Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Mario Rosati

Sottogruppi congruenziali principali del gruppo simplettico modulare

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **47** (1969), n.3-4, p. 167–172.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_47_3-4_167_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1969.

Geometria. — *Sottogruppi congruenziali principali del gruppo simplettico modulare* (*). Nota (**) di MARIO ROSATI, presentata dal Socio B. SEGRE.

SUMMARY. — A new general definition of the principal congruence subgroups of the symplectic modulary group Γ with regard to a matrix $\mathfrak{Q}$ is given, instead of—as usual—with respect to an integer q. Necessary and sufficient conditions for $\mathfrak{Q}$ in order that such subgroups may exist are then found, and then all the corresponding subgroups are obtained.

INTRODUZIONE.

Il gruppo simplettico modulare n-dimensionale $\Gamma_1 = S_p(n; Z)$ si presenta come naturale estensione del gruppo modulare classico di Hilbert, quando si passi dallo studio delle funzioni modulari in 1 variabile a quello delle funzioni abeliane modulari in n variabili.

Il gruppo Γ_1, la cui funzione e importanza è stata messa in evidenza a partire dal 1939 specialmente da C. L. Siegel, si può definire come gruppo automorfo di una forma bilineare antisimmetrica a divisori unitari; esso può quindi venire rappresentato come gruppo delle matrici $\mathfrak{T}$ intere di ordine $2n$ soddisfacenti la condizione

$$\mathfrak{T}\mathfrak{M}_1\mathfrak{T}_{-1} = \mathfrak{M}_1 \tag{1}$$

con

$$\mathfrak{M}_1 = \begin{Vmatrix} O & I \\ -I & O \end{Vmatrix}, \tag{2}$$

dove O ed I sono le matrici zero ed uno di ordine n, mentre $\mathfrak{T}_{-1}$ indica la trasposta di $\mathfrak{T}$.

L'interpretazione di Γ_1 come gruppo discontinuo di trasformazioni analitiche nello spazio $\mathcal{H}$ delle matrici simmetriche di ordine n, $Z = X + iY$, con la parte immaginaria Y definita positiva, e l'incidenza delle sue proprietà nello studio del campo fondamentale $\mathcal{H}/\Gamma_1$ come modello della varietà abeliana modulare relativa al caso dei divisori unitari, giustificano largamente l'interesse di molti altri ricercatori per il gruppo modulare Γ_1 (*Modulgruppe*).

Più recentemente alcuni allievi del Siegel (cfr. per esempio [2], [3], [7], [8]) hanno iniziato uno studio del gruppo modulare Γ a divisori arbitrari (*Paramodulare Gruppe*), generalizzazione del precedente, che era stato considerato di passaggio dallo stesso Siegel. Il gruppo Γ ha, nei confronti

(*) Lavoro eseguito nell'ambito dei contratti di ricerca del C.N.R.

(**) Pervenuta all'Accademia il 22 ottobre 1969.

delle funzioni abeliane a divisori arbitrari, la stessa posizione che il gruppo Γ_1 ha verso le funzioni abeliane a divisori unitari. Esso può identificarsi con il gruppo automorfo di una forma antisimmetrica a divisori arbitrari $\delta_1, \delta_2, \cdots, \delta_n$ (dove $\delta_1 = 1$, $\delta_{i-1} \mid \delta_i$ per $i = 2, 3, \cdots, n$), ed è pertanto rappresentabile nel gruppo delle matrici $\mathfrak{T}$ intere soddisfacenti ancora la (1) nella quale però al posto di $\mathfrak{M}_1$ si ponga la matrice

$$\mathfrak{M} = \begin{Vmatrix} O & \Delta \\ -\Delta & O \end{Vmatrix}, \tag{3}$$

essendo Δ la matrice diagonale che ha per elementi gli interi $\delta_1, \delta_2, \cdots, \delta_n$.

Le ricerche menzionate sul gruppo Γ sono in gran parte orientate alla determinazione di proprietà aritmetiche di Γ, in particolare la costruzione e lo studio dei suoi sottogruppi congruenziali (*Kongruenzuntergruppen*) i quali, essendo di indice finito in Γ, sono anch'essi discontinui nello spazio $\mathcal{H}$ ed ammettono un campo fondamentale le cui proprietà sono strettamente legate a quelle del campo fondamentale di Γ_1.

A questo punto, è doveroso ricordare che il gruppo Γ già in precedenza era stato oggetto di uno studio approfondito da parte di F. Conforto ([4], [5], [6]). In particolare nel volume [4], dopo aver sottolineato la impossibilità di limitarsi al gruppo Γ_1, se si vuole allargare lo studio a tutte le funzioni abeliane modulari oltre quelle a divisori unitari, viene posto esplicitamente, e portato a buon punto, il problema della costruzione del campo fondamentale $\mathcal{H}/\Gamma$.

Questa Nota vuol dare un contributo allo studio dei sottogruppi congruenziali del gruppo Γ nel senso che ora precisiamo.

In analogia con il caso classico ($n = 1$), solitamente si definiscono in primo luogo i sottogruppi congruenziali principali (*Hauptkongruenzuntergruppen*) $\Gamma(q)$: fissato l'intero $q > 1$, $\Gamma(q)$ è costituito dalle matrici soddisfacenti la condizione

$$\mathfrak{T} \equiv \mathfrak{I}\ (q), \tag{4}$$

dove $\mathfrak{I}$ è la matrice uno di ordine $2n$.

In secondo luogo si assume come sottogruppo congruenziale di Γ (*Kongruenzuntergruppe*) qualunque sottogruppo di Γ contenente un $\Gamma(q)$. I gruppi $\Gamma(q)$ risultano tutti di indice finito e normali in Γ, mentre un sottogruppo congruenziale qualunque non è necessariamente normale, ma è sempre ovviamente d'indice finito in Γ, proprietà questa essenziale per le applicazioni alle funzioni modulari.

Alcuni tipi particolari di sottogruppi congruenziali, oltre ai $\Gamma(q)$, sono stati studiati da vari Autori (una buona bibliografia sull'argomento si trova in [2]), che ne hanno dato una rappresentazione esplicita a mezzo di una o più relazioni di congruenza per le $\mathfrak{T}$, più generali della (4), che di solito però sono relative ad un solo modulo q.

Fino a che punto si può dare una costruzione dei sottogruppi congruenziali di Γ mediante relazioni di congruenza, le quali siano concretamente utilizzabili per lo studio dei sottogruppi stessi?

In questa Nota incominciamo col dare una definizione molto generale di sottogruppi congruenziali principali di Γ, utilizzando come modulo di congruenza una matrice $\mathfrak{Q}$ di ordine $2n$ in luogo del modulo q.

Un'indagine approfondita delle proprietà della $\mathfrak{Q}$ ci permette di ottenere delle condizioni necessarie e sufficienti affinché la $\mathfrak{Q}$ definisca effettivamente un sottogruppo congruenziale, condizioni che nel caso classico non si presentano.

Osserviamo infine che il problema si pone negli stessi termini nei confronti dei sottogruppi congruenziali del gruppo unimodulare o di altri gruppi analoghi.

1. *Definizione di* $\Gamma(n\,;\Delta\,;\mathfrak{Q})$.

Nel gruppo simplettico modulare n–dimensionale, relativo a divisori arbitrari, che indicheremo d'ora in avanti con $\Gamma(n\,;\Delta)$, consideriamo il sottoinsieme $\Gamma(n\,;\Delta\,;\mathfrak{Q})$ delle $\mathfrak{T}$ soddisfacenti la congruenza [1]

$$\mathfrak{T} \equiv \mathfrak{J}\,(\mathfrak{Q}) \tag{5}$$

dove $\mathfrak{J}$ è la matrice uno, e $\mathfrak{Q}$ è una matrice ad elementi interi positivi non tutti uno, entrambe di ordine $2n$. L'insieme considerato è non vuoto; in particolare per $\mathfrak{Q} = \|q_{rs}\|$ con $q_{rs} = q$ intero > 1, $r, s = 1, \cdots, n$ coincide con un sottogruppo congruenziale principale secondo la definizione classica.

Per una scelta arbitraria di $\mathfrak{Q}$, l'insieme $\Gamma(n\,;\Delta\,;\mathfrak{Q})$ non è un sottogruppo; nel numero 2 vedremo quando ciò accade. È chiaro comunque che, allorquando $\Gamma(n\,;\Delta\,;\mathfrak{Q})$ è un sottogruppo, esso è congruenziale in $\Gamma(n\,;\Delta)$ perché contiene il sottogruppo congruenziale principale relativo all'intero $q = \text{m.c.m.}\,(q_{rs})$.

2. *I sottogruppi* $\Gamma(n\,;\Delta\,;\mathfrak{Q})$.

Scriviamo la $\mathfrak{T}$ e la $\mathfrak{Q}$ rispettivamente nella forma

$$\mathfrak{T} = \begin{Vmatrix} A & B \\ C & D \end{Vmatrix} \quad , \quad \mathfrak{Q} = \begin{Vmatrix} Q^{(1)} & Q^{(2)} \\ Q^{(3)} & Q^{(4)} \end{Vmatrix}, \tag{6}$$

dove le matrici parziali hanno tutte ordine n, e ricordiamo che [2], analogamente, la $\mathfrak{T}^{-1}$ si scrive

$$\mathfrak{T}^{-1} = \begin{Vmatrix} \Delta D_{-1}\Delta^{-1} & -\Delta B_{-1}\Delta^{-1} \\ -\Delta C_{-1}\Delta^{-1} & \Delta A_{-1}\Delta^{-1} \end{Vmatrix}, \tag{7}$$

le quattro matrici parziali risultando necessariamente intere.

(1) Si intende, ovviamente, che la scrittura $A \equiv B\,(C)$ riassume le congruenze $a_{rs} \equiv b_{rs}\,(c_{rs})$ per ogni r, s.

(2) Cfr. per esempio [4], [11].

Supponiamo ora che $\Gamma(n;\Delta;\mathfrak{Q})$ sia un sottogruppo di $\Gamma(n;\Delta)$. La (5), tenendo conto delle (6), si esplicita nelle

$$A \equiv I \quad (Q^{(1)}) \quad , \quad B \equiv O \quad (Q^{(2)}) \quad , \quad C \equiv O \quad (Q^{(3)}) \quad , \quad D \equiv I \quad (Q^{(4)}), \tag{8}$$

mentre l'appartenenza di $\mathfrak{T}^{-1}$ a $\Gamma(n;\Delta;\mathfrak{Q})$ implica:

$$\begin{array}{llll} \Delta D_{-1}\Delta^{-1} \equiv I & (Q^{(1)}) \quad , & \Delta B_{-1}\Delta^{-1} \equiv O & (Q^{(2)}), \\ \Delta C_{-1}\Delta^{-1} \equiv O & (Q^{(3)}) \quad , & \Delta A_{-1}\Delta^{-1} \equiv I & (Q^{(4)}). \end{array} \tag{9}$$

Osserviamo ora che, nelle nostre ipotesi, fermo restando $\Gamma(n;\Delta;\mathfrak{Q})$, si può supporre che le

$$\Delta Q_{-1}^{(1)}\Delta^{-1} \quad , \quad \Delta Q_{-1}^{(2)}\Delta^{-1} \quad , \quad \Delta Q_{-1}^{(3)}\Delta^{-1} \quad , \quad \Delta Q_{-1}^{(4)}\Delta^{-1} \tag{10}$$

siano intere, eventualmente sostituendo un $q_{rs}^{(i)}$ $(r > s)$ con il m.c.m. $(q_{rs}^{(i)}, \delta_r/\delta_s)$ [si ricordi che sono intere le matrici parziali di (7)]. Dopodiché si può supporre, senza alterare $\Gamma(n;\Delta;\mathfrak{Q})$, che sia

$$\left\{\begin{array}{ll} Q^{(1)} = \Delta Q_{-1}^{(4)}\Delta^{-1} & \qquad (\text{e} \quad Q^{(4)} = \Delta Q_{-1}^{(1)}\Delta^{-1}). \\ Q^{(2)} = \Delta Q_{-1}^{(2)}\Delta^{-1} & \\ Q^{(3)} = \Delta Q_{-1}^{(3)}\Delta^{-1} & \end{array}\right. \tag{11}$$

Ci si convince di ciò pensando che, ferma restando la validità delle (8) e (9), si può eventualmente sostituire $q_{rs}^{(1)}$ e $q_{rs}^{(4)}$ rispettivamente con

$$\bar{q}_{rs}^{(1)} = \text{m.c.m.}\,(q_{rs}^{(1)}, q_{sr}^{(4)}\,\delta_r/\delta_s)$$

$$\bar{q}_{sr}^{(4)} = \bar{q}_{rs}^{(1)}\,\delta_s/\delta_r \qquad\qquad \text{quando} \quad r \leq s,$$

e invece con

$$\bar{q}_{rs}^{(1)} = \bar{q}_{sr}^{(4)}\,\delta_r/\delta_s$$

$$\bar{q}_{sr}^{(4)} = \text{m.c.m.}\,(q_{sr}^{(4)}, q_{rs}^{(1)}\,\delta_s/\delta_r) \qquad \text{quando} \quad r > s.$$

Ciò dimostra la prima delle (11). Le altre due si dimostrano in modo analogo. Si noti poi che le (11) equivalgono alla:

$$\mathfrak{Q} = \mathfrak{M}\,\mathfrak{Q}_{-1}\mathfrak{M}^{-1}. \tag{12}$$

Si conclude con la:

PROPOSIZIONE. *Quando la matrice* $\mathfrak{Q}$ *definisce, tramite la* (5), *un gruppo* $\Gamma(n;\Delta;\mathfrak{Q})$, *si può supporre, senza limitazione, che* $\mathfrak{Q}$ *soddisfi la condizione* (12).

D'altronde, se $\mathfrak{Q}$ soddisfa la (12), è subito visto che non appena una $\mathfrak{T}$ soddisfa le (8) essa soddisfa anche le (9), le quali esprimono che $\mathfrak{T}^{-1}$ soddisfa le (8).

Affinché $\Gamma(n ; \Delta ; \mathfrak{Q})$ sia effettivamente un gruppo, manca ancora la condizione relativa al prodotto. Vedremo che ciò comporta ulteriori onerose condizioni per $\mathfrak{Q}$.

Consideriamo a questo scopo i seguenti elementi di $\Gamma(n ; \Delta ; \mathfrak{Q})$

$$\mathfrak{T}_{rs}^{(1)} = \begin{Vmatrix} A & O \\ O & \Delta A_{-1}^{-1} \Delta^{-1} \end{Vmatrix} \qquad \text{con} \quad A = \| a_{ik} \|$$

e $a_{ii} = 1$, $a_{rs} = q_{rs}^{(1)}$ (altrimenti $a_{ik} = 0$) per $r \neq s$;

$$\mathfrak{T}_{rs}^{(2)} = \begin{Vmatrix} I & B \\ O & I \end{Vmatrix} \qquad \text{con} \quad B = \| b_{ik} \|$$

e $b_{rs} = q_{rs}^{(2)}$, $b_{sr} = q_{sr}^{(2)} = q_{rs}^{(2)} \delta_s/\delta_r$ (altrimenti $b_{ik} = 0$), per $r \leq s$;
invece $b_{rs} = q_{rs}^{(2)} = q_{sr}^{(2)} \delta_r/\delta_s$, $b_{sr} = q_{sr}^{(2)}$ (altrimenti $b_{ik} = 0$), per $r > s$;

$$\mathfrak{T}_{rs}^{(3)} = \begin{Vmatrix} I & O \\ C & I \end{Vmatrix} \qquad \text{con} \quad C = \| c_{ik} \|$$

e $c_{rs} = q_{rs}^{(3)}$, $c_{sr} = q_{sr}^{(3)} = q_{rs}^{(3)} \delta_s/\delta_r$ (altrimenti $c_{ik} = 0$), per $r \leq s$;
invece $c_{rs} = q_{rs}^{(3)} = q_{sr}^{(3)} \delta_r/\delta_s$, $c_{sr} = q_{sr}^{(3)}$ (altrimenti $c_{ik} = 0$), per $r > s$.

Imponendo che appartengano a $\Gamma(n ; \Delta , \mathfrak{Q})$ i prodotti del tipo

$$\mathfrak{T}_{rs}^{(1)} \mathfrak{T}_{si}^{(1)} \quad , \quad \mathfrak{T}_{rs}^{(2)} \mathfrak{T}_{si}^{(3)} \quad , \quad \mathfrak{T}_{rs}^{(1)} \mathfrak{T}_{si}^{(2)} \quad , \quad \mathfrak{T}_{rs}^{(3)} \mathfrak{T}_{si}^{(1)}$$

si ottengono le seguenti condizioni necessarie per $\mathfrak{Q}$:

$$(13) \qquad \begin{cases} a) & q_{rs}^{(1)} q_{si}^{(1)} \equiv 0 \quad (q_{ri}^{(1)}) \\ b) & q_{rs}^{(2)} q_{si}^{(3)} \equiv 0 \quad (q_{ri}^{(1)}) \\ c) & q_{rs}^{(1)} q_{si}^{(2)} \equiv 0 \quad (q_{ri}^{(2)}) \\ d) & q_{rs}^{(3)} q_{si}^{(1)} \equiv 0 \quad (q_{ri}^{(3)}). \end{cases}$$

Dalle (13) e dalla (12) seguono altri quattro gruppi analoghi di congruenze le quali, con le (13) costituiscono un sistema perfettamente simmetrico.

A questo punto è semplice verificare il fatto che per ogni $\mathfrak{T}, \mathfrak{S} \in \Gamma(n ; \Delta ; \mathfrak{Q})$ risulta $\mathfrak{T}\mathfrak{S} \in \Gamma(n ; \Delta ; \mathfrak{Q})$, proprio in forza delle (13).

Osserviamo poi che $\Gamma(n ; \Delta ; \mathfrak{Q})$ coincide con $\Gamma(n ; \Delta)$ quando e soltanto quando $q_{rs}^{(i)} = \delta_r/\delta_s \; (r > s)$, $q_{rs}^{(i)} = 1 \; (r \leq s)$, per $i = 1, 2, 3, 4$.

Concludiamo con il seguente:

TEOREMA. *Per le matrici* $\mathfrak{Q}$ *della forma* (12), *le congruenze* (13) *sono un sistema di condizioni necessarie e sufficienti affinché* $\Gamma(n ; \Delta ; \mathfrak{Q})$ *sia un sottogruppo di* $\Gamma(n ; \Delta)$.

I sottogruppi $\Gamma(n ; \Delta ; \mathfrak{Q})$ che possono ancora chiamarsi *sottogruppi congruenziali principali* di $\Gamma(n ; \Delta)$, se pure riferiti a una matrice $\mathfrak{Q}$ anziché ad un intero q, sono tutti e soli i sottogruppi congruenziali di $\Gamma(n ; \Delta)$ ottenibili attraverso la (5).

BIBLIOGRAFIA.

[1] BASS H., LAZARD M. e SERRE J. P., *Sous-groupes d'indice fini dans SL (n , Z)*, « Bulletin of the A.M.S. », *70*, 385–392 (1964).

[2] CHRISTIAN U., *Einführung in die Theorie der paramodularen Gruppen*, « Mathem. Annalen », *168*, 59–104 (1967).

[3] CHRISTIAN U., *Über die erste Zeile paramodularer Matrizen*, « Nachrichten der Akad. der Wiss. in Göttingen », n. 20, 239–245 (1967).

[4] CONFORTO F., *Funzioni abeliane modulari*, vol. I, « Istituto Naz. di Alta Matematica », Docet Ediz. Universitarie, Roma 1951, 434.

[5] CONFORTO F., *Problèmes résolus et non résolus de la théorie des fonctions abeliennes dans ses rapports avec la géométrie algébrique*, Colloque de Géometrie algébrique, Liege 1952, 89–110.

[6] CONFORTO F., *Un nuovo indirizzo nella teoria delle funzioni abeliane*, « Atti del IV Congresso dell'U.M.I. », Ed. Cremonese, 141–163 (1952).

[7] KLINGEN H., *Bemerkungen über Kongruenzuntergruppen der Modulgruppe n-ten Grades*, « Arch. Mathem. », *10*, 113–122 (1959).

[8] KOECHER M., *Zur Theorie der Modulfunktionen n-ten Grades I*, « Mathem. Zeitschrift », *59*, 389–416 (1954).

[9] NEWMAN M. e SMART J. R., *Symplectic modulary groups*, « Acta Arithmetica », *9*, 83–89 (1964).

[10] SIEGEL C. L., *Einführung in die Theorie der Modulfunktionen n-ten Grades*, « Mathem. Annalen », *116*, 617–657 (1939).

[11] SIEGEL C. L., *Analytic functions of several complex variables*, « The Institute for advanced study », Princeton (N. J.), 200 (1948–49).

[12] SIEGEL C. L., *Automorphe Funktionen in mehreren Variablen*, Universität Göttingen, 199 (1954–55).