LUIGI ANTONIO ROSATI

Sulle *S*-partizioni nei gruppi non abeliani d'ordine *pq*

Rendiconti del Seminario Matematico della Università di Padova, tome 38 (1967), p. 108-117

<http://www.numdam.org/item?id=RSMUP_1967__38__108_0>

SULLE S-PARTIZIONI NEI GRUPPI NON ABELIANI D'ORDINE pq

LUIGI ANTONIO ROSATI *)

Recentemente alcuni problemi sui piani grafici hanno messo in luce l'opportunità di generalizzare il concetto di partizione, introducendo quello di S-partizione di un gruppo rispetto ad un suo sottogruppo S [1, 3]. Lo studio delle S-partizioni dei gruppi finiti è stato oggetto di due lavori di G. ZAPPA, il primo [4] dedicato allo studio delle S-partizioni di HALL di un gruppo finito, il secondo [5] dedicato principalmente allo studio delle S-partizioni strette di un gruppo finito qualunque e delle S-partizioni semistrette dei gruppi finiti supersolubili. Il problema della determinazione delle S-partizioni non semistrette è stato affrontato dallo ZAPPA soltanto per un gruppo non abeliano G d'ordine pq (p, q primi ; $p > q$) e nell'ipotesi $|S| = q$. Precisamente in [5] G. ZAPPA ha trovato che G ammette una tale S-partizione solo se $p \equiv 1 \pmod{q^2 - q}$ ed ha ricondotto il problema dell'esistenza di una S-partizione non semistretta di G alla possibilità di decomporre un gruppo ciclico R d'ordine $p - 1$ in un prodotto $R = M \times N$ di tipo di HAJOS, essendo M un dato sottoinsieme di R. Dal lavoro [5] di ZAPPA segue anche che se $q = 2, 3$ la condizione $p \equiv 1 \pmod{q^2 - q}$ è sufficiente perchè G ammetta una S-partizione non semistretta.

In questa nota si caratterizzano i numeri primi p per cui esiste un gruppo non abeliano G d'ordine $5p$ ($p > 5$) che ammette una

*) Indirizzo dell'A. : Istituto matematico dell'Università di Modena.

S-partizione non semistretta, essendo S un 5-sottogruppo di SYLOW di G.

Si dà inoltre una condizione necessaria e sufficiente perchè un gruppo non abeliano G d'ordine pq (p, q primi) con $p = q(q-1)+1$ ammetta una S-partizione non semistretta, essendo S un q-sottogruppo di SYLOW di G.

1. Dati un gruppo G ed un suo sottogruppo S, dicesi *S-partizione* di G un insieme Π di sottogruppi di G tale che ogni elemento di G non appartenente ad S appartenga ad uno ed uno solo dei complessi SH ($H \in \Pi$). Una S-partizione di un gruppo finito G viene detta *semistretta* se, per ogni $H \in \Pi$, si ha $|S \cap H| = (|S|, |H|)$ e *non semistretta* in caso contrario.

Dati tre sottoinsiemi R, M, N di un gruppo abeliano A, scriveremo $R = M \times N$ se e solo se ogni elemento di R si ottiene in un modo solo come prodotto di un elemento di M per un elemento di N.

Diremo poi che N è periodico se esiste un elemento $g \in A$ tale che si abbia $gN = N$; l'elemento g verrà detto un periodo di N. È chiaro che un sottoinsieme N di un gruppo abeliano A è periodico se e solo se $N = C \times K$, dove C è un sottogruppo ciclico di A e K un sistema completo di rappresentanti di N mod C (N risulta costituito da un insieme di laterali di C).

G. ZAPPA ha dimostrato il seguente teorema [5]

a) *Sia G un gruppo non abeliano d'ordine pq, con p, q primi, $p > q$ e sia S un q-sottogruppo di Sylow di G. Allora, se G ammette una S-partizione Π non semistretta, è* $p \equiv 1 \pmod{q^2 - q}$.

Sia dunque G un gruppo non abeliano d'ordine pq, con p, q primi e $p \equiv 1 \pmod{q^2 - q}$ e sia S un suo q-sottogruppo di SYLOW. Sempre di G. ZAPPA è il seguente teorema [5]:

b) *G ammette una S-partizione Π non semistretta se, e solo se, detto R il gruppo moltiplicativo del campo, F, d'ordine p, esiste un elemento $x \in R$ d'ordine q tale che, posto*

$$M = \{1, 1 + x, \ldots, 1 + x + \ldots + x^{q-2}\}$$

si abbia $R = M \times N$, essendo N un opportuno sottoinsieme di R.

Supponiamo ora $q = 5$. Vogliamo dimostrare che

1. *Se esiste un insieme N di elementi $b_i \in R$ $(i = 1, \dots, (p-1)/4)$ tale che si abbia $R = M \times N$, allora N è periodico ed x è un suo periodo.*

Posto $a_i = x^0 + \dots + x^{i-1}$ $(i = 1, \dots, 4)$, otteniamo che, se A è un sottogruppo di R tale che gli elementi di R/A $\bar{a}_1 = a_1 A$, $\bar{a}_2 = a_2 A$, $\bar{a}_3 = a_3 A$, $\bar{a}_4 = a_4 A$ siano distinti, allora l'insieme $\bar{M}$ da essi formato è periodico se e solo se A contiene il sottogruppo X di R generato da x. Infatti si ha

$$a_3 = -x^3 a_2 , \qquad a_4 = -x^4 ;$$

perciò, se $A \supseteq X$, $\bar{M}$ è periodico di periodo $-1.A$.

Viceversa, supposto $\bar{M}$ periodico, si potrà ammettere che un suo periodo $\bar{g}$ abbia ordine $2 : \bar{g}^2 = \bar{1}$. Poichè esiste un intero i, $2 \leq i \leq 4$, tale che si abbia $\bar{a}_i \bar{g} = \bar{1}$, risulterà $\bar{g} = \bar{a}_i (2 \leq i \leq 4)$. Supponiamo $\bar{g} = \bar{a}_2 = a_2 A$. Allora $\bar{a}_2 \bar{a}_3 = \bar{1}$, oppure $\bar{a}_2 \bar{a}_3 = \bar{a}_4$; nel primo caso si ha $-x^3 \in A$, $x \in A$; nel secondo caso $-x^3 A = -x^4 A$ e ancora $x \in A$. Alla stessa conclusione si giunge nei casi $\bar{g} = \bar{a}_3$, $\bar{g} = \bar{a}_4$.

In particolare quindi M non è periodico. Ora R è ciclico ed il numero degli elementi di M è potenza di un numero primo. Da un risultato di A. D. Sands [2] segue allora che N è periodico. Sia g un periodo d'ordine massimo, t, di N. Indicato con A il sottogruppo di R generato da g, si ha $N = A \times K$, essendo $K = \{k_j\}$ $(j = 1, \dots, (p-1)/4t)$ un sistema completo di rappresentanti dei laterali di A contenuti in N. Quindi $R = M \times (A \times K)$ o anche, posto $B = M \times K$, $R = A \times B$, essendo B un sistema completo di rappresentanti dei laterali di A in R.

Ora $B = M \times K = \{a_i k_j\}$ $(i = 1, \dots, 4; j = 1, \dots, (p-1)/4t)$, perciò, posto $\bar{M} = \{a_i A\}$, $\bar{K} = \{k_j A\}$, risulta

$$G/A = \bar{M} \times \bar{K} ,$$

e poichè il numero degli elementi di $\bar{M}$ è una potenza di un numero primo, sempre per il citato teorema di Sands, si ha che $\bar{M}$ è periodico oppure lo è $\bar{K}$.

Supponiamo che $\bar{K}$ sia periodico: $\bar{K} = \{d_i z^j A\}$, con $j = 1, \dots, c$, essendo $c \neq 1$ il periodo relativo di z rispetto ad A, ed $i = 1, \dots$ $\dots, (p-1)/4tc$. Per ogni elemento $k_h \in K$ si avrà allora $k_h = d_i z^j g^s$, con i, j, s opportuni interi. Ora si ha $N = A \times K$ e quindi, per ogni elemento $n \in N$, risulterà

$$n = d_i z^j g^l,$$

dove, al variare di $n \in N$, j ed l varieranno indipendentemente in modo da descrivere rispettivamente gli insiemi $\{1, \dots, c\}$, $\{1, \dots, t\}$. Ne viene che detto u un generatore del sottogruppo di R generato da z e da g, si ha che u è un periodo di N. Ma g è un periodo d'ordine massimo di N, dunque $z \in A$, contro l'ipotesi che $\bar{K}$ sia periodico.

Sarà allora periodico $\bar{M}$. Ora i laterali $a_i A$, $i = 1, \dots, 4$ sono distinti: infatti $a_i \in M$ e quindi $a_i \in M \times K$ ed $M \times K$ è un sistema completo di rappresentanti dei laterali di A in R. Ne segue, per l'osservazione fatta in principio, che A contiene il sottogruppo X generato da x, ossia x è un periodo (d'ordine 5) di N.

Dimostriamo ora che

2. *Esiste un insieme N di elementi $b_i \in R$ tale che si abbia $R = M \times N$ se e solo se il periodo di $1 + x$ è divisibile per* 4.

Supponiamo che si abbia $R = M \times N$, con $N = \{b_i\}$ $(i = 1, \dots$ $\dots, (p-1)/4)$. Per il teorema 1, x è un periodo di N e si ha $N = X \times D$, essendo $D = \{d_i\}$ $(i = 1, \dots, (p-1)/20)$ un sistema completo di rappresentanti di N (mod X). Poichè $R = M \times N$, gli elementi di R saranno

$$d_i x^j, \quad d_i x^j (1 + x), \quad -d_i x^j,$$

$$-d_i x^j (1 + x) \quad (i = 1, \dots, k;\ k = (p-1)/20;\ j = 1, \dots, 4);$$

perciò, indicata con S_r la somma delle potenze r-me degli elementi di R e posto

$$T_{10h} = d_1^{10h} + \dots + d_k^{10h} \qquad (h = 1, \dots, k),$$

si avrà

$$S_{10h} = 2T_{10h}\,[1 + (1+x)^{10h}] \qquad (h = 1, \dots, k).$$

Ora, gli elementi di R sono le radici del polinomio di $F[x]$ $x^{p-1} - 1$. Si ha allora $S_1 = \dots = S_{p-2} = 0$. In particolare $S_{10h} = 0$ $(h = 1, \dots, k)$. Supponiamo $T_{10h} = 0$ $(h = 1, \dots, k)$. Detti $b_0 = 1$, $b_1, \dots, b_k$ i coefficienti del polinomio monico avente per radici $d_1^{10}, \dots, d_k^{10}$, dalle formule di GIRARD-NEWTON, che legano i coefficienti di un dato polinomio con le somme delle potenze di eguale esponente delle sue radici, si ricava allora successivamente $b_1 = = \dots = b_k = 0$, che è assurdo. Esiste allora un intero m, con $1 \leq m \leq k$, tale che risulti $1 + (1+x)^{10m} = 0$ ed il periodo, r, di $1 + x$ risulta un divisore di $20m$. Supposto r non divisibile per 4, si ha che r divide $10m$ e pertanto $(1+x)^{10m} = 1$, mentre invece $(1+x)^{10m} = -1$. Quindi r è divisibile per 4.

Viceversa, supposto r divisibile per 4, G. ZAPPA [5] ha dimostrato che esiste un insieme N di elementi di R tale che si abbia $R = M \times N$ ed il teorema risulta completamente dimostrato.

3. *Sia x un qualunque elemento d'ordine* 5 *di R. Esiste un insieme N di elementi di R tale che risulti $R = M \times N$ se e solo se p ($p \equiv 1 \pmod{20}$) è un divisore primo di uno dei seguenti interi*

$$5\left[\binom{10m}{0} + \binom{10m}{5} + \dots + \binom{10m}{10m}\right] + 4 - 2^{10m},\ m = 1, \dots, (p-1)/20.$$

Osserviamo prima di tutto che, se $x \in R$, $x^5 = 1$, $x \neq 1$, allora

$$(1) \quad (1+x^2)^{10} = (1+x^3)^{10},\ (1+x)^{10} = (1+x^4)^{10},\ (1+x^2)^{10} = (1+x)^{-10}.$$

Infatti

$$(1+x)(1+x^2) = -x^4, \qquad (1+x^2)(1+x^4) = -x^3,$$

$$(1+x)(1+x^3) = -x^2, \qquad (1+x^3)(1+x^4) = -x.$$

Supponiamo ora che esista un insieme N di elementi di R tali che si abbia $R = M \times N$. Per il teorema 2 esiste un intero m,

$1 \leq m \leq (p-1)/20$ tale che risulti $(1+x)^{10m}+1=0$; si avrà quindi

(2) $(1+x)^{10m}+(1+x^2)^{10m}+(1+x^3)^{10m}+(1+x^4)^{10m}+4=0.$

Viceversa se $x \in R$ è tale da verificare il sistema delle due equazioni (2) e

$$x^4+x^3+x^2+x+1=0, \tag{3}$$

tenuto conto della (1) sarà anche

$$(1+x)^{10m}+(1+x)^{-10m}+2=0$$

ossia $(1+x)^{10m}=-1$ e per il teorema 2 esisterà un insieme $N \subset R$ tale che risulti $R=M \times N$. Pertanto la condizione necessaria e sufficiente che cerchiamo sarà la condizione perchè esista un intero m, $1 \leq m \leq (p-1)/20$ tale che la risultante delle due equazioni (2) e (3) sia uguale a zero. Eliminando la x tra queste due equazioni si ha subito

$$5\left[\binom{10m}{0}+\binom{10m}{5}+\dots+\binom{10m}{10m}\right]+4-2^{10m}=0\,,$$

ed il teorema è dimostrato.

Fra i campi d'ordine primo $p \equiv 1 \pmod{20}$ quello d'ordine 101 è il campo d'ordine minimo per cui l'uguaglianza non sia verificata qualunque sia m, $1 \leq m \leq (p-1)/20$.

4. *Siano $p, q > 2$ due numeri primi e supponiamo che sia $p = q(q-1)+1$. Se x è un elemento d'ordine q di R esiste un insieme N di elementi di R tale che si abbia $R=M \times N$ se e solo se* $2^q \equiv 1 \pmod{p}$ *e due qualsiansi degli interi* $(2^u-1)^q$ $(u=1,\dots,q-1)$ *non appartengono alla stessa classe di resti* $\pmod{p}$.

Indicata con R_k la somma delle potenze k-me degli elementi di R, tenuto conto che questi sono le radici dell'equazione $x^{p-1}-1=0$, dalle formule di GIRARD-NEWTON si ha

$$R_k=0 \quad (k=1,\dots,p-2), \quad R_{p-1}=-1. \tag{4}$$

Inoltre, posto

$$\overline{a}_i = (x - 1)\, a_i = x^i - 1, \quad \overline{M} = \{\overline{a}_i\} \qquad (i = 1, \dots, q - 1),$$

risulta $R = M \times N$, con N assegnato sottoinsieme di R, se e solo se $R = \overline{M} \times N$.

Se poi poniamo

$$\overline{M}_k = \sum_i^{1 \dots q-1} (x^i - 1)^k = \sum_i^{0 \dots q-1} (x^i - 1)^k,$$

tenuto conto che $1 + x + \dots + x^{q-1} = 0$, risulta subito

$$\overline{M}_k = (-1)^k\, q \quad (k = 1, \dots, q - 1)\,; \qquad \overline{M}_q = 0. \tag{5}$$

Ammettiamo ora che si abbia $R = M \times N$, con $N = \{b_j\}$ $(j = 1, \dots, q)$. Posto

$$N_k = \sum_j^{1 \dots} b_j^k$$

sarà

$$R_k = \overline{M}_k \times N_k$$

e quindi, per le (4), $N_k = 0$ $(k = 1, \dots, q - 1)$. Ne viene che, se

$$z^q + c_1\, z^{q-1} + \dots + c_q$$

è il polinomio monico di $F[z]$ avente per radici $b_1, \dots, b_q$, ancora per le formule di GIRARD-NEWTON, si ha $c_1 = c_2 = \dots = c_{q-1} = 0$. Sarà allora

$$b_i = kx^i \qquad (i = 1, \dots, q\,;\ k \in R\,;\ k \neq 0).$$

Tenuto conto che $R = \overline{M} \times N$, questo significa che ogni elemento di R è esprimibile in uno ed un solo modo nella forma

$$x^s\,(x^r - 1) \qquad (s = 1, \dots, q\,;\ r = 1, \dots, q - 1). \tag{6}$$

Allora, detto

$$z^{q-1} + d_1\, z^{q-2} + \dots + d_{q-1}$$

il polinomio monico di $F[z]$ avente per radici $\overline{a}_1^q, \overline{a}_2^q, \dots, \overline{a}_{q-1}^q$, si ha che

$$z^{q(q-1)} + d_1 z^{q(q-2)} + \dots + d_{q-1}$$

ha per radici tutti gli elementi di R. Ne viene che

$$d_1 = d_2 = \dots = d_{q-2} = 0, \quad d_{q-1} = -1.$$

Posto

$$S_k = \overline{a}_1^{kq} + \overline{a}_2^{kq} + \dots + \overline{a}_{q-1}^{kq},$$

dalle formule di GIRARD-NEWTON si ricava successivamente $S_1 = S_2 = \dots = S_{q-2} = 0$ e, poichè è $q > 2$, risulta

(7) $$S_1 + S_2 + \dots + S_{q-2} = 0.$$

Poniamo ora

$$X_r = \overline{a}_r^q + \overline{a}_r^{2q} + \dots + \overline{a}_r^{(q-2)q};$$

si ha

$$\sum_r^{1 \dots q-1} X_r = \sum_k^{1 \dots q-2} S_k,$$

e pertanto per la (7)

(8) $$\sum_r^{1 \dots, q-1} X_r = 0.$$

D'altra parte se, per ogni intero s, risulta $x^r - 1 \neq x^s$ si ha $X_r = -1$. Tenuto conto della (8) esisteranno due potenze di x, x^r ed x^s, con $x^r \neq 1$, in modo che si abbia $x^r - 1 = x^s$. Quindi risulterà $x^{r-s} - 1 = x^{-s}$ e $(x^r - 1)\, x^{-s} = (x^{r-s} - 1)\, x^s$. Ora abbiamo visto che ogni elemento di R è esprimibile in un sol modo nella forma (6); sarà quindi $x^s = 1$, $x^r = 2$. Risulterà di conseguenza $2^q = 1$ ed ogni elemento di R si potrà esprimere in uno ed un solo modo nella forma

(9) $$2^u (2^v - 1) \quad (u = 1, \dots, q\,;\ v = 1, \dots, q-1).$$

Le potenze $(2^v - 1)^q$ $(v = 1, \dots, q-1)$ saranno tutte distinte perchè, se è $(2^v - 1)^q = (2^w - 1)^q$, sarà anche $2^w - 1 = (2^v - 1)\, 2^t$, con 2^t opportuna potenza di 2, che, tenuto conto del fatto che ogni elemento di R è esprimibile in un sol modo nella forma (9), risulta uguale a 1.

Supponiamo ora, viceversa, che si abbia $2^q = 1$ e che le potenze $(2^v - 1)^q$ $(v = 1, \dots, q-1)$ siano tutte distinte. Risulterà allora

$$2^u (2^v - 1) = 2^{\bar{u}} (2^{\bar{v}} - 1)$$

se e solo se si avrà $2^u = 2^{\bar{u}}$, $2^v = 2^{\bar{v}}$ e quindi ogni elemento di R si potrà esprimere in uno ed un sol modo nella forma (9). Questo significa che, posto

$$N_2 = \{2^r\} \ (r = 1, \dots, q), \ M_2 = \{2^0 + 2^1 + \dots + 2^s\} \ (s = 0, 1, \dots, q-2),$$

si ha $R = M_2 \times N_2$. Allora, se x è un qualunque elemento d'ordine q di R, tenuto conto che $2^q = 1$, posto $N = \{x^r\}$ $(r = 1, \dots, q)$, col solito significato per M, si avrà $R = M \times N$.

Tenuto conto dei teoremi a), b) di ZAPPA, possiamo enunciare nel seguente modo i teoremi 3 e 4:

5. *Sia G un gruppo non abeliano d'ordine $5p$ (p primo, $p > 5$) e sia S un suo 5-sottogruppo di Sylow. Allora G ammette una S-partizione non semistretta se e solo se $p \equiv 1 \pmod{q^2 - q}$ e p è un divisore di uno dei seguenti interi*

$$5\left[\binom{10\,m}{0} + \binom{10\,m}{5} + \dots + \binom{10\,m}{10\,m}\right] + 4 - 2^{10m}, \ m = 1, \dots, (p-1)/20.$$

6. *Sia G un gruppo non abeliano d'ordine pq (p, q primi, $q \neq 2$, $p = q(q-1) + 1$) e sia S un suo q-sottogruppo di Sylow. Allora G ammette una S-partizione non semistretta se e solo se $2^q \equiv 1 \pmod{p}$ e due qualsivogliano degli interi $(2^u - 1)^q$ $(u = 1, \dots, q-1)$ non appartengono alla stessa classe di resti* $\pmod{p}$.

BIBLIOGRAFIA

[1] R. LINGENBERG, « *Ueber Gruppen projektiver Kollineationen welche eine perspektive Dualität invariant lassen* », Archiv. der Math., 13 (1962), 385-400.

[2] A. D. SANDS, « *On the factorisation of finite abelian groups* », Acta Math. Acad. Sci. Hung., 8 (1957), 65-86.

[3] G. ZAPPA, « *Sugli spazi generali quasi di traslazione* », Le Matematiche, Catania, 19 (1964), 127-143.

[4] G. ZAPPA, « *Sulle S-partizioni di Hall di un gruppo finito* », Rend. Acc. Naz. Lincei, (8), 38 (1965), 755-759.

[5] G. ZAPPA, « *Sulle S-partizioni di un gruppo finito* », Annali di Matematica IV, 74 (1966), 1-14.

Manoscritto pervenuto in redazione il 22 febbraio 1967.