RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

GIORGIO TREVISAN

Costruzione di quasigruppi con relazioni di congruenza non permutabili

Rendiconti del Seminario Matematico della Università di Padova, tome 22 (1953), p. 11-22

<http://www.numdam.org/item?id=RSMUP_1953__22__11_0>

© Rendiconti del Seminario Matematico della Università di Padova, 1953, 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/conditions). 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/

COSTRUZIONE DI QUASIGRUPPI CON RELAZIONI DI CONGRUENZA NON PERMUTABILI

Nota (*) *di* GIORGIO TREVISAN (*a Padova*)

Nel « Problema 31 » [1]) del « *Lattice Theory* » di G. BIRKHOFF sono proposte le seguenti questioni:

I) Esistono *quasigruppi* con *relazioni di congruenza* non *permutabili?*

II) Può un tale *quasigruppo* essere un *cappio* [2])?

III) Può un tale *quasigruppo* contenere un numero finito di elementi?

Ora l'Autore di questa Nota, in un precedente lavoro [3]) ha risolto la questione III) mostrando che ogni *quasigruppo* con un numero finito di elementi ha tutte le sue *relazioni di congruenza* tra di loro *permutabili.*

Nella presente Nota si risolve la questione I) e si fa vedere

---

*) Pervenuta in Redazione il 4 agosto 1952.

[1]) G. BIRKHOFF: *Lattice Theory*, 1948, pag. 86.

[2]) Si è tradotto con *cappio* l'inglese *loop*. Si approfitta dell'occasione per dare risposta al « Problema 32 » del libro di BIRKHOFF (pag. 86). Le notazioni ed i significati sono quelli del testo. Nel teorema 2, sfruttando il fatto che $ux \equiv_{\cdot} x(\theta)$ implica $u \equiv 1(\theta)$ si dimostra che $\theta\theta' \leq \theta'\theta$. Ora si vedrà che quest'ultima comporta sempre $\theta\theta' = \theta'\theta$ e con ciò il problema risulterà risolto. Si osservi che sono equivalenti le $a\,\theta'\theta\,b$ e $b\,\theta\theta'\,a$. Allora se $a\,\theta'\theta\,b$ per l'equivalenza $b\,\theta\theta'\,a$, ma per ipotesi $\theta\theta' \leq \theta'\theta$, dunque $b\,\theta\theta'\,a$ comporta $b\,\theta'\theta\,a$ cioè per l'equivalenza $a\,\theta\theta'\,b$. E' dunque $\theta'\theta \leq \theta\theta'$ e di qui segue subito la tesi.

[3]) G. TREVISAN: *A proposito delle relazioni di congruenza sui quasigruppi* (Rendiconti Seminario Matematico, Università Padova, 1950), pag. 367).

che esistono *quasigruppi* con *relazioni di congruenza* tra loro non permutabili.

Per sommi capi, si è proceduto come segue. Si considerano certi sistemi moltiplicativi e per essi si introduce il concetto di *relazione di congruenza.* Detto I un siffatto sistema e θ una sua *relazione di congruenza* si definiscono due tipi di ampliamenti ciascuno dei quali trasforma I in un sistema analogo J e θ in una relazione di congruenza su J. Si considera una successione $I_1 = I, I_2, \ldots$ di sistemi, ottenuti a partire da I_2 (incluso) ciascuno dal precedente per ampliamento in modo che per quanto avanti si proceda nella successione si trovi sempre dall'aver operato con ampliamenti di ciascuno dei due tipi sopradetti. La relazione $\theta_1 = \theta$, si trasforma in una relazione θ_2 di I_2, questa in una relazione θ_3 di I_3 e così via. L'unione $Q = I_1 + I_2 + \ldots$ è un quasigruppo di cui l'unione $\theta_1 + \theta_3 + \ldots$ rappresenta una *relazione di congruenza* nell'accezione ordinaria. Le considerazioni svolte fino a questo punto (TEOREMI, I, II, III, IV e parte del VI) sono intuitive e le proprietà facili a stabilirsi. E' risultato invece più complesso stabilire (n. 8, TEOREMA V) quali caratteri debba possedere l'insieme iniziale I, con le sue *relazioni di congruenza* perchè Q risulti con *relazioni di congruenza* non *permutabili.*

1. - Per comodità del lettore si richiamano alcune definizioni fondamentali.

Un insieme di elementi G è un *quasigruppo* se è definita tra le sue coppie ordinate di elementi un'operazione (prodotto) verificante le,

(1) *se* $a \in G$ *e* $b \in G$, ab *è un determinato elemento di* G

(2) *se* $a \in G$ *e* $b \in G$, *esistono e sono unici gli elementi* x *ed* y *di* G *tali che* $ax = b$ *ed* $ya = b$.

Il *quasigruppo* G si dice *cappio* se esso è dotato di unità bilatera, cioè se esiste un suo elemento u tale che $au = ua = a$ per ogni $a \in G$. Chiamasi *relazione di congruenza* su G ogni relazione θ che distribuisce gli elementi di G in insiemi disgiunti, detti *blocchi* o *classi di equivalenza* della θ, e che gode

della proprietà

(3) $$a \equiv b(\theta),\ c \equiv d(\theta) \rightarrow ac \equiv bd(\theta),$$

con a, b, c, d elementi di G.

Due *relazioni di congruenza* su G, θ e θ_1, si dicono tra loro permutabili se dalle

(4) $$a \equiv x(\theta), \qquad x \equiv b(\theta_1)$$

segue che esiste y per cui

(5) $$a \equiv y(\theta_1), \qquad y \equiv b(\theta)$$

e *viceversa* [4]), con a, b, x, y elementi di G.

2. - Si estendono ora alcuni dei concetti precedenti a certi *sistemi moltiplicativi*. Nel seguito si chiamerà *sistema moltiplicativo* M ogni insieme I tale che,

(6) *contiene un numero finito di elementi,*

(7) *per alcune coppie* [5]) *ordinate di I è definita una operazione* O *che dà come risultato, per ciascuna di tali coppie, un determinato elemento di I,*

(8) *se a, b, b_1, sono elementi di I e $b \neq b_1$ allora $a\,O\,b \neq a\,O\,b_1$ e $b\,O\,a \neq b_1\,O\,a$, sempre che abbiano senso in I i prodotti considerati.*

Da quest'ultima proprietà discende che se a e b sono elementi di I le equazioni $a\,O\,x = b$, $y\,O\,a = b$ ammettono ciascuna al più una soluzione in I.

Una relazione θ che distribuisce in insiemi disgiunti gli elementi di I si dirà una *relazione di congruenza* su I se

(9) $a \equiv b\,(\theta),\ c \equiv d\,(\theta) \rightarrow a\,O\,c \quad b\,O\,d\,(\theta)$ *quando abbiano senso* $a\,O\,c$ e $b\,O\,d$.

3. - Sia I un *insieme moltiplicativo* M; si considerino tutte le coppie ordinate di elementi di I e si pongano in un in-

---

[4]) Per quanto detto nella nota (2) il viceversa è una conseguenza delle (4), (5).

[5]) In particolare per nessuna coppia può essere definita la O.

sieme I^* tutti gli elementi di I ed un elemento $x_{a,b}$ per ogni coppia ordinata a, b di I per la quale non ha senso $a \,O\, b$.

Gli elementi di I^* devono considerarsi tutti distinti; ne segue che, se non hanno senso $a \,O\, b$ ed $\alpha \,O\, \beta$, condizione necessaria e sufficiente perchè $x_{a,b} = x_{\alpha,\beta}$ è che $a = \alpha$, $b = \beta$.

Si definisce ora in I^* una operazione di prodotto O^* come segue:

(10) $a \,O^*\, b = a \,O\, b$ *se* $a \,O\, b$ *ha significato,*

(11) $a \,O^*\, b = x_{a,b}$ *se* $a \,O\, b$ *non ha significato.*

E' immediato il

TEOREMA I: *L'insieme* I^* *con rispetto all'operazione* O^* *è un sistema moltiplicativo* M.

Le proprietà (6), (7) sono ovvie. Per verificare la (8) si supponga che a, b, b_1, $b \neq b_1$ siano elementi di I^* e quindi necessariamente di I.

Per quanto detto in principio di questo numero se $a \,O^*\, b = x_{a,b}$ ed $a \,O^*\, b_1 = x_{a,b_1}$ da $b \neq b_1$ segue $x_{a,b} \neq x_{a,b_1}$, cioè la tesi; se ad esempio $a \,O^*\, b = a \,O\, b$ ed $a \,O^*\, b_1 = x_{a,b_1}$ la tesi è ovvia; se infine $a \,O^*\, b = a \,O\, b$, $a \,O^*\, b_1 = a \,O\, b_1$ la (8) segue perchè è vera in I.

4. - Sia I un *sistema moltiplicativo* M e si consideri un insieme $^*I$ che contenga ogni elemento di I e contenga un elemento $z_{a,b}$ per ogni equazione $a \,O\, x = b$ $(a \in I,\ b \in I)$ che non ammette soluzioni in I e contenga un elemento $w_{a,b}$ per ogni equazione $y \,O\, a = b$ $(a \in I,\ b \in I)$ che non ammette soluzioni in I.

Tutti gli elementi di $^*I$ sono da riguardarsi come distinti.

Si definisce in $^*I$ l'operazione di prodotto $^*O$ come segue:

(12) $a \,{}^*O\, b = a \,O\, b$ *se questo secondo membro ha significato*

(13) $a \,{}^*O\, z_{a,b} = b$ *se* $a \,O\, x = b$ *non ha soluzioni in* I $(a \in I,\ b \in I)$

(14) $w_{a,b} \,{}^*O\, a = b$ *se* $y \,O\, a = b$ *non ha soluzioni in* I $(a \in I,\ b \in I)$.

TEOREMA II: *L'insieme* $^*I$ *con rispetto all'operazione* $^*O$ *è un sistema moltiplicativo* M.

5. - Sia I un *sistema moltiplicativo* M e θ una *relazione di congruenza* su I. Si costruisce la relazione θ^* su I^* come segue:

(15) *Se A e B sono due blocchi della θ, distinti o no, tali che nessun elemento dell'insieme $C = A\ O^*\ B$ appartiene ad I, allora C è un blocco della θ^*,*

(16) *se A_r e B_r sono blocchi della θ, distinti o no, tutti gli elementi degli insiemi $C_r = A_r\ O^*\ B_r$ che contengono almeno un elemento di uno stesso blocco D della θ, costituiscono un blocco della θ^* assieme a tutti gli elementi di D.*

(17) *Ogni blocco della θ non contenuto in un blocco della θ^* di tipo* (16) *è un blocco della θ^*.*

Si ha il

LEMMA: *Se a, b sono elementi di I, essi vengono collocati dalla θ^* in uno stesso blocco, se solo se, $a \equiv b(\theta)$.*

Infatti se a e b vengono collocati dalla θ^* nello stesso *blocco* C, tale *blocco* non può essere del tipo descritto in (15) perchè i suoi elementi a e b appartengono ad I. Siano dunque a e b in uno stesso *blocco* F di tipo (16), che risulti formato di tutti gli elementi che si ottengono dai prodotti $A_r\ O^*\ B_r$ di *blocchi* della θ, tali che esiste almeno $p \in A_r$ e $q \in B_r$ con $p\ O\ q$ elemento di un *blocco* D, fissato, della θ.

Ora se $p' \in A_r$ e $q \in B_r$ ed ha senso $p'\ O\ q'$, tale elemento apparterrà a D perchè $p \equiv p'(\theta)$, $q \equiv q'(\theta)$ e per la (9); cioè in conclusione ogni elemento di F che appartenga ad I è un elemento di D. Tali saranno a e b e perciò $a \equiv b(\theta)$. Inversamente se $a \equiv b(\theta)$, a e b appartengono ad uno stesso blocco D della θ e quindi per le (16), (17) segue la tesi.

Si riconosce subito che i *blocchi* della θ^* sono insiemi disgiunti, ma in più si ha il

TEOREMA III: *La relazione θ^* su I^* è una relazione di congruenza su I^*.*

Bisogna dunque far vedere che se $a \equiv b(\theta^*)$ e $c \equiv d(\theta^*)$ allora $h = a\ O^*\ c \equiv b\ O^*\ d = k(\theta^*)$ tutte le volte che i prodotti considerati hanno senso.

Ora perchè h e k abbiano senso devono a, b, c, d, appartenere ad I e quindi per il LEMMA $a \equiv b(\theta)$, $c \equiv d(\theta)$. Se $h \in I$, $k \in \bar{I}$ allora $h = a \,O\, c$, $k = b \,O\, d$ e quindi $h \equiv k(\theta)$ per essere θ una *relazione di congruenza* su I ed ancora per il LEMMA $h \equiv k(\theta^*)$.

Se $h \in I$, $k \in I^* - I$ è $h \equiv k(\theta^*)$ per la (16). Analogamente se $h \in I^* - I$ e $k \in I$. Se infine $h \in I^* - I$, $k \in I^* - I$ detti E ed F i blocchi della θ che contengono rispettivamente a, b e c, d se nessun elemento di $E \,O^*\, F$ appartiene ad I allora la tesi discende dalla (15), se invece $l \in E$, $m \in F$ $l \,O^*\, m = l \,O\, m \in I$, h e k per la (16) appartengono allo stesso *blocco* della θ^* che contiene $l \,O^*\, m$ e quindi ancora la tesi.

6. - Sia I un *sistema moltiplicativo* M e θ una *relazione di congruenza* su I. Si definisce la relazione $^*\theta$ su $^*I$ come segue:

(18) *se* $a \equiv b(\theta)$ *allora* $a \equiv b(^*\theta)$, *e viceversa se* $a \in I$, $b \in I$.

(19) *ogni elemento di* $^*I - I$ *è congruo solo a se stesso modulo* $^*\theta$.

Si ha quindi il

TEOREMA III: *La relazione* $^*\theta$ *su* $^*I$ *è una relazione di congruenza su* $^*I$.

Intanto dalle (18), (19) si ha subito che la $^*\theta$ distribuisce gli elementi di $^*I$ in insiemi disgiunti. Sia quindi $a \equiv b(^*\theta)$, $c \equiv d(^*\theta)$; bisognerà dimostrare che $a \,{}^*O\, c \equiv b \,{}^*O\, d(^*\theta)$ se hanno senso i prodotti considerati.

Se a, b, c, d, appartengono tutti e quattro ad I allora è anche $a \equiv b(\theta)$, $c \equiv d(\theta)$ per la (18) e quindi la tesi per la (18) e perchè θ è una *relazione di congruenza* su I.

Sia $a \in {}^*I - I$, allora perchè abbia senso $a \,{}^*O\, c$ per la (14) deve essere $a = w_{\alpha,\beta}$ $c = \beta$ e poichè $a \equiv b(^*\theta)$, deve essere per la (19) $a = b = w_{\alpha,\beta}$ quindi ancora per la (14) $d = \beta$ perchè abbia senso $b \,{}^*O\, d$. Segue subito la tesi; lo stesso accade se si fa l'ipotesi che appartenga ad $^*I - I$ uno degli elementi b, c, d, basta eventualmente ricorrere alla (13) in luogo della (14).

7. - Da questo momento in poi, poichè non c'è più pericolo di equivoci si indicherà con O anche ciascuna delle operazioni *O ed O* e con θ ciascuna delle *relazioni di congruenza* *θ, θ*, inoltre per brevità si scriverà $a\,O\,b = ab$.

8. - Siano $\boldsymbol{a}$ e θ due simboli determinati e si considerino gli insiemi $\Sigma_{\boldsymbol{a}}(\theta)$ così definiti:

i_1) Il simbolo $\boldsymbol{a} \equiv \boldsymbol{p}(\theta)$ è l'insieme $\Sigma_{\boldsymbol{a}}(\theta)$, Ω_1. La $\boldsymbol{p}$ è una qualunque lettera diversa da $\boldsymbol{a}$, che si chiamerà *lettera terminale.*

i_2) Ogni $\Sigma_{\boldsymbol{a}}(\theta)$ contiene un numero finito di simboli.

i_3) Da un $\Sigma_{\boldsymbol{a}}(\theta)$, A, si ottiene ancora un $\Sigma_{\boldsymbol{a}}(\theta)$ sostituendo al posto di una *lettera terminale,* e sia per fissare le idee $\boldsymbol{q}$, che compare in un simbolo di A, il simbolo $\boldsymbol{rs}$ ed aggiungendo all'insieme A così modificato i due simboli $\boldsymbol{r} \equiv \boldsymbol{h}(\theta)\,\boldsymbol{s} \equiv \boldsymbol{k}(\theta)$ dove $\boldsymbol{r}, \boldsymbol{s}, \boldsymbol{h}, \boldsymbol{k}$ sono lettere qualunque però tra loro sempre diverse e diverse da tutte le lettere che compaiono in A. Le *lettere terminali* del nuovo $\Sigma_{\boldsymbol{a}}(\theta)$ sono quelle di A ($\boldsymbol{q}$ escluso) ed in più $\boldsymbol{h}, \boldsymbol{k}$. Si diranno *lettere fattori* quelle come $\boldsymbol{r}, \boldsymbol{s}$ che compaiono nel prodotto formale $\boldsymbol{rs}$. In più ogni insieme $\Sigma_{\boldsymbol{a}}(\theta)$ sia dedotto da Ω_1 con un numero finito di operazioni del tipo sopra descritto.

Si ha che se un $\Sigma_{\boldsymbol{a}}(\theta)$ contiene più di un simbolo esso non contiene il simbolo $\boldsymbol{a} \equiv \boldsymbol{p}(\theta)$ di cui si parla in i_1).

Un $\Sigma_{\boldsymbol{a}}(\theta_1)$, C, si dirà l'*associato* di un dato $\Sigma_{\boldsymbol{a}}(\theta)$, A, se C si ottiene sostituendo nei simboli di A, θ_1 al posto di θ, $\boldsymbol{c}$ al posto di $\boldsymbol{a}$ e dotando di un apice ogni *lettera fattore* che compare nei simboli di A. Come conseguenza ogni *lettera terminale* di A è una *lettera terminale* di C e viceversa.

L'insieme dei simboli A e C si dirà un sistema $X_{\boldsymbol{a},\,\boldsymbol{c}}(\theta, \theta_1)$. Si osservi che $\boldsymbol{a}, \boldsymbol{c}$ si deve pensare come una coppia ordinata e così pure θ, θ_1, talchè θ si riferirà ad $\boldsymbol{a}$ e θ_1 a $\boldsymbol{c}$.

Sia ora *I un sistema moltiplicativo* M e siano θ, θ_1 (si usano le stesse lettere adoperate in precedenza perchè ciò è utile nel seguito e non porta ad equivoci) una coppia ordinata di *relazioni di congruenza* su I ed a, c sia una coppia ordinata di elementi di I.

Si dirà che un sistema $X_{a,c}(\theta, \theta_1)$ è compatibile in I relativamente alla coppia di elementi a, c ed ai moduli θ, θ_1 se, sostituiti a al simbolo $\boldsymbol{a}$, c al simbolo $\boldsymbol{c}$ ed al posto di ogni *lettera fattore* e di ogni *lettera terminale* dei simboli di $X_{a,c}(\theta, \theta_1)$ un opportuno elemento di I (a lettere diverse può essere sostituito lo stesso elemento di I), accade che i simboli di A diventano congruenze di modulo θ valide in I ed i simboli di C diventano congruenze di modulo θ_1 valide in I. Ogni siffatto insieme di elementi di I si dirà una soluzione del sistema $X_{a,c}(\theta, \theta_1)$, relativa alle *origini* a e c ed ai *moduli* θ, θ_1 e per rappresentare una soluzione (quando basti considerarne una sola) si userà per ogni suo elemento la stessa lettera, scritta però in corsivo, dei simboli di $X_{a,c}(\theta, \theta_1)$, alla quale l'elemento si riferisce. — Si ha ora il

TEOREMA V: *Se non esiste alcun sistema $X_{a,c}(\theta, \theta_1)$ compatibile in I relativamente alla coppia di elementi a, c (di I) ed ai moduli θ e θ_1 (di I) lo stesso accade per I^* e $^*I$.*

CASO I^*. - Ragionando per assurdo si supponga che il sistema $X_{a,c}(\theta, \theta_1)$, X_1, ammetta in I^* una soluzione S_1 relativa alle *origini* a, c ed ai *moduli* θ e θ_1. Può darsi che tutti gli elementi di S_1 appartengano ad I, allora poichè X_1, per ipotesi, non ammette in I soluzioni del tipo voluto, bisogna che esista qualche simbolo in X_1 contenente un prodotto formale e sia ad esempio il simbolo $\boldsymbol{p} \equiv \boldsymbol{rs}(\theta)$, per cui rs non ha significato in I. Allora per la (16) devono esistere in I, r_1 ed s_1 tali che $r_1 s_1 \in I$, $r_1 \equiv r(\theta)$, $s_1 \equiv s(\theta)$, da cui consegue $r_1 s_1 \equiv rs(\theta)$ e così basta in S_1 sostituire r_1 ed s_1 rispettivamente ad r ed s per ottenere ancora una soluzione S_2 di X_1, di cui r_1 è l'elemento relativo ad $\boldsymbol{r}$ ed s_1 l'elemento relativo ad $\boldsymbol{s}$.

Per la soluzione S_2 il simbolo $\boldsymbol{p} \equiv \boldsymbol{rs}(\theta)$ non presenta la particolarità sopra considerata e lo stesso accade per i simboli di X_1 per cui S_1 non aveva tale particolarità e poichè X_1 contiene per (i_3) un numero finito di simboli procedendo a partire da S_2 con un numero finito di operazioni analoghe a quella compiuta per passare da S_1 a S_2 si perverrebbe ad una soluzione in I di X_1 contro l'ipotesi.

Si supponga ora che qualche elemento di S_1 appartenga ad $I^* - I$; questo elemento non può essere relativo ad una *let-*

tera fattore, ad esempio $\boldsymbol{w}$, perchè dovendo comparire in un prodotto formale nei simboli di X_1, e sia $\boldsymbol{wk}$ questo prodotto, se $w \in I^* - I$ non avrebbe senso in I^* il prodotto wk.

Appartenga dunque ad $I^* - I$ un elemento di S_1 relativo ad una *lettera terminale* di X_1 e sia la lettera $\boldsymbol{p}$ che comparisce perciò in due simboli del tipo $\boldsymbol{q} \equiv \boldsymbol{p}(\theta)$, $\boldsymbol{p} \equiv \boldsymbol{q}'(\theta_1)$, dove $\boldsymbol{q}$ e $\boldsymbol{q}'$ sono ciascuna una *lettera fattore* o $\boldsymbol{q} = \boldsymbol{a}$ e $\boldsymbol{q}' = \boldsymbol{c}$ quindi in ogni caso q e q' sono elementi di I.

In conclusione posto che sia $p = lm$ dovranno esistere in I gli elementi l_1, m_1, l'_1, m'_1 tali che $l_1 m_1 \in I$, $l'_1 m'_1 \in I$, $l_1 \equiv l(\theta)$, $m_1 \equiv m(\theta)$, $l'_1 \equiv l(\theta_1)$, $m'_1 \equiv m(\theta_1)$ e si può supporre che le lettere $\boldsymbol{l_1}$, $\boldsymbol{m_1}$, $\boldsymbol{l'_1}$, $\boldsymbol{m'_1}$ non compaiono nei simboli di X_1. Si tolgano da X_1 i simboli $\boldsymbol{q} \equiv \boldsymbol{p}(\theta)$, $\boldsymbol{p} \equiv \boldsymbol{q}'(\theta_1)$ e si aggiungano i simboli $\boldsymbol{q} \equiv \boldsymbol{l_1 m_1}(\theta)$, $\boldsymbol{p} \equiv \boldsymbol{l'_1 m'_1}(\theta_1)$, $\boldsymbol{l_1} \equiv \boldsymbol{l}(\theta)$, $\boldsymbol{m_1} \equiv \boldsymbol{m}(\theta)$, $\boldsymbol{l} \equiv \boldsymbol{l'_1}(\theta_1)$, $\boldsymbol{m} \equiv \boldsymbol{m'_1}(\theta_1)$; si vede per la (i_2) che gli insiemi A_1 e C_1 di X_1 si trasformano rispettivamente in un insieme $\Sigma_a(\theta)$ e nel suo associato $\Sigma_c(\theta_1)$ e così X_1 si trasforma in un X_2 che è ancora un $X_{a,c}(\theta, \theta_1)$.

Ora associando ad ogni lettera di X_2 che si trova nei simboli di X_1 l'elemento che S_1 associava alla stessa lettera in X_1 ed associando l_1, m_1, l'_1, m'_1 rispettivamente a $\boldsymbol{l_1}$, $\boldsymbol{m_1}$, $\boldsymbol{l'_1}$, $\boldsymbol{m'_1}$ si ottiene una soluzione S_2 di X_2 relativa alla coppia di elementi a, c ed ai *moduli* θ e θ_1. Se quindi S_1 associava ad n *lettere terminali* di X_1 elementi di $I^* - I$, S_2 associa ad $n-1$ *lettere terminali* di X_2 elementi di $I^* - I$. Così continuando ad operare, come si è fatto per passare da X_1 a X_2, si finirebbe col pervenire ad un $X_{a,c}(\theta, \theta_1)$ con soluzione in I relativa alla coppia di elementi a, c ed ai moduli θ, θ_1, contro l'ipotesi.

CASO $*I$. - Se tutti gli elementi di S_1 appartenessero ad I allora X_1 sarebbe compatibile in I contro l'ipotesi. Sia t un elemento di S_1 appartenente ad $*I - I$, cioè $t = w_{\alpha,\beta}$ con $\alpha \in I$, $\beta \in I$.

Sia $\boldsymbol{t}$ *lettera fattore* e per fissare le idee compaia nel simbolo

$$\boldsymbol{p} \equiv \boldsymbol{tk}(\theta)\,. \tag{20}$$

Se X_1 contenesse il simbolo $\boldsymbol{t} \equiv \boldsymbol{rs}(\theta)$ si perverrebbe ad un assurdo. Infatti sia che r, s appartengano ambedue ad I o

che uno di essi appartenga ad $^*I - I$ (e questi sono i soli casi possibili) comunque il prodotto $rs \in I$, ma per la (19) t appartiene ad un solo blocco delle (θ) e quindi non sarebbe $t \equiv rs(\theta)$.

Deve dunque X_1 contenere il simbolo

$$\boldsymbol{t \equiv r(\theta)} \tag{21}$$

con $\boldsymbol{r}$ *lettera terminale* e X_1 deve ancora contenere i simboli

$$\boldsymbol{r \equiv t'(\theta_1)} \quad , \quad \boldsymbol{t'k' \equiv p'(\theta_1)} , \tag{22}$$

(per non complicare si suppone qui contenuto anche il caso $\boldsymbol{p = a}$, $\boldsymbol{p' = c}$).

Allora sempre per la (19) segue $t = r = t' = w_{\alpha,\beta}$, $k = k' = \alpha$ e dalle (20), (22) risultano valide le congruenze

$$p \equiv \beta(\theta) \quad , \quad \beta \equiv p'(\theta_1) . \tag{23}$$

Conservi Ω_1 il significato attribuitogli in (i_1) e sia A_1 l'insieme $\Sigma_{\boldsymbol{a}}(\theta)$ di X_1, sarà possibile determinare gli insiemi $\Sigma_{\boldsymbol{a}}(\theta)$, Ω_1, Ω_2, ..., $\Omega_\sigma = A_1$ in modo che ciascuno degli Ω_2, ..., Ω_σ si deduca dal precedente con l'operazione descritta in (i_3) (σ è finito per (i_2)).

Il simbolo (20) apparirà dunque in un certo Ω_i $(i > 1)$ e nei successivi mentre in Ω_{i-1} vi sarà il simbolo

$$\boldsymbol{p \equiv n(\theta)} \tag{24}$$

con $\boldsymbol{n}$ *lettera terminale,* che si può sempre supporre non aver poi usato come lettera nei simboli di Ω_r con $r > i - 1$.

Ora Ω_{i-1} è un $\Sigma_{\boldsymbol{a}}(\theta)$ che insieme al suo *associato* $\Sigma_{\boldsymbol{c}}(\theta_1)$ darà un sistema $X_{\boldsymbol{a},\boldsymbol{c}}(\theta, \theta_1)$, X_2.

Se ad ogni lettera di X_2 si associa l'elemento che S_1 associa alla stessa lettera in X_1 e ad $\boldsymbol{n}$ si associa β, X_2 risulta compatibile perchè S_1 è soluzione di X_1 e perchè la (24) e la analoga $\boldsymbol{n \equiv p'(\theta_1)}$ risultano soddisfatte per le (23).

La soluzione S_2 di X_2, sopra considerata, contiene un numero di elementi di $^*I - I$, associati a *lettere fattori* di X_2, minore di quello di S_1, quindi dopo aver ripetuto un numero finito di volte il procedimento che ha fatto passare da X_1

a X_2 si perverrà ad un sistema $X_{a,c}(\theta, \theta_1)$, X, che ammette una soluzione S in $^*I$, relativa alla coppia di elementi a, c ed ai *moduli* θ, θ_1, tale che a nessuna sua *lettera fattore* S associa elementi di $^*I$. Ma se poi S associasse un elemento di $^*I - I$ ad una *lettera terminale*, e sia la $\boldsymbol{w}$, questa comparirebbe in un simbolo del tipo $\boldsymbol{p} \equiv \boldsymbol{w}(\theta)$ e dovrebbe essere $p = w$ contro il fatto che la $\boldsymbol{p}$ è una *lettera fattore* e $p \in {}^*I - I$. Concludendo S è una soluzione di X in I, contro l'ipotesi. Il caso che per la (20) fosse $k \in {}^*I - I$ si tratta come il caso $t \in {}^*I - I$ e con ciò il teorema risulta completamente dimostrato.

9. - E' estremamente facile costruire *sistemi moltiplicativi* M, dotati di due *relazioni di congruenza* θ, θ_1, contenenti due elementi a, c e tali che in essi ogni sistema $X_{a,c}(\theta, \theta_1)$ risulti non compatibile rispetto alla coppia di elementi a, c ed ai *moduli* θ, θ_1. Ad esempio si consideri l'insieme I formato dai tre elementi a, b, c (nessuno dei prodotti xy, $x \in I$, $y \in I$ abbia significato) e sia θ la *relazione di congruenza* (in questo caso una partizione di I) che colloca a in un blocco e b, c in un altro blocco e sia θ_1 la *relazione di congruenza* che colloca a, b in un *blocco* e c in un altro *blocco*. Ovviamente I è un *sistema moltiplicativo* M.

Ora ogni sistema $X_{a,c}(\theta, \theta_1)$ diverso da quello formato dai simboli di Ω_1 e da quelli del suo associato $\Sigma_c(\theta_1)$, contiene qualche prodotto formale e perciò non ha soluzione in I. Risulta che il solo $X_{a,c}(\theta, \theta_1)$ che può avere soluzioni in I è il sistema formato dai simboli $\boldsymbol{a} \equiv \boldsymbol{t}(\theta)$, $\boldsymbol{t} \equiv \boldsymbol{c}(\theta_1)$, ma ciò non è possibile perchè in caso contrario da $a \equiv t(\theta)$ si ricaverebbe $a = t$ e l'assurdo $a \equiv c(\theta_1)$.

TEOREMA VI: *Esistono quasigruppi con relazioni di congruenza non permutabili.*

Sia I il *sistema moltiplicativo* M considerato in questo n.ro 9. Si costruisca una successione, $I_1 = I$, I_2, I_3, ... dove sia o $I_r = {}^*I_{r-1}$ o $I_r = I^*_{r-1}$ $(r \geq 2)$ e tale che da un indice in poi non risulti per I_r verificata sempre la stessa delle due eventualità possibili. Per i TEOREMI I, II, IV, IV tutti gli

insiemi della successione sono *sistemi moltiplicativi M* dotati di due *relazioni di congruenza* θ e θ_1.

Ovviamente l'insieme $Q = I_1 + I_2 + I_3 + \ldots$ è un *quasi-gruppo* con le *relazioni di congruenza* θ, θ_1 [6]; si vede ora che tali relazioni non sono tra loro *permutabili.*

Per la costruzione di I si ha $a \equiv b(\theta_1)$, $b \equiv c(\theta)$, ma non può esistere $p \in Q$ per cui $a \equiv p(\theta)$, $p \equiv c(\theta_1)$.

Infatti, in caso contrario, tali congruenze risulterebbero soddisfatte per un certo I_r ed allora il sistema $X_{a,c}(\theta, \theta_1)$ formato con i simboli $\boldsymbol{a} \equiv \boldsymbol{p}(\theta)$, $\boldsymbol{p} \equiv \boldsymbol{c}(\theta_1)$ ammetterebbe in I_r soluzione relativa alla coppia di elementi a, c ed ai *moli* θ, θ_1 contro l'ipotesi fatta su I e per il TEOREMA V. Quindi per Q valgono le (5), ma queste non implicano le (4) cioè θ e θ_1 non sono *permutabili.*

---

[6]) In Q è $a \equiv b(\theta)$ se esiste I_r dove questo accade. Cioè θ è l'unione della *relazione di congruenza* θ di I_1 e di quelle che da questa si ottengono con gli ampliamenti successivi in I_2, I_3 ... analogamente per θ_1.