ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

ENNIO MATTIOLI

Altri teoremi di copertura dei gruppi

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 7, n^o 1-2 (1953), p. 43-52

<http://www.numdam.org/item?id=ASNSP_1953_3_7_1-2_43_0>

ALTRI TEOREMI DI COPERTURA DEI GRUPPI

di ENNIO MATTIOLI (Pisa)

SOMMARIO: Si estende a gruppi abeliani di ordine p^k un teorema dimostrate in un precedente lavoro (4). Si da inoltre un teorema di scomposizione dei gruppi a copertura lineare e si introduce il concetto di gruppi a copertura quadratica dimostrando l'effettiva esistenza di tali gruppi. Si è adottato per l'argomento il titolo introdotto da TAUSSKY e TODD (2).

PARTE I

Generalizzazione di un teorema di copertura

In un precedente lavoro si è definito perfetto un gruppo abeliano $\mathfrak{R}$ di ordine $P \geq 2$ se esso possiede un isieme $\mathfrak{A}$ di $P-1$ automorfismi aventi la proprietà di far corrispondere ad ogni elemento di $\mathfrak{R}$ diverso dall'identità tutti i $P-1$ elementi diversi dall'identità.

Poichè è stato dimostrato dallo ZAPPA (1) che il gruppo di automorfismi di un gruppo abeliano elementare H di ordine p^k (p primo) contiene un sottogruppo ciclico C di ordine p^k-1 semplicemente transitivo sugli elementi non identici di H, segue che un gruppo abeliano elementare è perfetto nel senso prima definito. Perciò vale per tale tipo di gruppi il teorema di copertura dimostrato in (4) per il caso di p^2 (*).

Dunque il teorema di *ripartizione delle disposizioni con ripetizione* può generalizzarsi nel seguente modo:

(*) Questo risultato è già stato raggiunto dallo ZAREMBA che si è occupato indipendentemente dello stesso argomento (6) (7). Dalle date di presentazione dei lavori risulterebbe una priorità dello scrivente nella prima dimostrazione a carattere generale (caso di p primo) e nella prima generalizzazione (caso di p^2). Mentre spetterebbe allo ZAREMBA la priorità della dimostrazione per il caso di p^k. Qui tale risultato raggiunto indipendentemente e per altra via si presenta in forma diversa, tanto che l'insieme, definito più avanti come nucleo di copertura. *è un gruppo.*

Se è $P = p^k$ *con* p *primo ed*

$$N = \frac{P^K - 1}{P - 1} \qquad (K \geq 2)$$

fra le P^N disposizioni con ripetizione di P oggetti della classe N è possibile sceglierne un insieme H di P^{N-K} tali che ogni altra disposizione differisca da una di H per un solo elemento.

PARTE II

Scomposizione di gruppi a copertura lineare

Un gruppo abeliano che soddisfa al teorema di copertura si chiamerà *gruppo a copertura lineare completa* ed il suo sottogruppo Γ verrà detto *nucleo di copertura.*

Siano

$$G^{(1)}, \ldots, G^{(N)}$$

N gruppi abeliani ciascuno di ordine p^n e di tipo $(1, \ldots, 1)$, indipendenti, a copertura lineare completa e siano

$$\Gamma^{(1)}, \ldots, \Gamma^{(N)}$$

i loro nuclei di copertura, ciascuno di ordine p^{n-k}. Per ipotesi è quindi

$$n = \frac{p^k - 1}{p - 1} \qquad (k \geq 2) \tag{1}$$

Poniamo

$$P = p^k \tag{2}$$

e supponiamo che sia

$$N = \frac{P^K - 1}{P - 1} \qquad (K \geq 2) \tag{3}$$

Siano inoltre

$$R_1^{(i)}, \ldots, R_n^{(i)}$$

le generatrici di un $G^{(i)}$ generico. Il fattoriale di $\Gamma^{(i)}$ rispetto a $G^{(i)}$ è un gruppo abeliano di tipo $(1, \ldots, 1)$ ed ordine p^k.

Detto $F^{(i)}$ tale fattoriale e detti

$$F_r^{(i)} \qquad (r = 1, \ldots, P)$$

i suoi elementi, sarà con notazioni evidenti:

$$F_1^{(i)} \equiv \Gamma^{(i)} \equiv 1\,,\ F_2^{(i)} \equiv \Gamma^{(i)} R_1^{(i)}\,, \ldots, F_P^{(i)} = \Gamma^{(i)} (R_n^{(i)})^{p-1}$$

essendo per la (1):

$$P = p^k = n(p-1) + 1\,.$$

Per il generico $F_s^{(i)}$ varrà la relazione:

$$F_s^{(i)} \equiv \Gamma^{(i)} (R_{a+1}^{(i)})^{b+1} \tag{4}$$

nella quale è:

$$s - 2 = a(p-1) + b \qquad \text{con } b < p-1\,. \tag{5}$$

Sia ora C il gruppo ottenuto dal prodotto degli $F^{(i)}$. Essendo soddisfatta la (3) il gruppo C, di ordine P^N, è a copertura lineare completa e detto Φ un suo nucleo di copertura sarà:

$$C = \Phi + \sum_{\substack{i,r \\ i=1,\ldots,N \\ r=2,\ldots,P}} \Phi\, F_r^{(i)}$$

Indichiamo con G' il gruppo ottenuto dal prodotto dei $G^{(i)}$.
Esso ha ordine $p^{n'}$ con

$$n' = n\,N\,. \tag{6}$$

Ma posto:

$$k' = k\,K \tag{7}$$

si ha, per le (1), (2), (3):

$$n' = \frac{p^{k'} - 1}{p - 1} \tag{8}$$

perciò G' è a copertura lineare completa.

Sostituiamo agli elementi $F_s^{(i)}$ di Φ le loro espressioni date dalla (4) ed effettuiamo i prodotti indicati. Da ogni elemento di Φ si avranno $p^{(n-k)N}$ prodotti, quindi in totale se ne avranno

$$P^{N-K} \cdot p^{(n-k)N} \tag{9}$$

i quali costituiscono un insieme Γ' che, come è facile vedere, è un sottogruppo di G'. *Dimostriamo che Γ' è un nucleo di copertura di G'* cioè che vale la relazione:

$$G' = \Gamma' + \sum_{\substack{i,s,\alpha \\ i=1,\dots,N \\ s=1,\dots,n \\ \alpha=1,\dots,p-1}} \Gamma' (R_s^{(i)})^\alpha .$$

Anzitutto dalla (9), tenendo conto delle (2), (6), (7) si ricava con facili passaggi che l'ordine Γ' è $p^{n'-k'}$. Il suo indice deve essere, affinchè esso sia un nucleo di copertura:

$$n\,N(p-1)+1 = n'(p-1)+1 = p^{k'}$$

perciò è soddisfatta la condizione che l'ordine di Γ' per il suo indice dà l'ordine di G'.

Resta da far vedere che gli elementi di Γ' contengono almeno tre generatrici di G', cioè che i prodotti del tipo:

$$(R_s^{(j)})^\alpha (R_t^{(j)})^\beta \tag{10}$$

sono fuori di Γ'.

Se uno degli esponenti, ad es. β, è nullo l'altra generatrice $(R_s^{(j)})^\alpha$ non può stare in Γ' perchè essa non sta in $\Gamma^{(i)} \equiv F_1^{(i)} = 1$.

Se $i = j$ il prodotto (10) non può stare in Γ' perchè esso non sta in $\Gamma^{(j)} \equiv F_1^{(i)} = 1$.

Se $i \neq j$ dall'ipotesi che il prodotto (10) stia in Γ' seguirebbe che l'elemento

$$F^{(i)}_{(s+1)(p-1)+\alpha+1} \cdot F^{(j)}_{(t+1)(p-1)+\beta+1}$$

starebbe in Φ e ciò è assurdo perchè Φ è un nucleo di copertura di C.

Dunque vale il seguente:

Teorema di scomposizione dei gruppi a copertura lineare: Sia

$$n' = \frac{p^{k'}-1}{p-1} \tag{11}$$

con p primo e con

$$k' = K k , \tag{12}$$

K e k interi ≥ 2. Posto:

$$P = p^k , n = \frac{p^k - 1}{p - 1} , N = \frac{P^K - 1}{P - 1} \tag{13}$$

risulterà:

$$n' = N n .$$

Sia G' un gruppo abeliano di ordine $p^{n'}$ e tipo $(1, \ldots, 1)$ e Γ' un suo nucleo di copertura. Scomposto G' nel prodotto di N sottogruppi abeliani $G^{(1)}, \ldots, G^{(N)}$ ciascuno di ordine p^n, e quindi fra loro indipendenti, detti $\Gamma^{(1)}, \ldots, \Gamma^{(N)}$ i rispettivi nuclei di copertura, detto C un gruppo a copertura lineare di ordine P^N e Φ un suo nucleo di apertura, il nucleo Γ' si ottiene da Φ sostituendo agli elementi di Φ i laterali di $\Gamma^{(i)}$ dentro $G^{(i)}$ per $i = 1, \ldots, N$.

Se la sostituzione dei laterali si effettua soltanto su $N - M$ elementi di Φ si ha come corollario il seguente:

Teorema generale di ripartizione delle disposizioni: siano dati

	M	*insiemi*	*contenenti ciascuno*	P *oggetti*
$(N - M)\, n$	»	»	»	p »

dove i numeri n, p, N, P sono legati fra loro dalle (13) *con k e K interi arbitrari. Fra tutte le*

$$P^M . p^{(N-M)n}$$

disposizioni che si possono formare prendendo 1 *ed* 1 *solo oggetto di ciascun insieme si può scegliere un gruppo H di*

$$P^{N-K} . (p^{n-k})^{N-M}$$

disposizioni tali che ognuna delle rimanenti differisca da una di esse per un solo elemento.

Facciamo una verifica di questo teorema dimostrando che il numero delle disposizione che si ottengono da H, cambiando un solo elemento (in tutti i modi possibili) in ciascuna disposizione di H, esaurisce la totalità delle disposizioni.

Infatti cambiando un elemento in tutti i modi possibili da una sola disposizione se ne ottengono altre

$$(P - 1)\, M + (p - 1)\, (N - M)\, n .$$

Perciò si deve dimostrare che:

$$(14)\quad [1+(P-1)M+(p-1)(N-M)n]\,.\,P^{N-K}\,p^{(n-k)(N-M)}=P^{M}\,p^{(N-M)n}\,.$$

Infatti per le (11), (12), (13) risulta:

$$1+(P-1)M+(p-1)(N-M)n=1+(p^{k}-1)M+(p^{k}-1)(N-M)=p^{k'}$$

$$P^{N-K}\,p^{(n-k)(N-M)}=p^{n'-(n-k)M-k'}$$

$$P^{M}\,p^{(N-M)n}\qquad =p^{n'-(n-k)M}$$

dalle quali segue immediatamente la (14).

ESEMPIO. — In un gioco con totalizzatore si deve indovinare il 1° arrivato di 9 corse delle quali 3 con 4 corridori ciascuna e 6 con due corridori ciascuna. Il totalizzatore dà un premio anche a chi indovina 8 risultati su 9.

I numeri scelti soddisfano alle condizioni del teorema di ripartizione quando si prenda:

$$p=2\,,\ k=2\,,\ K=2\,,\ M=3\,,$$

perchè allora è

$$P=2^{2}=4\,,\ n=\frac{2^{2}-1}{2-1}=3\,,\ N=\frac{4^{2}-1}{4-1}=5\,,\ (N-M)n=6\,.$$

Il giocatore per avere la certezza di totalizzare 9 punti su 9 dovrebbe effettuare

$$4^{3}.2^{6}=4096$$

giocate.

Ma può effettuarne soltanto

$$4^{3}.2^{2}=256$$

con la certezza matematica di indovinare 8 risultati su 9.

PARTE III

I gruppi a copertura quadratica

Fra le possibili generalizzazioni dei teoremi di copertura dei gruppi vi è la ricerca dei *gruppi a copertura quadratica completa*, cioè di quei gruppi

abeliani G, di tipo $(1, \dots, 1)$ ed ordine p^n, con generatrici $R_1, R_2, \dots, R_n$, nei quali esiste un sottogruppo Q per cui:

$$G = Q + \Sigma\, Q\, R_i^{\alpha} + \Sigma\, Q\, R_j^{\beta} R_l^{\gamma}\,. \qquad \begin{matrix} i, j, l = 1, \dots, n \\ \alpha, \beta, \gamma = 1, \dots, p-1 \end{matrix}$$

La ricerca si presenta ardua e ci limitiamo nel presente lavoro a dimostrare con un esempio l'esistenza di simili gruppi. L'esempio è di costruzione tutt'altro che semplice e può costituire un utile guida per la dimostrazione generale.

Il gruppo Q deve avere per ordine una potenza di p perciò affinchè la la (15) sia soddisfatta deve essere:

$$1 + \binom{n}{1}(p-1) + \binom{n}{1}(p-1)^2 = p^k\,.$$

Questa uguaglianza è soddisfatta da

$$n = 11\,,\ p = 3\,,\ k = 5\,.$$

Costituiamo per tali valori il sottogruppo Q: esso avrà ordine 3^6.

Siano $R_1, \dots, R_{11}$ le generatrici di G. Consideriamo il sottogruppo $\mathfrak{B}$ di G generato da $R_1, \dots, R_5$ e indichiamo con

$$B_1, \dots, B_6$$

gli elementi di $\mathfrak{B}$ che si ottengono dando come esponenti alla sua base $R_1, \dots, R_5$ rispettivamente i numeri della $1^a, \dots, 6^a$ riga della seguente matrice:

(16)
$$\left\| \begin{matrix} 0 & 1 & 1 & 2 & 2 \\ 1 & 0 & 2 & 1 & 2 \\ 1 & 2 & 0 & 2 & 1 \\ 2 & 1 & 2 & 0 & 1 \\ 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{matrix} \right\|$$

Gli elementi di $\mathfrak{B}$ così costruiti soddisfano alle seguenti proprietà

1^0. È

(17)
$$B_1 B_2 B_3 B_4 B_5 = 1$$

2°. Oltre al prodotto (17) ed al suo quadrato nessun altro prodotto della forma

$$B_1^{\alpha_1}, \ldots, B_6^{\alpha_6} \tag{18}$$

può dare l'identità. Infatti, se vi fosse, la matrice (16) avrebbe al massimo caratteristica 4 (mod. 3), mentre ha caratteristica 5.

Ne segue che il prodotto di *quattro* potenze di $B_i\,(i = 1, \ldots, 6)$ contiene almeno una generatrice $R_j\,(j = 1, \ldots, 5)$.

3°. I prodotti della forma (18) sono in numero di 3^6 ed ogni elemento di $\mathfrak{B}$ figura ripetuto tre volte (per il punto 1°).

4°. Gli elementi di B che si ottengono dando come esponenti a $B_1, \ldots, B_6$ ordinatamente i numeri della $1^a, \ldots, 5^a$ riga della seguente matrice:

$$\left\| \begin{matrix} 1 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 2 & 2 \\ 0 & 2 & 1 & 2 & 0 & 2 \\ 2 & 0 & 2 & 1 & 0 & 2 \\ 2 & 2 & 0 & 0 & 1 & 2 \end{matrix} \right\| \tag{19}$$

coincidono rispettivamente con

$$R_1, \ldots, R_5 .$$

La verifica è immediata perchè il prodotto della matrice (19) per la matrice (16) dà, mod. 3, la matrice identica di ordine 5.

5°. Dall'esame della (19), tenendo conto della (17), si vede che per ottenere un elemento di $\mathfrak{B}$ con una sola generatrice R_j occorre un prodotto di *almeno quattro* potenze di B_j.

Quindi ogni prodotto del tipo

$$B_i^{\alpha_i}\, B_j^{\alpha_j}\, B_k^{\alpha_k}$$

contiene almeno due generatrici

6°. Eseguendo il quadrato delle matrice (16) risulta che ogni prodotto del tipo

$$B_i^{\alpha_i}\, B_k^{\alpha_k}$$

contiene almeno tre generatrici distinte.

Poniamo ora

$$A_1 = B_1 R_6 , \; A_2 = B_2 R_7 , \ldots , A_6 = B_6 R_{11}$$

e indichiamo con Q il sottogruppo di G da essi generato.

Poichè gli A_i sono indipendenti Q avrà ordine 3^6. Per dimostrare che Q soddisfa alla (15) basterà far vedere che non contiene elementi con meno di 5 generatrici: se fosse infatti con opportuni valori degli indici:

$$q R_i^{\alpha i} R_j^{\alpha j} = q' R_k^{\alpha k} R_l^{\alpha l}$$

con q e q' in Q, allora sarebbe:

$$R_i^{\alpha i} R_j^{\alpha j} R_k^{-\alpha k} R_l^{-\alpha l} = q' q^{-1}$$

cioè vi sarebbe in Q un elemento con meno di 5 generatrici.

Ma dalla definizione degli A_i e della (16) segue che ogni A_i contiene almeno 5 generatrici di cui una di indice > 5 e quattro almeno di indice ≤ 5.

Inoltre per il punto 6^0 il prodotto di due $B_i^{\alpha i}$ contiene almeno tre generatrici, per il punto 5^0 il prodotto di tre $B_i^{\alpha i}$ ne contiene almeno due e per il punto 2^0 il prodotto di quattro $B_i^{\alpha i}$ ne contiene almeno una. Dunque il prodolto di r potenze $A_i^{\alpha i}$ (con indici diversi) per $r = 2 , 3 , 4$ contiene almeno 5 generatrici diverse, di cui r con indice > 5 e almeno $5 - r$ con indice ≤ 5.

Infine il prodotto di 5 o più $A_i^{\alpha i}$ contiene 5 o più generatrici con indice > 5. Perciò il teorema è dimostrato.

Se si applica il precedente risultato alle disposizioni con ripetizione si ha il seguente:

Teorema di ripartizione a due variazioni: Fra le 3^{11} disposizioni con ripetizione di 3 oggetti della classe 11 è possibile scegliere un insieme H di 3^6 disposizioni tali che ogni altra disposizione differisce da una di H per al più due elementi.

BIBLIOGRAFIA

1. G. ZAPPA - *Reticoli e geometrie finite* Liguori, Napoli, 1952.
2. O. TAUSSKY e J. TODD - *Covering theorems for groups.* Annales de le Société Polonnaise de Mathématique, XXI, 1948.
3. E. MATTIOLI - *Sopra una particolare proprietà dei gruppi abeliani finiti.* Annali della S. N. S. di Pisa. Vol. III, 1949, pagg. 59-65.
4. » - *Sopra un'altra proprietà di gruppi abeliani finiti.* Annali della S. N. S. di Pisa, Vol V, 1951, p. 121-141.
5. » - *Sui gruppi abeliani finiti.* Annali della S. N. S. di Pisa, Vol. VI, 1952, p. 51-57.
6. S. K. ZAREMBA - *A covering theorem for Abelian groups.* J. London Math. Soc. 26, 71-72, 1951.
7. » - *Covering. problems concerning abelian groups.* J. London Math. Soc. 27, 242-246, 1952.

[*Entrato in redazione il 9-5-53*]