Rendiconti del Seminario Matematico della Università di Padova

Giovanni Zacher

Sui gruppi finiti somma dei loro sottogruppi di Sylow

Rendiconti del Seminario Matematico della Università di Padova, tome 27 (1957), p. 267-275

<http://www.numdam.org/item?id=RSMUP_1957__27__267_0>

SUI GRUPPI FINITI SOMMA DEI LORO SOTTOGRUPPI DI SYLOW

Nota (*) *di* Giovanni Zacher (*a Padova*)

Nella presente Nota riprendo lo studio degli α-gruppi, cioè dei gruppi finiti che risultano somma (nel senso della teoria degli insiemi) dei loro sottogruppi di Sylow [6] [1]. Come risultato centrale dimostrerò il seguente teorema:

Sia G un α-gruppo, p il minimo divisore primo dell'ordine di G e p^β la massima potenza di p che divide l'ordine di G. Allora G è certamente risolubile ed ha un ordine divisibile al massimo per due fattori primi distinti per lo meno quando contiene un sottogruppo normale proprio non identico che abbia un ordine diverso da $p^3, p^4, \ldots, p^{\beta-2}$.

Provo inoltre con un esempio l'esistenza di un α-gruppo non risolubile che contiene un sottogruppo normale proprio non identico, ed espongo qualche ulteriore proprietà di cui gode un α-gruppo.

1\. - Per quanto riguarda le notazioni usate, ricordo che lettere maiuscole stampatello, quali $G, H, N, T, \ldots$ indicano gruppi; S_p indica un sottogruppo di Sylow d'ordine potenza di p; 1 è il sottogruppo identico oppure l'elemento identico; (G) indica l'ordine di G, $\mathfrak{N}_M(H)$ il normalizzante di H in M. La notazione $H \subset G$ significa che H è sottogruppo proprio di G.

(*) Pervenuta in Redazione il 1° agosto, 1957.

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

[1] I numeri tra parentesi quadre si riferiscono alla bibliografia posta in fondo a questo mio lavoro.

Premettiamo i seguenti due lemmi.

LEMMA I: *Il gruppo G è risolubile se è un α-gruppo e se possiede p-gruppi normali, p essendo un fattore primo di (G) diverso da quello minimo.*

Se fra quei sottogruppi normali ve ne fosse uno di Sylow, il lemma sarebbe già dimostrato nella mia Nota [6], senza nessuna condizione ulteriore per il numero p. Rimane quindi da esaminare il caso che G contenga un p-gruppo normale N, che non sia di Sylow, p essendo ora diverso appunto dal minimo divisore primo di G.

Per la dimostrazione usiamo induzione sull'ordine di G.

I sottogruppi di Sylow S_q di G con $q \neq p$ contengono ciascuno un solo sottogruppo ciclico d'ordine q in virtù delle ipotesi fatte e dei risultati esposti in [6]; perciò G è q-normale nel senso di Grün [2]) per $q \neq p$. Fissiamo un sottogruppo di Sylow S_q, con q minimo divisore primo di (G) di guisa che $q < p$.

Indicato con Z il centro di S_q, consideriamo il gruppo $\mathfrak{N}_G(Z)$. Poichè Z è ciclico, risulta $\mathfrak{N}_G(Z) = S_q$, perchè, se fosse $\mathfrak{N}_G(Z) \supset S_q$, G conterrebbe un sottogruppo H d'ordine qp, che sarebbe ciclico in quanto i suoi sottogruppi di Sylow degli ordini p e q sarebbero normali. Visto che $\mathfrak{N}_G(Z) = S_q$, per un teorema di Grün [3]), G contiene un sottogruppo normale M d'indice q in G; e risulta evidentemente $M \supset N$. Ora se q divide (M), applicando l'ipotesi induttiva, M è risolubile e quindi anche G è tale.

Sia invece q primo con (M). Supponiamo che esista un divisore primo q' di (G) diverso da p e q; poichè $S_{q'} \subset M$ e poichè M è normale in G, si ha $\mathfrak{N}_G(S_q')M = G$, sicchè risulta anche $\mathfrak{N}_G(S_{q'}) = S_q S_{q'}$ [4]).

Ma allora G contiene il sottogruppo risolubile $S_q' S_q N$, il che implica [5]) che sia $q' = p$, contro l'ipotesi.

---

2) Vedasi [7] pag. 141.
3) Vedasi [7] pag. 141.
4) Vedasi [6] pag. 173.
5) Vedasi [6] pag. 172.

LEMMA II: *Il gruppo G è risolubile se è un α-gruppo e se possiede almeno un sottogruppo normale N che abbia come indice una potenza di un numero primo.*

Usiamo induzione sull'ordine di G. Poichè G/N è un p-gruppo, in virtù dell'ipotesi induttiva è lecito supporre sen'altro che N abbia indice primo, p, in G. Sia S_q un sottogruppo di Sylow di G, con $q \neq p$. Allora S_q è un sottogruppo di Sylow di N e risulta $G = N\mathfrak{N}_G(S_q)$. Il gruppo $\mathfrak{N}_G(S_q)$ è risolubile e quindi l'ordine di $\mathfrak{N}_G(S_q)$ è $p^\beta q^\gamma$ con $(G) : p^\beta q^\gamma$ numero primo con $p^\beta p^\gamma$ [6]).

Distinguiamo due casi:

I° caso: (N) è primo con p.

II° caso: (N) è divisibile per p.

Studiamo anzitutto il I° caso. Dimostriamo che N è un sottogruppo di Sylow di G. Ragioniamo per assurdo: allo scopo basterà ridurre all'assurdo l'ipotesi che (N) sia divisibile per almeno due fattori primi distinti. Poichè l'ordine di $\mathfrak{N}_G(S_q)$ è pq^β ed N ha ordine primo col suo indice p in G, per ogni $q \neq p$ risulta $\mathfrak{N}_N(S_q) = S_q$. Sia $\bar{q}$ il massimo divisore primo di (N) e supponiamo, se possibile, che l'intersezione D di due certi coniugati $S'_{\bar{q}}$ ed $S''_{\bar{q}}$ di $S_{\bar{q}}$ sia diversa da 1 e scegliamo anzi D in guisa che non sia contenuto propriamente in nessun'altra intersezione dello stesso tipo. Il gruppo $\mathfrak{N}_N(D)$ è un gruppo d'ordine composto [7]) ed è risolubile pel lemma I; perciò è del tipo $\mathfrak{N}_N(D) = S_r\bar{S}_{\bar{q}}$ con $D \subset \bar{S}_{\bar{q}}$. Ma allora $\bar{S}_{\bar{q}}$ è un sottogruppo normale di $\mathfrak{N}_N(D)$ [8]), il che è impossibile [7]). Abbiamo dunque $D = 1$ ed $\mathfrak{N}_N(S_{\bar{q}}) = S_q$. Per un teorema di Frobenius [9]) possiamo concludere che $N = MS_{\bar{q}}$ con M sottogruppo normale di N ed (M) primo coll'indice di M in N. Per l'ipotesi d'induzione, N e quindi G risultano pertanto risolubili. Ma allora [10]) N è un sottogruppo di Sylow di G.

---

[6]) Vedasi [6] pag. 172.
[7]) Vedasi [7] pag. 108.
[8]) Vedasi [6] pag. 173.
[9]) Vedasi [3] pag. 202.
[10]) Vedasi [6] pag. 172.

Passiamo allo studio del II° caso. Sarà intanto $(S_p) = p^\beta$ con $\beta > 1$. Il gruppo $\mathfrak{N}_G(S_q)$ è d'ordine $p^\beta q^\gamma$ ed S_p contiene un solo sottogruppo d'ordine p, per cui G è p-normale. Se p è il più piccolo divisore primo di (G), detto Z il centro di un fissato sottogruppo di Sylow S_p e tenuto conto della struttura di S_p, si trova necessariamente $\mathfrak{N}_G(Z) = S_p$; sicchè per un già citato teorema di Grün [11]), G contiene un sottogruppo normale M d'indice almeno p^δ con $\delta \geq 2$. Ma allora $M \subset N \subset G$ e dall'ipotesi induttiva segue che N e quindi G sono risolubili.

Possiamo pertanto supporre p diverso dal minimo divisore primo di (G). Allora S_p è ciclico. Se $\mathfrak{N}_G(S_p) = S_p$, G per un teorema di Buruside [12]) ha un sottogruppo normale M d'indice p^β in G; e si conclude come sopra. Per completare la dimostrazione del lemma, proveremo che è assurdo supporre $\mathfrak{N}_G(S_p) \supset S_p$. Da $\mathfrak{N}_G(S_p) \supset S_p$, segue [13]) che $\mathfrak{N}_G(S_p)$ è del tipo $S_p\bar{S}_q$ con S_p, $\bar{S}_q$ entrambi ciclici, perchè tale è il sottogruppo normale S_p. Poichè il gruppo $\mathfrak{N}_G(S_p)$ non può essere ciclico, risulta $q < p$ ed il derivato di $\mathfrak{N}_G(S_p)$ coincide con S_p [14]). Ma il gruppo $T = N \cap S_p\bar{S}_q$ è un sottogruppo normale di $S_p\bar{S}_q$ che contiene $\bar{S}_q$ e non contiene S_p; d'altra parte $\mathfrak{N}_G(S_p)/T$ è abeliano: perciò risulta $T \supseteq S_q$, cosa impossibile.

2. - È ora quasi immediata la dimostrazione del teorema enunciato nell'introduzione.

Infatti se G possiede un sottogruppo di Sylow normale, il teorema è vero per quanto dimostrato in [6]. Se G possiede un p-gruppo normale con p diverso dal minimo divisore primo di (G), il teorema segue dal lemma I e da [6]. Se G possiede un sottogruppo normale N che non sia un p-gruppo e che abbia divisibile per p il proprio indice in G, il gruppo S_pN, pel lemma II, risulta risolubile; sicchè [15]) (S_pN) è divi-

[11]) Vedasi [7] pag. 141.
[12]) Vedasi [7] pag. 139.
[13]) Vedasi [6] pag. 173.
[14]) Vedasi [7] pag. 145.
[15]) Vedasi [6] pag. 172.

sibile per esattamente due fattori primi distinti. Ne segue che l'ordine di G è pure divisibile solo per due fattori primi distinti. Se G possiede un sottogruppo normale N d'ordine p o p^2, con p minimo divisore primo di (G), il gruppo G è necessariamente un p-gruppo, se $p \neq 2$, perchè N non può possedere automorfismi regolari [21]) d'ordine maggiore di p; se invece $p = 2$, il gruppo G/N e senz'altro un α-gruppo risolubile. Infine se N ha indice p in S_p, con p sempre minimo divisore primo di (G), i sottogruppi di Sylow S_q di G, con $q \neq p$, sono ciclici, per cui l'α-gruppo G/N ha tutti i suoi sottogruppi di Sylow ciclici e risulta quindi risolubile. E per la [6] si conclude nel modo desiderato.

3. - Diamo qui un esempio di un α-gruppo G non risolubile che contiene un sottogruppo normale proprio non identico; in base al teorema del numero precedente N dovrà essere un p-gruppo con p minimo divisore primo di (G).

Indichiamo con N un gruppo abeliano elementare d'ordine 2^4. Il gruppo A degli automorfismi di N risulta isomorfo al gruppo lineare $GL(4,2)$ [16]). Sono note [17]) le relazioni

$$A \backsimeq GL(4,\ 2) \backsimeq PSL(4,\ 2) \backsimeq \mathfrak{A}_8 \quad {}^{18)}.$$

Indicati con $a_1, a_2, \dots a_8$ gli otto elementi su cui operano le sostituzioni di $\mathfrak{A}_8$, consideriamo un elemento di periodo 3 di $\mathfrak{A}_8$. Non è restrittivo supporre che esso sia l'elemento $(a_1a_2a_3)$, oppure $(a_1a_2a_3)(a_4a_5a_6)$ [19]). Posto $s = (a_1a_2a_3)(a_4a_5a_6)$ e $t = (a_1a_2 \dots a_5)$, un computo materiale prova che $st = (a_1a_4)(a_5a_6)$ e quindi $(st)^2 = 1$.

Per cui i due elementi s, t soddisfano alle relazioni $s^3 = t^5 = 1$, $(st)^2 = 1$.

---

16) Per le notazioni vedasi [4].

17) Vedasi [4] pag. 9.

18) A_8 indica il gruppo alterno su 8 oggetti.

19) $(a_1, a_2, \dots a_n)$ indica una sostituzione ciclica sugli n oggetti $a_1, a_2, \dots, a^n$.

Ciò basta per concludere [20]) che il sottogruppo $\{s, t\}$ di $\mathfrak{A}_8$ è un gruppo isomorfo al gruppo alterno su 5 oggetti. Possiamo pertanto concludere che ogni elemento di periodo 3 di $\mathfrak{A}_8$ è contenuto in un sottogruppo isomorfo al gruppo alterno su 5 oggetti. Premesso ciò, sia α un automorfismo regolare [21]) di N di periodo 3. (È facile convincersi dell'esistenza di un tale automorfismo). Per quanto precede esiste un sottogruppo H di A che contiene α ed è isomorfo al gruppo alterno su 5 oggetti. Dico che ogni elemento di H di periodo primo con 2 è un automorfismo regolare di N. Infatti, se β è un elemento di H di periodo 3, esso è un automorfismo regolare in quanto coniugato di α o α^2, ambedue automorfismi regolari contenuti in H. Se invece β è un elemento di periodo 5, esso è un automorfismo regolare perchè, come vedremo, ogni automorfismo di periodo 5 di N è necessariamente un automorfismo regolare. Nel caso contrario, infatti, sia n un elemento non identico di N lasciato fermo da β. Allora il sottogruppo $\{n\}$ sarebbe lasciato fermo da tutti gli elementi di $\{\beta\}$, e quindi, pel teorema di Maschke [22]) risulterebbe $N = N_1 \times \{n\}$ con N_1 trasformato in sè regolarmente da tutti gli elementi di $\{\beta\}$. Ma ciò è assurdo perchè un sottogruppo proprio di N non può avere automorfismi di periodo 5. Consideriamo ora l'olomorfo G di N rispetto ad H. Proviamo che G ci fornisce l'esempio cercato. Un elemento g di G si può porre sotto la forma $g = \begin{pmatrix} x \\ yx^{\alpha} \end{pmatrix}$, con α elemento di H, y elemento fissato di N ed x elemento corrente in N. Dalla relazione di immediata verifica $g^n = \begin{pmatrix} x \\ yx^{\alpha} \end{pmatrix}^n = \begin{pmatrix} x \\ y^{1+\alpha+\dots+\alpha^{n-1}} x^{\alpha^n} \end{pmatrix}$ segue $g^4 = \mathbf{1}$, se $\alpha = \mathbf{1}$, oppure $\alpha^2 = \mathbf{1}$. Se poi α è diverso da $\mathbf{1}$ ed ha periodo n primo con 2, da $\alpha^n = \mathbf{1}$ segue, tenuto presente che N è abeliano, $0 = \alpha^n - \mathbf{1} = (\alpha - \mathbf{1})(\alpha^{n-1} + \dots + \alpha + \mathbf{1})$.

Ma α ora è un automorfismo regolare; indi l'endomorfismo $\alpha - \mathbf{1}$ di N è un automorfismo di N: infatti da $x_1^{\alpha-1} = x_2^{\alpha-1}$

[20]) Vedasi ad es. [1] pag. 176.

[21]) Un automorfismo α di G dicesi regolare se nessun elemento di $\{\alpha\}$ diverso da 1 lascia fermo un elemento di G che non sia 1.

[22]) Vedasi [5] pag. 182.

segue $(x_2^{-1}x_1)^\alpha = x_2^{-1}x_1$: dunque è $x_2^{-1}x_1 = \mathbf{1}$, ossia $x_2 = x_1$, perchè α non lascia elementi fissi all'infuori di $\mathbf{1}$.

Ma allora $\alpha^{n-1} + \alpha^{n-2} + \dots + \alpha + \mathbf{1} = 0$; da cui $g^n = \begin{pmatrix} x \\ y^0 x \end{pmatrix} = \begin{pmatrix} x \\ x \end{pmatrix} = \mathbf{1}$. Quindi G è un α-gruppo, contiene un sottogruppo normale, ma non è risolubile, essendo $\dfrac{G}{N}$ isomorfo al gruppo alterno su 5 soggetti.

4. - In questo numero esponiamo qualche considerazione complementare sugli α-gruppi.

È facile vedere che in un α-gruppo G, ogni serie principale di composizione di G contiene il sottogruppo di Fitting $F(G)$ di G [23]. Dimostriamo che:

Se G è un α-gruppo risolubile, il sottogruppo di Fitting $F(G)$ di G ha complemento in G; vale a dire, esiste un sottogruppo C di G per cui valgono le relazioni: $G = F(G) \cup C$, $F(G) \cap C = 1$.

Se G è un p-gruppo, evid. $C = \mathbf{1}$. Supponiamo dunque G diverso da un p-gruppo. Sia $N_0 = \mathbf{1} \subset N_1 \subset \dots \subset N_i = F(G) \subset \dots \subset G$ una serie principale di composizioni di G. Poichè G è risolubile, è $i \geq 1$. In $\dfrac{G}{N_{i-1}}$, il gruppo $\dfrac{F(G)}{N_{i-1}}$ è un p-gruppo abeliano normale minimo; il gruppo $\dfrac{N_{i-1}}{F(G)}$ è un p-gruppo abeliano ed il suo ordine è primo con $(F(G))$; sicchè N_{i+1} si presenta come un gruppo con l'ordine divisibile per due fattori primi distinti a sottogruppi di Sylow abeliani elementari uno dei quali è $F(G)$ e gli altri sono isomorfi ad $\dfrac{N_{i+1}}{F(G)}$. Detto S uno di questi ultimi, risulta $N_{i+1} = F(G)S$.

---

[23]) Dicesi sottogruppo di Fitting di G il sottogruppo normale speciale massimo di G. Ebbene supposto $F(G) \supset 1$, se N è un sottogruppo normale minimo di G, è $F(G) \cap N = N$. Allora, se G ha un solo sottogruppo normale minimo N, è $F(G) = N$; altrimenti, partendo da $F(G) \supset N$ ed $F\left(\dfrac{G}{N}\right) = \dfrac{F(G)}{N}$, si conclude come si desidera mediante induzione rispetto all'ordine di G.

In $\frac{G}{N_{i-1}}$, il gruppo $\frac{F(G)}{N_{i-1}}$ è un p-gruppo abeliano normale ed $\frac{SN_{i-1}}{N_{i-1}}$ è un gruppo d'ordine primo con $\left(\frac{F(G)}{N_{i-1}}\right)$. Inoltre l'unione $\frac{SN_{i-1}}{N_{i-1}} \cup \frac{F(G)}{N_{i-1}} = \frac{N_{i+1}}{N_{i-1}}$ è un sottogruppo normale di $\frac{G}{N_{i-1}}$. L'unico sottogruppo normale di $\frac{G}{N_{i-1}}$ contenuto propriamente in $\frac{N_i}{N_{i-1}}$ è il sottogruppo identico $\frac{N_{i-1}}{N_{i-1}}$, mentre l'unione $\frac{SN_{i-1}}{N_{i-1}} = \frac{SN_{i-1}}{N_{i-1}} \cup \frac{N_{i-1}}{N_{i-1}}$ non è normale in $\frac{G}{N_{i-1}}$. Allora in virtù di un teorema di Higman [24]), il gruppo $\frac{F(G)}{N_{i-1}}$ ha un complemento $\frac{C}{N_{i-1}}$ in $\frac{G}{N_{i-1}}$ sicchè si ha $F(G) \cup C = G$, $F(G) \cap C = N_{i-1}$.

Pertanto se $N_{i-1} = 1$, il teorema risulta provato.

Sia dunque $N_{i-1} \supset 1$. Da $C \cap F(G) = N_{i-1}$, segue $F(C) \supseteq N_{i-1}$. Proviamo che $F(C) = N_{i-1}$. Sia, per assurdo, $F(C) \supset N_{i-1}$. Il gruppo $F(G) \cup F(C)$ è normale in G, ed è un p-gruppo, sicchè $F(G) \supset F(C) \supset N_{i-1}$.

Poichè $\frac{F(G)}{N_{i-1}}$ è abeliano, $\frac{F(C)}{N_{i-1}}$ è normale in $\frac{F(G)}{N_{i-1}}$ e $\frac{C}{N_{i-1}}$ è quindi tale in $\frac{G}{N_{i-1}}$, cosa assurda, perchè $\frac{F(G)}{N_{i-1}}$ è normale minimo in $\frac{G}{N_{i-1}}$. Usando induzione sull'ordine di G, possiamo supporre che $F(C)$ abbia un complemento C' in C, di guisa che $F(C) \cup C' = C$ e $F(C) \cap C' = 1$.

Ne segue $C' \cup F(G) = C' \cup (F(C) \cup F(G)) = C \cup F(G) = G$.

Resta da provare che $C' \cap F(G) = 1$. Infatti posto $H = C' \cap F(G)$, segue $H \subseteq C \cap F(G) = N_{i-1} = F(C)$, essendo $H \subset F(G)$ ed $H \subset C' \subset C$. Ma da $H \subset C'$, $H \subset F(C)$, segue $H \subseteq C' \cap F(C) = 1$. c.v.d.

È facile assegnare la struttura di C. Si è già detto che se G è un p-gruppo $C = 1$. Altrimenti, poichè G è per ipo-

---

24) Vedasi [2] pag. 455.

tesi risolubile, l'ordine di G è divisibile solo per due fattori primi distinti: $(G) = p^{\beta}q^{\gamma}$. Sia p il divisore primo di $(F(G))$. Se $p > q$ risulta [25]) $F(G) = S_p$; e quindi $C = S_q$, con S_q ciclico o generalizzato dei quaternioni. Se $p < q$, i sottogruppi di Sylow di G d'ordine q sono ciclici. In tal caso, se $F(G) = S_p$, risulta $C = S_q$; se $F(G) \subset S_p$, allora $(C) = p^{\delta}q^{\gamma}$, con $0 < \delta < \beta$. Poichè ora C contiene un q-gruppo normale in C, il suo sottogruppo S_q è normale [26]) in C; dunque i sottogruppi di Sylow d'ordine p^{δ} sono ciclici. cioè C è un gruppo d'ordine $p^{\delta}q^{\gamma}$ a sottogruppi di Sylow ciclici a centro identico.

BIBLIOGRAFIA

[1] CARMICHAEL R. D.: *Introduction to the theory of groups of finite order;* Dover Publ., Inc. (1956).

[2] HIGMAN G.: *Complementation of abelian normal subgroups*, Public. Mathematicae, vol. 4, pag. 455, Debrecen (1956).

[3] SPEISER A.: *Die Theorie der Gruppen von endlicher Ordnung*, Verlag Birkhäuser, Basel (1956).

[4] VAN DER WAERDEN B. L.· *Gruppen von linearen Transformationen*, Erg. der Math., Springer Verlag (1935).

[5] VAN DER WAERDEN B. L.: *Moderne Algebra*, vol. 2, Springer Ver lag (1940).

[6] ZACHER G.: *Sull'ordine di un gruppo finito risolubile somma dei suoi sottogruppi di Sylow*, Rend. Acc. Naz. Lincei, vol. 20, fasc. 2 (1956).

[7] ZASSENHAUS H.: *The theory of groups*, Chelsea Publ. Comp., New York (1949).

---

[25]) Vedasi [6] pag. 173.

[26]) Vedasi [6] pag. 173.