LE MATEMATICHE
Vol. LI (1996) – Supplemento, pp. 149-157

DECOMPOSIZIONE ED s-m RAPPRESENTAZIONE DI GRUPPI FINITI

FRANCO MIGLIORINI - JENÖ SZÉP

Alla memoria di Umberto Gasapina

This paper is a survey of a few previous works of the authors with other new results. We introduce a special decomposition of a finite group [semigroup] and determine its main properties. From a such decomposition $\{C_i\}, i = 1, \ldots, n$ of a group $S(C_i \subset S)$, one can construct, for a special class of finite groups, a set-matrix representation. The group D_4 has a such representation. Several theorems were already obtained on groups with s-m representation.

Introduzione.

Questo lavoro è un riassunto (senza dimostrazioni, reperibili attraverso la bibliografia indicata) dei principali risultati ottenuti dagli autori in una serie di ricerche condotte negli ultimi anni ([1], [4], [5]). Compaiono qui anche alcuni nuovi risultati, corredati di dimostrazione, la trattazione in alcune parti è più lineare di quella originale e viene indicato qualche problema aperto. Alcuni errori ed imprecisioni (dovuti anche ad una stampa poco accurata) negli articoli [4] e [5] sono stati corretti.
Se S è un gruppo finito, sia $\Gamma = \{g_1, g_2, \ldots, g_m\}$ un sistema di generatori

The work is partially supported by contribution of MURST for Scientific Research (60% quota).

indipendenti di S. Restano univocamente determinati certi sottoinsiemi $C_r (r = 1, \ldots, n)$ ove C_r raccoglie gli elementi di S che hanno lunghezza minima r rispetto a Γ.
Tali insiemi hanno avuto un ruolo notevole in alcune ricerche riguardanti il problema di Burnside per i semigruppi (cfr. [1], [2], [3]).
I risultati principali che saranno esposti riguardano:

- proprietà della decomposizione $S = \bigcup_{i=1}^{n} C_i$;
- costruzione dei gruppi che hanno un dato numero m di generatori indipendenti ed un dato numero n di componenti C_i;
- studio di una particolare rappresentazione, mediante matrici quadrate, con componenti dei sottoinsiemi dei C_i, rappresentazione, però, che solo alcuni gruppi finiti ammettono;
- alcune proprietà dei gruppi che ammettono particolari rappresentazioni s-matriciali.

Lo scopo principale degli autori è di trasferire, in seguito, con le opportune modifiche, molti dei risultati ottenuti ai semigruppi inversi finiti.

1. In [1] abbiamo introdotto i sottoinsiemi C_i di S, semigruppo con un numero finito di generatori periodici, allo scopo di determinare condizioni di finitezza di S (problema di Burnside per i semigruppi). In seguito ([4]) abbiamo considerato tali sottoinsiemi in un gruppo.
Sia S un gruppo finitamente generato e $\Gamma = \{g_1, g_2, \ldots, g_m\}$ un sistema di generatori indipendenti di S (cioè tali che $g_i \notin \langle g_1, \ldots, \hat{g}_i, g_{i+1}, \ldots, g_m \rangle$, $i = 1, \ldots, m$) con $g_i^{\alpha_i} = 1$ ($\alpha_i \geq 2$, ordine di g_i).
È noto ([1]) che esiste una rappresentanza di lunghezza minimale, $l(s)$, per ogni elemento $s \in S$, mediante i generatori in Γ. Sia $C_i = \{s \in S / l(s) = i\}$; è chiaro che $C_1 = \Gamma$. Inoltre $C_i \neq \emptyset$ implica $C_{i-1} \neq \emptyset$ ed è:

$$(1) \qquad S = C_1 \cup \ldots \cup C_i \cup \ldots, \quad \text{ove } C_i \cap C_j = \emptyset \text{ per } i \neq j.$$

Se S è un gruppo finito, esiste $n > 1$ tale che in (1) $C_n \neq \emptyset$ e $C_j = \emptyset$ per $j > n$.
In tal caso la decomposizione di S è $S = \bigcup_{i=1}^{n} C_i$.

È chiaro che $S = Sg_i = \bigcup_{j=1}^{n} C_j g_i$, $\forall g_i \in \Gamma$, ove $C_j g_i \subseteq \bigcup_{k=1}^{j+1} C_k$.

Sia $C_k^{ij} = C_k \cap C_i g_j$.

Teorema 1. *Valgono le seguenti affermazioni:*

1. $|S| = \sum_{i=1}^{n} |C_i g_j| \ (j = 1, \ldots, m)$
2. $C_i g_j = \bigcup_{k=1}^{i+1} C_k^{ij}$
3. $C_i = \bigcup_{k=i-1}^{n} C_i^{kj}, \forall j$
4. $g_{i_1} g_{i_2} \ldots g_{i_t} g_j = g_{j_1} \ldots g_{j_u} \Rightarrow u - 1 \leq t \leq u + a_j - 1$
5. $1 \in C_k \Rightarrow k \leq \min_i \alpha_i$
6. $m \leq n$
7. *Se* $g_{i_1} \ldots g_{i_k} = 1$, *allora la molteplicità di ogni generatore nel prodotto è almeno 2.*

Dimostrazione. Cfr. Theorem 1 di [4].

Dato il numero n delle componenti $C_i (\neq \emptyset)$ nella decomposizione di S ed il numero m dei generatori in Γ, si può risalire (almeno per n ed m piccoli) ai gruppi S che ammettono una tale decomposizione $S = \bigcup_{i=1}^{n} C_i$.
In questa direzione di ricerca, abbiamo ottenuto ([4], Theorem 3 e 4 (corretto)), attraverso ragionamenti basati sulle proprietà delle componenti C_i, con l'ausilio del Teorema 1, il seguente risultato.

Teorema 2.
i) Per $m = 2, n = 2$, *esistono i gruppi* K_4 *(di Klein) ed* S_3;
ii) Per $m = 2, n = 3$, *esistono i gruppi* S_3, $Z_2 \times Z_3$, D_4 *(diedrale).*

Si trovano condizioni su C_1 e su C_2 affinchè S sia abeliano.

Teorema 3. *S è abeliano se e solo se* $g_i C_1 g_i^{-1} = C_1 \ (i = 1, \ldots, m)$.

Dimostrazione. Cfr. Theorem 9 di [4].

Teorema 4. *Se* $C_2 = \{g_1^2, g_1 g_2, \ldots, g_1 g_m\}$, *allora S è un gruppo abeliano.*

Dimostrazione. Non è una perdita di generalità, evidentemente, aver supposto primo fattore fisso g_1, anzichè g_h qualsiasi. Innanzitutto, un qualsiasi prodotto $g_i g_j$ sta in C_2. Infatti si vede facilmente che $g_i g_j$ non può appartenere a C_1. Allora per ipotesi esiste k tale che $g_i g_j = g_1 g_k$. Sia $i \neq 1$, $j \neq k$ (casi banali) e $i \neq j$. Se $j = 1$ si ha $g_i g_1 = g_1 g_k \Rightarrow i = k$ (altrimenti i generatori non sono indipendenti), quindi $g_i g_1 = g_1 g_i$. Se $j \neq 1$, sia $g_i g_j = g_1 g_k$: ne segue $j = k$, $i = 1$, quindi $g_i g_j = g_1 g_k = g_k g_1 = g_j g_i$. Pertanto S è abeliano.

Problema 1. Determinare una condizione sufficiente su C_3 affinchè S sia abeliano.

Teorema 5. *Se, per qualche* $s \in S$, $sC_1s^{-1} = C_1$, *allora* $sC_is^{-1} = C_i (i = 1, \ldots, n)$.

Dimostrazione. Cfr. Theorem 10 di [4].

Il Teorema 5 gioca un ruolo importante per lo sviluppo della ricerca.
Sia G_i il sottogruppo di S generato da $\Gamma - \{g_i\}$, cioè $G_i = \langle g_1, \ldots, \hat{g}_i, \ldots, g_m \rangle$.
Poichè Γ è indipendente, $G_i \neq S, \forall i$.
Sia $N(C_1) = \{s \in S \mid sC_1s^{-1} = C_1\}$ il normalizzante di C_1 in S. $N(C_1)$ è un sottogruppo si S.

Proposizione 6. *Se nessun sottogruppo* $G_i (i = 1, \ldots, m)$ *è fattore diretto di* S, *allora* $g_j \notin N(C_1), \forall j$.

Dimostrazione. Nel caso contrario, se g_j appartiene a NC_1, si ha $g_j g_i g_j^{-1} = g_i$, $\forall i$, quindi $S = G_j \times \langle g_j \rangle$, contro l'ipotesi.

2. Sia $s \in S$, si ha

$$S = sSs^{-1} = s\left(\bigcup_{i=1}^{n} C_i\right)s^{-1} = \bigcup_{i=1}^{n}(sC_is^{-1}) :$$

compaiono così, in modo naturale, i sottoinsiemi sC_is^{-1}.
Se $i \neq j$, $sC_is^{-1} \cap sC_js^{-1} = \emptyset$. Si rivelano importanti, per la nostra ricerca, anche i sottoinsiemi

$$sC_is^{-1} \cap C_j = C_{ij}(s) \quad (i, j = 1, \ldots, n; \ s \in S).$$

Ad ogni elemento $s \in S$ possiamo associare una matrice, o set-matrice (s-matrice), quadrata, $M(s)$, le cui componenti sono sottoinsiemi di S:

$$M(s) = \begin{bmatrix} C_{11}(s) & C_{12}(s) & \cdots & C_{1n}(s) \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ C_{n1}(s) & C_{n2}(s) & \cdots & C_{nn}(s) \end{bmatrix}.$$

In generale può accadere che elementi diversi $s \neq s'$ di S diano luogo a matrici uguali, $M(s) = M(s')$ (cioè $C_{ij}(s) = C_{ij}(s'), \forall i, j$).
Sia $\rho \subseteq S \times S$ l'equivalenza su S tale che $(a, b) \in \rho \Leftrightarrow M(a) = M(b)$, $(a, b \in S)$.

Proposizione 7. ρ *è una congruenza sinistra in* S.

Dimostrazione. Sia $(a, b) \in \rho$ e $s \in S$. Allora $C_{ij}(a) = C_{ij}(b)$, $\forall i, j$, quindi $aC_ia^{-1} \cap C_j = bC_ib^{-1} \cap C_j$, $\forall i, j$. Ne segue $aC_ia^{-1} = bC_ib^{-1}$, $\forall i$, quindi anche $C_{ij}(sa) = C_{ij}(sb)$, $\forall i, j$. Pertanto $(sa, sb) \in \rho$ e ρ è una congruenza sinistra.

Ma la stessa ρ non è una congruenza destra in S in generale.
Sia $\mathscr{M}(S) = \{M(s) \mid s \in S\}$. È chiaro che, se $s \in N(C_1)$,

$$M(s) = \begin{bmatrix} C_1 & \emptyset & \cdots & \emptyset \\ \emptyset & C_2 & \cdots & \emptyset \\ \cdots & \cdots & \cdots & \cdots \\ \emptyset & \emptyset & \cdots & C_n \end{bmatrix}.$$

E viceversa.
Sia $\varphi : S \to \mathscr{M}(S)$ l'applicazione suriettiva tale che $\varphi(s) = M(s)$, $\forall s \in S$. Definiamo una moltiplicazione in $\mathscr{M}(S)$.

Definizione 8. $M(s)M(s') = M(ss')$ $(s, s' \in S)$.

È chiaro che, affinchè la definizione sia valida, il prodotto $M(ss')$ deve essere indipendente dai rappresentatnti di $M(s)$ ed $M(s')$. Questa indipendenza si ha se e solo se ρ risulta una congruenza in S, e tale noi la supponiamo. In tal caso la moltiplicazione in $\mathscr{M}(S)$ è associativa. Inoltre φ risulta un epimorfismo ed S/ρ risulta isomorfo ad $\mathscr{M}(S)$, quindi $\mathscr{M}(S)$ è un gruppo, con unità $M(1)$. Un teorema di grande utilità è il seguente:

Teorema 9. *ρ è una congruenza in S se e solo se $N(C_1)$ è un sottogruppo normale di S.*

Dimostrazione. Se ρ è una congruenza, esiste un sottogruppo normale N di S tale che $S/\rho \equiv S/N$ ed $(a, b) \in \rho \Leftrightarrow ab^{-1} \in N$. Ma $(a, b) \in \rho \Leftrightarrow M(a) = M(b) \Leftrightarrow M(ab^{-1}) = M(1) \Leftrightarrow ab^{-1} \in N(C_1)$, quindi $N(C_1) = N$, onde $N(C_1) \lhd S$ ed $S/\rho = S/N(C_1)$.
Viceversa, se $N(C_1) \lhd S$, $N(C_1)$ determina una congruenza σ in S, tale che:

$$(a, b) \in \sigma \Leftrightarrow ab^{-1} \in N(C_1) \Leftrightarrow aN(C_1) = bN(C_1).$$

Ma è chiaro che, se $b = ac$ con $c \in N(C_1)$, si ha, per il Teorema 5, $C_{ij}(b) = C_{ij}(a)$, $\forall i, j = 1, \ldots, n$.
Pertanto $aN(C_1) = bN(C_1) \Leftrightarrow M(a) = M(b)$, onde $(a, b) \in \sigma \Leftrightarrow (a, b) \in \rho$, così $\sigma = \rho$ e ρ è una congruenza.
In conclusione, se ρ è una congruenza in S, $\mathscr{M}(S)$ è un gruppo isomorfo a $S/N(C_1)$. In questo caso si ha una rappresentazione matriciale, con set-matrici (s-matrici) di S su $\mathscr{M}(S)$. In altri termini, il Teorema 9 vale anche:

Teorema 10. *Un gruppo finito S ammette una rappresentazione set-matriciale (s-m rappresentazione) se e solo se, rispetto ad un opportuno sistema Γ di generatori indipendenti, $N(C_1)$ è normale in S.*

Se $N(C_1) = \langle 1 \rangle$, la s-m rappresentazione è un isomorfismo.

Esempio 1. Sia D_4 il gruppo diedrale, con generatori indipendenti $\Gamma = \{g, h\} = C_1$, $g^4 = h^2 = 1$.
Vale l'uguaglianza $g^r h = hg^{4-r}$, da cui $g^3 h = hg$. La tabella di Cayley di D_4 è la seguente:

	1	g	g^2	g^3	h	gh	g^2h	hg
1	1	g	g^2	g^3	h	gh	g^2h	hg
g	g	g^2	g^3	1	gh	g^2h	hg	h
g^2	g^2	g^3	1	g	g^2h	hg	h	gh
g^3	g^3	1	g	g^2	hg	h	gh	g^2h
h	h	hg	g^2h	gh	1	g^3	g^2	g
gh	gh	h	hg	g^2h	g	1	g^3	g^2
g^2h	g^2h	gh	h	hg	g^2	g	1	g^3
hg	hg	g^2h	gh	h	g^3	g^2	g	1

$C_2 = \{1, g^2, gh, hg\}$, $C_3 = \{g^3, g^2h\}$.

Si nota facilmente che C_2 è un sottogruppo normale di D_4. Determiniamo la rappresentazione $\varphi : D_4 \to \mathcal{M}(D_4)$.
Si ha, con facili calcoli:

$$M(1) = \begin{bmatrix} C_1 & \emptyset & \emptyset \\ \emptyset & C_2 & \emptyset \\ \emptyset & \emptyset & C_3 \end{bmatrix}, \quad M(g) = \begin{bmatrix} \{g\} & \emptyset & \{g^2h\} \\ \emptyset & C_2 & \emptyset \\ \{h\} & \emptyset & \{g^3\} \end{bmatrix},$$

$$M(h) = \begin{bmatrix} \{h\} & \emptyset & \{g^3\} \\ \emptyset & C_2 & \emptyset \\ \{g\} & \emptyset & \{g^2h\} \end{bmatrix}, \quad M(g^2) = \begin{bmatrix} C_1 & \emptyset & \emptyset \\ \emptyset & C_2 & \emptyset \\ \emptyset & \emptyset & C_3 \end{bmatrix},$$

$$M(g^3) = \begin{bmatrix} \{g\} & \emptyset & \{g^2h\} \\ \emptyset & C_2 & \emptyset \\ \{h\} & \emptyset & \{g^3\} \end{bmatrix}, \quad M(gh) = \begin{bmatrix} \emptyset & \emptyset & C_3 \\ \emptyset & C_2 & \emptyset \\ C_1 & \emptyset & \emptyset \end{bmatrix},$$

$$M(g^2h) = \begin{bmatrix} \{h\} & \emptyset & \{g^3\} \\ \emptyset & C_2 & \emptyset \\ \{g\} & \emptyset & \{g^2h\} \end{bmatrix} \quad , \quad M(hg) = \begin{bmatrix} \emptyset & \emptyset & C_3 \\ \emptyset & C_2 & \emptyset \\ C_1 & \emptyset & \emptyset \end{bmatrix} .$$

Pertanto si ha:

$$M(1) = M(g^2) \ , \ M(g) = M(g^3) \ , \ M(h) = M(g^2h) \ , \ M(hg) = M(gh).$$

Inoltre $N(C_1) = \{1, g^2\}$ è un sottogruppo normale di D_4. Allora ρ è una congruenza in D_4 e φ è un omomorfismo. Infine il gruppo

$$\frac{D_4}{N(C_1)} = \left\{N(C_1) \ , \ gN(C_1) \ , \ hN(C_1) \ , \ ghN(C_1)\right\}$$

è isomorfo al gruppo $\mathscr{M}(D_4) = \{M(1), M(g), M(h), M(gh)\}$.

Esempio 2. Nel lavoro [5] si considerano (Esempi 1 e 2) due diverse decomposizioni di S_3, rispetto a due diversi sistemi di generatori indipendenti. La prima di queste decomposizioni non dà luogo ad una s-m rappresentazione di S_3 (poichè $N(C_1)$ non è normale in S_3), mentre la seconda decomposizione di S_3 dà luogo ad un isomorfismo tra S_3 ed $\mathscr{M}(S_3)$.

Il teorema che segue è utile per successivi sviluppi.

Teorema 11. *$N(C_1) \lhd S$ se e solo se $C_{ij}(cs) = C_{ij}(s)$, $\forall i, j$ e $\forall s \in S$, $c \in N(C_1)$.*

Dimostrazione. Sia $N(C_1) \lhd S$; allora $cs = sc_1$ con $c_1 \in N(C_1)$, quindi per il Teorema 5 si ha:

$$C_{ij}(cs) = sc_1C_i(sc_1)^{-1} \cap C_j = sC_is^{-1} \cap C_j = C_{ij}(s).$$

Viceversa, sia $C_{ij}(cs) = C_{ij}(s)$, $\forall i, j$, $\forall s \in S$, $c \in N(C_1)$.
Allora: $csC_i(cs)^{-1} \cap C_j = sC_is^{-1} \cap C_j$, $\forall j$, implica $csC_i(cs)^{-1} = sC_is^{-1}$, $\forall i$. In particolare: $csC_1(cs)^{-1} = sC_1s^{-1}$, quindi $s^{-1}csC_1(s^{-1}cs)^{-1} = C_1$, cioè $s^{-1}cs \in N(C_1)$, $\forall s \in S$, $c \in N(C_1)$, onde $N(C_1)$ è normale in S.

Diamo ora una condizione sufficiente affinchè ρ sia una congruenza in S.

Teorema 12. *Sia S un gruppo finito e sia:*

$$(\alpha) \qquad sC_{ij}(s)s^{-1} = C_{ji}(s) \ , \ \forall i, j \ e \ \forall s \in s.$$

Allora si ha che $N(C_1) \lhd S$ e $[N(C_1)s]^2 = N(C_1)$. Viceversa, se $N(C_1) \lhd S$ e $[N(C_1)s]^2 = N(C_1)$, $\forall s \in S$, allora vale (α) in S.

Dimostrazione. Cfr. Theorem 9 di [5].

La condizione (α) è anche sufficiente affinchè S ammetta una s-m rappresentazione.

Problema 2. Trovare una condizione, sui $C_{ji}(s)$, più generale della (α), affinchè S sia rappresentabile con s-matrici.

Proposizione 13. *Per $s \in S$, si ha:*

i) $C_{ij}(s) = C_{kl}(s)(\neq \emptyset) \Rightarrow i = k,\ j = l.$

ii) $\bigcup_{j=1}^{n} C_{ij}(s) = sC_is^{-1},\ \bigcup_{i=1}^{n} C_{ij}(s) = C_j.$

Consideriamo, infine, un caso particolare.

Teorema 14. *Sia $\mathscr{M}(S)$ immagine omomorfa di S. Se esiste in $\mathscr{M}(S)$ una matrice diagonale, nxn, $(n \geq 2)$, della forma:*

$$M(s) = \begin{bmatrix} \emptyset & \emptyset & \cdots & \emptyset & * \\ \emptyset & \emptyset & \cdots & \cdots & \emptyset \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \emptyset & * & \cdots & \emptyset & \emptyset \\ * & \emptyset & \cdots & \emptyset & \emptyset \end{bmatrix},$$

ove $*$ indica una componente non vuota, allora si ha:

1) n è dispari

2) $|S|$ é pari

3) Esiste un sottogruppo S' di S tale che $S' = N(C_1) \cup N(C_1)s$.

Dimostrazione. Nel caso considerato, per la Proposizione 13, deve essere:

$$(*) \qquad sC_is^{-1} \cap C_{n-i+1} = C_{n-i+1}\,, \quad \forall i.$$

Dalla $(*)$ si ha anche:

$$sC_{n-i+1}s^{-1} \cap C_i = C_i.$$

Sempre da $(*)$ segue:

$$sC_is^{-1} \supseteq C_{n-i+1},$$

quindi

$$s^2C_is^{-2} \supseteq sC_{n-i+1}s^{-1} \supseteq C_i.$$

Ma poichè $|s^2C_is^{-2}| = |C_i|$, deve essere $s^2C_is^{-2} = C_i$, quindi $s^2 \in N(C_1)$. Allora $S' = N(C_1) \cup N(C_1)s$ è un sottogruppo di S ed è $[S' : N(C_1)] = 2$,

quindi $|S|$ è pari. Inoltre sia $1 \in C_i$, per qualche i. Allora anche C_{n-i+1} contiene 1, pertanto deve essere $i = n - i + 1$, quindi $i = (n+1)/2$, ed n risulta dispari. Osserviamo che nel precedente Esempio 1 troviamo una verifica del Teorema 14.

BIBLIOGRAFIA

[1] F. Migliorini - J. Szép, *A New Approach to the Burnside Problem for Semigroups,* Pu. M.A., Ser. A, 1 (1990), pp. 169-172.

[2] F. Migliorini - J. Szép, *Chains and Cycles in the Subsets C_n of Finitely Generated and Periodic Semigroups, I,* Pu. M.A., Ser. A, 3 (1992), pp. 117-125.

[3] F. Migliorini - J. Szép, *Chains and Cycles in the Subsets C_n of Finitely Generated and Periodic Semigroups, II,* Pu. M.A., Ser. A, 3 (1992), pp. 233-242.

[4] F. Migliorini - J. Szép, *The Subsets C_n in Finite Groups, I,* Pu. M.A., 5 (1994), pp. 205-216.

[5] F. Migliorini - J. Szép, *The Subsets C_n in Finite Groups and Inverse Semigroups, II,* Pu. M.A., 6 (1995), pp. 57-67.

Franco Migliorini,
Dipartimento di Matematica,
Università di Siena,
53100 Siena (ITALY)

Jenö Szép,
Institute of Mathematics and Computer Science,
University of Economic Sciences,
H1828 Budapest (HUNGARY)