ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

ENNIO MATTIOLI

Sopra una particolare proprietà dei gruppi abeliani finiti

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 3, n^o 1-4 (1950), p. 59-65

<http://www.numdam.org/item?id=ASNSP_1950_3_3_1-4_59_0>

SOPRA UNA PARTICOLARE PROPRIETÀ DEI GRUPPI ABELIANI FINITI

di ENNIO MATTIOLI (Pisa)

PREFAZIONE. — Viene qui presentata una nuova proprietà dei gruppi abeliani finiti. Si dimostra, precisamente, che se G è un gruppo abeliano di tipo $(1, \ldots, 1)$ e ordine p^n, con p primo ed $n = \dfrac{p^k - 1}{p - 1}$, ($k$ intero ≥ 2), data una base $R_1, \ldots, R_n$ di G, si può trovare un sottogruppo Γ di G tale che ciascuno dei laterali di Γ rispetto a G contenga uno ed uno solo degli elementi $R_1, \ldots, R_1^{p-1}, R_2, \ldots, R_2^{p-1}, R_n \ldots, R_n^{p-1}$.

Questo risultato è sorto da applicazioni matematiche ai giochi del Totocalcio e Totip [1] che io espongo nel n. 2. Al n. 3 dò un'altra interessante applicazione al gioco del lotto.

1. — Sia G un gruppo abeliano d'ordine p^n e tipo $(1, \ldots, 1)$ e siano $R_1, \ldots, R_n$ gli elementi di una sua base. Chiameremo $R_1, \ldots, R_n$ *generatrici*.

Dimostriamo il seguente:

TEOREMA. — *Se il numero* n *è della forma*

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

essendo k *un numero intero* ≥ 2, *è possibile trovare in* G *un sottogruppo* Γ *di ordine* p^{n-k} *tale che la scomposizione di* G *secondo* Γ *ed i suoi laterali si possa effettuare nella forma:*

$$G = \Gamma + \Gamma R_1 + \ldots \Gamma R_1^{p-1} + \Gamma R_2 + \Gamma R_2^2 + \ldots + \Gamma R_n^{p-1}. \tag{2}$$

---

[1] Si tratta dei sistemi ormai noti nei giochi con totalizzatore col nome di sistemi ridotti a « undici certo » Malgrado la difficoltà delle ricerche bibliografiche su tale argomento ritengo che il primo lavoro pubblicato in proposito sia l'opuscolo « Regolo Combinatorio » (Tipografia B. Giordano — Pisa — 1948) da me compilato in collaborazione col collega prof. L. Cernigliaro, al quale porgo i miei ringraziamenti per aver richiamato la mia attenzione sull'argomento.

Osserviamo anzitutto che per la (2) l'indice di Γ deve essere

$$n(p \quad 1) + 1$$

e quindi il prodotto di tale numero per l'ordine p^{n-k} di Γ deve uguagliare l'ordine di G; ciò è vero se è soddisfatta la (1). Infatti in tal caso si à:

$$p^{n-k}\left[n(p-1)+1\right] = p^{n\ k}\left[\frac{p^k-1}{p-1}(p-1)+1\right] = p^n .$$

Consideriamo il gruppo di ordine p^k generato dalle prime k generatrici

$$R_1, \ldots, R_k .$$

Togliamo da tale gruppo l'identità e gli elementi che contengono una sola generatrice. Rimarrà un insieme θ formato da

$$m = p^k - 1 - k(p-1) \tag{3}$$

elementi, avente la proprietà che *le potenze di una qualunque operazione di* θ, *con esponente compreso fra* 1 *e* p $-$ 1, *appartengono ancora a* θ.

Scelto un qualunque elemento B_1 di θ le sue $p-1$ potenze, dalla prima alla $(p-1)^{ma}$, appartengono dunque a θ e sono distinte fra loro. Un secondo elemento B_2 di θ diverso dalle potenze di B_1 à le sue prime $(p-1)$ potenze tutte distinte da quelle di B_1, se fosse infatti, con certi x_1 e x_2 compresi fra 1 e $p-1$:

$$B_1^{x_1} = B_2^{x_2}$$

detto x_2' il numero per cui

$$x_2 x_2' \equiv 1 \qquad \text{mod } p$$

si avrebbe

$$B_1^{x_1 x_2'} = B_2^{x_2 x_2'} = B_2$$

cioè B_2 sarebbe tra le potenze di B_1 contro l'ipotesi.

Analogamente un terzo elemento B_3 di θ, distinto dalle potenze di B_1 e di B_2, avrà tutte le sue potenze distinte da quelle di B_1 e di B_2. Così procedendo potremo scegliere

$$\frac{m}{p-1}$$

elementi di θ in modo che *le loro prime* p $-$ 1 *potenze siano tutte distinte fra loro ed esauriscano* θ : diremo che essi formano una *base* di θ.

Si verifica facilmente che a causa della (3) e della (1) risulta:

$$\frac{m}{p-1} = n - k.$$

Escludendo il caso, privo di interesse, di $p = 2$ e $k = 2$ è sempre $n - k \geq 3$.

Indichiamo con:

$$B_1, B_2, \ldots, B_{n-k}$$

una base di θ, e con B il generico di essi.

Consideriamo ora gli $n - k$ elementi di G che si ottengono moltiplicando ordinatamente i B per $R_{k+1}, R_{k+2}, \ldots, R_n$; poniamo cioè

$$A_1 = B_1 R_{k+1}, A_2 = B_2 R_{k+2}, \ldots, A_{n-k} = B_{n-k} B_n.$$

Il sottogruppo Γ generato dagli elementi $A_1, A_2, \ldots, A_{n-k}$ soddisfa alla (2).

Intanto Γ è di ordine p^{n-k} perchè $A_1, \ldots, A_{n-k}$ sono indipendenti. Se fosse infatti

$$A_1^{x_1} \ldots A_{n-k}^{x_{n-k}} = 1,$$

sarebbe

$$B_1^{x_1} \ldots B_{n-k}^{x_{n-k}} \cdot R_{k+1}^{x_1} \ldots R_n^{x_{n-k}} = 1$$

cioè, essendo $R_{k+1}, \ldots, R_n$ indipendenti da $R_1, \ldots, R_k$ e quindi anche da $B_1, \ldots, B_{n-k}$,

$$B_1^{x_1} \ldots B_{n-k}^{x_{n-k}} = R_{k+1}^{x_1} \ldots R_n^{x_{n-k}} = 1$$

il che è assurdo.

Per far vedere che vale la (2) basterà dimostrare che in Γ non vi sono elementi contenenti una sola o due generatrici distinte. Infatti se fosse

$$\gamma R_i^{x_i} = \bar{\gamma} R_j^{x_j}$$

(γ e $\bar{\gamma}$ in Γ; x_i e $x_j < p$; $i \neq j$ oppure $i = j, x_i \neq x_j$) si avrebbe

$$\bar{\gamma}^{-1} \gamma = R_j^{x_j} R_i^{-x_i},$$

cioè esisterebbe un elemento di Γ contenente al più due generatrici distinte.

Tenendo presente che ogni B contiene almeno due generatrici segue dalla definizione stessa delle A che *ogni elemento* A, *ed ogni sua potenza* diversa dall'identità, *contiene almeno tre generatrici* di cui una di indice maggiore di k e almeno due di indice minore o uguale a k.

In secondo luogo non può essere $B_i^{x_i} B_j^{x_j} = 1$ con $i \neq j$, e $x_i < p$; $x_j < p$, altrimenti sarebbe $B_i^{x_i} = B_j^{-x_j}$, mentre le B sono state costruite in modo da non avere potenze di esponente $< p$ a comune. Dunque il prodotto di due potenze di B, di esponente $< p$ contiene almeno una generatrice, perciò *il prodotto di due elementi* A *o di loro potenze contiene almeno tre generatrici* di cui due di indice $> k$ ed una almeno di indice $\leq k$.

Infine è evidente che *un prodotto di tre elementi* A *distinti*, o di loro potenze, *contiene almeno tre generatrici,* di cui tre di indice $> k$, e un prodotto contenente più di tre elementi A, o di loro potenze, contiene più di tre generatrici di indice $> k$.

Dunque il sottogruppo Γ generato dalle A non possiede elementi contenenti meno di tre generatrici e la (2) è dimostrata.

Nei paragrafi 2 e 3 daremo due applicazioni del precedente teorema.

2. — *Se* n *soddisfa alla* (1), *con* p *numero primo e* k *intero* ≥ 2, *tra le* p^n *disposizioni con ripetizione di* p *oggetti della classe* n *è possibile sceglierne un insieme* H *di* p^{n-k} *tale che ogni altra disposizione differisca da una di quelle per un solo elemento.*

Siano $h_1, h_2, \ldots, h_p$, p oggetti distinti. Consideriamo tutte le p^n disposizioni con ripetizione di classe n che si possono formare con essi. Indicheremo, per maggior chiarezza, l'oggetto h_i rispettivamente coi simboli

$$h_{i_1}, h_{i_2}, \ldots, h_{i_n}$$

a seconda che lo consideriamo, in una data disposizione, al primo, al secondo, ..., all'n-esimo posto. Ciascuna disposizione può allora scriversi così:

$$h_{i_1,1}, h_{i_2,2}, \ldots, h_{i_n,n}$$

dove $i_1, \ldots, i_n$ è una disposizione con ripetizione di classe n dei numeri $1, \ldots, p$.

Chiamiamo R_j il ciclo

$$(h_{1,j}, h_{2,j}, \ldots, h_{p,j}).$$

Gli elementi $R_1, \ldots, R_n$ sono evidentemente permutabili, e indipendenti, perchè operano su simboli diversi: inoltre ànno ciascuno periodo p. Pertanto essi generano un gruppo G d'ordine p^n, isomorfo a quello del n. precedente.

Chiamiamo disposizione fondamentale la seguente

$$h_{11}, h_{12}, \ldots, h_{1n}.$$

È evidente che, applicando alla disposizione fondamentale le sostituzioni del gruppo G, si ottengono tutte le disposizioni con ripetizione di classe n sui p oggetti dati.

Poichè per ipotesi n soddisfa alla (1) costruiamo il sottogruppo Γ di cui al n. precedente. *L'insieme* H *delle disposizioni che si ottengono applicando le sostituzioni di* Γ *alla disposizione fondamentale* coincide con l'insieme H di cui all'enunciato. Infatti ogni altra disposizione si ottiene applicando alla fondamentale una delle sostituzioni di G contenute nei laterali di Γ; tenendo presente la (2) risulta cioè che ogni altra disposizione si à da una disposizione di H cambiando un oggetto in uno solo degli n posti. E l'asserzione è dimostrata.

Questa proprietà si può utilizzare in quei *giochi con totalizzatore* nei quali vengono premiati non solo i giocatori che totalizzano il massimo punteggio, ma anche coloro che realizzano un punto di meno del massimo.

Se le partite da pronosticare sono n e consideriamo come p oggetti i possibili risultati di una partita, il numero complessivo dei pronostici uguaglia le disposizioni con ripetizione dei p oggetti della classe n. Se n soddisfa alla (1) un giocatore può limitarsi a giocare le disposizioni dell'insieme H con la certezza di realizzare o il punteggio massimo o il punteggio inferiore al massimo di una sola unità.

A titolo di esempio consideriamo il caso $p = 3$, $n = 4$. La (1) risulta soddisfatta con $k = 2$. Se, per usare simboli assai in voga, indichiamo con 1, X, 2 i possibili risultati di una partita avremo:

1^0 i possibili pronostici sulle 4 partite formano le disposizioni con ripetizione della classe 4 dei tre simboli 1, X, 2; sono perciò in numero di $3^4 = 81$;

2^0 in base al teorema del presente paragrafo è possibile scieglierne $p^{n-k} = 3^{4-2} = 9$ in modo che ognuna delle 72 rimanenti differisca da una di esse per un solo elemento: perciò il giocatore che punti sopra quelle 9 disposizioni è certo di realizzare almeno 3 punti su 4.

Le 9 disposizioni si ottengono costruendo per questo caso il sottogruppo Γ.

Poniamo

$$B_1 = R_1 R_2 \qquad B_2 = R_1^2 R_2$$

quindi

$$A_1 = R_1 R_2 R_3 \qquad A_2 = R_1^2 R_2 R_4 .$$

Il sottogruppo Γ generato dalla base A_1, A_2 contiene i seguenti 3^2 elementi:

$$1 \quad , \quad A_1 = R_1 R_2 R_3 \ , \ A_1^2 = R_1^2 R_2^2 R_3^2$$

$$A_2 = R_1^2 R_2 R_4 \ , \ A_1 A_2 = R_2^2 R_3 R_4 \ , \ A_1^2 A_2 = R_1 R_3^2 R_4$$

$$A_2^2 = R_1 R_2^2 R_4^2 \ , \ A_1 A_2^2 = R_1^2 R_3 R_4^2 \ , \ A_1^2 A_2^2 = R_2 R_3^2 R_4^2 .$$

Applicando alla disposizione fondamentale

1 1 1 1

le sostituzioni di Γ si ottiene l'insieme H delle 9 disposizioni cercate:

1 1 1 1 .	X X X 1 .	2 2 2 1 .
2 X 1 X ,	1 2 X X .	X 1 2 X .
X 2 1 2 ,	2 1 X 2 ,	1 X 2 2 .

È facile verificare che ognuna delle rimanenti 72 disposizioni differisce da una di queste per un solo elemento.

3. — *Se* n *è della forma*

$$n = 2^k - 1 \tag{4}$$

con $k \geq 2$ *fra gli* $\binom{n}{3}$ *terni che si possono formare coi numeri interi da* 1 *ad* n *è possibile sceglierne* $\frac{1}{3}\binom{n}{2}$ *in modo che ogni ambo figuri in essi una e una sola volta.*

Infatti se il numero n è della forma 4 soddisfa alla (1) con $p = 2$, perciò si può costruire il sottegruppo Γ. Gli *elementi di* Γ *formati con tre generatrici* danno, coi loro indici, i terni richiesti.

Difatti ogni elemento di G contenente due generatrici non potendo stare in Γ si troverà in qualche laterale: dunque in Γ vi sarà un elemento, necessariamente di tre generatrici, da cui esso differirà soltanto per la 3ª generatrice. Ne segue che ogni ambo è contenuto in uno dei terni.

D'altra parte due elementi di Γ formati da tre generatrici non possono avere due generatrici comuni, perchè il loro prodotto, che sta in Γ, conterrebbe due sole generatrici; ne segue che i terni non possono avere un ambo comune, e il teorema è dimostrato.

Ad es. per $k = 3$ si à dalla (4)

$$n = 2^3 - 1 = 7 .$$

Posto

$$B_1 = R_1 R_2 , \quad B_2 = R_1 R_3 , \quad B_3 = R_2 R_3 , \quad B_4 = R_1 R_2 R_3$$

e quindi

$$A_1 = R_1 R_2 R_4 , \quad A_2 = R_1 R_3 R_5 , \quad A_3 = R_2 R_3 R_6 , \quad A_4 = R_1 R_2 R_3 R_7 ,$$

il sottogruppo Γ consta delle $2^{7-3} = 16$ sostituzioni:

1, $R_1 R_2 R_4$, $R_1 R_3 R_5$, $R_2 R_3 R_1 R_5$, $R_2 R_3 R_6$ $R_1 R_3 R_4 R_5$, $R_1 R_2 R_5 R_6$, $R_4 R_5 R_6$, $R_1 R_2 R_3 R_7$, $R_3 R_1 R_7$, $R_2 R_5 R_7$, $R_1 R_4 R_5 R_7$, $R_1 R_6 R_7$, $R_2 R_4 R_6 R_7$, $R_3 R_5 R_6 R_7$, $R_1 R_2 R_3 R_4 R_5 R_6 R_7$.

I terni richiesti sono:

$$(124)\ (135)\ (236)\ (456)\ (347)\ (257)\ (167)$$

ed è facile verificare che ogni ambo vi è contenuto una ed una sola volta.

[*Pervenuta alla Redazione il 25-10-49*]