ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

ENNIO MATTIOLI

Teoremi di copertura dei gruppi

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 7, n^o 3-4 (1953), p. 301-309

<http://www.numdam.org/item?id=ASNSP_1953_3_7_3-4_301_0>

TEOREMI DI COPERTURA DEI GRUPPI

di ENNIO MATTIOLI (Pisa)

SOMMARIO: Si definiscono i gruppi a copertura quasi-lineare e si dimostra che tali sono i gruppi che si ottengono dal prodotto di n^k p-gruppi abeliani elementari di ordine $n = p^a$, con p numero primo ed $n > 2$. Se ne deduce una semplice legge di costruzione dei nuclei di copertura dei gruppi a copertura lineare completa (1).

1. — Si dirà che un *gruppo G è a copertura quasi-lineare* se è possibile scomporlo in sistemi formati dallo stesso numero di insiemi di ugual ordine:

$$S_1 = (H_{11}, H_{12}, \dots)$$
$$S_2 = (H_{21}, H_{22}, \dots)$$
$$\dots\dots\dots$$

aventi le seguenti proprietà:

a) ogni elemento di G compare una ed una sola volta nella scomposizione;

b) due elementi di G appartenenti ad uno stesso insieme H_{ij} differiscono fra loro per almeno tre elementi base di G;

c) due elementi di G appartenenti a due diversi insiemi $H_{i,j}$ ed $H_{i,s}$ dello stesso sistema S_i differiscono fra loro per almeno due elementi base di G;

d) tanto H_{11} quanto S_1 sono sottogruppi di G.

Dalla proprietà *a*) segue che elementi di G appartenenti ad insiemi diversi differiscono fra loro per almeno un elemento base di G.

---

(1) cfr. E. MATTIOLI, *Altri teoremi di copertura dei gruppi*. Annali della S. N. S. di Pisa, 1953, pagg. 44-51. In tale lavoro sta scritto che la dimostrazione dell'esistenza di un certo sottogruppo ciclico nell'automorfo di un p-gruppo abeliano elementare è di G. Zappa. L'Autore ha pregato di rettificare la citazione nel senso che egli, nel testo citato, si è limitato ad esporre una dimostrazione di un teorema già noto.

2. — Sia G_1 *un p-gruppo abeliano elementare* di ordine $n = p^a$ con p primo, $n > 2$. *Sia* α *un automorfismo di* G_1 *ciclico di ordine* $n-1$; α deve operare transitivamente sugli elementi di G_1 perchè se li dividesse in cicli questi dovrebbero avere ugual ordine e quindi α sarebbe di ordine $< n-1$. Perciò se R_1 è un elemento di G_1 diverso dall'identità l'espressione

$$\alpha^i R_1$$

al variare di i tra o ed $n-2$ darà tutti gli elementi di G_1 diversi dall'identità, ciascuno una volta sola.

Ricordando che α è un'automorfismo si dimostrano facilmente le seguenti relazioni:

(1) $$\alpha^i . \alpha^j R_1 = \alpha^{i+j} R_1$$

(2) $$\text{se } \alpha^i R_1 . \alpha^j R_1 = \alpha^l R_1 \quad \text{anche} \quad \alpha^{i+c} R_1 . \alpha^{j+c} R_1 = \alpha^{l+c} R_1$$

(3) $$\alpha^i R_1 . \alpha^{i+\frac{n-1}{2}} R_1 = 1$$

Nelle uguaglianze scritte gli esponenti vanno presi mod $n-1$; a secondo membro della (2) può figurare l'identità.

Consideriamo n gruppi isomorfi a G_1 e sia

$$G = G_1 G_2 \ldots G_n$$

il loro prodotto. Gli elementi dei gruppi componenti e cioè gli elementi:

$$\alpha^i R_r \qquad \begin{pmatrix} i = 0, \ldots, n-2 \\ r = 1, \ldots, n \end{pmatrix}$$

si chiameranno *elementi base di* G.

Poniamo:

(4) $$A_{rs} = \alpha^{s-1} R . \alpha^{r+s-2} R_2 . \alpha^{s-1} R_{r+2}$$

(5) $$T_s = \alpha^{s-1} R_1 . \alpha^{n-3+s} R_2$$

$$\begin{pmatrix} r = 1, \ldots, n-2 \\ s = 1, \ldots, n-1 \end{pmatrix}$$

Dalla definizione data, tenendo conto delle (2) e (3), si vede facilmente che *il prodotto di due* A_{rs} *aventi uguali il primo indice* r *è un altro* $A_{rs''}$ avente lo stesso primo indice, oppure è l'identità. Anche il prodotto di due T_s e $T_{s'}$ è un $T_{s''}$ oppure è l'identità.

Perciò tutti i possibili prodotti degli A_{rs} sono in numero di n^{n-2} e costituiscono un sottogruppo di G che indicheremo con H.

TEOREMA. *Ogni elemento di H contiene almeno tre elementi base di G.*

Ciò è vero per definizione per ogni A_{rs}. È pure vero per il prodotto di tre o più A_{rs} aventi diverso il primo indice perchè in tale prodotto figurano elementi base di almeno tre diversi gruppi G_{r+2} con indice $r+2>2$. Infine ogni prodotto del tipo $A_{rs}.A_{r's'}$ con $r \neq r'$ contiene due elementi base uno del gruppo G_{r+2} ed uno di $G_{r'+2}$; facciamo vedere che ne contiene anche almeno uno del gruppo $G_1.G_2$.

Se ciò non fosse si dovrebbe avere:

$$\alpha^{s-1} R_1 . \alpha^{s'-1} R_1 = 1$$

$$\alpha^{r+s-2} R_2 . \alpha^{r'+s'-2} R_2 = 1$$

dalle quali seguirebbe

$$\begin{aligned} s &\equiv s' + \frac{n-1}{2} \\ & \qquad\qquad (\text{mod } n-1) \\ r+s &\equiv r' + s' + \frac{n-1}{2} \end{aligned}$$

e quindi $r = r'$ contro l'ipotesi.

TEOREMA. *La scomposizione di G secondo H ed i suoi laterali è la seguente:*

$$G = H + \sum_{i,r} H.\alpha^i R_r + \sum_{s} H.T_s \qquad \begin{matrix} i = 0, \ldots, n-2 \\ r = 1, \ldots, n \\ s = 1, \ldots, n-1 \end{matrix} \tag{6}$$

Detto h un elemento generico di H le uguaglianze

$$h = \alpha^i R_r \,,\; h\,\alpha^i R_r = \alpha^{i'} R_{r'} \,,\; h = T_s \,,\; h\,T_s = T_{s'} \tag{7}$$

sono assurde perchè implicherebbero l'esistenza di un elemento di H, diverso dall'identità, contenente meno di tre elementi base.

Anche l'uguaglianza:

$$h\,\alpha^i R_r = T_{s'} \tag{8}$$

è assurda. Infatti non può essere $r \leq 2$ perchè si avrebbe un h con due soli elementi base. Supposto perciò $r > 2$ la (8) può essere riscritta nella se-

guente forma:

$$h\,\alpha^i R_{r+2} = T_{s'} \tag{8'}$$

con $0 < r \leq n-2$.

Perchè la (8') sia soddisfatta h deve coincidere con l'A_{rs} il cui indice s è legato ad i dalla relazione:

$$s - 1 \equiv i + \frac{n-1}{2} \pmod{n-1}$$

e inoltre, con detto valore di s, deve essere:

$$\alpha^{s-1} R_1 \cdot \alpha^{r+s-2} R_2 = \alpha^{s'-1} R_1 \cdot \alpha^{n-3+s'} R_2 . \tag{9}$$

Ma dalla (9) seguirebbe $s = s'$, $r \equiv 0 \pmod{n-1}$ e ciò è assurdo perchè r varia tra 1 ed $n-2$.

Dunque gli elementi che compaiono a secondo membro della (6) sono tutti distinti e poichè il loro numero è:

$$n^{n-2}[1 + n(n-1) + (n-1)] = n^n$$

essi esauriscono G.

3. — TEOREMA. *Il gruppo G definito nel precedente numero è un gruppo a copertura quasi-lineare.*

Poniamo

$$H_{11} = H\,,\ H_{1s} = H\,T_{s-1} \qquad (s = 2, \ldots, n) \tag{10}$$

$$S_1 = (H_{11}, H_{12}, \ldots, H_{1n}) . \tag{11}$$

In base alla (6) possiamo affermare che H_{11} è un sottogruppo di G i cui elementi differiscono fra loro per almeno tre elementi base. Per la definizione (10) anche gli H_{1s} godono della stessa proprietà.

Il prodotto di due T_s è un altro T_s o è l'identità, perciò anche S_1 è un sottogruppo di G. Facciamo vedere che due elementi di G appartenenti rispettivamente ad H_{1s} ed $H_{1s'}$ con $s \neq s'$ differiscono fra loro per almeno due elementi base di G. Infatti, se ciò non fosse, si dovrebbe verificare, con notazioni evidenti, una delle seguenti relazioni:

$$h\,T_{s-1} = h'\,T_{s-1}\,,\ h\,T_{s-1}\cdot\alpha^i R_r = h'\,T_{s'-1}\,,\ h\,T_{s-1}\cdot\alpha^i\,R_r = h'\,; \tag{12}$$

ma queste sono assurde perchè si riconducono immediatamente alle forme (7) od (8).

Vale per G la seguente scomposizione:

$$G = S_1 + \sum_{i=0}^{n-2} S_1 \cdot \alpha^i R_t \tag{13}$$

per qualunque valore prefissato di t (compreso fra 1 ed n).

Infatti le uguaglianze:

$$h\, T_{s-1} \cdot \alpha^i R_t = h'\, T_{s'-1}\,,\; h\, T_{s-1} \cdot \alpha^i R_t = h'\, T_{s'-1}\, \alpha^{i'} R_t$$

sono assurde perchè si riducono facilmente alla forma (8). Pertanto gli elementi a secondo membro della (13) sono tutti distinti e poichè il loro numero è n^n essi esauriscono G.

Poniamo

$$S_r = S_1 \cdot \alpha^{r-2} R_1 \tag{14}$$

quindi

$$H_{rs} = H_{1s} \cdot \alpha^{r-2} R_1 \cdot \qquad \begin{matrix} r = 2, \ldots, n \\ s = 1, \ldots, n \end{matrix}$$

Ogni H_{rs} gode della proprietà di H_{11} (escluso il fatto di essere un gruppo). Ogni S_r gode della proprietà di S_1 (escluso il fatto di essere un gruppo).

Dunque *i sistemi* $S_1, \ldots, S_n$ *costituiscono i sistemi di copertura quasi-lineare di* G.

Gli H_{rs} coincidono, a meno dell'ordine, coi laterali di H dentro G.

Osserviamo che, considerando gli H_{1s} come elementi, S_1 è un gruppo di ordine n isomorfo a G_1; e, considerando gli S_r come elementi, G risulta un gruppo di ordine n, pure isomorfo a G_1.

4. — TEOREMA. *Ogni gruppo che si ottenga come prodotto di n^k p-gruppi abeliani elementari uguali a G_1 è un gruppo a copertura quasi-lineare, e precisamente si può dividerlo in n sistemi, formati ciascuno di n^k insiemi di ordine*

$$n^{n^k - k - 1} \tag{15}$$

aventi le proprietà enunciate nel n° 1.

Il teorema è già stato dimostrato per $k = 1$. Procediamo per induzione: per semplicità di notazioni supporremo il teorema valido per l'intero k e lo dimostreremo per l'intero $k + 1$. Posto

$$N = n^k\,,$$

sia $G^{(k)}$ il gruppo $G_1 G_2 \dots G_N$ e siano

$$S_1^{(k)}, S_2^{(k)}, \dots, S_n^{(k)}$$

i suoi sistemi di copertura quasi-lineare, con

$$S_r^{(k)} = (H_{r1}^{(k)}, \dots, H_{rN}^{(k)}) \qquad (r = 1, \dots, n)$$

Ogni $S_r^{(k)}$ avrà ordine n^{N-1} ed ogni $H_{rs}^{(k)}$ avrà ordine n^{N-k-1}. Il gruppo $G^{k+1)}$ si può pensare ottenuto *moltiplicando fra loro N gruppi di tipo* $G^{(1)} = G$.

Sia $H_{i_s j_s}$ uno degli insiemi di copertura dell's.mo di questi gruppi $G^{(1)}$. Sarà $s = 1, \dots, N$ e gli indici i_s, j_s saranno interi compresi fra 1 ed n. Consideriamo tutti i possibili prodotti

$$H_{i_1 j_1} . H_{i_2 j_2} \dots H_{i_N j_N} \tag{16}$$

Poichè gli $H_{i_s j_s}$ eseuriscono l's.mo $G^{(1)}$ gli elementi ottenuti dai prodotti (16) esauriranno $G^{(k+1)}$.

Sia

$$\alpha^{u_1} R_1 . \alpha^{u_2} R_2 \dots \alpha^{u_N} R_N \tag{17}$$

un elemento generico di $H_{11}^{(k)}$ e

$$\alpha^{v_1} R_1 . \alpha^{v_2} R_2 \dots \alpha^{v_N} R_N \tag{18}$$

un elemento generico di $S_1^{(k)}$. Eventualmente al posto di qualche $\alpha^{u_t} R_t$ o $\alpha^{v_t} R_t$ potrà esservi l'identità.

In virtù dell'isomorfismo che esiste tra gli insiemi $H_{11}, H_{12}, \dots, H_{1n}$ e G_1, e dell'isomorfismo che esiste fra i sistemi $S_1, S_2, \dots, S_n$ ed il gruppo G_1, ad ogni coppia di elementi (17) e (18) possiamo far corrispondere un prodotto (16) con la convenzione che l'insieme $H_{i_s j_s}$ sia individuato dall'indice i_s dell'insieme $H_{1 i_s}$ che corrisponde ad $\alpha^{u_s} R_s$ e dall'indice j_s del sistema S_{j_s} che corrisponde ad $\alpha^{v_s} R_s$ (negli isomorfismi riguardanti l's-mo gruppo di tipo $G^{(1)}$).

I prodotti che si ottengono dalla (16) con questa convenzione *formano gruppo* perchè tanto $H_{11}^{(k)}$ quanto $S_1^{(k)}$ sono gruppi. Indichiamo questo gruppo con $H_{11}^{(k+1)}$. Il suo ordine:

$$(n^{n-2})^N . n^{N-k-1} . n^{N-1} = n^{n^{k+1}-(k+1)-1}$$

soddisfa alla (15) scritta per l'esponente $k + 1$.

Gli elementi di $H_{11}^{(k+1)}$ *differiscono fra loro per almeno tre elementi base di* $G^{(k+1)}$. Ciò è vero per tutti gli elementi generati da uno stesso prodotto (16) perchè tale proprietà vale per ciascun fattore $H_{i_s j_s}$.

Se due elementi provengono da due prodotti (16) corrispondenti alla medesima successione dei primi indici, avremo una differenza di almeno due indici nelle successioni dei secondi indici (successioni generate da due elementi di $S_1^{(k)}$); quindi per la proprietà degli H_{rs} i due elementi considerati differiscono fra loro per almeno due elementi base di $G^{(k+1)}$).

Se due elementi provengono da due prodotti (16) aventi diverse le successioni dei primi indici essi differiranno per almeno tre elementi base perchè le successioni dei primi indici differiscono di almeno tre indici (sono generate da due diversi elementi di $H_{11}^{(k)}$).

Scriveremo simbolicamente:

$$H_{11}^{(k+1)} = f(H_{11}^{(k)}, S_1^{(k)}).$$

Costruiamo in modo analogo:

$$H_{1,(r-1)n+s}^{(k+1)} = f(H_{1r}^{(k)}, S_s^{(k)}) \qquad \begin{matrix} r = 1, \ldots, N \\ s = 1, \ldots, n \end{matrix}$$

Al variare degli indici r ed s *si ottengono* n^{k+1} *insiemi in ciascuno dei quali due elementi qualunque differiscono fra loro per almeno tre elementi base di* $G^{(k+1)}$.

Dimostriamo che due elementi appartenenti a diversi $H^{(k+1)}$ differiscono fra loro per almeno due elementi base. Consideriamo due elementi h ed h' appartenenti rispettivamente ai due sistemi:

$$(19) \qquad H_{1,(r-1)n+s}^{(k+1)}, \; H_{1,(r'-1)n+s'}^{(k+1)}$$

diversi fra loro.

Se $r = r'$ dovrà essere $s \neq s'$. Nei due prodotti (16) che generano rispettivamente h ed h' le successioni dei primi indici provengono in entrambi i casi da $H_{1r}^{(k)}$ perciò possono essere uguali o differire di almeno tre indici. Nella seconda eventualità h ed h' differiranno di almenò tre elementi base. Nella prima eventualità potremo essere certi che le successioni dei secondi indici differiscono fra loro di almeno un indice (esse provengono rispettivamente da $S_s^{(k)}$ ed $S_{s'}^{(k)}$); ma allora nei prodotti che generano h ed h' vi sarà ad un certo posto t un $H_{i_t j_t}$ e un $H_{i_t j'_t}$ rispettivamente, *aventi uguali il primo indice e diverso il secondo.* Perciò h ed h' differiscono fra loro per almeno due elementi base.

Se $r \neq r'$ le successioni dei primi indici, nei prodotti (16) che generano h ed h', differiranno di almeno due indici (provengono da $H_{1r}^{(k)}$ e $H_{1r'}^{(k)}$; perciò h ed h' differiranno di almeno due elementi base.

Scriviamo simbolicamente:

$$S_1^{(k+1)} = (H_{11}^{(k+1)}, \ldots, H_{1n^{k+1}}^{(k+1)}) = f(S_1^{(k)}, G^{(k)}),$$

S_1 sarà un gruppo perchè tali sono $S_1^{(k)}$ e $G^{(k)}$.

Costruiamo in modo analogo i sistemi:

$$S_r^{(k+1)} = f(S_r^{(k)}, G_r^{(k)}) \qquad r = 1, \ldots, n.$$

Essi godono le stesse proprietà di $S_1^{(k+1)}$, salvo quella di essere un gruppo: perciò costituiscono il sistema di copertura quasi-lineare di $G^{(k+1)}$.

5. — TEOREMA DI RIPARTIZIONE DELLE DISPOSIZIONI.

Le disposizioni con ripetizione di n oggetti della classe n^k, con n potenza di un numero primo ed $n > 2$, si possono suddividere in n sistemi contenenti ciascuno n^k insiemi aventi le proprietà che:

a) due disposizioni di uno stesso insieme differiscono fra loro per almeno tre oggetti;

b) due disposizioni di due diversi insiemi di uno stesso sistema differiscono fra loro per almeno due oggetti.

Per la dimostrazione basta applicare il gruppo $G^{(k)}$ alle disposizioni con ripetizione degli n oggetti nel modo indicato in (2).

Si noti che il ragionamento del n°. 4 si può applicare direttamente alle disposizioni; in tal caso le successioni dei primi indici e dei secondi indici dei prodotti (16) saranno disposizioni con ripetizione, della classe N, degli interi da 1 ad n.

6. — TEOREMA DI COPERTURA LINEARE COMPLETA.

Posto

$$m = \sum_{e=0}^{k} n^e$$

il gruppo ${}_kG$ *ottenuto dal prodotto di* m *p-gruppi abeliani elementari del tipo* G_1 *ammette la copertura lineare completa.*

---

(2) E. MATTIOLI. *Sopra una particolare proprietà dei gruppi abeliani finiti.* Annali della S. N. S. di Pisa, 1949, p. 62.

Il teorema è già stato dimostrato per altra via [3]; ma la presente dimostrazione ha il vantaggio di *consentire una semplice costruzione del nucleo di copertura mediante un procedimento di induzione.*

Per $k = 1$ il teorema è immediato. Posto infatti

$$\Gamma = H_{11} + \sum_{i=2}^{n} H_{1i} \cdot \alpha^{i-2} R_{n+1}$$

Γ sarà un sottogruppo di ${}_1G = G_1 G_2 \dots G_{n+1}$; il suo ordine è n^{n-1} e i suoi elementi differiscono fra loro per almeno tre elementi base (ciò segue subito dalle proprietà degli H_{1i}). Pertanro Γ è il nucleo di copertura di ${}_1G$.

Procediamo per induzione supponendo il teorema già dimostrato per l'intero $k-1$ e dimostriamolo per l'intero k. Sia ${}_{k-1}G$ il gruppo ottenuto dal prodotto di $1 + n + n^2 + \dots + n^{k-1}$ gruppi del tipo G_1; e siano

$$\Gamma_1 = \Gamma, \Gamma_2, \dots, \Gamma_{n^k}$$

i laterali del suo nucleo di copertura Γ ordinati in isomorfismo con gli $H_{1i}^{(k)}$. Moltiplichiamo ordinatamente questi insiemi per

$$H_{11}^{(k)}, H_{12}^{(k)}, \dots, H_{1n^k}^{(k)}$$

e sommiamo i prodotti ottenuti. In questo modo si ottengono

$$n^{1+n+\dots+n^{k-1}-k} \cdot n^{n^k-k-1} \cdot n^k = n^{1+n+\dots+n^h-(k+1)}$$

elementi di un gruppo che costituisce il nucleo di copertura del gruppo ${}_kG = {}_{k-1}G \cdot G^{(k)}$. Infatti dalle proprietà dei Γ_r e degli $H_{1s}^{(k)}$ segue subito che gli elementi generati differiscono fra loro per almeno tre elementi base di ${}_kG$.

---

[3] cfr. S. K. ZAREMBA, *Covering problems concerning abelian groups*, J. London Math. Soc., 27, 1952, 242-246.

cfr. inoltre nota [1].