Teoria delle sostituzioni che operano su una infinità numerabile di elementi.

Memoria 3ª (*) di LUIGI ONOFRI (a Bologna).

Sunto. - *In questa terza ed ultima Memoria sulle sostituzioni operanti su infiniti elementi, l'A. tratta della transitività e della intransitività nelle sue varie forme, del gruppo totale e di altri gruppi speciali.*

CAPITOLO V.

TRANSITIVITÀ ED INTRANSITIVITÀ

A) Transitività.

98. Sia $\mathfrak{C}$ un gruppo od uno pseudogruppo di sostituzioni sull'insieme numerabile I di elementi:

$$1,\ 2,\ldots,\ n,\ldots.$$

Diremo che il complesso $\mathfrak{C}$ possiede *transitività finita di grado* m quando, estratti ad arbitrio da I due sistemi di m elementi:

$$x_1,\ x_2,\ldots,\ x_m,$$
$$y_1,\ y_2,\ldots,\ y_m,$$

esiste almeno una sostituzione s di $\mathfrak{C}$ tale che:

$$s(x_1) = y_1,\quad s(x_2) = y_2,\ldots,\quad s(x_m) = y_m.$$

99. Sia $\mathfrak{C}$ un gruppo od uno pseudogruppo transitivo. Se si può determinare un numero intero μ tale che il complesso $\mathfrak{C}$ non abbia transitività di grado superiore a μ, si dirà che il complesso dato possiede *transitività finita limitata*. Nel caso contrario si dirà che $\mathfrak{C}$ possiede *transitività finita illimitata*.

(*) Vedi Memorie 1ª e 2ª, « Annali di Matematica », serie IV, tomo IV, fasc. 1-2; tomo V, fasc. 1-2.

100. Passiamo ora a definire la *transitività infinita.* Estratti da I due sistemi di infiniti elementi:

$$X=[x_1,\ x_2,\ldots,\ x_n,\ldots],$$
$$Y=[y_1,\ y_2,\ldots,\ y_n,\ldots],$$

chiameremo *sistemi residui di* I *rispetto ad* X *ed* Y i sistemi formati con gli elementi di I che non appartengono rispettivamente ad X e ad Y.

Ciò posto, diremo che un complesso $\mathfrak{C}$ possiede *transitività infinita di grado* m se, estratti ad arbitrio da I due sistemi X, Y in modo che i relativi residui abbiano egual potenza m, esiste almeno una sostituzione s di $\mathfrak{C}$ tale che:

$$s(x_i)=y_i \qquad (i=1,\ 2,\ldots).$$

101. Dato uno pseudogruppo composto:

$$C''=C+C',$$

supponiamo che esista un sistema A di m elementi:

$$a_1,\ a_2,\ldots,\ a_m$$

tale che, preso un sistema arbitrario X pure di m elementi:

$$x_1,\ x_2,\ldots,\ x_m,$$

si possa determinare una sostituzione c'' di C'' soddisfacente alle eguaglianze:

$$c''(a_i)=x_i \qquad (i=1,\ 2,\ldots,\ m).$$

Sotto questa ipotesi vogliamo dimostrare che nello pseudogruppo semplice C' esiste una operazione c' avente la medesima proprietà della c''.

Scelta infatti una operazione qualunque k' di C', poniamo:

$$k'(y_1)=a_1,\quad k'(y_2)=a_2,\ldots,\quad k'(y_m)=a_m,$$

e determiniamo una operazione k'' di C'' tale che:

$$k''(a_i)=y_i \qquad (i=1,\ 2,\ldots,\ m).$$

Il prodotto $c'=k''\cdot k'\cdot c''$ appartiene a C' e sostituisce al sistema A il sistema X.

Un'analoga proposizione vale nel caso in cui i sistemi A e X siano formati con infiniti elementi ed i relativi residui siano di egual potenza m.

Da queste considerazioni consegue che:

Se uno pseudogruppo composto $\mathrm{C}''=\mathrm{C}+\mathrm{C}'$ *ha transitività finita od infinita di grado* m, *lo pseudogruppo semplice* C' *possiede transitività finita od infinita di egual grado.*

102. Se nello pseudogruppo C' esiste una sostituzione c_1'' tale che:

$$c_1''(x_i) = a_i,$$

si dimostra, in maniera del tutto simile alla precedente, l'esistenza di una operazione c_1' di C' avente la stessa proprietà della c_1''.

103. *Affinchè un complesso* $\mathfrak{C}$ *abbia transitività finita di grado* m *occorre e basta che esista un sistema:*

$$A = [a_1, a_2, \ldots, a_m]$$

di m *elementi tale che, preso un sistema ad arbitrio:*

$$X = [x_1, x_2, \ldots, x_m]$$

pure di m *elementi, si possano determinare due sostituzioni* s *e* σ *di* $\mathfrak{C}$ *soddisfacenti alle eguaglianze:*

$$(a) \qquad s(a_i) = x_i,$$

$$(b) \qquad \sigma(x_i) = a_i \qquad (i = 1, 2, \ldots, m).$$

La condizione è sufficiente.

Siano infatti:

$$x_1, \quad x_2, \ldots, \quad x_m,$$
$$y_1, \quad y_2, \ldots, \quad y_m,$$

due sistemi arbitrari e siano s e σ le due operazioni di $\mathfrak{C}$ tali che:

$$s(a_i) = y_i, \quad \sigma(x_i) = a_i \qquad (i = 1, 2, \ldots, m).$$

Il prodotto $\sigma \cdot s$ appartiene a $\mathfrak{C}$ e sostituisce agli elementi x_i gli elementi y_i.

La condizione enunciata è poi manifestamente necessaria.

OSSERVAZIONE. Se il complesso $\mathfrak{C}$ è un gruppo, la (b) è una conseguenza della (a) potendosi scegliere come sostituzione σ l'inversa della s.

Se $\mathfrak{C}$ è invece uno pseudogruppo, le (a), (b) sono generalmente fra loro indipendenti e, come vedremo più avanti, vi sono casi in cui una sola di esse è verificata.

104. *Condizione necessaria e sufficiente affinchè un complesso* $\mathfrak{C}$ *abbia transitività infinita di grado* m *è che esista un sistema:*

$$A = [a_1, a_2, \ldots, a_n, \ldots]$$

d'infiniti elementi, avente il residuo A' *di potenza* m, *tale che, preso ad arbitrio un sistema:*

$$X = [x_1, x_2, \ldots, x_n, \ldots]$$

col residuo X′ *di potenza* m, *si possa determinare una sostituzione* s *di* $\mathfrak{C}$ *soddisfacente alle eguaglianze:*

(*a*) $$s(a_i) = x_i \qquad (i = 1, 2, \ldots, n, \ldots).$$

Per provare l'asserto basterà, evidentemente, costruire una operazione σ di $\mathfrak{C}$ per la quale sia:

(*b*) $$\sigma(x_i) = a_i.$$

Consideriamo dapprima il caso in cui m è infinito. Indichiamo con X'' ed X''' i residui di A e A' rispetto ad X e supponiamo che X'' sia formato con infiniti elementi.

In tale ipotesi, possiamo determinare una operazione c di $\mathfrak{C}$ tale che:

$$c(X) = A_1,$$

essendo A_1 una parte propria di A. Basta infatti scegliere come operazione c quella che sostituisce ad X'' il sistema A'.

Prendiamo quindi una operazione k di $\mathfrak{C}$ che sostituisca ad A_1 il sistema A e formiamo il prodotto $\sigma = c \cdot k$.

Questa operazione appartiene a $\mathfrak{C}$ e, come subito si verifica, soddisfa alla (*b*).

In particolare, si può fare $X = A'$ e, per conseguenza, $X'' = A$.

Se poi il residuo con infiniti elementi è X''' anzichè X'', bisognerà assumere come operazione c quella che sostituisce ad X''' il sistema A'.

Infine, nel caso in cui m è un numero finito, il complesso $\mathfrak{C}$ è un gruppo perchè esistono in esso delle sostituzioni su un numero finito di elementi (n.° 101). Si può pertanto assumere come operazione σ l'inversa della s.

Un'analoga proposizione vale nel caso in cui si supponga soddisfatta la (*b*) in luogo della (*a*).

105. Sia $\mathfrak{C}$ un complesso avente transitività finita di grado m.

Il gruppo:

$$G = (\mathfrak{C}, \mathfrak{C}^{-1})$$

generato da $\mathfrak{C}$, contiene per intero $\mathfrak{C}$ e perciò possiede transitività finita di grado m almeno.

Indichiamo con H il gruppo formato con le sostituzioni di G che lasciano fermi gli elementi:

(α) $$1, \quad 2, \ldots, \quad m,$$

e decomponiamo a destra il gruppo G rispetto ad H:

(δ) $$G = \Sigma(H \cdot g).$$

Mediante considerazioni facilissime si riesce a provare che tutte le operazioni di un quasi-gruppo di (δ) sostituiscono al sistema (α) un medesimo sistema:

(β) $$x_1, \quad x_2, \ldots, \quad x_m,$$

e che le operazioni di due quasi-gruppi distinti sostituiscono al sistema (α) dei sistemi che differiscono fra loro almeno per l'ordine con cui si presentano gli elementi nei sistemi stessi.

Da ciò consegue che i quasi-gruppi di (δ) corrispondono biunivocamente alle disposizioni degli elementi di I ad m ad m, e cioè che: *l'indice di* H *in* G *è la potenza del numerabile.*

106. Se si trasforma il gruppo H mediante una operazione g di G tale che ad (α) sostituisca (β), si ottiene un gruppo K formato con le operazioni di G che lasciano fermi gli elementi di (β).

Da qui si deduce che il gruppo comune ai trasformati di H mediante G si riduce alla sola identità e che i complessi $\mathfrak{C}$ e $\frac{\mathfrak{C}}{H}$ sono oloedricamente isomorfi.

107. Le considerazioni svolte nei precedenti n.i 105, 106, si possono ripetere integralmente nell'ipotesi che $\mathfrak{C}$ abbia transitività infinita. L'unica variazione da apportare è relativa all'indice di H in G che, in questo caso, è la potenza del continuo.

108. Diremo che un complesso $\mathfrak{C}$ di sostituzioni su I è *regolare* quando ogni sostituzione di $\mathfrak{C}$ (esclusa l'identità, se esiste in $\mathfrak{C}$) opera su tutti gli elementi di I.

Ciò posto, vogliamo dimostrare il seguente teorema:

Un complesso $\mathfrak{C}$ transitivo e regolare è necessariamente un gruppo avente per ordine la potenza del numerabile e per grado di transitività uno.

Il complesso $\mathfrak{C}$ deve contenere l'identità perchè altrimenti, e per le ipotesi fatte, nessuna operazione di $\mathfrak{C}$ lascierebbe fermo un elemento prefissato x.

Se $\mathfrak{C}$ fosse uno pseudogruppo composto $C + C'$, per la proposizione del n.° 101, sarebbe pure transitivo lo pseudogruppo semplice e regolare C' la qual cosa, come ora s'è visto, è impossibile.

Il complesso $\mathfrak{C}$ deve dunque essere un gruppo.

Inoltre, poichè il sottogruppo H di $\mathfrak{C}$ che abbiamo definito al n.° 105, si riduce alla sola operazione identica, l'ordine di $\mathfrak{C}$ sarà eguale all'indice di H in $\mathfrak{C}$ e cioè sarà la potenza del numerabile.

È infine manifesto che la transitività di $\mathfrak{C}$ non può essere di grado superiore ad 1.

109. *Un complesso abeliano e transitivo $\mathfrak{C}$ è un gruppo avente per ordine la potenza del numerabile.*

In virtù della proposizione precedente, basta dimostrare che $\mathfrak{C}$ è un complesso regolare.

Sia c quella operazione di $\mathfrak{C}$ che lascia fermo l'elemento 1 e sia k una sostituzione che al posto di 1 porta x.

Si ha allora:

$$k^{-1} \cdot c \cdot k = c, \quad k^{-1} \cdot c \cdot k(x) = c(x) = x,$$

e cioè:

$$c = 1.$$

Segue da ciò che ogni sostituzione di $\mathfrak{C}$, diversa dalla identità, deve operare su tutti gli elementi di I.

110. *Un gruppo* G *di sostituzioni su* I *avente transitività infinita coincide col gruppo totale.*

Per ragioni evidenti, basterà dimostrare il teorema nel caso in cui G abbia transitività infinita di grado infinito.

Decomponiamo anzitutto l'insieme I in una infinità numerabile di successioni:

$$\begin{aligned}
X &= [x_1, \quad x_2, \ldots, \quad x_n, \ldots], \\
Y &= [y_1, \quad y_2, \ldots, \quad y_n, \ldots], \\
A_1 &= [\alpha_{11}, \quad \alpha_{12}, \ldots, \quad \alpha_{1n}, \ldots], \\
A_2 &= [\alpha_{21}, \quad \alpha_{22}, \ldots, \quad \alpha_{2n}, \ldots], \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
A_m &= [\alpha_{m1}, \quad \alpha_{m2}, \ldots, \quad \alpha_{mn}, \ldots], \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

ed indichiamo con a_1 una sostituzione qualsiasi sull'insieme A_1 e con a_2, $a_3, \ldots, a_m, \ldots$ delle sostituzioni simili alla a_1 ed operanti rispettivamente sugli insiemi A_2, $A_3, \ldots, A_m, \ldots$.

Nel gruppo G esisterà allora, per le ipotesi fatte, una sostituzione s del tipo:

$$s = \sigma \cdot a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_m \cdot \ldots,$$

dove σ è una operazione sugli elementi di X.

Costruiamo poi una sostituzione t di G che abbia la proprietà di trasfor-

mare σ in sè stessa, a_1 in a_2,...., a_m in a_{m+1}, ecc.. Una siffatta operazione avrà la forma:

$$t = \begin{pmatrix} X;\ A_1;\ A_2;\ldots.;\ A_m\ ;\ldots.;\ Y \\ X;\ A_2;\ A_3;\ldots.;\ A_{m+1};\ldots.;\ Y, A_1 \end{pmatrix}$$

e trasformerà la s in:

$$s_1 = \sigma \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{m+1} \cdot \ldots.$$

Poichè nel gruppo G esiste l'operazione $s \cdot s_1^{-1} = a_1$, possiamo intanto affermare che in questo gruppo figurano tutte quelle sostituzioni che operano su insiemi A di elementi tali che gli elementi di I non appartenenti ad A siano infiniti. In particolare, esisteranno in G le sostituzioni che operano su un numero finito di elementi e quelle che si possono decomporre in un numero infinito di cicli.

Resta pertanto da provare l'esistenza in G di quelle sostituzioni che operano su infiniti elementi e che si decompongono in un numero finito di cicli.

Poichè alcuni di questi cicli sono necessariamente aperti, basterà dimostrare che un qualsiasi ciclo aperto su I:

$$g = (\ldots., \beta_{-n}, \ldots., \beta_{-1}, \beta_0, \beta_1, \ldots., \beta_n, \ldots.)$$

appartiene a G.

Invero, il ciclo g si può considerare come il prodotto delle due operazioni:

$$h = (\beta_{-1}, \beta_{-2}) \cdot (\beta_{-3}, \beta_{-4}) \cdot \ldots. \cdot (\beta_{-n}, \beta_{-n-1}) \cdot \ldots.,$$
$$k = (\ldots., \beta_{-2n}, \ldots., \beta_{-4}, \beta_{-2}, \beta_0, \beta_1, \beta_2, \ldots., \beta_n, \ldots.)$$

che appartengono, per quanto s'è detto superiormente, a G.

Questo gruppo è dunque il totale su I.

OSSERVAZIONE. Il teorema che abbiamo ora dimostrato, mentre ci assicura che non esistono gruppi, all'infuori del totale, aventi transitività infinita, nulla ci dice circa all'esistenza di pseudogruppi infinitamente transitivi.

Su ciò non siamo in grado di dire niente di preciso perchè, pur non conoscendo esempi di siffatti pseudogruppi, non abbiamo ragioni sufficienti per escluderne l'esistenza.

Se però sappiamo che un complesso $\mathfrak{C}$ ha transitività infinita di grado finito m, possiamo affermare che $\mathfrak{C}$ coincide col gruppo totale.

Infatti $\mathfrak{C}$ è necessariamente un gruppo (n.^{i} 101, 104) e ad esso è applicabile il precedente teorema.

111. Diamo ora alcuni esempi di gruppi e di pseudogruppi transitivi.

ESEMPIO I. Il gruppo generato dalle potenze positive e negative del ciclo aperto:

$$g = (\ldots, -n, \ldots, -1, 0, 1, \ldots, n, \ldots)$$

ha transitività finita di grado uno.

ESEMPIO II. Il gruppo formato con tutte le sostituzioni del tipo:

$$\begin{pmatrix} x \\ ax + b \end{pmatrix}$$

dove a, b sono numeri razionali determinati e dove x può assumere tutti i valori razionali positivi e negativi, ha transitività finita di grado due.

Invero, fissati gli elementi 0, 1 e presi due elementi qualsiasi α, β, esiste nel gruppo dato l'operazione:

$$\begin{pmatrix} x \\ (\beta - \alpha)x + \alpha \end{pmatrix}$$

che al posto di 0, 1 porta rispettivamente α, β.

ESEMPIO III. Il sottogruppo G_1 del totale formato con tutte le sostituzioni che operano su un numero finito di elementi possiede transitività finita di grado illimitato.

La medesima transitività è posseduta dal sottogruppo G_2 di G_1 formato con le sostituzioni di G_1 che sono di classe pari.

ESEMPIO IV. Consideriamo tutte le sostituzioni del tipo:

$$g = \begin{pmatrix} x \\ mx + r \end{pmatrix}$$

dove x può assumere tutti i valori razionali e dove m è un numero intero ed r un numero razionale.

Il complesso di queste sostituzioni costituisce uno pseudogruppo G'' perchè, come agevolmente si può verificare, il prodotto di due di esse è una sostituzione della stessa classe, e perchè le inverse di quelle sostituzioni che corrispondono a valori di $m \neq 1$ non appartengono al complesso dato.

Questo pseudogruppo possiede inoltre transitività finita di grado uno ma non di grado superiore.

Infatti, scelto un elemento ξ ad arbitrio, le sostituzioni di G'':

$$g_1 = \begin{pmatrix} x \\ mx + \xi \end{pmatrix}, \quad g_2 = \begin{pmatrix} x \\ mx - m\xi \end{pmatrix}$$

sono tali che:

$$g_1(0) = \xi, \quad g_2(\xi) = 0.$$

Osservando poi che non esiste alcuna sostituzione g di G'' tale che:

$$g(0)=0, \quad g(1)=\frac{1}{2},$$

si può affermare che il grado di transitività di G'' non supera l'unità.

ESEMPIO V. Diamo infine un esempio di uno pseudogruppo avente transitività finita illimitata.

Sia G_1 il gruppo considerato nell'Es. III e sia γ una operazione senza periodo o con periodo infinito.

Il complesso:

$$G''=G_1+G_1\cdot\gamma+\ldots.+G_1\cdot\gamma^n+\ldots.$$

è uno pseudogruppo composto avente la stessa transitività posseduta da G_1, e cioè di grado illimitato.

Per la proposizione del n.° 101, lo pseudogruppo semplice:

$$G'=G_1\cdot\gamma+\ldots.+G_1\cdot\gamma^n+\ldots.$$

ha pure transitività finita illimitata.

B) **Semitransitività.**

112. Al n.° 103 abbiamo osservato che le condizioni (a) e (b), relative alla transitività finita di un complesso di sostituzioni, sono fra loro generalmente indipendenti e che esistono dei complessi per i quali è soddisfatta una sola delle due condizioni suddette.

I complessi di questo tipo, che sono necessariamente degli pseudogruppi, verranno chiamati *semitransitivi.*

Sempre riferendoci al n.° 103, diremo poi che un complesso $\mathfrak{C}$ possiede *semitransitività superiore (inferiore) di grado m* se è soddisfatta la condizione (a) ma non la (b) [la condizione (b) ma non la (a)].

Se il numero m può essere preso ad arbitrio, si dirà che $\mathfrak{C}$ possiede *semitransitività illimitata.*

Osserviamo infine che, in virtù delle considerazioni svolte al n.° 104, si può escludere l'esistenza di complessi aventi semitransitività infinita.

113. Se $\mathfrak{C}$ possiede semitransitività superiore di grado m, lo pseudogruppo $\mathfrak{C}^{-1}$, formato con le inverse delle operazioni di $\mathfrak{C}$, possiede semitransitività inferiore dello stesso grado.

114. Il gruppo:

$$G = (\mathfrak{C},\ \mathfrak{C}^{-1})$$

generato da $\mathfrak{C}$, possiede transitività di grado eguale o superiore a quello relativo alla semitransitività di $\mathfrak{C}$.

Segue da ciò che le proposizioni che abbiamo date ai n.i 105, 106 per i complessi transitivi sono valide anche per gli pseudogruppi semitransitivi perchè esse sono esclusivamente fondate sulla transitività di G.

Dal n.° 101 si deduce poi che:

Se lo pseudogruppo composto:

$$C'' = C + C'$$

ha semitransitività di grado m, *lo pseudogruppo semplice* C' *possiede semitransitività di egual grado.*

115. Sia $\mathfrak{C}$ uno pseudogruppo avente semitransitività superiore di grado m.

Consideriamo tutti i possibili sistemi di m elementi che si possono formare con l'insieme I ed indichiamo con K l'aggregato di questi sistemi.

Poichè $\mathfrak{C}$ è semitransitivo, esistono dei sistemi X di K al posto dei quali si possono portare, mediante sostituzioni di $\mathfrak{C}$, tutti gli altri sistemi di K stesso, ed esistono dei sistemi Y per i quali è esclusa tale possibilità.

È pertanto conveniente di scindere K nelle due classi K_1 e K_2 formate rispettivamente con tutti i sistemi del tipo di X e con tutti i sistemi del tipo di Y.

Scriveremo:

$$(\alpha) \qquad \begin{aligned} K_1 &= [X_1,\ X_2,\ldots,\ X_n,\ldots], \\ K_2 &= [Y_1,\ Y_2,\ldots,\ Y_n,\ldots], \end{aligned}$$

e chiameremo K_1 e K_2 *classi di semitransitività.*

È poi evidente che le operazioni di $\mathfrak{C}$ debbono sostituire ad ogni sistema di K_2 un sistema pure appartenente a K_2.

Vogliamo ora dimostrare che: *le classi* K_1 *e* K_2 *contengono entrambe infiniti sistemi.*

Prendiamo infatti una operazione c di $\mathfrak{C}$ tale che:

$$c(X_1) = Y_1.$$

Poichè, come abbiamo superiormente detto, l'operazione c deve sostituire ad ogni Y_r un Y_s, essa dovrà sostituire ai sistemi di K_1 tutti i sistemi di K_1 ed in più il sistema Y_1. Ciò richiede evidentemente che i sistemi X siano in numero infinito.

Se poi i sistemi Y fossero in numero finito, la stessa operazione c sostituirebbe ad un sistema di K_2 un sistema di K_1, il che è assurdo.

116. Consideriamo ancora il complesso $\mathfrak{C}$ del numero precedente e supponiamo che esista in K_2 un sistema Z tale che, mediante le operazioni di $\mathfrak{C}$, possa essere sostituito ad un sistema arbitrario di m elementi.

In tale ipotesi, il complesso $\mathfrak{C}$ è semitransitivo superiormente ed inferiormente senza però avere transitività di grado m.

La classe K_2 si può allora dividere in due nuove classi K_2', K_2'' formate rispettivamente con i sistemi di K_2 che sono della stessa specie di Z e con quelli che sono di specie diversa. Scriveremo:

$$K_1 = [X_1,\ X_2,\ldots,\ X_n,\ldots],$$
$$K_2' = [Z_1,\ Z_2,\ldots,\ Z_n,\ldots],$$
$$K_2'' = [Y_1',\ Y_2',\ldots,\ Y_n',\ldots].$$

È poi facile provare che: *le operazioni di* $\mathfrak{C}$ *sostituiscono ad ogni sistema di* K_2' *un sistema della medesima classe.*

Considerazioni analoghe si possono fare partendo da un complesso semitransitivo inferiormente.

117. Sia $\mathfrak{C}$ un complesso semitransitivo (ad es. superiormente) avente le classi (α) (n.° 115) e sia t una sostituzione qualsiasi sull'insieme I.

In virtù della semitransitività di $\mathfrak{C}$, le operazioni del complesso $t^{-1}\cdot\mathfrak{C}\cdot t$ sostituiscono ad ogni sistema $t(Y_r)$ un sistema $t(Y_s)$ e ad un sistema $t(X_r)$ un sistema arbitrario.

Da ciò discende che il complesso $t^{-1}\cdot\mathfrak{C}\cdot t$ è pure semitransitivo e che ha le classi:

$$K_1' = [t(X_1),\ldots,\ t(X_n),\ldots],$$
$$K_2' = [t(Y_1),\ldots,\ t(Y_n),\ldots].$$

Se poi l'operazione t appartiene a $\mathfrak{C}$, la classe K_1 è contenuta in K_1' o coincide con essa, e la classe K_2 contiene K_2' o coincide con K_2'.

In particolare, se:

$$t(X_1) = Y_1,$$

la classe K_1' contiene, oltre a K_1, il sistema Y_1, ed il complesso $t^{-1}\cdot\mathfrak{C}\cdot t$ non può essere contenuto in $\mathfrak{C}$.

Considerazioni analoghe valgono per un complesso $\mathfrak{D}$ avente semitransitività inferiore.

Possiamo inoltre affermare che:

a) *Un complesso semitransitivo superiormente (inferiormente) non è invariante nè riducibile (nè ampliabile) in sè stesso.*

b) *Non esistono complessi abeliani semitransitivi.*

118. Diamo ora alcuni esempi di semitransitività.

ESEMPIO I. Consideriamo lo pseudogruppo $\mathfrak{C}$ formato con tutte le sostituzioni del tipo:

$$(o) \qquad \begin{pmatrix} x \\ mx + r \end{pmatrix}$$

dove x è razionale, m è intero positivo ed r è razionale positivo.

Questo complesso possiede semitransitività superiore di grado uno perchè, come agevolmente si può verificare, è possibile di portare al posto di -1 qualsiasi elemento, mentre al posto di 0 si possono portare solo numeri positivi.

La classe K_1 è formata con tutti i numeri razionali negativi e la classe K_2 è formata con lo zero ed i numeri razionali positivi.

Osservando poi che nessuna sostituzione di $\mathfrak{C}$ lascia fermo un elemento $x \geq 0$, possiamo affermare che $\mathfrak{C}$ non è semitransitivo inferiormente.

ESEMPIO II. Supponiamo ora che nelle sostituzioni (o) i numeri m ed r possano assumere qualsiasi valore razionale positivo.

Lo pseudogruppo $\mathfrak{D}$, formato con tutte queste sostituzioni, contiene il precedente $\mathfrak{C}$ ed è semitransitivo superiormente con le medesime classi di $\mathfrak{C}$.

Inoltre, il complesso $\mathfrak{D}$ possiede semitransitività inferiore perchè, presi ad arbitrio un numero razionale positivo p ed un numero razionale qualsiasi x, è sempre possibile di determinare due numeri razionali positivi m ed r tali che:

$$p = mx + r.$$

In questo esempio, le classi K_1, K_2', K_2'' (n.° 116) sono rispettivamente formate con i numeri razionali negativi, con i numeri razionali positivi e con lo zero.

ESEMPIO III. Costruiamo infine uno pseudogruppo $\mathfrak{C}$ avente semitransitività superiore di grado illimitato.

Prendiamo come insieme I la successione:

$$\ldots, \quad -n, \ldots, \quad -2, \quad -1, \quad 1, \quad 2, \ldots, \quad n, \ldots,$$

e scegliamo ad arbitrio un numero intero m ed un sistema X di m elementi estratti da I:

$$X = [x_1, x_2, \ldots, x_m].$$

Ciò fatto, costruiamo la sostituzione:

$$c = \begin{pmatrix} 1, & 2, \ldots, & m; & m+1, & m+2, \ldots, & m+r, \ldots; & -1, & -2, \ldots, & -n, \ldots \\ x_1, & x_2, \ldots, & x_m; & p_1, & p_2, \ldots, & p_r, \ldots; & \mu_1, & \mu_2, \ldots, & \mu_n, \ldots \end{pmatrix}$$

dove le successioni:

$$p_1, p_2, \ldots, p_r, \ldots; \quad \mu_1, \mu_2, \ldots, \mu_n, \ldots$$

sono formate rispettivamente con i numeri positivi e negativi di I che non appartengono ad X.

Ripetendo questa costruzione per tutti i possibili m e per tutti i sistemi X relativi, otteniamo un complesso $\mathfrak{K}$ di infinite sostituzioni. Lo pseudogruppo $\mathfrak{C}$, generato da $\mathfrak{K}$, non è transitivo perchè le sue operazioni sostituiscono ad ogni elemento negativo un elemento pure negativo, ma possiede semitransitività superiore di grado illimitato perchè al posto del sistema 1, 2,...., m (m arbitrario) si può portare un qualsiasi sistema di m elementi.

C) **Intransitività.**

119. Dato un complesso $\mathfrak{C}$ di sostituzioni su I, diremo che esso è *intransitivo* quando le condizioni (a) e (b) del n.° 103 non sono verificate per nessun elemento a dell'insieme I.

Diremo poi che $\mathfrak{C}$ possiede:

α) *intransitività di 1ª specie* quando il gruppo:

$$G = (\mathfrak{C}, \mathfrak{C}^{-1})$$

è intransitivo;

β) *intransitività di 2ª specie* quando il suddetto gruppo è transitivo.

L'intransitività di 2ª specie può presentarsi solo negli pseudogruppi.

120. Dalla proposizione del n.° 101 si deduce immediatamente che:

Uno pseudogruppo composto:

$$C'' = C + C'$$

è intransitivo nel solo caso che sia intransitivo C'.

Inoltre, poichè:

$$(C'', C''^{-1}) = (C', C'^{-1}),$$

possiamo affermare che: *le intransitività di* C'' *e di* C' *sono della stessa specie.*

121. Consideriamo dapprima un complesso $\mathfrak{C}$ avente intransitività di 1ª specie.

Prendiamo un elemento x di I e costruiamo il sistema X di tutti gli elementi diversi che le operazioni di G portano al posto di x.

Il gruppo G opera transitivamente sugli elementi di X e non può contenere delle operazioni che sostituiscano ad elementi di X degli elementi estranei ad X stesso.

Ripetendo per tutti gli elementi di I ciò che si è fatto per x veniamo ad ottenere un insieme numerabile J di sistemi del tipo di X.

Da quanto si è ora detto risulta chiaramente che due qualunque di questi sistemi o hanno tutti gli elementi in comune, oppure non ne hanno nessuno. Segue da ciò che se si estraggono da J tutti i sistemi fra loro diversi che in esso compariscono, si vengono a distribuire gli elementi di I in un numero finito od in una infinità numerabile di sistemi:

$$(\tau) \qquad X_1, \quad X_2, \ldots, \quad X_n, \ldots,$$

che verranno chiamati *sistemi di transitività di* $\mathfrak{C}$.

Le operazioni di $\mathfrak{C}$, appartenendo a G, sostituiscono agli elementi di un sistema gli elementi del medesimo sistema, ma non è detto che esse possano congiungere due elementi arbitrari di uno stesso sistema (vedi n.° 123).

Ciò significa che, mentre un gruppo è sicuramente transitivo rispetto a ciascun X_n, uno pseudogruppo può anche essere, rispetto ad X_n, semitransitivo od intransitivo di 2ª specie.

Osserviamo infine come non sia possibile di decomporre un qualunque sistema X_n in parti:

$$(\delta) \qquad Y_1, \quad Y_2, \ldots, \quad Y_r, \ldots$$

in modo che ogni operazione di $\mathfrak{C}$ sostituisca ad Y_r il sistema stesso.

Infatti, se esistesse una decomposizione come (δ), ogni operazione g di G, potendosi porre sotto la forma:

$$g = c_1^{\varepsilon_1} \cdot c_2^{\varepsilon_2} \cdot \ldots \cdot c_m^{\varepsilon_m}, \qquad (\varepsilon_1, \ \varepsilon_2, \ \ldots, \ \varepsilon_m = \pm 1)$$

avrebbe la medesima proprietà delle operazioni di $\mathfrak{C}$, il che è contrario alla transitività di G rispetto ad X_n.

122. Se:

$$c = k_1 \cdot k_2 \cdot \ldots \cdot k_m \cdot \ldots$$

è una decomposizione della sostituzione c di $\mathfrak{C}$ nei suoi cicli, ogni ciclo k_m deve evidentemente operare su elementi di un medesimo sistema di transitività.

In conseguenza di ciò, se ogni sistema X_n ha un numero finito di elementi, le operazioni di $\mathfrak{C}$ hanno periodo finito od infinito.

Se poi $\mathfrak{C}$ deve essere uno pseudogruppo, è necessario che ad ogni intero positivo μ corrisponda qualche sistema X_μ avente un numero di elementi superiore a μ.

123. Diamo ora un esempio di uno pseudogruppo intransitivo di 1ª specie.

Sia $\mathfrak{H}$ uno pseudogruppo semitransitivo superiormente di grado uno avente le classi:

$$K_1 = [x_1,\ x_2,\ldots,\ x_n,\ldots],$$
$$K_2 = [y_1,\ y_2,\ldots,\ y_n,\ldots],$$

e sia:

$$c = (a_1,\ a_2)\cdot(\ldots,\ -n,\ldots,\ -1,\ 0,\ 1,\ldots,\ n,\ldots)$$

una sostituzione su elementi diversi da quelli su cui operano le sostituzioni di $\mathfrak{H}$.

Lo pseudogruppo:

$$\mathfrak{C} = (\mathfrak{H},\ c),$$

generato da c e da $\mathfrak{H}$, è, come facilmente si verifica, intransitivo di 1ª specie, ed ammette i tre sistemi di transitività:

$$\begin{array}{c} a_1,\ a_2 \\ \ldots,\ -n,\ldots,\ -1,\ 0,\ 1,\ldots,\ n,\ldots \\ x_1,\ x_2,\ldots,\ x_n,\ldots;\ y_1,\ y_2,\ldots,\ y_n,\ldots \end{array}$$

Lo pseudogruppo $\mathfrak{C}$ è transitivo rispetto al primo sistema, intransitivo di 2ª specie rispetto al secondo e semitransitivo rispetto al terzo.

124. Occupiamoci infine della intransitività di 2ª specie.

Un esempio assai semplice di tale intransitività ci è offerto dallo pseudogruppo semplice C' generato dalla operazione:

$$c = (\ldots,\ -n,\ldots,\ -1,\ 0,\ 1,\ldots,\ n,\ldots).$$

Invero, il gruppo $(C',\ C'^{-1})$ è transitivo (n.° 111), e:

$$c^r(n) > n,\quad c^r(-n) > -n.$$

125. L'insieme I di elementi su cui operano le sostituzioni di uno pseudogruppo $\mathfrak{C}$ intransitivo di 2ª specie, non si può dividere (come si è fatto nel caso dell'intransitività di 1ª specie) in sistemi:

$$X_1,\ X_2,\ldots,\ X_n,\ldots$$

tali che le operazioni di $\mathfrak{C}$ sostituiscano ogni elemento di un sistema generico X_n con un elemento del medesimo sistema.

Infatti, se fosse possibile una tale suddivisione, le operazioni del gruppo $(\mathfrak{C}, \mathfrak{C}^{-1})$, potendosi porre sotto la forma:

$$g = c_1^{\varepsilon_1} \cdot c_2^{\varepsilon_2} \cdot \ldots \cdot c_m^{\varepsilon_m}, \qquad (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m = \pm 1)$$

avrebbero la medesima proprietà delle operazioni di $\mathfrak{C}$.

126. Le considerazioni svolte ai n.i 105, 106, 107 si possono integralmente ripetere per il caso attuale perchè esse sono fondate sulla transitività del gruppo G.

È da notare poi che se $\mathfrak{C}$ è abeliano, tale è anche il gruppo G, e che l'ordine di $\mathfrak{C}$ è la potenza del numerabile (n.° 109).

D) **Imprimitività.**

127. Dato un gruppo o pseudogruppo $\mathfrak{C}$ di sostituzioni su I, diremo che esso è *imprimitivo* se è possibile di dividere l'insieme I in un numero finito ≥ 2 od in una infinità numerabile di sistemi:

$$(\sigma) \qquad X_1, \quad X_2, \ldots, \quad X_n, \ldots$$

(contenenti ciascuno almeno due elementi) tali che ogni operazione c di $\mathfrak{C}$ soddisfi all'eguaglianze:

$$(a) \qquad c(X_n) = X_m \qquad (n = 1, 2, \ldots).$$

Chiameremo $X_1, \ldots, X_n, \ldots$ *sistemi di imprimitività.*

Se la suddetta suddivisione è impossibile, diremo che il complesso $\mathfrak{C}$ è *primitivo.*

128. Un complesso intransitivo di 1ª specie è sicuramente imprimitivo, potendosi scegliere come suddivisione (σ) la suddivisione (τ) fatta al n.° 121. Questo caso (rientrando nello studio generale dell'intransitività) non ci interessa particolarmente; qui ci occuperemo invece di quei complessi imprimitivi che sono transitivi o semitransitivi od intransitivi di 2ª specie.

129. *Se $\mathfrak{C}$ è imprimitivo, tale è il gruppo:*

$$G = (\mathfrak{C}, \mathfrak{C}^{-1})$$

e viceversa.

Una qualsiasi operazione g di G, potendosi porre sotto la forma:

$$g = c_1^{\varepsilon_1} \cdot c_2^{\varepsilon_2} \cdot \ldots \cdot c_m^{\varepsilon_m} \qquad (\varepsilon_1,\ \varepsilon_2, \ldots,\ \varepsilon_m = \pm 1),$$

soddisfa sicuramente alla condizione (a) del n.° 127.

La reciproca è manifesta essendo $\mathfrak{C}$ contenuto in G.

Da questa proposizione consegue immediatamente che:

α) *Se* $\mathfrak{C}$ *è imprimitivo,* $\mathfrak{G}$ *non può avere transitività multipla.*

β) *Affinchè lo pseudogruppo composto:*

$$C'' = C + C'$$

sia imprimitivo, occorre e basta che tale sia C'.

130. *I sistemi di imprimitività hanno tutti egual potenza.*

Infatti, presi ad arbitrio da (σ) due sistemi X_m ed X_n, esiste, nel gruppo transitivo G, una sostituzione g tale che:

$$g(X_m) = X_n .$$

131. *Se esiste un gruppo* H *invariante per* $\mathfrak{G}$ *ed intransitivo, i sistemi di transitività di* H*:*

(σ) $$X_1,\ X_2, \ldots,\ X_n, \ldots$$

sono di imprimitività per $\mathfrak{G}$ *e quindi per* $\mathfrak{C}$.

Prendiamo una sostituzione g qualsiasi di G, due elementi x ed y di un sistema X_n ed una operazione h di H tale che:

$$y = h(x).$$

La trasformata $g^{-1} \cdot h \cdot g$ appartiene per ipotesi ad H e sostituisce all'elemento $g(x)$ l'elemento $g(y)$.

Ciò prova che $g(x)$ e $g(y)$ appartengono ad un medesimo sistema X_m.

Ripetendo poi per l'operazione g^{-1} il ragionamento ora fatto si giunge a stabilire che:

$$g(X_n) = X_m .$$

Pertanto, i complessi G e $\mathfrak{C}$ sono imprimitivi.

132. *Condizione necessaria e sufficiente affinchè* $\mathfrak{C}$ *sia imprimitivo è che il gruppo* A, *formato con le sostituzioni di* $\mathfrak{G}$ *che lasciano fermo un elemento prefissato* x_1, *sia contenuto in un sottogruppo proprio* B *di* $\mathfrak{G}$.

La condizione è necessaria.

Sia X_1 il sistema di imprimitività che contiene l'elemento x_1.

Le sostituzioni g di G tali che:

$$g(X_1) = X_1,$$

costituiscono evidentemente un sottogruppo B di G contenente A.

La condizione è sufficiente.

Poiché gli elementi che le operazioni di B sostituiscono ad x_1, formano un sistema X_1 di transitività per B, le operazioni di G, non appartenenti a B, debbono sostituire agli elementi di X_1 degli elementi estranei al sistema stesso.

Da ciò segue che una operazione h sul sistema X_1 e le sue trasformate mediante G, generano un gruppo invariante ed intransitivo.

Si può pertanto affermare (n.° 131) che G e $\mathfrak{C}$ sono imprimitivi.

133. *Se* G *è regolare, il complesso* $\mathfrak{C}$ *è imprimitivo.*

Infatti, poichè A si riduce alla sola operazione identica, si può scegliere come gruppo B un qualsiasi sottogruppo di G.

In particolare si ha che *i complessi abeliani sono imprimitivi.*

134. ESEMPIO I. Lo pseudogruppo generato dal ciclo:

$$g = (\ldots, -n, \ldots, -1, 0, 1, \ldots, n, \ldots)$$

è imprimitivo poichè G è, in questo caso, abeliano.

Ponendo:

$$B = [1, g^{kr}] \qquad (k > 1,\ r = \pm 1, \pm 2, \ldots),$$

si hanno k sistemi di imprimitività di facilissima costruzione.

ESEMPIO II. Il gruppo G formato con le sostituzioni del tipo:

$$\begin{pmatrix} x \\ mx + r \end{pmatrix},$$

dove x, m, r sono numeri razionali ed $m > 0$, è primitivo.

Infatti, scelto come gruppo A l'insieme delle sostituzioni che lasciano fermo l'elemento 0, e presa una sostituzione qualunque di G:

$$g = \begin{pmatrix} x \\ \mu x + \rho \end{pmatrix},$$

si consideri il gruppo generato da A e da g. Questo gruppo, contenendo le

operazioni:

$$\gamma = \left(\frac{x}{\frac{m\rho}{\mu r}\, x}\right)\cdot\left(\frac{x}{\mu x + \rho}\right)\cdot\left(\frac{x}{\frac{r}{\rho}\, x}\right) = \left(\frac{x}{mx + r}\right)$$

e le loro inverse γ^{-1}, coincide con G.

Si può pertanto escludere l'esistenza di sottogruppi di G contenenti A.

CAPITOLO VI.

IL GRUPPO TOTALE ED ALTRI GRUPPI SPECIALI

A) **Il gruppo totale.**

135. Abbiamo detto altrove che cosa s'intende per gruppo totale G di sostituzioni su una infinità numerabile I di elementi ed abbiamo anche date, per questo gruppo, alcune proprietà. Ad esempio, si è visto come G abbia per ordine la potenza del continuo (n.° 27) e come esso sia l'unico gruppo avente transitività infinita (n.° 110).

Il gruppo totale contiene infiniti sottogruppi ed infiniti sottopseudogruppi; fra essi hanno particolare importanza, per le considerazioni che faremo in seguito, il gruppo G_1 formato con le sostituzioni di G che operano su un numero finito di elementi, ed il gruppo G_2 formato con le sostituzioni di G_1 che hanno classe pari.

136. *Un complesso* $\mathfrak{C}$, *contenente una sostituzione* h *su infiniti elementi e le sue trasformate mediante* G, *coincide con il totale.*

Poichè il complesso $\mathfrak{C}$ contiene il gruppo H generato da h e dalle sue trasformate, basterà dimostrare che H possiede transitività infinita.

Supponiamo dapprima che h sia un ciclo aperto:

$$h = (\ldots, -n, \ldots, -1, 0, 1, \ldots, n, \ldots).$$

Per le ipotesi fatte, il gruppo H conterrà anche il ciclo:

$$h_1 = (\ldots, 8, 7, 5, 6, 4, 3, 1, 2, 0, -1, -2, -3, \ldots)$$

e, conseguentemente, il prodotto:

$$h \cdot h_1 = (0, 2, 1)\cdot(4, 6, 5)\cdot(8, 10, 9)\cdot\ldots$$

che è formato con infiniti cicli chiusi.

Se invece h contiene, nella sua decomposizione in cicli, almeno un ciclo aperto ed eventualmente dei cicli chiusi, è possibile, mediante un procedimento del tutto analogo al precedente, di costruire una operazione di H formata con infiniti cicli tutti chiusi.

Si può pertanto supporre che esista in H una operazione del tipo:

$$s = c_0 \cdot c_1 \cdot c_2 \cdot \ldots \cdot c_n \cdot \ldots$$

dove $c_0, c_1, \ldots, c_n, \ldots$ sono cicli tutti chiusi.

Scegliamo ad arbitrio un sistema X di infiniti elementi:

$$X = [x_0, x_1, \ldots, x_n, \ldots]$$

con il residuo X' formato pure con infiniti elementi, ed indichiamo con:

$$A = [a_0, a_2, \ldots, a_{2n}, \ldots]$$

un sistema ottenuto prendendo a_0 da c_0, a_2 da c_2, ecc..

La trasformata di s mediante una operazione g di G tale che:

$$g(a_{2n}) = x_n \qquad (n = 0, 1, 2, \ldots),$$

è una operazione:

$$\sigma = k_0 \cdot k_1 \cdot k_2 \cdot \ldots \cdot k_n \cdot \ldots$$

nella quale i cicli $k_0, k_2, \ldots, k_{2n}, \ldots$ contengono rispettivamente gli elementi $x_0, x_1, \ldots, x_n, \ldots$.

Ciò posto, estragghiamo da X' un sistema:

$$Y = [y_0, y_1, \ldots, y_n, \ldots]$$

in modo che il residuo di X' rispetto ad Y contenga infiniti elementi, e trasformiamo σ mediante una operazione γ di G soddisfacente alle eguaglianze:

$$\gamma(x_n) = x_n, \quad \gamma(k_{2n}(x_n)) = y_n \qquad (n = 0, 1, 2, \ldots).$$

Questa trasformata appartiene ad H ed ha la proprietà di sostituire al sistema X il sistema Y.

Consideriamo ora un sistema:

$$Z = [z_0, z_1, \ldots, z_n, \ldots]$$

avente elementi in comune con X ma tale che il residuo Z' di X' rispetto a Z contenga infiniti elementi.

Poichè un sistema Z_1, estratto da Z', è del medesimo tipo del precedente Y, esistono in H due operazioni che sostituiscono ai sistemi X e Z_1 rispettivamente i sistemi Z_1 e Z. Il prodotto di queste due operazioni appartiene ad H e sostituisce ad X il sistema Z.

Resta infine da provare che, mediante le operazioni di H, si può sostituire al sistema X un sistema T tale che il residuo di X' rispetto a T contenga un numero finito di elementi.

Indicato con T_1 un sistema estratto dal residuo di X rispetto a T, è possibile, per quanto s'è detto superiormente, di costruire due operazioni l e λ di H soddisfacenti alle eguaglianze:

$$l(X) = T_1, \ \lambda(T) = T_1.$$

Segue da ciò che il prodotto $l \cdot \lambda^{-1}$ sostituisce ad X il sistema T.

137. *Un complesso chiuso* $\mathfrak{C}$, *contenente una operazione* h *su un numero finito di elementi e le sue trasformate mediante* G, *coincide con* G.

Sia:

$$(\alpha) \qquad h_1, \ h_2, \ldots, \ h_n, \ldots$$

una successione di trasformate di h tale che ogni h_n operi su elementi diversi da quelli su cui operano le altre sostituzioni di (α).

Il prodotto $\prod_{n=1}^{\infty} h_n$ è convergente, opera su infiniti elementi e, per le ipotesi fatte, appartiene a $\mathfrak{C}$. È dunque applicabile il criterio del n.° 136.

138. Al n.° 58 abbiamo definito il gruppo commutatore G_c ed il gruppo derivato G_d di un complesso $\mathfrak{A}$.

Se $\mathfrak{A}$ è il gruppo totale G, si ha:

$$G_c = G_d = G.$$

Infatti, i gruppi G_c e G_d sono invarianti in G e contengono sicuramente delle operazioni su infiniti elementi.

139. TEOREMA. *Il gruppo totale non possiede sottogruppi aventi indice finito e diverso da 1.*

Sia H un sottogruppo di G avente indice finito m e sia:

$$(\delta) \qquad G = \sum_{n=1}^{m} (H \cdot g_n)$$

una decomposizione di G rispetto ad H.

Una operazione γ di G su infiniti elementi e con periodo primo $p > m$, deve appartenere ad H.

Infatti, se due diverse potenze γ^r e γ^s appartengono ad un medesimo quasi-gruppo di (δ), l'operazione γ^{r-s} appartiene ad H. Se invece l'ipotesi

precedente non è verificata, il gruppo H dovrà necessariamente contenere una delle prime m potenze di γ.

Poichè queste considerazioni si possono ripetere per tutte le trasformate di γ mediante G, si può affermare che $H = G$ e, conseguentemente, che $m = 1$.

140. Il precedente teorema ci permette di dimostrare assai rapidamente come non sia possibile di scindere il gruppo totale G in due complessi $\mathfrak{S}$ e $\mathfrak{D}$ simili a quelli formati con le sostituzioni pari e con le sostituzioni dispari del gruppo totale su m elementi (1).

Invero, se fosse possibile la suddetta decomposizione di G, il complesso $\mathfrak{S}$ sarebbe un sottogruppo di G di indice 2.

141. Vogliamo ora vedere quali sono i complessi invarianti contenuti in G.

Osserviamo anzitutto che un complesso invariante per G, non potendo contenere operazioni su infiniti elementi, deve appartenere al gruppo G_1 (n.° 135).

Si può dunque escludere l'esistenza in G di pseudogruppi invarianti.

Sia poi H un sottogruppo invariante di G e sia:

$$h = (1,\ 2,\ 3,\ldots,\ n)\cdot c_2\cdot\ldots\cdot c_r$$

una sua operazione qualsiasi.

Scelto un elemento x, distinto da quelli su cui opera h, si considerino le due operazioni di H:

$$h_1 = (1,\ x,\ 3,\ldots,\ n)\cdot c_2\cdot\ldots\cdot c_r,$$
$$k = h\cdot h_1^{-1} = (1,\ 2,\ x).$$

Insieme alla operazione k, il gruppo H conterrà, in virtù della sua invarianza, tutte le trasformate di k e quindi tutte le operazioni del gruppo G_2.

Inoltre, poichè G_2 ha indice 2 in G_1, non esisterà alcun gruppo contenuto in G_1 e contenente G_2.

Possiamo dunque concludere che:

I gruppi G_1 *e* G_2 *sono gli unici sottogruppi invarianti del totale* G.

142. Passiamo alla ricerca dei sottogruppi invarianti di G_1 e G_2. Mediante considerazioni del tutto analoghe a quelle fatte al numero precedente si può provare che:

a) *Il gruppo* G_2 *è l'unico sottogruppo invariante di* G_1.

(1) Cfr. G. VITALI, *Sostituzioni sopra una infinità numerabile di elementi.* (Bollettino della « Mathesis », anno VII, 1915).

b) *Il gruppo* G_2 *non ammette sottogruppi invarianti all'infuori della identità.*

143. Dai precedenti risultati consegue immediatamente che il gruppo G ammette un'unica serie di composizione così formata:

$$G, \quad G_1, \quad G_2, \quad 1.$$

B) Il gruppo lineare.

144. Intenderemo per *gruppo lineare* l'insieme di tutte le sostituzioni del tipo:

$$(\alpha) \qquad x_1 = \frac{ax + b}{cx + d},$$

dove a, b, c, d sono numeri razionali determinati e dove x può assumere tutti i valori razionali e l'infinito.

Affinchè l'espressione (α) rappresenti una effettiva sostituzione occorre e basta che il determinante:

$$\delta = ad - bc$$

sia diverso da zero.

Le sostituzioni (α), per le quali il determinante è eguale ad 1 o può ridursi tale, costituiscono un sottogruppo invariante del lineare che diremo *gruppo modulare.*

I gruppi lineare e modulare verranno rispettivamente indicati con L ed M e le sostituzioni (α) si rappresenteranno col noto simbolo:

$$\begin{pmatrix} a, b \\ c, d \end{pmatrix}.$$

145. Il gruppo L è triplamente transitivo poichè i parametri indipendenti che figurano in (α) sono precisamente tre; il gruppo M possiede soltanto transitività di grado due perchè i suddetti parametri debbono soddisfare alla relazione:

$$ad - bc = 1.$$

146. Diremo che una sostituzione di L è *iperbolica, parabolica,* od *ellittica* secondo che essa lascia fermi due elementi, uno solo, oppure opera su tutti gli elementi.

Affinchè una sostituzione (α) lasci fermi due elementi od uno solo, occorre

che il discriminante:

$$(d-a)^2+4bc=(a+d)^2-4\delta \tag{\beta}$$

dell'equazione:

$$cx^2+(d-a)x-b=0,$$

sia il quadrato di un numero razionale oppure sia zero.

147. Mediante facilissime considerazioni si può dimostrare che:

a) *Le sostituzioni di* L *sono formate con tutti cicli chiusi di egual ordine oppure con tutti cicli aperti.*

b) *Una sostituzione iperbolica è formata con tutti cicli aperti o con tutti scambi.*

c) *Una sostituzione parabolica è formata con tutti cicli aperti.*

148. *Il gruppo generato dalle sostituzioni paraboliche coincide col modulare.*

Osserviamo anzitutto che, in virtù della (β), ogni sostituzione parabolica appartiene ad M.

Presa poi una sostituzione qualsiasi di M:

$$h=\begin{pmatrix}a, b\\ c, d\end{pmatrix},$$

determiniamo una sostituzione parabolica:

$$k=\begin{pmatrix}m, n\\ p, q\end{pmatrix}$$

tale che $h\cdot k$ sia ancora una sostituzione parabolica.

Tale determinazione è possibile, comunque sia h, poichè essa è collegata alla risoluzione del sistema indeterminato:

$$\begin{cases} am+cn+bp+dq=2\\ mq-np=1\\ m+q=2\end{cases}$$

nelle incognite m, n, p, q.

Segue da ciò che h può esprimersi come prodotto delle sostituzioni paraboliche $h\cdot k$ e k^{-1}.

149. *Il gruppo modulare non ammette sottogruppi invarianti all'infuori della identità.*

Un gruppo H invariante in M, essendo transitivo, contiene una operazione h tale che:

$$h(0) = \infty .$$

Le trasformate di h mediante le operazioni del tipo:

$$(\gamma) \qquad x_1 = \rho^2 x,$$

appartengono ad H, sono fra loro diverse, ed hanno la stessa proprietà di h. Pertanto, il prodotto di una di queste operazioni per h^{-1} è diverso dall'identità e lascia fermo l'elemento 0.

Se questo prodotto è una operazione iperbolica, il gruppo H contiene una operazione k tale che:

$$k(0) = 0, \quad k(\infty) = \infty ,$$

e contiene la trasformata k_1 di k mediante la sostituzione:

$$x_1 = x + 1.$$

Il prodotto $k_1 \cdot k^{-1}$ appartiene ad H e, come facilmente si verifica, è una sostituzione parabolica del tipo:

$$l = \begin{pmatrix} 1, & b \\ 0, & 1 \end{pmatrix}.$$

Sia poi:

$$\lambda = \begin{pmatrix} 1, & m\rho^2 b \\ 0, & 1 \end{pmatrix}$$

la trasformata di l^m mediante una operazione della forma (γ). Poichè m e ρ^2 sono in nostro arbitrio, si può disporre di essi in modo che λ ci rappresenti una qualunque delle sostituzioni paraboliche che lasciano fermo l'elemento ∞.

Il gruppo H, contenendo perciò tutte le sostituzioni paraboliche, coincide con M.

150. Vediamo ora quali sono i sottogruppi invarianti di L.

Notiamo anzitutto che ogni commutatrice di L appartiene ad M, che il gruppo $\frac{L}{M}$ è abeliano (n.° 78) e che le sue operazioni hanno periodo due.

Indichiamo poi con H un sottogruppo invariante di L e con D il gruppo comune ad H ed M.

Poichè H ed M sono invarianti in L, il gruppo D sarà invariante in M e, non potendo ridursi alla identità, dovrà coincidere con M. Pertanto, possiamo affermare che H, contenendo interamente M, è formato con tutte le operazioni di L che corrispondono ad un sottogruppo di $\frac{L}{M}$.

Reciprocamente, il complesso formato con tutte le operazioni di L che corrispondono ad un sottogruppo di $\frac{L}{M}$ costituisce un sottogruppo invariante di L.

In particolare, i sottogruppi invarianti massimi di L dovranno corrispondere ai sottogruppi di $\frac{L}{M}$ che hanno indice due (n.° 56).

151. Le precedenti considerazioni si possono evidentemente ripetere per un qualsiasi sottogruppo K di L contenente il gruppo modulare. Da ciò segue che una qualunque successione di gruppi:

$$L,\ L_2,\ldots,\ L_m,\ldots,$$

tale che ciascun L_m sia invariante massimo nel precedente, non soddisfa alla condizione *b*) del n.° 84 e cioè che *il gruppo* L *non ammette serie di composizione.*

C) Il gruppo metaciclico.

152. Sia G il gruppo generato dal ciclo aperto:

$$g = (\ldots,\ -n,\ldots,\ -1,\ 0,\ 1,\ldots,\ n,\ldots).$$

Chiameremo *gruppo metaciclico* il più ampio sottogruppo M del totale sugli elementi:

$$\ldots,\ -n,\ldots,\ -1,\ 0,\ 1,\ldots,\ n,\ldots$$

che contiene G come sottogruppo invariante.

Una qualsiasi sostituzione m di M deve trasformare g in sè stessa oppure nella sua inversa g^{-1}.

Nel primo caso si deve avere:

$$m(n+1) = m(n) + 1,$$

e cioè:

$$m = g^{m(0)}.$$

Nel secondo caso, l'operazione m deve essere della forma:

$$m = g^r \cdot \gamma$$

dove:

$$\gamma = (1,\ -1)\cdot(2,\ -2)\cdot\ldots\cdot(n,\ -n)\cdot\ldots$$

Si ha infatti:

$$m^{-1}\cdot g\cdot m = \gamma^{-1}\cdot g\cdot\gamma = g^{-1},$$
$$\gamma\cdot m^{-1}\cdot g\cdot m\cdot\gamma^{-1} = g,$$

da cui:

$$m \cdot \gamma^{-1} = g^r, \quad m = g^r \cdot \gamma.$$

Le sostituzioni di M sono pertanto tutte e sole le seguenti:

$$M = [G, \ G \cdot \gamma].$$

È poi evidente come tutte le operazioni di $G \cdot \gamma$ abbiano periodo due.

153. Determiniamo tutti i possibili sottogruppi di M: sia N uno di essi. Se N appartiene a G, esso deve avere la forma:

$$N = [1, \ g^{rk}] \qquad (k = \pm 1, \ \pm 2, \ldots).$$

Se invece N è formato soltanto con operazioni di $G \cdot \gamma$, esso deve avere ordine due perchè, se contenesse due operazioni $g^r \cdot \gamma$ e $g^s \cdot \gamma$, conterrebbe anche il loro prodotto:

$$g^r \cdot \gamma \cdot g^s \cdot \gamma = g^{r-s}.$$

Consideriamo infine il caso in cui N contenga operazioni di G e di $G \cdot \gamma$.

Indichiamo con g^ϱ la più piccola potenza positiva di g che figura in N e con $g^r \cdot \gamma$ una operazione di N appartenente a $G \cdot \gamma$.

Se $g^x \cdot \gamma$ è un'altra operazione di N, si ha:

$$g^x \cdot \gamma \cdot g^r \cdot \gamma = g^{x-r};$$

e poichè le potenze di g che figurano in N sono del tipo $g^{\lambda\varrho}$, deve aversi:

$$x = \lambda\varrho + r.$$

Le operazioni di N sono dunque tutte e sole le seguenti:

$$g^{\lambda\varrho}, \quad g^{\mu\varrho+r} \cdot \gamma \qquad (\lambda \text{ e } \mu = 0, \ \pm 1, \ \pm 2, \ldots).$$

Il gruppo N ha poi, evidentemente, indice ϱ in M.

Inversamente, se ϱ ed r sono due numeri interi presi ad arbitrio ($\varrho > 0$), il complesso:

$$N = [g^{\lambda\varrho}, \ g^{\mu\varrho+r} \cdot \gamma] \qquad (\lambda \text{ e } \mu = 0, \ \pm 1, \ \pm 2, \ldots)$$

è un sottogruppo di M avente indice ϱ.

Per un determinato ϱ si hanno ϱ sottogruppi corrispondenti ai valori di r:

$$0, \quad 1, \quad 2, \ldots, \quad \varrho - 1.$$

154. I sottogruppi del primo tipo, cioè i sottogruppi di G, sono invarianti in M per la definizione stessa di M; quelli del secondo tipo non possono

essere invarianti perchè:

$$g^{-1}\cdot g^{r}\cdot\gamma\cdot g = g^{r-2}\cdot\gamma.$$

Vediamo infine quali sono i sottogruppi invarianti del terzo tipo. Se:

$$N=[g^{\lambda\rho},\ g^{\mu\rho+r}\cdot\gamma]$$

è uno di essi, deve aversi:

$$g^{-1}\cdot g^{\mu\rho+r}\cdot\gamma\cdot g = g^{\mu\rho+r-2}\cdot\gamma = g^{\mu_1\rho+r}\cdot\gamma,$$

e cioè:

$$\mu\rho+r-2=\mu_1\rho+r,\quad(\mu-\mu_1)\rho=2.$$

Quest'ultima eguaglianza è soddisfatta soltanto da $\rho=1$ oppure da $\rho=2$: per $\rho=1$ si ha il gruppo M, per $\rho=2$ si hanno i due seguenti sottogruppi invarianti in M:

$$N_1=[g^{2\lambda},\ g^{2\mu}\cdot\gamma],\quad N_2=[g^{2\lambda},\ g^{2\mu+1}\cdot\gamma].$$

155. Osserviamo infine che i gruppi G, N_1, N_2 sono invarianti massimi in M e che essi ammettono il gruppo:

$$G_1=[g^{2\lambda}]$$

quale comune sottogruppo invariante massimo.

Da ciò discende che M è un gruppo risolubile avente infinite serie di composizione (n.° 90).