RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

REMO GATTAZZO

Sottogruppi Q-congruenziali di $SL(n, R)$

Rendiconti del Seminario Matematico della Università di Padova, tome 55 (1976), p. 179-193

<http://www.numdam.org/item?id=RSMUP_1976__55__179_0>

© Rendiconti del Seminario Matematico della Università di Padova, 1976, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (http://rendiconti.math.unipd.it/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/legal.php). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

REND. SEM. MAT. UNIV. PADOVA, Vol. 55 (1976)

Sottogruppi Q-congruenziali di $SL(n, R)$.

REMO GATTAZZO (*)

SUMMARY - Let R be a principal ideal domain. The classical notion of q-congruence subgroup $G(n, q) \subset SL(n, R)$, $(q \in R - \{0\})$ is generalized here to Q-congruence subgroup $G(n, Q)$, Q an $n \times n$ matrix over R. Properties of subgroups $G(n, Q)$ are studied. This class of groups contains some classes of congruence groups previously studied by M. Newman and I. Reiner.

Introduzione.

Sia R un anello commutativo con unità, privo di divisori dello zero e ad ideali principali; e sia R_n l'anello delle matrici $n \times n$ su R. È ben nota, in più di una teoria matematica, l'importanza dei sottogruppi congruenziali di $\Gamma = SL(n, R)$. Alcuni autori, tra i quali M. Newman e I. Reiner, hanno studiato diverse proprietà aritmetico-gruppali di tali gruppi, in alcuni casi in cui è possibile caratterizzare i gruppi stessi mediante un sistema di congruenze.

L'idea che sta alla base del presente lavoro è quella di considerare quei gruppi congruenziali $G(n, Q)$ di Γ definibili attraverso una congruenza matriciale del tipo

$$(a) \qquad X \equiv I \bmod.(Q)$$

(*) Indirizzo dell'A.: Istituto di Matematica Applicata, Università di Padova.

Lavoro eseguito nell'ambito dei Gruppi di ricerca matematica del C.N.R. (G.N.S.A.G.A.).

(dove $X \in SL(n, R)$, I è la matrice identica, $Q \in R_n$ è una fissata matrice).

La (a) è una evidente generalizzazione della classica definizione di sottogruppo congruenziale principale data dalla congruenza

$$X \equiv I \bmod. (q)$$

($q \in R - \{o\}$); mentre però in tal caso l'elemento q non è soggetto ad alcuna condizione, la Q definisce qui un gruppo tramite la (a) se e soltanto se soddisfa ben precise condizioni aritmetiche che vengono stabilite nel n. 1.

I gruppi considerati comprendono come casi particolari quelli già definiti e studiati (cfr. [1], [2]), per i quali viene costruita la relativa Q.

Dopo aver studiato, nel n. 2, alcune proprietà generali dei gruppi Q-congruenziali, si passa ad analizzare la relazione tra la Q e il corrispondente gruppo $G(n, Q)$; osservato che $G(n, Q_1) = G(n, Q_2)$ non implica $Q_1 = Q_2$, nel n. 3 si affronta il problema di determinare una Q « canonica » per ciascun gruppo $G(n, Q)$.

Vengono infine fatte alcune applicazioni, tra cui la determinazione dell'indice $[\Gamma: G(2, Q)]$.

1. – Sottogruppi Q-congruenziali di $SL(n, R)$.

DEFINIZIONE 1. Data $Q = \|q_{ij}\| \in R_n$, dove gli elementi q_{ij} si suppongono tutti non nulli, e date $A = \|a_{ij}\|$ e $X = \|x_{ij}\| \in R_n$, diciamo *Q-congruenza* la congruenza matriciale

$$X \equiv A \bmod. (Q)$$

che equivale al sistema delle n^2 congruenze

$$x_{ij} \equiv a_{ij} \bmod. (q_{ij}) \qquad (i, j = 1, \ldots, n)$$

LEMMA 1. *L'insieme*

$$\mathfrak{L}(Q) = \{X \in R_n : X \equiv I \bmod. (Q)\}$$

è stabile rispetto al prodotto se e solo se gli elementi della matrice

$Q = \|q_{ij}\|$ *soddisfano alle relazioni*

$$(1) \qquad q_{ik}\, q_{kj} \equiv o \bmod. (q_{ij}) \qquad (i, k, j, = 1, \ldots, n)$$

(le (1) *risultano soddisfatte banalmente quando almeno uno fra* i, j *è uguale a* k*).*

Le (1) sono necessarie. Si ponga

$$X_{ik} \equiv I + q_{ik} E_{ik} \in \mathfrak{L}(Q) \qquad (i \neq k;\ i, k = 1, \ldots, n)$$

ove $E_{ik} \in R_n$ con 1 al posto (i, k) e 0 nei rimanenti.

Per ogni terna $\{i, j, k\}$ con i, j diversi da k, si ha

$$X_{ik} X_{kj} = I + q_{ik} E_{ik} + q_{kj} E_{kj} + q_{ik} q_{kj} E_{ij}$$

dalle quali

$$X_{ik} X_{kj} \in \mathfrak{L}(Q) \Leftrightarrow q_{ik} q_{kj} \equiv o \bmod. (q_{ij}) .$$

Le (1) sono sufficienti. Se X, $Y \in R_n$ sono tali che

$$X \equiv I \bmod. (Q) , \qquad Y \equiv I \bmod. (Q)$$

sono soddisfatte pure le Q-congruenze ad esse equivalenti

$$X - I \equiv O \bmod. (Q) , \qquad Y - I \equiv O \bmod. (Q) .$$

Queste relazioni comportano, in forza delle (1), la

$$(X - I)(Y - I) \equiv O \bmod. (Q)$$

e, per l'identità fra matrici

$$XY - I = (X - I)(Y - I) + (X - I) + (Y - I)$$

risulta

$$XY - I \equiv O \bmod. (Q)$$

che equivale alla $XY \equiv I \bmod. (Q)$, come si voleva provare.

LEMMA 2. *Sia* $X \in R_n$. *Se* $X \equiv I \bmod.(Q)$ *e valgono le*

$$q_{ik}\, q_{kj} \equiv o \bmod.(q_{ij}) \qquad (i, k, j = 1, \ldots, n) \tag{1}$$

la matrice aggiunta della X, $Agg\, X$, *soddisfa alla* Q*-congruenza*

$$(Agg\, X)_{-1} \equiv (det\, X) \cdot I \bmod.(Q)\,.$$

X soddisfi alla $X \equiv I \bmod.(Q)$, e sia X_{ij} il complemento algebrico di x_{ij} nella matrice X, con $i \neq j$. X_{ij} è somma di prodotti del tipo

$$\varepsilon x_{i_1 j_1} x_{i_2 j_2} \ldots x_{i_{n-1} j_{n-1}} \qquad \text{con} \quad \varepsilon = \pm 1 \tag{2}$$

dove $(i_1, \ldots, i_{n-1})$ è una qualunque permutazione degli indici $\{1, \ldots, i-1, i+1, \ldots, n\}$ e $(j_1, \ldots, j_{n-1})$ è una (conveniente) permutazione degli indici $\{1, \ldots, j-1, j+1, \ldots, n\}$. In ciascun prodotto (2) figura un fattore col primo indice uguale ad j, perciò sarà multiplo di almeno uno degli elementi

$$q_{ji},\ q_{jr_1} q_{r_1 i},\ \cdots,\ q_{jr_1} q_{r_1 r_2} \cdots q_{r_{n-2} i}$$

con $r_1, \ldots, r_{n-2}$ interi positivi minori di n, distinti tra loro e diversi da i e da j. Perciò ogni prodotto (2) è multiplo anche di q_{ji} in forza delle (1). Sono così provate le

$$X_{ij} \equiv O \bmod.(q_{ji}) \qquad (i \neq j;\ i, j = 1, \ldots, n) \tag{3}$$

Valendo inoltre la $X \equiv I \bmod.(Q)$ e le (3) ora stabilite, esistono degli elementi $a_i, b_{ri} \in R$, $(i, r = 1, \ldots, n)$, tali che

$$\begin{cases} x_{ii} = 1 + a_i q_{ii} \\ x_{ir} X_{ir} = b_{ir} q_{ii} \qquad (i, r = 1, \ldots, n)\,. \end{cases} \tag{4}$$

Sviluppando ora $det\, X$ secondo gli elementi della i-sima riga, e tenendo conto delle (4), si ha

$$det\, X = x_{i1} X_{i1} + \ldots + x_{ii} X_{ii} + \ldots + x_{in} X_{in} =$$
$$= X_{ii} + (b_{i1} + \ldots + b_{ii-1} + a_i X_{ii} + b_{ii+1} + \ldots + b_{in})\, q_{ii}.$$

Valgono perciò anche le relazioni

$$(3') \qquad X_{ii} \equiv det\, X \text{ mod. } (q_{ii}) \qquad (i = 1, \ldots, n);$$

ma le (3) e le (3') si possono mettere nella forma equivalente

$$(Agg\, X)_{-1} \equiv (det\, X) \cdot I \text{ mod. } (Q) .$$

OSSERVAZIONE. Dalla identità

$$det\, X = x_{11} x_{22} \ldots x_{nn} + \Sigma \varepsilon x_{1j_1} x_{2j_2} \ldots x_{nj_n}, \qquad \text{con} \quad \varepsilon = \pm 1$$

dove $(j_1, \ldots, j_n)$ è una qualunque permutazione di $\{1, \ldots, n\}$, diversa da quella identica, segue che

$$(5) \qquad det\, X \equiv 1 \text{ mod. } ((q_{11}, \ldots, q_{nn}))$$

e, essendo anche X_{ii} un determinante, le analoghe

$$(5') \quad X_{ii} \equiv 1 \text{ mod. } ((q_{11}, \ldots, q_{i-1\,i-1}, q_{i+1\,i+1}, \ldots, q_{nn})) \qquad (i = 1, \ldots, n)$$

sempre in forza delle (1).

COROLLARIO. *Se all'ipotesi del lemma 2 si aggiunge quella che* $det\, X = 1$, *allora* $X^{-1} \equiv I$ mod. (Q).

A questo punto risulta ovvia la seguente

PROPOSIZIONE 1. *Per una fissata* $Q \in R_n$, *le matrici* $X \in \Gamma$ *che soddisfano alla* Q*-congreunza*

$$(6) \qquad X \equiv I \text{ mod. } (Q)$$

formano un sottogruppo se e solo se per la Q *valgono le relazioni* (1):

$$q_{ik} q_{kj} \equiv o \text{ mod. } (q_{ij}) \qquad (i, k, j = 1, \ldots, n)$$

DEFINIZIONE 2. Diciamo *gruppo* Q*-congruenziale* ogni sottogruppo $G(n, Q)$ di Γ i cui elementi sono tutte e sole le soluzioni di una Q-congruenza (6).

Si vede subito che, se $Q = \|q_{ij}\|$, con $q_{ij} = q$, $(i, j = 1, \ldots, n)$, il gruppo Q-congruenziale $G(n, Q)$ si riduce al gruppo congruenziale

principale

$$G(n, q) = \{X \in \Gamma\colon\ X \equiv I \bmod. (q)\}$$

ben noto nel caso classico. Se $Q = \|q_{ij}\|$, con $q_{ij} = 1$, $(i, j = 1, \ldots, n)$ e $n > 1$, allora $G(n, Q) = \Gamma$; se invece $n = 1$, allora $G(n, Q)$ coincide col gruppo $\{1\}$. Si supporrà sempre $n > 1$.

Si osservi inoltre che, se $G(n, Q)$ è un gruppo Q-congruenziale allora $G(n, Q)$ è un sottogruppo congruenziale nella accezione usuale, nel senso cioè che contiene un sottogruppo congruenziale principale (cfr. [4]). Si assuma per esempio, q_1, q_2, q_3 rispettivamente generatori degli ideali

$$\bigcap_{ij} (q_{ij}), \qquad \Big(\prod_{i \neq j} q_{ij}\Big), \qquad \Big(\prod_{ij} q_{ij}\Big) \qquad (i, j = 1, \ldots, n)$$

si hanno allora le inclusioni

$$G(n, q_3) \subset G(n, q_2) \subset G(n, q_1) \subset G(n, Q)\ .$$

I gruppi Q-congruenziali sopra definiti comprendono, come casi particolari, diversi tipi di gruppi congruenziali studiati in precedenza da vari autori. Tra questi ricordiamo i gruppi $G(m, n, r) \subset SL(3, Z)$ considerati da I. Reiner e J. D. Swift (cfr. [1]):

$$G(m, n, r) = \{\|a_{ij}\| \in SL(3, Z)\colon\ m|a_{21}, n|a_{32}, r[m, n]|a_{31} \ \text{ con } r|(m, n)\}$$

e i gruppi $G_t(\eta) \subset SL(t, Z)$ di M. Newman e I. Reiner (cfr. [2]) così definiti

$$G_t(\eta) = G_{1,t-1}(n_1) \cap G_{2,t-2}(n_2) \cap \ldots \cap G_{t-1,1}(n_{t-1})$$

con $\eta = (n_1, \ldots, n_{t-1})$, $n_i \in Z$, $n_i > 0$, avendo posto

$$G_{r,s}(n) = \left\{ \left\| \begin{matrix} A^{(r)} & B \\ C & D^{(s)} \end{matrix} \right\| \in SL(t, Z)\colon\ C \equiv 0 \bmod. (n) \right\}$$

con r, s interi positivi tali che $r + s = t$, e, se $t = 2r$, anche i gruppi

$$G_r(m, n) = \left\{ \left\| \begin{matrix} A^{(r)} & B \\ C & D^{(s)} \end{matrix} \right\| \in SL(2r, Z)\colon\ B \equiv 0 \bmod. (m),\ C \equiv 0 \bmod. (n) \right\}.$$

Essi rientrano tutti nella classe dei gruppi Q-congruenziali relativi ad una conveniente matrice Q. Così, per esempio, $G(m, n, r)$ è il gruppo $G(3, Q)$ con

$$Q = \begin{Vmatrix} 1 & 1 & 1 \\ m & 1 & 1 \\ r[m, n] & n & 1 \end{Vmatrix} \quad \text{con } r|(m, n) .$$

e $G_t(\eta) = G(t, Q)$ con $Q = \|q_{ij}\|$ definita dalle

$$\begin{cases} q_{ij} = 1 & \text{se } i \leqslant j \\ q_{ij} = [n_j, n_{j+1}, \ldots, n_{i-1}] & \text{se } i > j \quad (i, j = 1, \ldots, n) \end{cases}$$

$G_r(m, n) = G(2r, Q)$ con $Q = \|q_{ij}\|$ definita ponendo

$$\begin{cases} q_{ij} = m & \text{se } 1 \leqslant i \leqslant r,\ r+1 \leqslant j \leqslant 2r \\ q_{ij} = n & \text{se } r+1 \leqslant i \leqslant 2r,\ 1 \leqslant j \leqslant r \\ q_{ij} = 1 & \text{se } 1 \leqslant i,\ j \leqslant r, \text{ oppure } r+1 \leqslant i,\ j \leqslant 2r . \end{cases}$$

È facile convincersi che i gruppi Q-congruenziali qui introdotti rappresentano una effettiva generalizzazione dei precedenti (questi ultimi, in particolare, sono relativi a matrici Q con $q_{ii} = 1$ $(i = 1, \ldots, n)$). Classi di gruppi Q-congruenziali di tipo più generale si ottengono subito assumendo, per esempio:

a) $Q = \|r^{\alpha_{ij}}\|$ dove $r \in R - \{o\}$ e α_{ij} sono interi non negativi tali che $\alpha_{ik} + \alpha_{kj} \geqslant \alpha_{ij}$ $(i, k, j = 1, \ldots, n)$

b) $Q = \|r_i s_j\|$ dove $r_1, \ldots, r_n,\ s_1, \ldots, s_n \in R - \{o\}$.

2. – Alcune proprietà dei gruppi Q-congruenziali.

La nozione di sottogruppo Q-congruenziale permette di definire una mappa dall'insieme Σ'_n delle matrici di R_n soddisfacenti le (1) nell'insieme $\mathfrak{X}$ dei sottogruppi Q-congruenziali di Γ:

$$\gamma: \Sigma'_n \to \mathfrak{X} \tag{7}$$

avendo posto $\gamma(Q) = G(n, Q)$, per ogni $Q \in \Sigma'_n$.

Se S è un insieme completo di elementi non associati di R, desi-

gneremo con Σ_n l'insieme delle matrici di Σ'_n aventi gli elementi in S.

È facile dedurre alcune proprietà di γ.

1) *Se* $Q^{(1)} = \|q_{ij}^{(1)}\| \in \Sigma'_n$, *e* $Q^{(2)} = \|q_{ij}^{(2)}\| \in \Sigma'_n$ *e si ha*

$$(q_{ij}^{(1)}) \subseteq (q_{ij}^{(2)}) \qquad (i, j = 1, \ldots, n)$$

allora risulta $G(n, Q^{(1)}) \subseteq G(n, Q^{(2)})$.

2) *Se* $Q^{(1)} = \|q_{ij}^{(1)}\| \in \Sigma'_n$, *e* $Q^{(2)} = \|q_{ij}^{(2)}\| \in \Sigma'_n$, *posto* $Q^{(3)} = \|q_{ij}^{(3)}\|$ *con* $(q_{ij}^{(3)}) = (q_{ij}^{(1)}) \cap (q_{ij}^{(2)})$ *e* $q_{ij}^{(3)} \in S$, *si ha*

$$Q^{(3)} \in \Sigma_n \quad e \quad G(n, Q^{(3)}) = G(n, Q^{(1)}) \cap G(n, Q^{(2)}) .$$

3) *Se* $Q = \|q_{ij}\| \in \Sigma'_n$, *posto* $Q' = \|q'_{ij}\|$ *con*

$$(q'_{ij}) = \begin{cases} (q_{ij}) & (i \neq j) \\ (q_{i1}q_{1i}, \ldots, q_{ii-1}q_{i-1i}, q_{ii+1}q_{i+1i}, \ldots, q_{in}q_{ni}) & (i = j) \end{cases}$$

e $q'_{ij} \in S$, $(i, j = 1, \ldots, n)$, *si ha*

$$Q' \in \Sigma_n \quad e \quad G(n, Q') \subset G(n, Q) .$$

4) *Se* $Q = \|q_{ij}\| \in \Sigma'_n$, *posto* $Q'' = \|q''_{ij}\|$ *con*

$$(q''_{ij}) = \begin{cases} (q_{ij}) & (i \neq j) \\ (q_{11}, \ldots, q_{i-1i-1}, q_{i+1i+1}, \ldots, q_{nn}) & (i = j) \end{cases}$$

e $q''_{ij} \in S$, $(i, j = 1, \ldots, n)$, *si ha*

$$Q'' \in \Sigma_n \quad e \quad G(n, Q'') \supset G(n, Q) .$$

Il fatto che $Q'' \in \Sigma_n$ segue dalle (1). Sia $X \in G(n, Q)$. Sappiamo che i complementi algebrici X_{ii} in X soddisfano al sistema di congruenze

$$X_{ii} \equiv 1 \bmod ((q_{11}, \ldots, q_{i-1i-1}, q_{i+1i+1}, \ldots, q_{nn})) \qquad (i = 1, \ldots, n)$$

per le (5′). Quindi è pure soddisfatta l'inclusione $G(n, Q'') \supset G(n, Q)$.

5) *Se* $Q = \|q_{ij}\| \in \Sigma'_n$, *posto* $\hat{Q} = \|\hat{q}_{ij}\|$, *con*

$$(\hat{q}_{ij}) = \begin{cases} (q_{ij}) & (i \neq j) \\ (q_{ii}) \cap (q_{11}, \ldots, q_{i-1i-1}, q_{i+1i+1}, \ldots, q_{nn}) & (i = j) \end{cases}$$

e $\hat{q}_{ij} \in S$, $(i, j = 1, \ldots, n)$, *si ha*

$$\hat{Q} \in \Sigma_n \quad e \quad G(n, Q) = G(n, \hat{Q}) .$$

Ciò segue dalle proprietà 1), 2) e 4).

6) *Sia* $Q = \|q_{ij}\| \in \Sigma_n'$ *e* $q_i \in S$ *il prodotto degli eventuali fattori, di norma* 2 [1] *tra loro non associati, di* $(q_{i1}q_{1i}, \ldots, q_{ii-1}q_{i-1i}, q_{ii+1}q_{i+1i}, \ldots, q_{in}q_{ni})$; *altrimenti* $q_i = 1$. *Allora, posto* $\check{Q} = \|\check{q}_{ij}\|$, *con*

$$(\check{q}_{ij}) = \begin{cases} (q_{ij}) & (i \neq j) \\ (q_i) \cap (q_{ii}) & (i = j) \end{cases}$$

e $\check{q}_{ij} \in S$, $(i, j = 1, \ldots, n)$, *si ha*

$$\check{Q} \in \Sigma_n \quad e \quad G(n, \check{Q}) = G(n, Q) .$$

$\check{Q} \in \Sigma_n$ perchè soddisfa alle (1). Per la proprietà 1) risulta $G(n, \check{Q}) \subset G(n, Q)$. Sia $X = \|x_{ij}\| \in G(n, Q)$. Dalla identità

$$det\, X = x_{i1}X_{i1} + \ldots + x_{in}X_{in} = 1 \qquad (i = 1, \ldots, n)$$

segue, in forza delle (1) e del lemma 2,

$$(x_{ii}, q_{i1}q_{1i}, \ldots, q_{ii-1}q_{i-1i}, q_{ii+1}q_{i+1i}, \ldots, q_{in}q_{ni}) = 1 \qquad (i = 1, \ldots, n)$$

e perciò sarà anche $(x_{ii}, q) = 1$, $(i = 1, \ldots, n)$, per ogni arbitrario fattore q di q_i di norma $N(q) = 2$. Perciò $x_{ii} - 1 \in (q)$ e quindi $x_{ii} - 1 \in (q_i)$, essendo primi tutti i fattori di q_i. Ne segue che $x_{ii} - 1 \in (q_i) \cap (q_{ii})$ e allora $X \in G(n, \check{Q})$.

OSSERVAZIONE. Se $R = Z$, e S è l'insieme degli interi non negativi, $q_i \in \{1, 2\}$.

Per ogni $Q \in \Sigma_n'$ si possono considerare le matrici $\hat{Q}$ e $\check{Q}$ definite nell'enunciare le proprietà 5) e 6). Risulta immediato che le mappe

$$\hat{} : \Sigma_n' \to \Sigma_n' \quad e \quad \check{} : \Sigma_n' \to \Sigma_n'$$

sono idempotenti, cioè $(\hat{Q})\hat{} = \hat{Q}$ e $(\check{Q})\check{} = Q\check{}$. Inoltre $\hat{}$ e $\check{}$ non sono

---

[1] In accordo con M. Newman (cfr. [4]) chiameremo *norma* di r, $r \in R$, il cardinale di $R/(r)$; essa sarà indicata con $N(r)$.

banali come si può riconoscere assumendo, per esempio nel caso $n = 2$, $Q = \begin{Vmatrix} 3 & 4 \\ 9 & 9 \end{Vmatrix}$. Si ha allora

$$\hat{Q} = \begin{Vmatrix} 9 & 4 \\ 9 & 9 \end{Vmatrix}, \quad \check{Q} = \begin{Vmatrix} 6 & 4 \\ 9 & 18 \end{Vmatrix}, \quad (\hat{Q})\check{} = \begin{Vmatrix} 18 & 4 \\ 9 & 18 \end{Vmatrix} = (\check{Q})\hat{}.$$

3. – La matrice canonica di un gruppo Q-congruenziale.

In base alle proprietà 5) e 6) si vede che la mappa $\gamma: \Sigma_n' \to \mathfrak{X}$ non è iniettiva. Evidentemente ha importanza il problema di scegliere un rappresentante in ogni antiimmagine di un elemento di $\mathfrak{X}$; ciò porta ad individuare per ogni gruppo Q-congruenziale G una matrice « *canonica* » ad esso associata. Il problema viene risolto dalla prop. 2. A tale scopo è conveniente dare la

DEFINIZIONE 3. Siano $Q^{(1)} = \|q_{ij}^{(1)}\| \in \Sigma_n'$ e $Q^{(2)} = \|q_{ij}^{(2)}\| \in \Sigma_n'$ diremo che $Q^{(1)} \prec Q^{(2)}$ se e solo se $(q_{ij}^{(1)}) \supset (q_{ij}^{(2)})$ $(i, j = 1, \ldots, n)$

Risulta che $\prec$ è una relazione di preordine filtrante crescente. Infatti se $Q^{(1)}$, $Q^{(2)} \in \Sigma_n'$ esiste sempre (proprietà 2) $Q^{(3)} \in \Sigma_n'$ tale che $Q^{(1)} \prec Q^{(3)}$ e $Q^{(2)} \prec Q^{(3)}$. Inoltre se $Q^{(1)} \prec Q^{(2)}$ e $Q^{(2)} \prec Q^{(1)}$ allora $Q^{(1)}$ e $Q^{(2)}$ hanno elementi di ugual posto tra loro associati. Per ogni $Q \in \Sigma_n'$, se si assumono le notazioni usate negli enunciati delle proprietà 3), 4), 5) e 6), risulta

$$Q'' \prec Q \prec Q', \quad Q \prec \hat{Q}, \quad Q \prec \check{Q}.$$

PROPOSIZIONE 2. *Sia G un sottogruppo Q-congruenziale di $\Gamma = SL(n, R)$ e sia S un sistema completo di elementi non associati di R. Posto*

$$\Sigma_n = \{Q = \|q_{ij}\| \in \Sigma_n' : \ q_{ij} \in S\}$$

$$\mathcal{M} = \{Q \in \Sigma_n : \ G = G(n, Q)\}$$

$\mathcal{M}$ ammette un massimo Q^* che si può assumere quale matrice canonica del gruppo G. Se $Q^* = \|q_{ij}^*\|$, risulta

$$(q_{ij}^*) = \bigcap_Q (q_{ij}) \qquad (i, j = 1, \ldots, n)$$

al variare di $Q = \|q_{ij}\| \in \mathcal{M}$.

Dimostreremo la prop. 2 premettendo il

LEMMA 3. *Se* $Q^{(1)} = \|q_{ij}^{(1)}\| \in \Sigma_n'$ *e* $Q^{(2)} = \|q_{ij}^{(2)}\| \in \Sigma_n'$ *e risulta* $G(n, Q^{(1)}) = G(n, Q^{(2)})$, *allora si ha*

$$(q_{ij}^{(1)}) = (q_{ij}^{(2)}) \qquad (i \neq j;\ i, j = 1, \ldots, n)$$

In effetti $I + q_{ij}^{(1)} E_{ij} \in G(n, Q^{(1)})$ e $I + q_{ij}^{(2)} E_{ij} \in G(n, Q^{(2)})$ $(i \neq j;\ i, j = 1, \ldots, n)$. Da $G(n, Q^{(1)}) = G(n, Q^{(2)})$ seguono allora le

$$(q_{ij}^{(1)}) = (q_{ij}^{(2)}) \qquad (i \neq j;\ i, j = 1, \ldots, n)\,.$$

DIM. DELLA PROP. 2. Si consideri una matrice qualunque $Q \in \mathcal{M}$ e da questa si formi la $Q' = \|q_{ij}'\|$ come nell'enunciato della proprietà 3). Per il lemma 3, Q' non dipende dalla particolare Q scelta in $\mathcal{M}$. Sia ora

$$\mathcal{N} = \{Q = \|q_{ij}\| \in \Sigma_n\colon\ (q_{ij}) \supseteq (q_{ij}')\,;\ (i, j = 1, \ldots, n)\}\,.$$

Valendo in R la fattorizzazione unica risulta che $\mathcal{N}$ è finito e così $\mathcal{M}$ essendo $\mathcal{M} \subset \mathcal{N}$. Poichè la relazione $\prec$ è filtrante crescente su $\mathcal{M}$ e $\mathcal{M}$ è finito, $\mathcal{M}$ ammette un elemento massimo Q^*. Dalla definizione di $\prec$ e dalla proprietà 2) risulta inoltre che, posto $Q^* = \|q_{ij}^*\|$,

$$(q_{ij}^*) = \bigcap_{Q} (q_{ij}) \qquad (i, j = 1, \ldots, n)$$

al variare di $Q = \|q_{ij}\| \in \mathcal{M}$.

4. – Applicazioni.

Facciamo ora due applicazioni, relative al caso $n = 2$. La prima (4*a*) fornisce un procedimento costruttivo della matrice canonica Q^* di un gruppo $G(2, Q)$, a partire da una qualunque Q che lo definisce. La seconda (4*b*) è la formula dell'indice (quando è finito) $[\Gamma\colon G(2, Q)]$. La formula include casi precedentemente noti.

4*a*. Diamo un procedimento per la effettiva costruzione della matrice canonica Q^*, nel caso $n = 2$. Osserviamo innanzi tutto che, in forza della proprietà 5), si può iniziare la costruzione a partire diret-

tamente da una matrice del tipo $Q = \hat{Q}$; in tale ipotesi, essendo $n = 2$, $Q = \|q_{ij}\| \in \Sigma_2$ soddisfa alla $q_{11} = q_{22}$.

LEMMA 4. *Siano* $q, q_1, q_2 \in R$, *con* $(q_1) \supset (q)$ *e* $(q_2) \supset (q)$. *Gli insiemi*

$$H_k = \{x \in R: (x, q) = 1 \ e \ x - 1 \in (q_k)\} \qquad (k = 1, 2)$$

coincidono tra loro se e solo se risulta

$$(q_1) \cap (q_3) = (q_2) \cap (q_3)$$

essendo q_3 *il prodotto degli eventuali fattori non associati di* q *di norma* 2; *altrimenti* $q_3 = 1$.

Sia $\bar{q}$ un elemento primo di R; l'equazione $(x, \bar{q}) = 1$, con $x \in R$, è equivalente alla $x - 1 \in (\bar{q})$ se e solo se $N(\bar{q}) = 2$. Per il lemma del resto cinese risulta allora che, se q_3 è il prodotto degli eventuali fattori non associati di q di norma 2, ogni $x \in R$ tale che $(x, q) = 1$ soddisfa necessariamente alla $x - 1 \in (q_3)$. Pertanto gli insiemi H_1 e H_2 coincidono se e solo se risulta

$$(q_1) \cap (q_3) = (q_2) \cap (q_3) .$$

Se q non ammette alcun fattore di norma 2, allora si può porre $q_3 = 1$ e la conclusione è la stessa, anzi, allora si ha $(q_1) = (q_2)$, come del resto risulta anche quando $(q_1) \subset (q_3)$ e $(q_2) \subset (q_3)$.

LEMMA 5. *Siano*

$$Q_1 = \begin{Vmatrix} q_1 & q_{12} \\ q_{21} & q_1 \end{Vmatrix} \in \Sigma_2' \quad \text{e} \quad Q_2 = \begin{Vmatrix} q_2 & q_{12} \\ q_{21} & q_2 \end{Vmatrix} \in \Sigma_2'$$

e q_3 *il prodotto degli eventuali fattori non associati di* $q_{12} q_{21}$ *di norma* 2; *altrimenti* $q_3 = 1$. *Risulta allora*

$$G(2, Q_1) = G(2, Q_2) \Leftrightarrow (q_1) \cap (q_3) = (q_2) \cap (q_3)$$

equivalente alla

$$G(2, Q_1) = G(2, Q_2) \Leftrightarrow \breve{Q}_1 = \breve{Q}_2 .$$

Si ponga

$$H_k = \{x \in R\colon\ (x,\ q_{12}q_{21}) = 1 \quad \text{e} \quad x - 1 \in (q_k)\} \qquad (k = 1, 2)$$

Per il lemma 4 basta provare che $H_1 = H_2$ e $G(2, Q_1) = G(2, Q_2)$ sono relazioni equivalenti. Definiamo le mappe

$$\alpha_k\colon\ G(2, Q_k) \to H_k \qquad (k = 1, 2)$$

tali che $\alpha_k(X) = x_{11}$, se $X = \|x_{ij}\| \in G(2, Q_k)$. Poichè $det\, X = 1$, risulta ovvio che $\alpha_k(G(2, Q_k)) \subset H_k$. Proviamo che α_1 e α_2 sono suriettive. Sia x un arbitrario elemento di H_k, allora esiste (per un noto lemma) $y \in H_k$ tale che $xy \equiv 1$ mod. $(q_{12}q_{21})$ e perciò esiste almeno uno $z \in R$ tale che $xy - 1 = zq_{12}q_{21}$ e tutti e soli gli elementi dell'insieme

$$F_k(x) = \left\{X = \left\| \begin{matrix} x & z_1 q_{12} \\ z_2 q_{21} & y \end{matrix} \right\| \in G(2, Q_k)\colon\ z_1 z_2 = z\right\} \qquad (k = 1, 2)$$

soddisfano alla condizione $\alpha_k(X) = x$.

Se si suppone che $G(2, Q_1) = G(2, Q_2)$ allora necessariamente si ha $H_1 = H_2$; viceversa se $H_1 = H_2$ allora, per ogni $x \in H_1 = H_2$ risulta $F_1(x) = F_2(x)$ e quindi $G(2, Q_1) = G(2, Q_2)$. Da ciò segue anche che

$$G(2, Q_1) = G(2, Q_2) \Leftrightarrow \check{Q}_1 = \check{Q}_2$$

perchè $(\check{q}_1) = (q_1) \cap (q_3) = (q_2) \cap (q_3) = (\check{q}_2)$.

Osservando che per $n = 2$ si ha $(\check{Q})\hat{} = (\hat{Q})\check{}$, per ogni $Q \in \Sigma_2'$, risulta provata la

PROPOSIZIONE 3. *Sia $G = G(2, Q)$ un gruppo Q-congruenziale di $\Gamma = SL(2, R)$. La matrice canonica Q^* del gruppo G risulta*

$$Q^* = (\hat{Q})\check{} = (\check{Q})\hat{}$$

qualunque sia la matrice Q tale che $G = G(2, Q)$. In particolare una matrice

$$Q = \left\| \begin{matrix} q_1 & q_2 \\ q_3 & q_1 \end{matrix} \right\|, \qquad con\ \ (q_1) \supset (q_2 q_3) \neq (o)$$

è la matrice canonica di $G(2,Q)$ *se e solo se il prodotto di tutti gli eventuali fattori non associati di* $q_2 q_3$ *di norma* 2 *divide* q_1.

4*b*. A questo punto si può dedurre una formula per l'indice $[\Gamma\colon G(2,Q)]$, qualunque sia $Q \in \Sigma_2'$ nell'ipotesi che la norma di $q_{12} q_{21} \in R$ sia finita.

PROPOSIZIONE 4. *Sia*

$$Q = \begin{Vmatrix} q_1 & q_2 \\ q_3 & q_1 \end{Vmatrix} \in \Sigma_2' \qquad e \qquad N(q_2 q_3) < \infty .$$

L'indice del gruppo $G(2,Q)$ *in* $\Gamma = SL(2,R)$ *è dato dalla formula*

$$[\Gamma\colon G(2,Q)] = \frac{N(q_2 q_3)^2 \varphi(q_1)}{\varphi(q_2 q_3)} \prod_{p \mid q_2 q_3} \left(1 - \frac{1}{N(p)^2}\right)$$

avendo indicato con $N(q_2 q_3)$ *e con* $\varphi(q_2 q_3)$ *rispettivamente la norma di* $q_2 q_3$ *e l'ordine del gruppo delle unità di* $R/(q_2 q_3)$.

La dimostrazione si può effettuare seguendo un procedimento simile a quelli usati per il calcolo di formule analoghe ricordando il ben noto isomorfismo (cfr. [4])

$$SL(n,R)/G(n,q) \xrightarrow{\sim} SL(n, R/(q)) \qquad \text{per ogni } \; q \in R - \{o\}$$

e la formula

$$[\Gamma\colon (G(2,q)] = N(q)^3 \prod_{p \mid q} \left(1 - \frac{1}{N(p)^2}\right) \qquad \text{con } p \text{ fattore primo di } q.$$

BIBLIOGRAFIA

[1] I. REINER - J. D. SWIFT, *Congruence subgroups of matrix groups*, Pacific Journal Math., **6** (1956), pp. 529-540.

[2] M. NEWMAN - I. REINER, *Inclusion theorems for congruence subgroups*, Trans. A.M.S., **91** (1959), pp. 369-379.

[3] H. Bass - M. Lazard - J. P. Serre, *Sous-groupes d'indice fini dans $SL(n, Z)$*, Bulletin A.M.S., **70** (1964), pp. 385-392.
[4] M. Newman, *Integral matrices*, Academic Press (1972).
[5] M. Rosati, *Sottogruppi congruenziali principali del gruppo simplettico modulare*, Rend. Acc. Naz. dei Lincei, **47** (1969), pp. 167-172.
[6] R. A. Rankin, *Subgroups of the modular group defined by a single linear congruence*, Acta Arithmetica, **24** (1973), pp. 313-323.

Manoscritto pervenuto in redazione il 9 ottobre 1975.