

ANNALI DELLA SCUOLA NORMALE SUPERIORE DI PISA *Classe di Scienze*

ENNIO MATTIOLI

Sui gruppi abeliani finiti

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 6, n° 1-2 (1952), p. 51-57

http://www.numdam.org/item?id=ASNSP_1952_3_6_1-2_51_0

© Scuola Normale Superiore, Pisa, 1952, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUI GRUPPI ABELIANI FINITI

di ENNIO MATTIOLI (Pisa)

Sia \mathcal{R} un gruppo abeliano di ordine $P \geq 2$ e siano

$$R_0 = 1, R_1, \dots, R_{P-1}$$

i suoi elementi in un qualunque ordine prefissato.

Indichiamo con (r', r'') il numero d'ordine del prodotto dei due elementi di posto r' ed r'' :

$$R_{r'} \cdot R_{r''} = R_{(r', r'')}.$$

Consideriamo un automorfismo A_s di \mathcal{R} e indichiamo con R_{sr} l'elemento che esso fa corrispondere ad R_r . Per definizione di automorfismo ⁽¹⁾:

$$(1) \quad \text{se } R_{r'} \cdot R_{r''} = R_{(r', r'')} \quad \text{anche } R_{sr'} \cdot R_{sr''} = R_{s(r', r'')}$$

e in particolare:

$$(2) \quad \text{se } R_{r'} \cdot R_{r''} = 1 \quad \text{anche } R_{sr'} \cdot R_{sr''} = 1.$$

Supponiamo che esista un insieme \mathcal{A} di $P - 1$ automorfismi di \mathcal{R} :

$$(3) \quad A_0 = 1, A_1, \dots, A_{P-2}$$

aventi la proprietà di far corrispondere ad ogni elemento di \mathcal{R} diverso dall'identità tutti i $P - 1$ elementi diversi dell'identità. Diremo allora che \mathcal{R} è un gruppo *perfetto*: tale proprietà si traduce nella relazione:

$$(4) \quad \text{se } R_{s'r} = R_{s''r} \quad \text{con } r > 0 \quad \text{allora } s' = s'',$$

⁽¹⁾ Cfr. G. ZAPPA. *Gruppi, corpi, equazioni*. Ed. Liguori, Napoli 1950.

valevole per s' ed s'' compresi fra 0 e $P - 2$, ed $1 \leq r \leq P - 1$.

Poniamo:

$$(5) \quad N = \frac{P^k - 1}{P - 1}$$

con k intero ≥ 2 .

Consideriamo N gruppi di ordine P perfetti nel senso sopra definito:

$$(6) \quad \mathcal{R}^{(1)}, \dots, \mathcal{R}^{(N)}$$

isomorfi fra loro e perciò ordinati nello stesso modo. Indichiamo con

$$R_r^{(i)} \quad \left(\begin{array}{l} i = 1, \dots, N \\ r = 0, \dots, P - 1 \end{array} \right)$$

l'elemento generico del gruppo $\mathcal{R}^{(i)}$ e con

$$R_{sr}^{(i)} \quad (s = 0, \dots, P - 2)$$

il suo corrispondente nell'automorfismo A_s .

Evidentemente per ogni i si ha:

$$(7) \quad R_{0r}^{(i)} = R_r^{(i)},$$

e

$$(8) \quad R_{s0}^{(i)} = 1.$$

Chiameremo i *indice superiore*, r *indice inferiore* ed s *indice di automorfismo*.

Formiamo il prodotto G dei gruppi R ; G sarà di ordine P^N . Agli elementi $R_r^{(i)}$ daremo il nome di *fattori primitivi*.

Dimostriamo il seguente:

TEOREMA. — *Nel gruppo abeliano G è possibile trovare un sottogruppo Γ di ordine P^{N-k} tale che la scomposizione di G secondo Γ ed i suoi laterali si presenta nella forma:*

$$(9) \quad G = \Gamma_* + \sum_{i=1}^N \sum_{r=1}^{P-1} \Gamma R_r^{(i)}.$$

Indichiamo con

$$(10) \quad i_1, i_2, \dots, i_f \quad (2 \leq f \leq k)$$

una combinazione semplice di classe f dei numeri interi da 1 a k , ordinata per valori crescenti dei numeri che la compongono.

Ad ognuna di tali combinazioni associamo tutte le possibili disposizioni con ripetizione della classe $f - 1$ dei numeri $0, \dots, P - 2$:

$$(11) \quad i_1, \dots, i_f; s_2, \dots, s_f \cdot \left(\begin{array}{c} 1 \leq i_1 < i_2 < \dots < i_f \leq k \\ s_2, \dots, s_f \text{ compresi fra } 0 \text{ e } P - 2 \end{array} \right)$$

Al variare di f tra 2 e k (estremi compresi) di successioni del tipo (11) ne avremo:

$$(12) \quad \sum_{f=2}^k \binom{k}{f} (P - 1)^{f-1} = \frac{P^k - 1}{P - 1} - k = N - k.$$

Le ordiniamo con una legge qualunque e indichiamo con $j - k$ il numero d'ordine della generica di esse. Sarà:

$$1 \leq j - k \leq N - k$$

quindi:

$$k + 1 \leq j \leq N.$$

Consideriamo tutti i prodotti della forma:

$$(13) \quad \gamma_r^{(j)} = R_r^{(i_1)} \cdot R_{s_2 r}^{(i_2)} \cdot \dots \cdot R_{s_f r}^{(i_f)} \cdot R_r^{(j)} \quad \left(\begin{array}{l} r = 0, \dots, P - 1 \\ j = k + 1, \dots, N \end{array} \right)$$

nella quale la successione degli indici $i_1, \dots, i_f; s_2, \dots, s_f$ è stata costruita com'è detto sopra e j rappresenta il suo numero d'ordine.

Si vede facilmente che:

$$(14) \quad \gamma_{r'}^{(j)} \cdot \gamma_{r''}^{(j)} = \gamma_{(r', r'')}^{(j)}$$

per ogni coppia di indici r' ed r'' (anche uguali fra loro); basta infatti eseguire il prodotto tenendo presente che l'uguaglianza dell'indice j implica l'identità degli indici superiori e degli indici di automorfismo e che per qualunque i e qualunque s è

$$(15) \quad R_{sr'}^{(i)} \cdot R_{sr''}^{(i)} = R_{s(r', r'')}^{(i)}.$$

Indichiamo con Γ il minimo sottogruppo di G che contiene tutti gli elementi $\gamma_r^{(j)}$ della forma (13).

L'ordine di Γ è P^{N-k} .

Infatti ogni prodotto del tipo :

$$(16) \quad \gamma_{r_{k+1}}^{(k+1)} \cdot \gamma_{r_{k+2}}^{(k+2)} \cdot \dots \cdot \gamma_{r_N}^{(N)}$$

e con gli indici inferiori variabili tra 0 e $P-1$, deve far parte di Γ e poichè tali prodotti sono in numero di P^{N-k} , tutti distinti fra loro, l'ordine di Γ non può essere inferiore a tale numero.

D'altra parte in base alla (14) qualunque prodotto di elementi $\gamma_r^{(j)}$ dati dalla (13) può essere messo nella forma (16) (nella quale alcuni degli indici inferiori saranno eventualmente nulli). Perciò i prodotti della forma (16) esauriscono Γ .

Dimostriamo che ogni elemento di Γ , diverso dall'identità, contiene almeno tre fattori primitivi con indici superiori differenti. Dividiamo la dimostrazione in tre parti a), b), c).

a) La proprietà vale per ciascuno dei $\gamma_r^{(j)}$: ciò risulta subito dalla formula (13) ricordando che $f \geq 2$.

Si noti che per ogni j è $\gamma_0^{(j)} = 1$.

b) Dimostriamo la proprietà per ogni prodotto del tipo :

$$(17) \quad \gamma_{r'}^{(j')} \cdot \gamma_{r''}^{(j'')}$$

con $r' \neq 0$, $r'' \neq 0$ altrimenti si ricade nel caso a).

Se $j' = j''$ il prodotto risulta uguale a $\gamma_{(r', r'')}^{(j')}$ e si ricade nel caso a).

Se $j' \neq j''$ nel prodotto (17) compaiono due fattori primitivi $R_{r'}^{(j')}$ e $R_{r''}^{(j'')}$ con indici superiori $> k$ e diversi fra loro. Facciamo vedere che vi compare anche un fattore primitivo con indice superiore $\leq k$. Siano infatti:

$$(18) \quad \begin{aligned} & i'_1, \dots, i'_{f'}; s'_2, \dots, s'_{f'} \\ & i''_1, \dots, i''_{f''}; s''_2, \dots, s''_{f''} \end{aligned}$$

le successioni degli indici superiori e degli indici di automorfismo individuate da j' e j'' .

Se le due combinazioni degli indici superiori differiscono fra loro (differiscono certamente se $f' \neq f''$, ma anche per $f' = f''$ possono essere diverse) vi sarà un dato indice \bar{i} che figurerà in una sola delle successioni (18). Perciò nel prodotto (17) sarà presente necessariamente un fattore primitivo, $R^{\bar{i}}$ con indice superiore $\bar{i} \leq k$.

Se invece nelle due successioni (18) sono identiche le combinazioni degli indici superiori, per essere $j' \neq j''$ dovrà almeno uno degli indici di automorfismo della prima successione, sia esso s'_m , differire dal corrispondente s''_m . Notiamo che in questo caso $i'_m = i''_m$; $f' = f''$; m compreso fra 2 ed f' , estremi inclusi.

Con questa ipotesi facciamo vedere che se $(r', r'') = 0$ nella (17) rimane un fattore primitivo con indice superiore $i'_m \leq k$; se invece $(r', r'') \neq 0$ rimane un fattore primitivo di indice superiore $i'_1 < k$.

Sudposto infatti $(r', r'') = 0$ il prodotto:

$$R_{s'_m r'}^{(i'_m)} \cdot R_{s''_m r''}^{(i'_m)}$$

dà un fattore primitivo di indice superiore $i'_m \leq k$, diverso dall'identità; perchè se fosse

$$(20) \quad R_{s'_m r'}^{(i'_m)} \cdot R_{s''_m r''}^{(i'_m)} = 1,$$

dalla relazione:

$$R_{r'}^{(i'_m)} \cdot R_{r''}^{(i'_m)} = 1$$

seguirebbe per la (2)

$$R_{s'_m r'}^{(i'_m)} \cdot R_{s''_m r''}^{(i'_m)} = 1;$$

quindi confrontando con la (20):

$$R_{s'_m r'}^{(i'_m)} = R_{s''_m r''}^{(i'_m)}$$

e per la (4)

$$s'_m = s''_m$$

contro l'ipotesi.

Se poi $(r', r'') \neq 0$ si vede subito, tenendo presente che $i'_1 = i''_1$, che nella (17) rimane il fattore primitivo $R_{(r', r'')}^{(i'_1)}$ con indice superiore $< k$.

c) Ammettiamo che la proprietà sia stata dimostrata per ogni prodotto di $n \geq 2$ fattori $\gamma_r^{(j)}$ e facciamo vedere che essa vale per un prodotto di $n + 1$ fattori $\gamma_r^{(j)}$.

Consideriamo il prodotto:

$$(22) \quad \gamma_{r_1}^{(j_1)} \cdot \gamma_{r_2}^{(j_2)} \cdot \dots \cdot \gamma_{r_{n+1}}^{(j_{n+1})}.$$

Se gli indici superiori sono tutti distinti nel prodotto (22) compaiono i fattori primitivi indipendenti

$$R_{r_1}^{(j_1)}, R_{r_2}^{(j_2)}, \dots, R_{r_{n+1}}^{(j_{n+1})}$$

in numero di $n + 1 \geq 3$. Gli indici inferiori debbono essere tutti $\neq 0$ altrimenti il prodotto (22) avrebbe meno di $n + 1$ fattori.

Se almeno due indici superiori coincidono, per es. $j_m = j_h$ si ha per la (14):

$$\gamma_{r_m}^{(j_m)} \cdot \gamma_{r_h}^{(j_h)} = \gamma_{(r_m, r_h)}^{(j_m)}$$

ed il prodotto (22) viene a contenere n od $n - 1$ fattori secondo che $(r_m, r_h) \neq 0$ o $(r_m, r_h) = 0$.

Quindi la proprietà di Γ è dimostrata.

Consideriamo ora tutti gli elementi di G contenuti nell'espressione:

$$(24) \quad \Gamma + \sum_{i=1}^N \sum_{r=1}^{P-1} \Gamma R_r^{(i)}$$

dove Γ è il sottogruppo di G sopra costruito.

Gli elementi della (24) sono tutti diversi fra loro perchè se fosse:

$$\gamma_1 R_{r_1}^{(i_1)} = \gamma_2 R_{r_2}^{(i_2)}$$

con γ_1 e γ_2 in Γ detto r_3 l'indice per cui $(r_1, r_3) = 0$ sarebbe

$$\gamma_1 \gamma_2^{-1} = R_{r_3}^{(i_1)} \cdot R_{r_2}^{(i_2)}$$

perciò l'elemento a secondo membro, formato di due soli fattori primitivi, dovrebbe stare in Γ . Dunque sarà:

$$R_{r_3}^{(i_1)} \cdot R_{r_2}^{(i_2)} = 1$$

cioè

$$R_{r_1}^{(i_1)} = R_{r_2}^{(i_2)}$$

e di conseguenza

$$i_1 = i_2; r_1 = r_2.$$

Gli elementi che compaiono nella (24) sono in numero di:

$$P^{N-K} [1 + N(P - 1)] = P^N$$

e poichè sono tutti distinti esauriscono G e la (24) rappresenta la scomposizione di G secondo I ed i suoi laterali. c. v. d.

Osserviamo che un gruppo può essere perfetto nel senso sopra definito solo se i suoi elementi hanno tutti lo stesso ordine e questo è un numero primo.

Perciò sarà $P = p^a$, con p numero primo. Sulla sufficienza della condizione ritorneremo in un successivo lavoro. In base alla proprietà del sottogruppo I segue che per ogni P per cui esista un gruppo abeliano perfetto vale il teorema di ripartizione delle disposizioni con ripetizione della classe N di P oggetti, dimostrato dallo scrivente in un precedente lavoro⁽²⁾ per $P = p^2$.

[Entrato in redazione il 17-4-952]

⁽²⁾ E. MATTIOLI, *Sopra un'altra proprietà di gruppi abeliani finiti*. Annali della Scuola Normale Superiore di Pisa. Fasc. I-II 1951.

⁽³⁾ L'autore ritiene doveroso segnalare un lavoro sull'argomento sfuggitogli nelle precedenti ricerche bibliografiche: O. TAUSKY e J. TODD. Covering theorems for groups. *Annales de La Société Polonaise de Mathématique*, XXI, 1948.

Aggiunta in data 20-5-52. A lavoro già stampato mi è stato segnalato un altro articolo sullo stesso argomento: S. K. ZAREMBA - Covering problems concerning abelian groups - *Journal of the London Mathematical Society*, Vol. 27, 1952. - L'A.