'assurdo prova che $(\{a^p\}H_1) \cap H_2 = H_1 \cap H_2$; ma allora il reticolo $\{\{a\}, H_1, H_2\}$ non è modulare.

Utilizzando le due ultime proposizioni, dimostreremo ora che:

3,4): Se il derivato di $G$ è d'ordine $p^\alpha$, e se uno dei suoi sottogruppi non identici è modulare. $\mathfrak{L}(G)$ è modulare.

Sia $M$ un sottogruppo proprio del derivato di $G$; per 3,2) esiste un sottogruppo di Sylow $S_{q^\beta}$ di $\{b\}$ non direttamente permutabile con $M$, e quindi nemmeno col $p$-gruppo $L$ che copre $M$. Allora $M$ non può essere un elemento modulare in $LS_{q^\beta}$. Se poi fosse $M = S_{p^\alpha}$ con $\alpha > 1$, detto $N$ il sottogruppo nor-

male di $G$ d'indice $p$ in $S_{p^\alpha}$, il reticolo $Z\left(\frac{G}{N}\right)$ è modulare ( 1,4)). Ora mentre il reticolo $\{NH_1, H_2, H_3\}$ è modulare, perchè $NH_i$ contiene un sottogruppo normale d'indice $pq$ in $G$, il reticolo $\{S_{p^\alpha}, NH_1, H_2, H_3\}$ non è modulare, contenendo esso il sottoreticolo non modulare $\{NH_2, H_2, H_3\}$. Questo assurdo prova che $\alpha$ non può essere maggiore di 1. E il teorema è dimostrato. Passiamo ad esaminare il caso che in $G$ il gruppo $\{b\}$ contenga un elemento modulare. Per quanto ci servirà nel seguito, potremo supporre per semplicità che l'ordine di $G$ sia divisibile solo per due fattori primi distinti: $(G:\mathbf{1}) = p^\alpha q^\beta$. Vediamo se $\{b\}$ può essere un elemento modulare. Possiamo supporre che $\{b\} \cap \{a^r b\} = \{b\} \cap \{a^{r-1} b\} = \{a^r b\} \cap \{a^{r-1} b\} = \mathbf{1}$. Allora se $\alpha > 1$, anche l'intersezione di $\{a^{p^{\alpha-1}}\}\{b\}$ con uno almeno dei tre gruppi $\{b\}$, $\{a^r b\}$, $\{a^{r-1} b\}$ è identica. Si supponga, ad es. $(\{a^{p^{\alpha-1}}\}\{b\}) \cap \{a^r b\} = \mathbf{1}$. Allora $\{\{b\}, \{a^r b\}, \{a^{p^{\alpha-1}}\}\}$ non è modulare. Pertanto risulta $\alpha = 1$ e l'intersezione $S_{q^\beta} \cap S'_{q^\beta}$ ha come indice $pq$ in $G$; indi $\mathfrak{L}(G)$ è modulare ( 1,3)). Sia ora $\{b^t\}$ un elemento modulare non identico contenuto propriamente in $\{b\}$. Il gruppo $\{b^t\}$ è modulare nel gruppo $H = \{a\}\{b^t\}$. Se $H$ è riducibile, $\{b^t\}$ sta nel centro di $G$. Se invece $H$ è irriducibile, $\mathfrak{L}(H)$ è modulare, per quanto precede, sicchè l'ordine di $G$ è $pq^\beta$. Ma allora $\{b^t\}$ deve essere normale in $G$, perchè altrimenti il reticolo $\{\{b^t\}, \{b\}, \{a^r b\}\}$ non è modulare. Pertanto:

1,4): Se $G$ è irriducibile d'ordine $p^\alpha q^\beta$, se $M$ è un elemento modulare contenuto in $\{b\}$, allora o $\mathfrak{L}(G)$ è modulare, oppure $M$ sta nel centro di $G$.

Dimostriamo finalmente:

5,4): Se $G$ è irriducibile e se il suo ordine è uguale al prodotto di tre fattori primi a due a due diversi, gli elementi modulari di $G$ sono soltanto quelli banali.

Se il derivato $\{a\}$ di $G$ ha ordine primo, $\{a\}$ non è un elemento modulare ( 1,4)). Sia ora $L$ un sottogruppo proprio non identico di $H_1 = \{b\}$: allora $H_1 \cap H_2 = \mathbf{1}$, perchè $G$ è irriducibile; indi $L \cup H_2 = G$; pertanto $\{H_1, H_2, L\}$ non è modulare; e modulari non sono perciò nè $H_1$ nè i suoi sottogruppi propri non identici. L'elemento modulare $M$ non può neppure contenere $\{a\}$, perchè $H_1$ ed $H_2$ si possono scegliere

in modo tale che $\mathbf{1} \neq M \cap H_1 = S$, $M \cap H_2 = \mathbf{1}$ di guisa che il reticolo $\{M, S, H_2\}$ non è modulare. Se invece il derivato $\{a\}$ di $G$ ha ordine divisibile per due fattori primi $p_1$ e $p_2$, mentre i reticoli $\{S_{p_i} H_1, H_2, H_3\}$ con $i = 1$ o 2, e $\{H_1, H_2, H_3\}$ sono modulari, tale non è il reticolo $\{\{a\}, S_{p_i} H_1, H_2, H_3\}$ perchè contiene il sottoreticolo non modulare $\{S_{p_i} H_2, H_2, H_3\}$. Pertanto nè $\{a\}$, nè $H_2$ (e quindi nessun suo coniugato), nè $S_{p_i}$ possono essere elementi modulari. L'elemento modulare $M$ dovrà quindi necessariamente contenere propriamente ad es. $H_1$; ma in tal caso $\{H_1, H_2, M\}$ non è reticolo modulare. L'assurdo prova il teorema.

Concludiamo osservando che:

6,4): Se $G$ è irriducibile e se i suoi sottogruppi di Sylow sono ciclici ed il suo ordine è del tipo $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ con $p_1, p_2, p_3$ fattori primi distinti a due a due, ed $\alpha_1 > 0$, $\alpha_2 > 0$, $\alpha_3 > 0$, i sottogruppi di Hall di $G$ diversi da $G$ ed $\mathbf{1}$ non sono modulari.

Nel caso contrario, infatti, $G$ oppure un suo conveniente fattoriale contiene (in virtù della 1,2) insieme colle 3,4) e 4,4)) un sottogruppo irriducibile d'ordine $p_1 p_2 p_3$ con un sottogruppo di Hall modulare; il che contraddice la 5,4).

**5.** - Passiamo ora alla caratterizzazione dei sottogruppi di Hall modulari in un gruppo $G$, qualunque (purchè d'ordine finito).

In questo numero consideriamo il caso che l'ordine di $G$ sia del tipo $p^\alpha p^\beta$, con $p > q$, $\alpha > 0$, $\beta > 0$, e che un sottogruppo di Sylow di $G$ sia modulare.

Nelle ipotesi poste, se l'ordine dell'elemento $a$ è una potenza di $p$ e quello dell'elemento $b$ è una potenza di $q$, i gruppi $\{a\}$, $\{b\}$ sono permutabili ( 5,3)) ed il reticolo $\mathfrak{L}(\{a\}\{b\})$ è modulare ( 6,3), 3,4), 4,4)); quindi o risulta $\{a\} \cup \{b\} = \{a\} \times \{b\}$, oppure l'ordine di $\{a\}$ è $p$ e $\{b^q\}$ è un sottogruppo normale in $\{a\}\{b\}$ ( 4,3), 7,3)). In ogni caso ogni $p$-gruppo di $G$ è normale in $G$ (e $G$ contiene pertanto un solo sottogruppo di Sylow, $S_{p^\alpha}$, relativo al numero primo $p$), e se $(\{a\} : \mathbf{1}) > p$, $a$ è permutabile con ogni elemento di $G$ il cui ordine sia una potenza di $q$. Fissiamo un elemento $b$ non identico di un fissato sottogruppo di Sylow $S_{q^\beta}$ di $G$, e suddividiamo gli elementi di $S_{p^\alpha}$ in due classi $K_1$ e $K_2$, mettendo in $K_1$ tutti quelli non permutabili con $b$

più l'elemento identico, e in $K_2$ tutti quelli permutabili con $b$. Allora $K_1$ e $K_2$ hanno soltanto l'elemento identico in comune. $K_2$ è il centralizzante di $b$ in $S_{p^\alpha}$. Siano ora $k_1$ e $k_1'$ due elementi non identici di $K_1$: i loro ordini sono uguali a $p$.

Consideriamo il prodotto $k_1k_1'$. Se $k_1' \in \{k_1\}$, $k_1k_1'$ è un elemento di $K_1$. Se invece $\{k_1\} \cap \{k_1'\} = \mathbf{1}$, risulta $k_1k_1' \neq \mathbf{1}$. Supponiamo $k_1k_1'$ permutabile con $b$. Allora $k_1k_1' = bk_1k_1'b^{-1} = k_1^{v_1}k_2^{v_2}$ ($v_1$, $v_2$ interi convenienti), da cui $k_1^{v_1-1} = k_1'^{v_2-1} = \mathbf{1}$ quindi $k_1^{v_1} = k_1$, $k_1'^{v_2} = k_1'$, ossia $k_1$ e $k_1'$ sarebbero permutabili con $b$, contro ipotesi: Pertanto anche $K_1$ è un sottogruppo di $S_{p^\alpha}$. In conclusione o è $K_1 = \mathbf{1}$, o è $K_2 = \mathbf{1}$ non potendo un gruppo essere somma di due suoi sottogruppi propri.

Pertanto abbiamo che:

1,5): Se $G = S_{p^\alpha}S_{q^\beta}$ ha un sottogruppo di Sylow modulare, se l'ordine dell'elemento non identico $b$ è uguale a una potenza del minore dei due numeri primi $p$ e $q$, e sia questo $q$, allora o $b$ è permutabile con tutti gli elementi di $S_{p^\alpha}$, o con nessuno, nel qual caso $S_{p^\alpha}$ è d'esponente $p$.

Diamo ora la dimostrazione del seguente teorema

2,5): Se $G = S_{p^\alpha}S_{q^\beta}$, con $p > q$, se qualche sottogruppo di Sylow di $G$ è modulare e se $G$ non si spezza nel prodotto diretto di $S_{p^\alpha}$ e di $S_{q^\beta}$, il sottogruppo $S_{p^\alpha}$ è abeliano elementare e per ogni elemento $a$ risulta

$$b^{-1}ab = a^\sigma$$

se $b$ ha come ordine una potenza di $q$, e $\sigma$ è un conveniente numero naturale che non dipende da $a$.

Se $\alpha = 1$, il teorema segue dal fatto che $S_{p^\alpha}$ è normale, d'ordine $p$.

Escluso questo caso, ricordiamo che tutti gli elementi non identici di $S_{p^\alpha}$ hanno ancora ordine $p$; consideriamo due tali elementi non identici, $a$ e $c$, di $S_{p^\alpha}$, che $\{a\} \cap \{c\} = \mathbf{1}$, ed indichiamo con $b$ un elemento, certo esistente, che abbia come ordine una potenza di $q$ e che non appartenga al centralizzante $C_G(S_{p^\alpha})$. Allora $bab^{-1} = a^\mu$ e $bcb^{-1} = c^\nu$ con $\mu$ e $\nu$ non congrui ad 1 modulo $p$. Dimostriamo che $\mu \equiv \nu$ mod. $p$, vale a dire appunto che $\mu$ si può supporre uguale ad un numero $\sigma$ ($\not\equiv 1$ mod. $p$), indipendente da $a$ (e da $c$).

Sia pel momento $ac = ca$. Allora $b(ac)b^{-1} = (ac)^\rho = a^\rho c^\rho = a^\rho c^\nu$.

Ma $\{a\} \cap \{c\} = \mathbf{1}$. quindi $\mu \equiv \rho \equiv r \bmod p$. Se $a$ non è permutabile con $c$, sia $z$ un elemento non identico del centro di $S_{p^\alpha}$.

Risulta $\{a\} \cap \{z\} = \mathbf{1} = \{a\} \cap \{z\}$: posto $bab^{-1} = a^\mu$, $bzb^{-1} = z^\rho$, $bcb^{-1} = c^\nu$, per quanto precede risulta di nuovo $\mu \equiv \rho \equiv \nu \bmod p$.

L'automorfismo interno di $G$ generato da $b$ subordina un automorfismo di $S_{p^\alpha}$. Pertanto risulta $a^\sigma c^\sigma = (ac)^\sigma$, potendosi anzi supporre $1 < \sigma < p$. Di qui e da risultati noti [4]), si trae che il sistema $S_{p^\alpha}^{(\sigma)}$ è permutabile elemento per elemento col sistema $S_{p^\alpha}^{(\sigma-1)}$. Ma $S_{p^\alpha}^{(\sigma)} = S_{p^\alpha}^{(\sigma-1)} = S_{p^\alpha}$, poichè $(\sigma.\ p) = (\sigma - 1,\ p) = \mathbf{1}$. In conclusione $S_{p^\alpha}$ è un gruppo abeliano (elementare). Donde il teorema. Mantenute le ipotesi del teorema precedente, sia di nuovo $a$ un elemento non identico di $S_{p^\alpha}$ e $T = C_{S_{q^\beta}}(\{a\})$. Allora $S_{q^\beta}/T$ è isomorfo ad un sottogruppo del gruppo di automorfismi di $\{a\}$, e quindi è ciclico. Sia $bT$ un elemento generatore di $S_{q^\beta}/T$. Poichè il reticolo $\mathfrak{L}(\{a\}\{b\})$ è modulare (in virtù delle 3.3), 3,4), 4,4)), $\{b^q\}$ appartiene a $T$, sicchè $T$ è d'indice $q$ in $S_{q^\beta}$. Inoltre abbiamo visto che è $C_{S_{q^\beta}}(\{a\}) = C_{S_{q^\beta}}(S_{p^\alpha})$. Dimostriamo che $S_{q^\beta}$ è ciclico.

Nel gruppo $\{a\}S_{q^\beta}$ almeno uno dei due gruppi $\{a\}$ ed $S_{q^\beta}$ è modulare (3,3)). Contenga $S_{q^\beta}$ oltre $T$ un altro sottogruppo $T'$ d'indice $q$. Il gruppo di Frattini $\Phi(S_{q^\beta})$ di $S_{q^\beta}$ è allora contenuto in $T$, e quindi è normale in $G$. Sia poi $N$ un sottogruppo normale di $G$ contenuto in $S_{q^\beta}$, d'indice $q$ in $T$, con $N \supseteq \Phi(S_{q^\beta})$. Il gruppo $\overline{G} = \dfrac{\{a\}S_{q^\beta}}{N}$ ha come ordine $pq^2$; inoltre i suoi sottogruppi di Sylow relativi al numero $q$ sono abeliani elementari e contengono sia elementi (non identici) permutabili che elementi non permutabili con $\bar{a}$, se $\bar{a}$ è un elemento d'ordine $p$ di $\overline{G}$, cioè un elemento generatore del sottogruppo di Sylow $\overline{S}_p$ di $\overline{G}$ relativo al numero $p$, $\bar{b}$ e $\bar{c}$ si possono scegliere entro uno stesso sottogruppo di Silow, $\overline{S}_{q^2}$ di $\overline{G}$

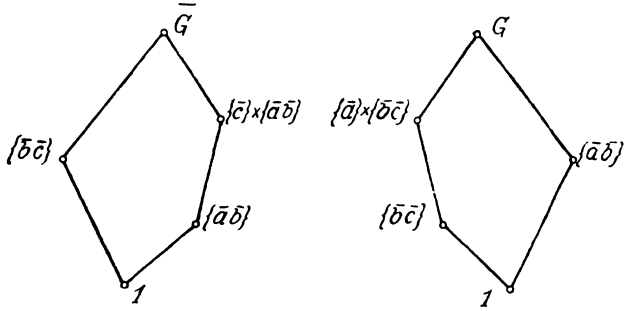
[4]) Vedi [7] pag. 29.

relativo al numero $q$, in guisa da aversi

$$\bar{a}^p = \mathbf{1},\ \bar{b}^q = \bar{c}^q = \mathbf{1},\ \bar{b}\,\bar{c} = \bar{c}\,\bar{b},\ \bar{a}\,\bar{c} = \bar{c}\,\bar{a},\ \bar{b}\,\bar{a}\,\bar{b}^{-1} = \bar{a}^v$$

con $v \equiv 1 \bmod p$.

Nelle nostre ipotesi almeno uno dei due sottogruppi $\bar{S}_p$ ed $\bar{S}_{q^2}$ è modulare e $\bar{G}$ contiene i due elementi $\bar{a}\bar{b}$ e $\bar{b}\bar{c}$ che hanno come ordine $q$ e che generano $\bar{G}$. Ma allora $\mathfrak{L}(G)$ contiene i due sottoreticoli




che dimostrano che nè $\{a\}$ nè $\{\bar{c}\}\times\{\bar{a}\bar{b}\}$ possono essere elementi modulari. Riassumendo, tenuto conto delle 1,3), 3,4), 4,4) abbiamo dimostrato il teorema

3,5): Se $G$ è un gruppo irriducibile d'ordine $p^z q^{z'}$, un suo sottogruppo di Sylow è un elemento modulare di $G$ se e solo se $\mathfrak{L}(G)$ è modulare.

**6.** - Oramai siamo in grado di dimostrare il teorema enunciato nelle righe introduttive, precisamente di provare che:

1,6): *Se un sottogruppo di Hall, $M$, del gruppo (finito) $G$ è anche un elemento modulare, o*

*α) $G$ è il prodotto diretto di $M$ per un altro sottogruppo $H$ di $G$;*

*oppure:*

*β) detto $S$ un sottogruppo di Sylow di $M$ non direttamente permutabile con un sottogruppo di Sylow $S_1$ di $G$ d'ordine primo con $M$, il reticolo $\mathfrak{L}(S \cup S_1)$ è modulare, e $G$ è il prodotto di $S \cup S_1$ per il suo complemento $T$ in $G$;*

*viceversa, tanto la* α) *quanto la* β) *implicano che* $M$ *è elemento modulare per* $G$, *se per* $G$ *esso è un sottogruppo di Hall.*

Se $G$ è un $p$-gruppo, il teorema è banale, nel senso che allora $M$ coincide con $G$, oppure col sottogruppo identico.

Se l'ordine di $G$ è del tipo $p^\alpha q^\beta$ $(\alpha > 0,\ \beta > 0)$ il teorema segue dalla 4,3) e dal teorema 3,5).

Rimane da esaminare il caso che l'ordine di $G$ ammette almeno tre divisori primi (a due a due diversi). Posto che allora sia $(G:1) = p_1 \dots p_t$, con $p_1, p_2, \dots, p_t$ numeri primi, il teorema è vero se $t = 3$ per la 5,4); pertanto possiamo procedere per induzione rispetto al numero $t$.

Se $G = M \times H$, il teorema segue dalla 4,3).

Supponiamo ora che sia $G = MS_1$, con $S_1$ sottogruppo di Sylow di $G$. Allora se $N(S_1) \subset G$, si può scegliere un sottogruppo di Silow $S$ di $M$ in guisa che $S$ non sia direttamente permutabile con $S_1$ e che $S$ non sia normale in $SS_1$. Inoltre ( 1,3)) $\{a\}S_1$ è dato dall'unione dei coniugati di $S_1$ in $\{a\}S_1$. Ne segue, poichè $S_1$ è permutabile con ogni sottogruppo di $M$ per la 5,3), che tale è pure $\{a\}S_1$. Pertanto se $b$ è un elemento di un sottogruppo di Sylow di $M$ d'ordine primo con quello di $SS_1$, risulta $\{b\} \cup \{a\} S_1 = \{b\}(\{a\} S_1)$. Quest'ultimo gruppo ha tutti i sottogruppi di Sylow ciclici e possiede un sottogruppo di Hall modulare e non banale; epperò $\{b\} \cup \{a\}S_1 = \{b\} \times \{a\}S_1$, a norma della 6,4). Ne segue $G = SS_1 \times L$.

Sia invece $N(S_1) = G$. Allora se $SS_1$ è normale in $G$, in particolare se $N_M(S) = M$, $SS_1$ è permutabile con ogni sottogruppo di $G$, ogni sottogruppo di $S_1$ è normale in $G$, per cui si conclude come sopra. Per esaurire il caso in esame riduciamo all'assurdo l'ipotesi che $SS_1$ non sia normale in $G$. Allora $N_M(S)$ è contenuto propriamente in $M$, e, per quanto precede, risulta $N_M(S)S_1 = L \times SS_1$; sicchè $S$, che è ciclico ( 1,3)), viene a trovarsi nel centro del proprio normalizzante. Pertanto il complemento $T$ di $S$ in $M$ è normale in $M$, epperò $G = TSS_1$. Se $TS_1 = T \times S_1$, $T$ è normale anche in $G$. Inoltre $S_1$ è abeliano elementare ed i suoi sottogruppi sono normali in $G$. L'ipotesi alla base del procedimento d'induzione, ci consente di limitarci ad esaminare il caso che $S_1$ sia ciclico: $S_1 = \{a\}$. Poichè $SS_1$ non è normale in $G$, esiste un elemento $t$ di $T$,

per il quale risulta $tSt^{-1} = S' \neq S$. Posto $S'' = atSt^{-1}a^{-1}$, proviamo che nessun elemento di $\{a\}$ è atto a trasformare $S$ in $S''$. Infatti da $a^v Sa^{-v} = atSt^{-1}a^{-1}$, seguirebbe $a^{1-v}t \in N(S)$; ma $N(S)$ ha ordine primo con $S_1$, epperò $a^{1-v} = \mathbf{1}$, atteso che altrimenti l'ordine di $a^{1-v}t$, essendo $a^{1-v}$ permutabile con $t$, non sarebbe primo con $(S_1 : \mathbf{1})$; da cui $S = tSt^{-1}$. Similmente si vede che $S''$ non è coniugato di $S$ secondo $T$; e quindi, per l'ipotesi induttiva, che $G$ è l'unione $S \cup S''$.

Ma allora il reticolo $\{S_1S,\ S'',\ M\}$ non è modulare, in quanto contiene il sottoreticolo $\{S_1S,\ S,\ S''\}$; e il caso che sia $TS_1 = T \times S_1$ è ridotto all'assurdo. Consideriamo ora il caso che $T$ ed $S_1$ non siano direttamente permutabili. Allora $TS_1 = L \times \bar{S}S_1$, sicchè $\bar{S}$ è ciclico ed $L$ è normale in $M$; di guisa che $M = L\bar{S}\bar{S}'$ con $\bar{S}'$ coniugato di $\bar{S}$. Ma per la 6,4) risulta $S'SS_1 = \bar{S}' \times SS_1$; per l'ipotesi induttiva riesce $LSS_1 = L \times SS_1$. E, in definitiva, $G = T \times SS_1$, che contraddice la $N_M(S) \subset M$. In questo modo il caso che l'indice del sottogruppo modulare $M$ in $G$ sia potenza di un numero primo è esaurito.

Passiamo ora al caso che il gruppo modulare $M$ non sia soltanto di Hall in $G$, ma abbia il proprio indice in $G$ divisibile per almeno due fattori primi distinti. E studiamo separatamente il sottocaso:

1) $N(M) \subset G$

ed il sottocaso

2) $N(M) = G$.

Nel primo sottocaso esiste in $G$ un sottogruppo di Sylow, $S_1$, d'ordine primo con quello di $M$, tale che $M$ non sia normale in $MS_1$. Ne segue che esiste un sottogruppo di Sylow, $S$, di $M$ tale che $S$ non sia normale in $SS_1$. Il sottogruppo $S$ è modulare in $SS_1$ (per la 3,3)), pertanto modulare è il reticolo $\mathfrak{L}(SS_1)$ (vedi 3,5)); indi i coniugati di $M$ in $MS_1$ danno per unione $MS_1$. Pertanto $MS_1$ è un elemento modulare di $G$ al pari di $M$. Allora $SS_1$ è permutabile con ogni sottogruppo di Sylow $S'$ di $G$ d'ordine primo con $MS_1$. Sicchè, a norma del caso precedente, è intanto $MS_1 = SS_1 \times L$; di guisa che, se contiene propriamente $(SS_1)S'$, si può applicare l'ipotesi induttiva, ottenendo $(SS_1)S' = SS_1 \times S'$; donde la conclusione.

Resta da esaminare, per concludere questo primo sottocaso, l'eventualità che sia $G = (SS_1)S'$. Se non fosse $(SS_1)S' = SS_1 \times S'$, a norma della 5,3) $G$ conterrebbe un sottogruppo irriducibile a sottogruppi di Sylow ciclici, con l'ordine divisibile per tre fattori primi (distinti) e con un sottogruppo di Hall modulare e non banale; tutte cose queste che contraddirebbero la 6,4). E l'esame del primo sottocaso è terminato.

Ci resta il secondo sottocaso. Allora $M$ è normale in $G$ e quindi possiede in $G$ un complemento $T$. E possiamo supporre che $T$ non sia un $p$-gruppo (perchè altrimenti si ricadrebbe nel caso precedente). Se $M$ è un $p$-gruppo, per concludere basta ragionare come quando si aveva $G = MS_1$, dando ad $M$ il ruolo di $S_1$ ed a $T$ quello di $M$. Se $M$ non è un $p$-gruppo, siano $S$ ed $S_1$ due sottogruppi di Sylow non direttamente permutabile rispettivamente contenuti in $M$ e $T$; allora per l'ipotesi induttiva risulta $ST = SS_1 \times L$, e quindi è anche $MS_1 = SS_1 \times H$. Donde la $\alpha$) e la $\beta$). Il risultato si lascia poi invertire anche nel caso della $\beta$) perchè $\mathfrak{L}(SS_1)$ è modulare, di guisa che si può applicare la 4,3).

**7.** - Caratterizziamo ora gli elementi modulari in un gruppo a sottogruppi di Sylow ciclici.

Incominciamo col provare che:

1,7): Se $G$ è un gruppo irriducibile d'ordine $p^\alpha q^\beta$, a sottogruppi di Sylow ciclici, se $M$ è un elemento modulare non banale di $G$, ed $\mathfrak{L}(G)$ non è modulare, $M$ è contenuto nel centro di $G$.

Posto $G = \{a\}\{b\}$, dove $a$ e $b$ naturalmente sono legati dalle (1), sia $M = HK$, con $H \subseteq \{a\}$ e $K \subseteq \{b\}$. In virtù della 3,3) e della 4,3) è lecito supporre inoltre $H$ e $K$ non identici, mentre la 5,2) ci autorizza a supporre $M$ normale in $G$. Di conseguenza è $K \subset \{b\}$, perchè il gruppo $G$ sarebbe riducibile. Ciò premesso, se $K$ è normale in $G$, il gruppo $\frac{HK}{K}$ è contenuto nel derivato di $\frac{G}{K}$ ed è per $\frac{G}{K}$ un elemento modulare non banale; sicchè $\mathfrak{L}\left(\frac{G}{K}\right)$ è modulare (3,4)) e quindi anche $\mathfrak{L}(G)$ è

tale ( 3,4)). Se $K$ non è normale in $G$, l'ordine di $\{a\}$ è necessariamente $p$ (e quindi $H$ coincide con $\{a\}$): nel caso contrario, infatti, se $N$ è d'indice $p$ in $\{a\}$, è $\mathbf{1} \subset H \subseteq N$ ed il gruppo $\frac{KN}{N}$ è modulare per $\frac{G}{N}$ e quindi per la 4,4) i gruppi $\frac{\{a\}}{N}$ e $\frac{KN}{N}$ sono direttamente permutabili e $K$ è normale in $G$, contro ipotesi. Se ora $\{b\}$, $\{b'\}$ sono due sottogruppi di $G$ distinti e d'ordine $q^\beta$, risulta $\{b\} \cup \{b'\} = G$ e $\{b\} \cap \{b'\}$ è almeno d'indice $q^2$ in $\{b\}$, perchè $\mathfrak{L}(G)$ non è modulare ( 1,3)); sicchè $\{b\} \cup \{b'^q\} = G$, $\{b\} \cap \{b'\} = \{b\} \cap \{b'^q\}$. Dunque il reticolo $\{M, \{b'^q\}, \{b\}\}$ non è modulare. Pertanto nemmeno $M$ è modulare.

Ora siamo in grado di dimostrare il seguente teorema

2,7): Se $G$ è irriducibile, a sottogruppi di Sylow ciclici, se $\mathfrak{L}(G)$ non è modulare e se $M$ è un elemento modulare non banale, $M$ sta nel centro di $G$.

Posto di nuovo $G = \{a\}\{b\}$, dove $a$ e $b$ hanno il solito significato, sia ancora $M = HK$, con $\mathbf{1} \subseteq H \subseteq \{a\}$, $\mathbf{1} \subseteq H \subseteq \{b\}$. Se $K$ possiede sottogruppi di Sylow che non siano tali per $G$, questi formano un sottogruppo $T$ di $K$ contenuto nel centro di $G$, a norma della 1,7); se tutti i sottogruppi di Sylow di $K$ son tali anche per $G$, $T$ sarà il sottogruppo identico di $G$. In ogni caso per $M$ sussiste una scomposizione del tipo $M = L \times T$. Proviamo ora che tutti i sottogruppi di Sylow di $H$ son tali anche per $G$: infatti, sia per assurda ipotesi, $P$ un sottogruppo di Sylow di $H$ ma non di $G$; sia $S$ il sottogruppo di Sylow di $\{a\}$ che contiene $P$ ed $\overline{S}$ un sottogruppo di Sylow di $G$ non direttamente permutabile con $S$; allora è $S\overline{S} \supset S\overline{S} \cap M \supset \mathbf{1}$; epperò, per la 3,4) e la 1,7), $SS = S \times \overline{S}$ contro l'ipotesi. In conclusione $L$ è un sottogruppo di Hall di $G$ ed $\frac{M}{T}$ un sottogruppo di Hall per $\frac{G}{T}$. Ma $\frac{G}{T}$ è irriducibile, al pari di $G$; e quindi, in virtù del teorema 1,6), il gruppo $\frac{M}{T}$ è identico, avendo escluso la modularità di $\mathfrak{L}(G)$; donde la conclusione, perchè $T$ appartiene appunto al centro di $G$.

Sia ora di nuovo $G$ un gruppo irriducibile a sottogruppi di Silow ciclici, ed il sottogruppo $M$ appartenga al centro di $G$.

Allora $M$ è ([2] e [6]) un elemento neutro nel reticolo $\mathfrak{L}(G)$. D'altra parte un elemento neutro è pure un elemento modulare, per la 6,3). Quindi $M$ è un elemento modulare di $G$. Concludiamo pertanto che:

*Se $G$ è un gruppo irriducibile a sottogruppi di Sylow ciclici e se $\mathfrak{L}(G)$ non è modulare, gli elementi modulari di $G$ sono $G$ e i sottogruppi del centro di $G$.*

Sia infine $G$ un gruppo a sottogruppi di Sylow ciclici. Scomposto $G$ nei suoi fattori irriducibili, che sono univocamente determinati, $G = H_1 \times H_2 \times \ldots \times H_1$, se $M$ è un sottogruppo di $G$, sarà $M = (M \cap H_1) \times \ldots \times (M \cap H_t)$.

In virtù della 3,3) e 4,3) $M$ è un elemento modulare di $G$ se e solo se il gruppo $M \cap H_i$ è tale in $H_i$ per $i = 1, 2, \ldots t$. Dunque, tenendo conto della conclusione precedente, *$M$ è un elemento modulare di $G$ se e solo se il gruppo $M \cap H_i$ appartiene ad uno dei seguenti tipi*: $\alpha$) $M \cap H_i = H_i$, $\beta$) $M \cap M_i$ *sta nel centro di* $H_i$, $\gamma$) $M \cap H_i$ *è un sottogruppo qualunque di* $H_i$, *però* $\mathfrak{L}(H_i)$ *è modulare.*

## BIBLIOGRAFIA


[1] IWASAWA, K.: *Über die endlichen Gruppen und die Verbände ihrer Untergruppen.* J. Fac. Sc. Imp. Univ. Tokyo, Sect. I, 4 ('41).

[2] SUZUKI, M.: *On the L-homomorphisms of finite groups.* Trans. A. Math. Soc., 70 ('51).

[3] ZACHER, G.: *Sugli elementi modulari in un p-gruppo.* Rend. Sem. Mat. di Padova, col. XXIV, 165-182.

[4] ZACHER, G.: *Un criterio di non semplicità di un gruppo finito.* Ibidem.

[5] ZAPPA, G.: *Caratterizzazione dei gruppi di Dedekind finiti.* Com. Pont. Acad. Sc., vol. VIII, n. 15.

[6] ZAPPA, G.: *Determinazione degli elementi neutri nel reticolo dei sottogruppi di un gruppo finito.* Rend. Accad. Sc. Fis. Mat., Napoli, vol. 18.

[7] ZASSENHAUS, H.: *The theory of groups.* Chelsea Publ. Comp. New Jork, ('49).