RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

DOMENICO BOCCIONI

Simmetrizzazione di una operazione n-aria

Rendiconti del Seminario Matematico della Università di Padova, tome 35, nº 1 (1965), p. 82-106

<http://www.numdam.org/item?id=RSMUP_1965__35_1_82_0>

SIMMETRIZZAZIONE DI UNA OPERAZIONE n-ARIA

Nota *) *di* DOMENICO BOCCIONI (*a Padova*) **)

Un n-semigruppo ($n \geqslant 2$) è un insieme, S_n, dotato di un'operazione (moltiplicazione) n-aria associativa (n. 1). Un 2-semigruppo è quindi un ordinario semigruppo.

Un n-gruppo è un n-semigruppo, G_n, nel quale ogni equazione del tipo $a_1 \ldots a_{i-1} x_i a_{i+1} \ldots a_n = a_{n+1}$ ($1 \leqslant i \leqslant n$) è univocamente risolubile (n. 2). Un 2-gruppo è quindi un ordinario gruppo.

La teoria degli n-gruppi, iniziata da W. Dörnte ([3] [1]), fu poi ampiamente sviluppata da E. L. Post ([5]). Di importanza fondamentale per questa teoria è il « teorema del laterale » di Post ([5]), in base al quale ogni n-gruppo G_n è immergibile in un certo gruppo G (individuato da G_n a meno di isomorfismi), in modo che la consueta moltiplicazione di n fattori in G subordini in G_n l'operazione n-aria ivi data, e che gli elementi di G_n costituiscano in G un laterale di un certo sottogruppo normale di G. Questo gruppo G viene denotato con $C(G_n)$, (n. 2).

Nel presente lavoro si considera il problema di vedere sotto quali condizioni un n-semigruppo S_n, con $n > 2$, è immergi-

---

*) Pervenuta in Redazione il 18 luglio 1964.

Indirizzo dell'A.: Seminario Matematico, Università, Padova.

**) Lavoro eseguito nell'ambito dell'attività dei gruppi di ricerca matematica del C. N. R.

1) I numeri fra parentesi quadre rimandano alla bibliografia alla fine della nota.

bile in un n-gruppo, (problema che, per $n = 2$, si riduce dunque a quello, ben noto, dell'immersione di un semigruppo in un gruppo).

Questo problema viene ricolto (nel § 3), per un'operazione n-aria commutativa (n. 1), con un risultato identico a quello classico del caso binario: *Un n-semigruppo commutativo Sn, con $n > 2$, è immergibile in un n-gruppo se, e soltanto se, S_n è cancellativo* (n. 11).

Questo risultato, del quale vengono date due dimostrazioni (n. 13-15), è stato raggiunto in seguito ad una indagine preliminare (§ 2) sulla struttura del sotto-n-gruppo, $\overline{G_n} = [S_n]_n$, generato da un sotto-n-semigruppo S_n di un n-gruppo (n. 9).

Questa indagine è stata fatta nel caso generale, cioè per un'operazione n-aria non necessariamente commutativa. Si è trovato (n. 10 ,teor. 2) che, nel gruppo $C(\overline{G_n})$, $(S_n)^{n-1}$ è un sotto-semigruppo, che in $C(\overline{G_n})$ è normale il sottogruppo $[(S_n)^{n-1}]$, generato dal semigruppo $(S_n)^{n-1}$, e che ivi $\overline{G_n} = [S_n]_n$ è un laterale di $[(S_n)^{n-1}]$.

Se, in particolare, S_n è commutativo (§ 3), risultano contemporaneamente commutativi $\overline{G_n} = [S_n]_n$ e $C(\overline{G_n})$ (n. 11), quindi pure il sotto-semigruppo $(S_n)^{n-1}$ di $C(\overline{G_n})$. Ma allora la struttura del sottogruppo $[(S_n)^{n-1}]$ di $C(\overline{G_n})$ rimane notoriamente individuata da quella di $(S_n)^{n-1}([(S_n)^{n-1}]$ è il classico gruppo dei quozienti del semigruppo commutativo $(S_n)^{n-1})$, e quindi da quella di S_n. Dalla struttura dell'n-semigruppo commutativo S_n rimane dunque individuata la struttura dell'n-gruppo $G_n = [S_n]_n$ (laterale di $[(S_n)^{n-1}]$ in $C(\overline{G_n})$). Precisamente (n. 11, VI)), si è trovato che ogni elemento x di $\overline{G_n}$ si può scrivere (come prodotto di n fattori in $\overline{G_n}$) nella forma

$$x = a_1(a_{2,1} \dots a_{2,n-2})^{-1} \dots (a_{n,1} \dots a_{n,n-2})^{-1} \quad (a_1, a_{r,r} \in S_n),$$

dove il simbolo $(a_{r,1} \dots a_{r,n-2})^{-1}$ $(2 \leqslant r \leqslant n)$ rappresenta il cosidetto inverso (o simmetrico) della $(n-2)$-upla (ordinata) $(a_{r,1}, \dots, a_{r,n-2})$, (n. 3), il quale è un (ben determinato) elemento di G_n, che coincide con l'ordinario inverso del prodotto $a_{r,1} \dots a_{r,n-2}$ nel gruppo $C(\overline{G_n})$.

In conseguenza di questo risultato, un n-gruppo $\overline{G}_n$ che sia generato da un suo sotto-n-semigruppo commutativo S_n, viene chiamato un n-gruppo dei quozienti di S_n, e denotatato con $Q(S_n)$. Il risultato centrale di questo lavoro, sopra segnalato, ammette dunque la seguente precisazione (n. 12, teor. 3): *Di ogni n-semigruppo commutativo e cancellativo S_n, con $n > 2$, esiste un n-gruppo dei quozienti, $Q(S_n)$, univocamente determinato da S_n a meno di isomorfismi.*

Ad esempio, uno qualsiasi dei due metodi di immersione di S_n in $Q(S_n)$ sopra citati (XI), n. 14, oppure XII), n. 15), se applicato all'n-semigruppo additivo S_n (addizione ordinaria di n addendi) dei numeri naturali congrui ad 1 modulo $n - 1$, fornisce come $\overline{G_n} = Q(S_n)$ l'n-gruppo additivo degli interi $\equiv 1$ (mod $n - 1$); (in questo esempio, $C(\overline{G_n})$ coincide col gruppo additivo degli interi). In particolare ($n = 3$), il 3-semigruppo additivo S_3 (commutativo e cancellativo) dei numeri naturali dispari, viene così esteso al 3-gruppo additivo, $Q(S_3)$, degli interi (relativi) dispari.

Da segnalare infine il teor. 1 (n. 4), che fornisce, per $n > 2$ (e solo per $n > 2$), una nuova definizione di n-gruppo, come n-semigruppo dotato di $(n - 1)$-uple identiche di elementi (n. 3) ed in cui ogni $(n - 2)$-upla di elementi ammette un inverso.

§ 1

1. – Consideriamo un insieme non vuoto, S_n, dotato di un'operazione n-aria ($n \geqslant 2$) univoca ed ovunque definita:

$$(a_1, a_2, \dots, a_n) \to f(a_1, a_2, \dots, a_n) \in S_n \qquad (a_i \in S_n).$$

Nel presente lavoro, porremo $f(a_1, \dots, a_n) = a_1 \dots a_n$ (*prodotto di n fattori*), e chiameremo quindi *moltiplicazione n-aria* l'operazione f.

Diremo che questa moltiplicazione n-aria è *associativa* (cfr. [5], p. 213) se, qualunque siano $a_1, \ldots, a_{2n-1} \in S_n$, risulta

$$(1) \qquad (a_1 \ldots a_n)a_{n+1} \ldots a_{2n-1} = a_1(a_2 \ldots a_{n+1})a_{n+2} \ldots a_{2n-1} = \ldots$$
$$= a_1 \ldots a_{n-1}(a_n \ldots a_{2n-1}) \, .$$

Un insieme non vuoto S_n, dotato di una moltiplicazione n-aria associativa, verrà detto un *n-semigruppo* (moltiplicativo), ([6], p. 19). Un 2-semigruppo è dunque un ordinario semigruppo.

È noto (cfr. [6], p. 19; [5], p. 214) che in un n-semigruppo S_n si può definire, per induzione su k, il *prodotto* (*generalizzato*) *di* $k(n-1)+1$ *fattori* $a_1, \ldots, a_{k(n-1)+1} \in S_n$ $(k = 0, 1, 2, 3, \ldots)$: Il prodotto generalizzato di un fattore a_1 è a_1; il prodotto generalizzato di $k(n-1)+1$ fattori, con $k \geqslant 1$, è il prodotto del prodotto generalizzato dei primi $(k-1)(n-1)+1$ fattori e dei rimanenti $n-1$ fattori. Denoteremo tale prodotto (che è un ben determinato elemento di S_n) col simbolo

$$(2) \qquad a_1 \ldots a_{k(n-1)+1} \, .$$

È pure noto che tale prodotto (2) non cambia sostituendo a $k'(n-1)+1$ consecutivi qualsiasi fra i suoi fattori $(1 \leqslant k' \leqslant k-1)$ il loro prodotto (*proprietà associativa generalizzata*).

Un n-semigruppo S_n si dirà *commutativo* se in esso ogni prodotto di n fattori non cambia, cambiando comunque l'ordine di questi fattori. È noto (cfr. [6], p. 19) che allora anche ogni prodotto (generalizzato) (2) non cambia, cambiando comunque l'ordine dei suoi $k(n-1)+1$ fattori (*proprietà commutativa generalizzata*).

Se S_n ed S'_n sono due n-semigruppi, per un *omomorfismo* di S_n in S'_n si intenderà un'applicazione (univoca), $\omega\colon a \to a\omega$, di S_n in S'_n tale che $(a_1 \ldots a_n)\omega = (a_1\omega) \ldots (a_n\omega)$, qualunque siano $a_1, \ldots, a_n \in S_n$. Un omomorfismo iniettivo e suriettivo si dirà un *isomorfismo* di S_n su S'_n; se un tale isomorfismo esiste, S_n ed S'_n si diranno *isomorfi*. (cfr. [5], pp. 225, 226).

Gli elementi di un semigruppo S costituiscono evidentemente un n-semigruppo (per ogni dato n) rispetto alla consueta moltiplicazione di n elementi di S, (cfr. [6], p. 19). In questo senso alluderemo ad S come ad un n-semigruppo.

Per un *sotto-n-semigruppo* di un n-semigruppo S_n intenderemo un sottinsieme non vuoto di S_n contenente i prodotti di n elementi qualsiasi del sottinsieme stesso (cfr. [6], p. 20).

2. – Ricordiamo ora la nozione di n-gruppo, dovuta a Dörnte ([3]). Dicesi *n-gruppo* (cfr. [5], p. 213) un n-semigruppo G_n nel quale l'equazione nell'incognita x_i

$$a_1 \dots a_{i-1} x_i a_{i+1} \dots a_n = a_{n+1} \tag{3}$$

ammette una e una sola soluzione, per $i = 1, 2, \dots, n$, qualunque siano gli elementi a_j di G_n. Un 2-gruppo è quindi un ordinario gruppo.

È noto ([5], p. 213, [17]); cfr. [6], pp. 19 e 25) che un n-semigruppo G_n è un n-gruppo, se in G_n esiste una soluzione dell'equazione (3) per $i = 1$ e per $i = n$ (qualunque siano $a_j \in G_n$).

Tutte le definizioni e le considerazioni del n. 1, relative agli n-semigruppi, valgono anche per gli n-gruppi. È chiaro che gli elementi di un gruppo G costituiscono un n-gruppo rispetto alla consueta moltiplicazione di n elementi di G.

Dicesi *sotto-n-gruppo* di un n-gruppo G_n (cfr. [5], p. 221; [6], p. 20) un sotto-n-semigruppo H_n di G_n che è un n-gruppo rispetto alla moltiplicazione n-aria subordinata in H_n da quella di G_n (cioè che contiene la soluzione x_i dell'equazione (3), se ogni $a_j \in H_n$). Dicendo che H_n è un sotto-n-gruppo di un gruppo G, penseremo naturalmente G come n-gruppo (rispetto alla consueta moltiplicazione di n elementi di G), (v. preced. capov.).

Diremo che un gruppo G è *circoscritto* ad un n-gruppo G_n se: *a*) G_n è un sotto-n-gruppo di G; *b*) $(G_n)^{n-1}$ (cioè il sottinsieme di G costituito da tutti i prodotti di $n-1$ elementi di G_n) è un sottogruppo normale di G; *c*) gli elementi di G_n costituiscono un laterale di $(G_n)^{n-1}$ in G; *d*) il gruppo quoziente $G/(G_n)^{n-1}$ è ciclico di ordine $n-1$; *e*) il gruppo $G/(G_n)^{n-1}$ è generato dal suo elemento G_n.

La nozione precedente, di gruppo G circoscritto a G_n, è dovuta a Post ([5], p. 219), che chiama G un « abstract containing gruop » di G_n, e la relativa definizione è quella adottata in [6], p. 22 (circoscritto = umschrieben). Fondamentale, per la teoria degli n-gruppi, è il seguente teorema ([5], p. 218; cfr. [6], pp. 23 e 24, od anche [2], p. 37).

Teorema del laterale (*di Post*): Ad ogni n- gruppo G_n è circoscritto un gruppo G. Questo gruppo G è univocamente determinato da G_n a meno di isomorfismi.

Il gruppo circoscritto all'n-gruppo G_n verrà denotato con

$$C(G_n)\ .$$

In base alla precedente definizione, la decomposizione di $C(G_n)$ nei laterali del suo sottogruppo normale $(G_n)^{n-1}$ si può scrivere:

$$C(G_n) = G_n \cup (G_n)^2 \cup \dots \cup (G_n)^{n-2} \cup (G_n)^{n-1}\ , \tag{4}$$

da cui appare chiaramente che ogni elelemento di $C(G_n)$ si può rappresentare come prodotto $a_1 \dots a_r$ di un numero finito di elementi a_i di G_n (quindi il gruppo $C(G_n)$ è generato dal suo sottinsieme G_n), e che un tale prodotto $a_1 \dots a_r$ appartiene al laterale $(G_n)^s$ se e soltanto se $r \equiv s$ (mod $n - 1$). (Cfr. [6], p. 23).

Il sottogruppo normale $(G_n)^{n-1}$ di $C(G_n)$ verrà chiamato il gruppo *associato* all'n-gruppo G_n ([5], p. 219) e denotato con $A(G_n)$:

$$A(G_n) = (G_n)^{n-1}\ .$$

3. – Per una $(n - 1)$-*upla identica* di elementi di un n-semigruppo S_n intenderemo una $(n - 1)$-upla (ordinata) $(u_1, \dots, u_{n-1})$ di elementi u_i di S_n tale che

$$au_1 \dots u_{n-1} = u_1 \dots u_{n-1}a = a \quad \text{per ogni } a \in S_n\ . \tag{5}$$

È noto ([5], pp. 214-215) che: *i*) in ogni n-gruppo G_n esistono $(n - 1)$-uple identiche; *ii*) se $(u_1, \dots, u_{n-1})$ è una $(n - 1)$-upla identica in G_n, tale è pure ciascuna delle $(n - 1)$-uple $(u_{i+1}, \dots, u_{n-1}, u_1, \dots, u_i)$ che si ottengono dalla data permutandone circolarmente gli elementi; *iii*) scelti ad arbitrio in G_n gli $n - 2$ elementi $u_1, \ldots, u_{n-2}$, esiste in G_n un unico elemento u_{n-1} tale che $(u_1, \ldots, u_{n-2}, u_{n-1})$ sia una $(n - 1)$-upla identica.

La verità delle precedenti affermazioni appare evidente appena si pensi G_n immerso nel gruppo $C(G_n)$ (si veda la (4)), poichè $(u_1, \ldots, u_{n-1})$ è una $(n - 1)$-upla identica se e solo se il prodotto $u_1 \ldots u_{n-1}$ (eseguito in $C(G_n)$) è l'elemento identico di $C(G_n)$. In particolare, per quanto riguarda la *iii*), u_{n-1} non è altro, se $n > 2$, che l'inverso del prodotto $u_1 \ldots u_{n-2}$ in $C(G_n)$: $u_{n-1} = (u_1 \ldots u_{n-2})^{-1}$ $(u_{n-1} \in G_n$, perchè $u_1 \ldots u_{n-2} \in (G_n)^{n-2} = (G_n)^{-1})$.

Se S_n è un n- semigruppo in cui esistono $(n - 1)$-uple identiche, e se $n > 2$, chiameremo *inverso* (o *simmetrico*: [1], p. 33) di una $(n - 2)$-upla (ordinata) $(u_1, \ldots, u_{n-2})$ di elementi di S_n (cfr. [5], p. 215), e lo denoteremo con $(u_1 \ldots u_{n-2})^{-1}$, un elemento di S) tale che ciascuna delle due $(n - 1)$-uple

$$(6) \qquad (u_1, \ldots, u_{n-2}, (u_1 \ldots u_{n-2})^{-1}) \,, \qquad ((u_1 \ldots u_{n-2})^{-1}, u_1, \ldots, u_{n-2n}$$

sia una $(n - 1)$-uplia identica.

Le precedenti considerazioni (v. *ii*) e *iii*)) assicurano l'esistenza e l'unicità dell'inverso $(u_1 \ldots u_{n-2})^{-1}$ di una qualunque $(n - 2)$-upla $(u_1, \ldots, u_{n-2})$ di elementi di un n-gruppo G_n (con $n > 2$). Questo inverso coincide con l'(usuale) inverno del prodotto $u_1 \ldots u_{n-2}$ nel gruppo $C(G_n)$.

4. – Invertiamo ora i (noti) risultati esposti nel n. precedente, dimostrando il seguente

TEOREMA 1: *Se $n > 2$, un n-semigruppo G_n in cui esistono $(n - 1)$-uple identiche ed in cui esiste un inverso di ogni $(n - 2)$-upla è un n-gruppo.*

Dimostriamo anzitutto che l'equazione (3), per $i = 1$:

$$(7) \qquad x_1 a_2 \ldots a_n = a_{n+1}$$

è risolubile in G_n. Infatti, se esiste un $x_1 \in G_n$ per cui vale la (7), allora, se $n > 3$, vale pure l'eguaglianza che si deduce dalla (7) moltiplicandone (v. (2)) a destra ambo i membri per la $((n-3)(n-1))$-upla $(u_1, \ldots, u_{n-1}, \ldots, u_1, \ldots, u_{n-1})$ ottenuta scrivendo di seguito, $n-3$ volte, una qualsiasi $(n-1)$-upla identica $(u_1, \ldots, u_{n-1})$ eguaglianza che si può scrivere:

$$x_1 a_2 \ldots a_n u_1 \ldots u_{n-1} \ldots u_1 \ldots u_{n-1} = a_{n+1} , \tag{8}$$

in cui il 2° membro a_{n+1} è il risultato dell'applicazione della proprietà associativa generalizzata e delle (5). Viceversa, se vale la (8), vale evidentemente anche la (7). Dunque l'equazione (7) è equivalente (alla (8) cioè) ad una equazione del tipo $(b_{i,j},\, b \in G_n)$:

$$x_1 b_{1,1} \ldots b_{1,n-2} b_{2,1} \ldots b_{2,n-2} \ldots b_{n-1,1} \ldots b_{n-1,n-2} = b , \tag{9}$$

(che, per $n = 3$, coincide con la (7) stessa). Basterà perciò occuparsi della risolubilità in G_n di questa equazione (9). Ora è assai facile verificare che il seguente elemento di G_n:

$$b(b_{n-1,1} \ldots b_{n-1,n-2})^{-1} \ldots (b_{2,1} \ldots b_{2,n-2})^{-1}(b_{1,1} \ldots b_{1,n-2})^{-1}$$

è appunto una soluzione della (9).

Abbiamo così dimostrato che l'equazione (3) è risolubile per $i = 1$. Con un ragionamento del tutto analogo si vede che la (3) è risolubile anche per $i = n$. Ciò è sufficiente (n. 2, 2° capov.) per concludere che G_n è appunto un n-gruppo.

Il teor. 1 fornisce una nuova definizione di n-gruppo, per $n > 2$, che è analoga alla ben nota definizione di gruppo come semigruppo dotato di una identità e di un inverso di ogni suo elemento.

Si osservi che, se si lasciasse cadere, nella definizione di inverso di una $(n-2)$-upla (n. 3), la condizione $n > 2$, il precedente teor. 1 avrebbe senso anche per $n = 2$, ma per $n = 2$ sarebbe falso: di un 2-semigruppo G_2 soddisfacente alle ipotesi del teor. 1, si potrebbe soltanto dire che è un comune semigruppo con identità. Quindi, se si assumesse anche per $n = 2$

come definizione di « n-gruppo » quella fornita dal teor. 1, un ordinario gruppo non sarebbe più un « 2-gruppo », ma un « 2-gruppo » particolare, la particolarità consistendo nell'ordinaria invertibilità di ogni suo elemento.

§ 2

5. – Dopo le considerazioni, di carattere introduttivo, esposte nel § 1, consideriamo ora il problema oggetto del presente lavoro.

Si tratta di trovare condizioni sufficienti per l'immergibilità di un dato n-semigruppo in un n-gruppo, in modo da poter estendere al caso di una operazione n-aria associativa (con $n > 2$) almeno i più noti criteri di immergibilità di un semigruppo (operazione binaria associativa) in un gruppo.

Risolveremo questo problema, nel successivo § 3, per gli n-semigruppi commutativi. A questo scopo è necessaria una indagine preliminare (alla quale è dedicato questo § 2), riguardante il sotto-n-gruppo generato da un dato sotto-n-semigruppo di un n-gruppo.

Questa indagine, il cui risultato è il teor. 2 del n.10, verrà fatta nel caso generale; quindi gli n-semigruppi e gli n-gruppi considerati in questo § 2 sono tutti non necessariamente commutativi. (Ciò al fine di poter utilizzare questi risultati, come si spera di fare in un successivo lavoro, per una soluzione del suddetto problema anche nel caso non commutativo).

6. – Supponiamo dunque che S_n, con $n > 2$, sia un sotto-n-semigruppo (n. 1) di un n-gruppo G_n, e pensiamo G_n come sotto-n-gruppo del gruppo $C(G_n)$ (n. 2):

$$S_n \subseteq G_n \subseteq C(G_n)\,. \tag{10}$$

Denotiamo con S il sotto-semigruppo di $C(G_n)$ generato da (gli elementi di) S_n. Evidentemente S è l'insieme degli elementi di $C(G_n)$ che sono prodotti finiti di elementi di S_n.

I) *Se S_n, con $n > 2$, è un sotto-n-semigruppo di un n-gruppo G_n, il sotto-semigruppo S del gruppo $C(G_n)$* (n. 2) *generato da S_n*

rmmette la seguente decomposizione in classi a due a due disgiunte:

$$S = S_n \cup (S_n)^2 \cup \ldots \cup (S_n)^{n-2} \cup (S_n)^{n-1} . \tag{11}$$

E precisamente, se un elemento x di S è il prodotto di r elementi di S_n, allora $x \in (S_n)^i$, con $1 \leqslant i \leqslant n-1$, se *e solo se $r = i + k(n-1)$, con k intero $\geqslant 0$.*

Infatti, se $x \in S$, cioè se $x = s_1 \ldots s_r$ con $s_1, \ldots, s_r \in S_n$, e se $a \equiv i \pmod{n-1}$ con $1 \leqslant i \leqslant n-1$, cioè se $r = i + k(n-1)$ con k intero $\geqslant 0$, risulta $x = (s_1 \ldots s_{i-1})(s_1 \ldots s_r)$, dove i fattori $s_i, \ldots, s_r$ del prodotto $s_i \ldots s_r$ sono in numero di $1 + k(n-1)$ e perciò (n. 1) $s_i \ldots s_r \in S_n$; dunque x è il prodotto di i elementi di S_n, ossia appunto $x \in (S_n)^i$. Viceversa, se $x = s_1 \ldots s_r \in (S_n)^i$, con $s_1, \ldots, s_r \in S_n$ ed $1 \leqslant i \leqslant n-1$, allora, poichè dalla (10) segue evidentemente

$$(S_n)^j \subseteq (G_n)^j \qquad (j = 1, 2, 3, \ldots) \tag{12}$$

e poichè $s_1 \ldots s_r \in (S_n)^r$, risulta $x \in (G_n)^r \cap (G_n)^i$, da cui (n. 2) $(G_n)^r = (G_n)^i$, donde $r \equiv i \pmod{n-1}$, cioè appunto $r = i + k(n-1)$ con $k \geqslant 0$, poichè $1 \leqslant i \leqslant n-1$. Infine, se $1 \leqslant j < t \leqslant n-1$, poichè (per le (12)) $(S_n)^j \cap (S_n)^t \subseteq (G_n)^j \cap (G_n)^t = \varnothing$ (v. (4)), $(S_n)^j$ ed $(S_n)^t$ sono appunto disgiunte.

II) *Ciascuno dei sottinsiemi del semigruppo S*:

$$S_n, (S_n)^2, \ldots, (S_n)^{n-2}, (S_n)^{n-1}$$

che figurano nella (11), *è un sotto-n-semigruppo* (n. 1) *di S, e fra questi sottinsiemi l'unico che sia un sotto-semigruppo di S è $(S_n)^{n-1}$.*

Infatti, se $1 \leqslant i \leqslant n-1$, da $in = i + i(n-1)$ segue, per la *I*), $((S_n)^i)^n = (S_n)^{in} \subseteq (S_n)^i$, cioè appunto $(S_n)^i$ è un sotto-n-semigruppo di S. Se poi, per un certo i $(1 \leqslant i \leqslant n-1)$, $(S_n)^i$ è un sotto-semigruppo di S, allora $(S_n)^{2i} = ((S_n)^i)^2 \subseteq (S_n)^i$, donde, per la I), $2i = i + k(n-1)$, da cui $k = 1$ e quindi appunto $i = n-1$; viceversa, se $i = n-1$, $(S_n)^i$ è appunto un sotto-semigruppo di S (sempre per la I)).

7. – Se A è un qualsiasi sottinsieme di un gruppo G, denoteteremo con

$$[A]$$

il sottogruppo di G generato da A.

Nelle ipotesi della I) (n. 6), consideriamo il sottogruppo $[S_n]$ di $C(G_n)$ generato da (gli elementi di) S_n. Evidentemente

$$[S_n] = [S] \,. \tag{13}$$

Consideriamo inoltre il sottogruppo $[(S_n)^{n-1}]$ di $C(G_n)$ generato da $(S_n)^{n-1}$, e dimostriamo che

(14 $\qquad [S_n] \cap (G_n)^{n-1} = [(S_n)^{n-1}] \,.$

Infatti, osserviamo intanto che dalle (4), (11) e (12) segue evidentemente

$$(S_n)^i = S \cap (G_n)^i \qquad (i = 1, 2, ..., n-1), \tag{15}$$

di modo che, per $i = n - 1$, abbiamo ([7], p.22): $[(S_n)^{n-1}] = = [S \cap (G_n)^{n-1}] \subseteq [S] \cap [(G_n)^{n-1}] = [S_n] \cap (G_n)^{n-1}$ (per la (13) e poichè $(G_n)^{n-1}$ è un sottogruppo di $C(G_n)$); quindi resta da dimostrare che

$$[S_n] \cap (G_n)^{n-1} \subseteq [(S_n)^{n-1}] \,. \tag{16}$$

E invero, se $x \in [S_n] \cap (G_n)^{n-1}$, allora $x \in [S_n]$, quindi x è un prodotto finito del tipo ($a_{ij} \in S_n$):

$$x = a_{11} \ldots a_{1r_1}(a_{21})^{-1} \ldots (a_{2r_2})^{-1} a_{31} \ldots a_{3r_3} \ldots (a_{h1})^{-1} \ldots (a_{hr_h})^{-1} \,, \tag{17}$$

(si può sempre infatti supporre, previa eventuale moltiplicazione di x a sinistra o a destra per $aa^{-1} = 1$, con $a \in S_n$, che il primo fattore di x sia un elemento di S_n, e che l'ultimo sia l'inverso di un elemento di S_n). Poichè, ad es., $(a_{21})^{-1} \ldots (a_{2r_2})^{-1} = = (a_{2r_2} \ldots a_{21})^{-1}$, è lecito supporre (per la I)) che nella (17) ciascuno dei numeri naturali $r_1, r_2, ..., r_h$ sia $\leqslant n - 1$. Eseguiamo ora sul 2° membro della (17) le seguenti operazioni: Se $r_1 = n - 1$, passiamo oltre; altrimenti, se $r_1 < n - 1$, inseriamo tra i due fattori a_{1r_1} ed $(a_{21})^{-1}$ il prodotto $a^{n-1-r_1}(a^{-1})^{n-1-r_1} = 1$ $(a \in S_n)$. Ciò fatto, consideriamo il prodotto $(a^{-1})^{n-1-r_1}(a_{21})^{-1} ... (a_{2r_2})^{-1}$; riduciamone eventualmente (in base alla I)) il numero $n - 1 - r_1 + r_2$ dei fattori ad un numero $t_2 \leqslant n - 1$; se $t_2 = n - 1$, passiamo oltre; altrimenti, se $t_2 < n - 1$, inseriamo fra l'ultimo di questi t_2 fattori ed a_{31} il prodotto $(a^{-1})^{n-1-t_2}a^{n-1-t_2} = 1$. Ciò fatto, consideriamo il prodotto $a^{n-1-t_2}a_{31} ... a_{3r_3}$, e in relazione ad esso ripetiamo un passo del tutto analogo al precedente. E così continuiamo. Arriviamo così a scrivere x sotto la forma $(b_{i,j} \in S_n)$:

$$(18) \quad x = b_{1,1} ... b_{1,n-1}(b_{2,1})^{-1} ... (b_{2,n-1})^{-1} ... b_{h-1,1} ... b_{h-1,n-1}(b_{h,1})^{-1} ... (b_{h,t_h})^{-1}$$

con t_h naturale $\leqslant n - 1$. Facciamo vedere che:

$$(18') \qquad t_h = n - 1 .$$

Invero, applicando ad ambo i membri della (18) l'omomorfismo canonico $C(G_n) \to C(G_n)/(G_n)^{n-1}$, ricordando che $x \in (G_n)^{n-1}$ e che $S_n \subseteq G_n$, si trova (osservando che $(b_{2,1})^{-1} ... (b_{2,n-1})^{-1} = (b_{2,n-1} ... b_{2,1})^{-1} \in (G_n)^{n-1}$):

$$(G_n)^{n-1} = (G_n)^{(n-1)(h-1)}(G_n)^{-t_h}$$

da cui $t_h \equiv 0 \pmod{n-1}$, donde appunto la (18') (poichè $1 \leqslant t_h \leqslant n - 1$). Dalle (18), (18') risulta che x è un prodotto finito di elementi di $(S_n)^{n-1}$ e di inversi di elementi di $(S_n)^{n-1}$, quindi che $x \in [(S_n)^{n-1}]$. La (16) è perciò dimostrata. In conclusione:

III) *Nelle ipotesi della I)* (n. 6), *i sottogruppi* $[S_n]$ *e* $[(S_n)^{n-1}]$ *di* $C(G_n)$, *rispettivamente generati da* S_n *e* $(S_n)^{n-1}$ *sono legati dalla relazione* (14). *Inoltre vale la* (13).

8. – Sempre nelle ipotesi della I) (n. 6), osserviamo ora che il gruppo $C(G_n)$ è il prodotto dei suoi sottogruppi $[S_n]$ ed $A(G_n) =$

$= (G_n)^{n-1}$ (n. 2):

$$C(G_n) = [S_n]A(G_n) = A(G_n)[S_n] \,. \tag{19}$$

Infatti, se $s \in S_n$, la decomposizione (4) di $C(G_n)$ nei laterali (destri e sinistri) di $A(G_n)$ si può scrivere, per le (12), (cfr. [5], p. 220):

$$C(G_n) = \bigcup_{i=1}^{n-1} s^i A(G_n) = \bigcup_{i-1}^{n=1} A(G_n)s^i \,, \tag{20}$$

donde appunto la (19), poichè $s^i \in [S_n]$.

Applicando allora uno dei teoremi sull'isomorfismo tra gruppi-si può concludere (v. (14)) che $[(S_n)^{n-1}]$ è un sottogruppo normale di $[S_n,]$ e (v. (4), e cfr. [4], pp. 257-258) che la corrispondenza

$$(G_n)^i \rightarrow (G_n)^i \cap [S_n] \qquad (i = 1, 2, \dots n-1) \tag{21}$$

è un isomorfismo (di $[S_n]A(G_n)/A(G_n)$ su $[S_n]/([S_n] \cap A(G_n))$, cioè — per le (19) e (14) —) del gruppo $C(G_n)/A(G_n)$ sul gruppo $[S_n]/[(S_n)^{n-1}]$.

In particolare, per $i = 1$, la (21) dà: $G_n \rightarrow G_n \cap [S_n]$, donde (poichè la (21) è un isomorfismo): $(G_n)^i \rightarrow (G_n \cap [S_n])^i$ $(i = 1, \dots, n-1)$, da cui (per l'univocità della (21)):

$$(G_n)^i \cap [S_n] = (G_n \cap [S_n])^i \quad (i = 1, 2, \dots, n-1). \tag{22}$$

Quindi, in particolare ((22), per $i = n-1$, e (14)):

$$[(S_n)^{n-1}] = (G_n \cap [S_n])^{n-1} \,. \tag{23}$$

Dunque, posto

$$\overline{G_n} = G_n \cap [\, S_n] \quad , \tag{24}$$

la decomposizione del gruppo $[S_n]$ nei laterali del suo sotto, gruppo normale $[(S_n)^{n-1}] = (G_n)^{n-1}$ si può scrivere (v. (21), (22) e 24)):

$$[S_n] = \overline{G}_n \cup (\overline{G}_n)^2 \cup \dots \cup (\overline{G}_n)^{n-2} \cup (\overline{G}_n)^{n-1} . \tag{25}$$

Quindi (cfr. [6], Satz 2) $\overline{G}_n$ è un sotto-n-gruppo di $[S_n]$, e (n. 2) il gruppo $[S_n]$ è circoscritto all'n-gruppo $\overline{G}_n$, al quale risulta associato il gruppo $[(S_n)^{n-1}]$:

$$[S_n] = C(\overline{G}_n) , \quad [(S_n)^{n-1}] = A(\overline{G}_n) . \tag{26}$$

Che $\overline{G}_n$ sia un sotto-n-gruppo di $[S_n]$ (oltre che di G_n e di $C(G_n)$), risulta pure dalla (24). Infatti l'intersezione di sotto-n-gruppi di un n- gruppo, quando non sia vuota (cfr. [5], p. 222) è evidentemente un sotto-n-gruppo di quel n-gruppo. Concludendo:

IV) *Nelle ipotesi della I)* (n. 6), *per il sotto-n-gruppo* $\overline{G}_n$ *di* $C(G_n)$, *definito dalla* (24), *valgono le* (26), (*cfr.* III)).

9. – Se A è un qualsiasi sottinsieme non vuoto di un n-gruppo G_n, denotermo con

$$[A]_n$$

il sotto-n-gruppo di G_n *generato* da A, cioè l'intersezione di tutti i sotto-n-gruppi di G_n che contengono A. Evidentemente $[A]_n$ è caratterizzato dall'essere un sotto-n-gruppo di G_n che contiene A e che è contenuto in ogni sotto-n-gruppo di G_n contenente A.

V) *Nelle ipotesi della I)* (n. 6), $\overline{G}_n$ (v. (24), cfr. III)) *è il sotto-n-gruppo di* G_n *generato da* (gli elementi di) S_n:

$$\overline{G}_n = [S_n]_n .$$

Infatti, poichè $\overline{G}_n$ è un sotto-n-gruppo di G_n contenente S_n, è sufficiente dimostrare che, se un sotto-n-gruppo H_n di G_n contiene S_n:

$$S_n \subseteq H_n \subseteq G_n \,, \tag{27}$$

di conseguenza H_n contiene $\overline{G}_n$.

E invero, denotiamo con H il sotto-semigruppo del gruppo $C(G_n)$ costituito dagli elementi di $C(G_n)$ che sono prodotti finiti di elementi di H_n. Poichè H_n è un sotto-n-gruppo di $C(G_n)$, l'inverso (nel gruppo $C(G_n)$) del prodotto di $n-2$ elementi di H_n appartiene ad H_n (n. 3, iii)). Quindi ciascuna delle due equazioni $ax = b$, $ya = b$, con $a, b \in H$, è risolubile in H (poichè esse sono equivalenti risp. ad equazioni $a'x = b'$, $ya'' = b''$, ottenute moltiplicandole per un opportuno elemento di H, con $a', b', a'', b'' \in H$ ed a', a'' prodotti di elementi di H_n in numero eguale ad un multiplo di $n-2$). Dunque H è un sotto-gruppo di $C(G_n)$, ed è chiaro che $H = [H_n]$. Quindi (I), n. 6):

$$[H_n] = H_n \cup (H_n)^2 \cup \ldots \cup (H_n)^{n-2} \cup (H_n)^{n-1} \,,$$

da cui (poichè $H_n \subseteq G_n$ e per la (4)):

$$H_n = G_n \cap [H_n] \,, \tag{28}$$

(ed inoltre, evidentemente — cfr. n. 8 —, $[H_n] = C(H_n)$, $(H_n)^{n-1} = A(H_n)$). Allora, poichè dalla (27) segue $[S_n] \subseteq [H_n]$, e quindi $G_n \cap [S_n] \subseteq G_n \cap [H_n]$, risulta appunto ((24) e (28)) $\overline{G}_n \subseteq H_n$. E la V) è dimostrata.

10. – In base ai risultati I), ..., V) di questo § 2, possiamo dunque affermare che vale il seguente

Teorema 2: *Supponiamo che un n-semigruppo S_n* (moltiplicativo e non necessariamente commutativo), *con $n > 2$, sia «immerso» in un n-gruppo G_n:*

$$S_n \subseteq G_n$$

(cioè che S_n sia un sotto-n-semigruppo di G_n), *e denotiamo con*

$\overline{G}_n$ *il sotto-n-gruppo di* G_n *generato da* S_n (n. 9):

$$S_n \subseteq \overline{G}_n = [S_n]_n \subseteq G_n \,.$$

Se pensiamo (com'è sempre lecito: n. 2) *l'n-gruppo* G_n *immerso, a sua volta, in un gruppo,* $C(G_n)$, *ad esso circoscritto*:

$$G_n \subseteq C(G_n) \,,$$

e denotiamo con S *il sotto-semigruppo del gruppo* $C(G_n)$ *generato da* S_n, *allora il sottogruppo* $[S_n] = [S]$ *di* $C(G)_n$, *generato sia da* S_n *che da* S, *è circoscritto all'n-gruppo* $\overline{G}_n$:

$$[S_n] = [S] = C(\overline{G}_n) \,, \tag{29}$$

di modo che (n. 2) *il gruppo* $C(G_n)$ *ed il suo sottogruppo* $C(\overline{G}_n)$ *ammettono rispettivamente le seguenti decomposizioni nei laterali dei loro rispettivi sottogruppi normali* $A(G_n) = (G_n)^{n-1}$ *ed* $A(\overline{G}_n) = (\overline{G}_n)^{n-1}$:

$$C(G_n) = G_n \cup (G_n)^2 \cup \ldots \cup (G_n)^{n-2} \cup (G_n)^{n-1} \,, \tag{30}$$

$$C(\overline{G}_n) = \overline{G}_n \cup (\overline{G}_n)^2 \cup \ldots \cup (\overline{G}_n)^{n-2} \cup (\overline{G}_n)^{n-1} \,. \tag{31}$$

D'altra parte ,il semigruppo S *ammette la seguente decomposizione in classi a due a due disgiunte*:

$$S = S_n \cup (S_n)^2 \cup .. \cup (S_n)^{n-2} \cup (S_n)^{n-1} \,, \tag{32}$$

l'ultima delle quali, $(S_n)^{n-1}$, *è un sotto-semigruppo del gruppo* $(\overline{G}_n)^{n-1} = A(\overline{G}_n)$. *Inoltre questo gruppo è generato dal semigruppo* $(S_n)^{n-1}$:

$$A(\overline{G}_n) = (\overline{G}_n)^{n-1} = [(S_n)^{n-1}] \,, \tag{33}$$

cosicchè, nel gruppo $C(\overline{G}_n)$, *risulta*

$$\overline{G}_n = [S_n]_n = s[(S_n)^{n-1}] = [(S_n)^{n-1}]s \,, \tag{34}$$

s *denotando un qualsiasi elemento dell'n-semigruppo* S_n.

Quest'ultima affermazione (34) si verifica immediatamente (cfr. (20), n. 8).

§ 3

11. – Diremo che un n-semigruppo S_n (non necessariamente commutativo) *è cancellativo*, se valgono le due seguenti implicazioni:

$$a_1b_2 \dots b_n = c_1b_2 \dots b_n \Rightarrow a_1 = c_1 \,, \tag{35}$$

$$d_1 \dots d_{n-1}a_n = d_1 \dots d_{n-1}c_n \Rightarrow a_n = c_n \,, \tag{35'}$$

qualunque siano $a_h, b_i, c_j, d_k \in S_n$.

Le (35), (35') sono evidentemente condizioni necessarie per l'immergibilità di S_n in un n-gruppo. Basta infatti pensare che, se S_n è immerso in un n-gruppo, esso è pure immerso in un gruppo (n. 2, teor. del laterale).

Diremo che un n-gruppo $\overline{G}_n$, con $n > 2$, è un *n-gruppo dei quozienti* di un n-semigruppo commutativo S_n, e scriveremo

$$\overline{G}_n = Q(S_n) \,,$$

se S_n è un sotto-n-semigruppo di $\overline{G}_n$, e se ogni elemento x di $\overline{G}_n$ è rappresentabile nella forma (n. 3):

$$x = a_1(a_{2,1} \dots a_{2,n-2})^{-1} \dots (a_{n,1} \dots a_{n,n-2})^{-1} \,, \tag{36}$$

con $a_1, a_{r,s} \in S_n$.

VI) *Un n-gruppo $\overline{G}_n$, con $n > 2$, è generato* (n. 9) *da un suo sotto-n-semigruppo commutativo S_n se, e soltanto se, $\overline{G}_n$ è un n-gruppo dei quozienti di S_n.*

Infatti, se $\overline{G}_n = Q(S_n)$, poichè ogni sotto-n-gruppo di $\overline{G}_n$ che contenga S_n deve pure contenere tutti i prodotti (36), risulta appunto (n. 9) $\overline{G}_n = [S_n]_n$.

Viceversa, se $\overline{G}_n = [S_n]_n$, applichiamo il teor. 2 (n. 10). Poichè S_n è, per ipotesi, commutativo, tale è pure il sotto-semigruppo S del gruppo $C(\overline{G}_n)$ generato da S_n: e invero, se $a_1 \dots$

$a_r, b_1 \dots b_s \in S$ $(a_i, b_j \in S_n)$, poniamo

$$u = a_1 \dots a_r b_1 \dots b_s \,, \qquad v = b_1 \dots b_s a_1 \dots a_r,$$

e diciamo t un intero non negativo tale che $r + s + t \equiv 1$ (mod $n - 1$); allora, se $c \in S_n$, i prodotti uc^t, vc^t appartengono ad S_n (I), n. 6) e risulta $uc^t = vc^t$ per la proprietà commutativa generalizzata (n. 1), donde appunto, semplificando, $u = v$. Poichè il semigruppo S è commutativo, tale è pure il gruppo $[S] = C(\overline{G}_n)$ da esso generato: e invero $[S]$ coincide col ben noto gruppo dei quozienti del semigruppo commutativo S. Quindi anche $[(S_n)^{n-1}]$ è il gruppo dei quozienti del semigruppo commutativo $(S_n)^{n-1}$, e perciò dalla (34) risulta che ogni elemento x di $\overline{G}_n$ è rappresentabile (nel gruppo $C(\overline{G}_n)$) nella forma

$$x = s(a_1 \dots a_{n-1})(b_1 \dots b_{n-1})^{-1} \qquad (s, a_i, b_i \in S_n)\,. \tag{37}$$

Moltiplicando allora, se $n > 3$, il 2° membro della (37) per $c^{(n-1)(n-3)}(c^{-1})^{(n-1)(n-3)} = 1$, con $c \in S_n$, è chiaro che si ottiene per x un'espressione del tipo (36) (si ricordi l'osservazione alla fine del n. 3). Dunque risulta appunto $\overline{G}_n = Q(S_n)$. E la VI) è dimostrata.

Nel corso di questa dimostrazione si è pure riconosciuto che:

VII) *Un n-gruppo dei quozienti di un n-semigruppo commutativo* (se esiste) *è un n-gruppo commutativo* (al pari del gruppo ad esso circoscritto).

La seconda parte della dimostrazione della VI), sopra esposta, è quella che ha permesso di riconoscere che $[S_n]_n$ è l'insieme delle espressioni (36). Ora che questo fatto è noto, è però possibile anche una dimostrazione diretta della VI) (che non faccia, cioè, ricorso al teor. 2): È facile infatti verificare che, se S_n è immerso in un n-gruppo, in questo gli elementi (36) costituiscono un sotto-n-gruppo commutativo contente S_n.

VIII) *n-gruppi dei quozienti di n-semigruppi commutativi isomorfi* (se esistono) *sono pure isomorfi.*

Infatti, supponiamo che S_n ed S'_n siano due n-semigruppi commutativi, e che esista un isomorfismo $\varphi : a \to a\varphi$ di S_n su S'_n. È allora facile verificare (pensando S_n e S'_n immersi risp. nei gruppi commutativi — v. VIII) — $C(\overline{G}_n)$ e $C(\overline{G}'_n)$, e ricordando l'osservazione finale del n. 3) che la corrispondenza che associa all'elemento (36) di $\overline{G}_n = Q(S_n)$ l'elemento

$$(36') \qquad (a_1\varphi)((a_{2,1}\varphi) \dots (a_{2,n-2}\varphi))^{-1} \dots ((a_{n,1}\varphi) \dots (a_{n,n-2}\varphi))^{-1}$$

di $\overline{G}'_n = Q(S'_n)$ è appunto un isomorfismo dell'n-gruppo $Q(S_n)$ sull'n-gruppo $Q(S'_n)$ (subordinate φ sopra S_n).

12. – Osserviamo ora che:

IX) *Se un n-gruppo* $\overline{G}_n$, *con* $n > 2$, *è generato da un suo sotto-n-semigruppo commutativo* S_n:

$$\overline{G}_n = [S_n]_n ,$$

allora $\overline{G}_n$ *è l'insieme degli elementi* x *del gruppo* (commutativo) $C(\overline{G}_n)$, *circoscritto a* $\overline{G}_n$, *che sono* (in questo gruppo) *rappresentabili nella forma*

$$(38) \qquad x = a_1(a_2 \dots a_n)^{-1} \qquad (a_i \in S_n) .$$

Infatti $x \in \overline{G}_n = [S_n]_n$ implica appunto (v. (37)) che x è rappresentabile nella forma (38). Viceversa, se x è dato dalla (38), allora appunto $x \in a_1[(S_n)^{n-1}] = [S_n]_n = \overline{G}_n$ (teor. 2, (34)). Che $C(\overline{G}_n)$ (e quindi $\overline{G}_n$) sia commutativo, risulta poi dalle VI) e VII).

Nei successivi n. 13 e 14 dimostreremo che (anche per $n > 2$):

X) *Un n-semigruppo commutativo* S_n *è «immergibile» in un n-gruppo* (cioè è isomorfo ad un sotto-n-semigruppo di un n-gruppo) *se, e soltanto se,* S_n *è cancellativo* (n. 11).

Osserviamo subito che, dimostrata la X), resterà pure dimostrato il seguente

Teorema 3: *Affinchè esista un n-gruppo dei quozienti,* $Q(S_n)$, *di un n-semigruppo* (moltiplicativo) *commutativo* S_n (n. 11), *con* $n > 2$, *è necessario e sufficiente che* S_n *sia cancellativo* (n. 11).

$Q(S_n)$, quando esiste, è un n-gruppo commutativo, generato da S_n (n. 9), *e univocamente determinato da S_n a meno di isomorfismi.*

Infatti, questo teor. 3 è una evidente conseguenza delle proposizioni VI), VII), VIII) e X).

13. – Per quanto riguarda la X), essa è ben nota per $n = 2$. Per $n > 2$, la necessità delle condizioni (35), (35′) è stata già rilevata nel 2° capoverso del n. 11.

Rimane dunque soltanto da dimostrare che un n-semigruppo commutativo e cancellativo S_n, con $n > 2$, è immergibile in un n-gruppo.

A questo scopo, fissiamo l'attenzione sulla proposizione IX) del n. 12, che suggerisce (v. la (38)) uno dei possibili mezzi per realizzare l'immersione desiderata (un'altro si vedrà nel n. 15).

Consideriamo l'insieme, N, delle n-uple (ordinate) di elementi di S_n, che denoteremo anche abbreviatamente con (a_i):

$$(a_i) = (a_1, a_2, \ldots, a_n) \in N \qquad\qquad (a_i \in S_n) ,$$

e definiamo in N una relazione binaria ϱ, ponendo

$$(a_1, a_2, \ldots, a_n)\varrho(b_1, b_2, \ldots, b_n) \tag{39}$$

se, e solo se, nell'n-semigruppo S_n (quest'ultima, ovvia, precisazione sarà sottintesa nel seguito):

$$a_1 b_2 \ldots b_n = b_1 a_2 \ldots a_n . \tag{39'}$$

La relazione ϱ, evidentemente riflessiva e simmetrica, è anche transitiva: Infatti, se $(a_i)\varrho(b_i)$ e $(b_i)\varrho(c_i)$, assieme alla (39′) vale pure la

$$b_1 c_2 \ldots c_n = c_1 b_2 \ldots b_n . \tag{40}$$

Moltiplicando allora (n. 1) membro a membro le (39′), (40) e le $n - 2$ eguaglianze $u_1 = u_1, \ldots, u_{n-2} = u_{n-2}$ $(u_i \in S_n)$, e poi cancellando (n. 11), in ambo i membri dell'eguaglianza ottenuta, gli $n-1$ fattori $u_1, \dots, u_{n-2}, b_1 b_2 \dots b_n$, si ottiene

$$a_1 c_2 \dots c_n = c_1 a_2 \dots a_n ,$$

cioè appunto $(a_i)\varrho(c_i)$.

Denotiamo allora con $\overline{G}_n$ l'insieme quoziente di N per la relazione di equivalenza ϱ, i cui elementi sono le classi di equivalenza modulo ϱ:

$$[a_i] = [a_1, a_2, \dots, a_n] \in \overline{G}_n = N/\varrho ,$$

il simbolo $[a_i]$ (che non sarà possibile confondere con quello definito all'inizio del n. 7) denotando la classe contenente l'n-upla (a_i).

Definiamo in $\overline{G}_n$ una moltiplicazione n-aria, ponendo:

$$[a_{1i}] \dots [a_{ni}] = [a_{1i} \dots a_{ni}] \tag{41}$$

(cioè moltiplicando fra di loro gli elementi che occupano lo stesso posto). Questa moltiplicazione n-aria è univoca, infatti da $(a_{1i})\varrho(a'_{1i}), \dots, (a_{ni})\varrho(a'_{ni})$ segue appunto direttamente (moltiplicando membro a membro le relative eguaglianze (39')): $(a_{1i} \dots a_{ni})\varrho(a'_{1i} \dots a'_{ni})$, e inoltre è evidentemente associativa e commutativa (n. 1), in conseguenza dell'associatività e commutatività della moltiplicazione n-aria di S_n. Dunque $\overline{G}_n$ (rispetto alla (41)) è un n-semigruppo commutativo.

14. – Poichè $\overline{G}_n$ è commutativo, per dimostrare ora che $\overline{G}_n$ è un n-gruppo, è sufficiente verificare (n. 2, 2° capov.) che è risolubile in $\overline{G}_n$ l'equazione ((3) per $i = 1$, ossia):

$$x_1[a_{21}, a_{22}, \dots, a_{2n}] \dots [a_{n1}, a_{n2}, \dots, a_{nn}] = [b_1, b_2, \dots, b_n] . \tag{42}$$

Infatti l'equazione (42) ammette in $\overline{G}_n$ la soluzione

$$x_1 = [a_{11}, a_{12}, \dots, a_{1n}] , \tag{43}$$

dove:

(43′) $$a_{11} = b_1 a_{22} \dots a_{2n} a_{32} \dots a_{3n} \dots a_{n2} \dots a_{nn} ,$$

$$a_{12} = b_2 a_{21} a_{31} \dots a_{n1} , \quad a_{13} = b_3, \dots, a_{1n} = b_n ,$$

(cfr. (2), n. 1), e ciò si riconosce facilmente con una verifica diretta ((41), (39): nella relativa (39′) si trovano nei due membri gli stessi $1 + (n+1)(n-1)$ fattori). Dunque $\overline{G}_n$ (rispetto alla (41)) è un n-gruppo (commutativo).

Fissato un qualsiasi elemento, a, di S_n, se b_i, c_i sono elementi qualsiasi di S_n, risulta evidentemente

(44) $$(ab_2 \dots b_n, b_2, \dots, b_n)\varrho(ac_2 \dots c_n, c_2, \dots, c_n) .$$

Viceversa, da

$$(ab_2 \dots b_n, b_2, \dots, b_n)\varrho(c_1, c_2, \dots, c_n)$$

segue, cancellando (n. 11) in ambo i membri della relativa eguaglianza (39′) gli $n-1$ fattori $b_2, \dots, b_n$:

$$c_1 = ac_2 \dots c_n .$$

L'elemento a di S_n individua dunque una classe modulo ϱ:

(45) $$a \xrightarrow{\omega} [ab_2 \dots b_n, b_2, \dots, b_n] = a\omega ,$$

cioè un elemento di $\overline{G}_n = N/\varrho$, costituita dalle n-uple del tipo (44) e da queste soltanto.

L'applicazione ω di S_n in $\overline{G}_n$, data dalla (45), è iniettiva. Infatti da $a\omega = a'\omega$, ossia da

$$(ab_2 \dots b_n, b_2, \dots, b_n)\varrho(a'b_2 \dots b_n, b_2, \dots, b_n) ,$$

segue appunto (cancellando — n. 11 — in ambo i membri della relativa (39′) gli $n-1$ fattori $b_2 \dots b_n b_2, b_3, \dots, b_n$): $a = a'$. Inoltre ω è un isomorfismo (di S_n in $\overline{G}_n$). Infatti, se $a_1, \dots, a_n \in S_n$, si ha appunto:

$$(a_1 \dots a_n)\omega = (a_1\omega) \dots (a_n\omega) ,$$

ossia, come si verifica direttamente, in base alle (41) e (39):

$$[a_1 \dots a_n b_2 \dots b_n, b_2, \dots, b_n] = [a_1 b_2 \dots b_n, b_2, \dots, b_n] \dots$$
$$\dots [a_n b_2 \dots b_n, b_2, \dots, b_n],$$

(nella relativa (39′) si trovano nei due membri gli stessi $1 + (n+2)(n-1)$ fattori).

Diciamo $\overline{S}_n$ l'immagine di S_n mediante l'isomorfismo ω di S_n in $\overline{G}_n$:

$$\overline{S}_n = S_n \omega \subseteq \overline{G}_n .$$

Se $\overline{a}_1, \dots, \overline{a}_n \in \overline{S}_n$, allora $\overline{a}_i = a_i \omega$, con $a_i \in S_n$ $(i = 1, \dots, n)$, quindi (moltiplicando le $\overline{a}_i$ in $\overline{G}_n$): $\overline{a}_1 \dots \overline{a}_n = (a_1 \dots a_n)\omega$, donde $\overline{a}_1 \dots \overline{a}_n \in \overline{S}_n$. Perciò $\overline{S}_n$ è un sotto-n-semigruppo dell'n-gruppo $\overline{G}_n$, e il dato n-semigruppo S_n è isomorfo ad $\overline{S}_n$. Dunque S_n è appunto immergibile in un n-gruppo. La X) (n. 12) è quindi completamente dimostrata, e con essa è dimostrato il teor. 3.

Nel corso di questa dimostrazione (n. 13-14) abbiamo visto che:

XI) *Se S_n, con $n > 2$, è un n-semigruppo commutativo e cancellativo* (n. 11), *la relazione binaria ϱ, definita mediante le* (39), (39′) nell'insieme N delle n-uple ordinate di elementi di S_n, *è una relazione di equivalenza, e il relativo insieme quoziente $\overline{G}_n = N/\varrho$ è un n-gruppo commutativo rispetto alla moltiplicazione n-aria in esso definita mediante la* (41). *Inoltre, la corrispondenza* (45) *è un isomorfismo dell'n-semigruppo S_n su un sotto-n-semigruppo $\overline{S}_n$ di $\overline{G}_n$.*

Si osservi che questa proposizione XI) è vera anche per $n = 2$, nel qual caso essa coincide col classico teorema di immersione di un semigruppo commutativo e cancellativo nel proprio gruppo dei quozienti. Altrettanto non si può dire invece per la successiva proposizione XII). Ciò risulta in accordo con le osservazioni finali del n. 4.

15. – L'immersione di un n-semigruppo commutativo e cancellativo S_n, con $n > 2$, in un n-gruppo si può anche realizzare

con un'altra costruzione, concettualmente simile alla precedente (v. XI)).

Questa seconda costruzione, come ora vedremo, è però più espressiva della precedente nei riguardi della nozione di n-gruppo dei quozienti di S_n (n. 11).

Poichè le due costruzioni sono analoghe ,e poichè l'esposizione dettagliata della seconda sarebbe formalmente meno agevole di quanto sia stata quella della prima, sorvoleremo sui (facili) particolari dimostrativi.

Punto di partenza di questa seconda costruzione (ispirata alla VI) — v. (36) — invece che alla IX)) è l'insieme, E, delle $(1 + (n-2)(n-1))$-uple (ordinate) di elementi di S_n, che si possono anche denotare abbreviatamente con (a_1, a_{rs}):

$$(a_1, a_{rs}) = (a_1, a_{2,1}, \ldots, a_{2,n-2}, \ldots, a_{n,1}, \ldots, a_{n,n-2}) \in E \ ,$$

$(a_1, a_{r,s} \in S_n)$. La relazione binaria β, definita in E ponendo

$$(46) \qquad (a_1, a_{rs})\beta(b_1, b_{rs})$$

se e solo se (in S_n):

$$(46') \quad a_1 b_{2,1} \ldots b_{2,n-2} \ldots b_{n,1} \ldots b_{n,n-2} = b_1 a_{2,1} \ldots a_{2,n-2} \ldots a_{n,1} \ldots a_{n,n-2} \ ,$$

è una relazione di equivalenza. Consideriamo l'insieme quoziente E/β, che denoteremo con $\overline{G}_n$, cioè l'insieme delle classi $[a_1, a_{rs}]$ modulo β:

$$[a_1, a_{rs}] \in \overline{G}_n = E/\beta \ ,$$

($[a_1, a_{rs}]$ è la classe contenente (a_1, a_{rs})). In G_n la posizione:

$$(47) \qquad [a_{11}, a_{1rs}] \ldots [a_{n1}, a_{nrs}] = [a_{11} \ldots a_{n1}, a_{1rs} \ldots a_{nrs}]$$

(si moltiplicano fra di loro, in S_n, gli elementi che occupano lo stesso posto) definisce una moltiplicazione n-aria, rispetto alla quale $\overline{G}_n$ è un n-gruppo commutativo. La corrispondenza (a, $b_{rs} \in S_n$):

$$(48) \qquad a \xrightarrow{\ v\ } [ab_{2,1} \ldots b_{2,n-2} \ldots b_{n,1} \ldots b_{n,n-2}, b_{rs}] = av$$

è un isomorfismo dell'n-semigruppo S_n su un sotto-n-semigruppo $\overline{S}_n = S_n\nu$ dell'n-gruppo $\overline{G}_n$.

Avendo sempre in mente la (36) (n. 11), è facile trovare, in funzione dei dati (cfr. (43), (43')), la soluzione $x_1 = \xi_1 \in \overline{G}_n$ dell'equazione $x_1\xi_2 \ldots \xi_{n-1}\xi_n = \xi_{n+1}$ $(\xi_i \in \overline{G}_n)$. Se $\xi_{n-1} = \xi_n = \xi_{n+1}$, questa soluzione coincide con l'inverso $(\xi_2 \ldots \xi_{n-1})^{-1}$ della $(n-2)$-upla $(\xi_2, \ldots, \xi_{n-1})$, (n. 3). Si vede allora che, per ogni elemento $[a_1, a_{rs}]$ di $\overline{G}_n = E/\beta$, vale l'eguaglianza:

$$[a_1, a_{rs}] = (a_1\nu)((a_{2,1}\nu) \ldots (a_{2,n-2}\nu))^{-1} \ldots ((a_{n,1}\nu) \ldots (a_{n,n-2}\nu))^{-1} . \tag{49}$$

Identificando S_n con la sua immaginazione isomorfa $S_n\nu \subseteq \overline{G}_n$, possiamo dunque dire (n. 11) che $\overline{G}_n = E/\beta$ è (nel modo più naturale) l'n-gruppo dei quozienti del dato n-semigruppo S_n. Riassumendo:

XII) *Se S_n, con $n > 2$, è un n-semigruppo commutativo e cancellativo* (n. 11), *la relazione binaria β, definita mediante le* (46), (46') *nell'insieme E delle* $(1 + (n-2)(n-1))$-uple *ordinate di elementi di S_n, è una relazione di equivalenza, e il relativo insieme quoziente $\overline{G}_n = E/\beta$ è un n-gruppo commutativo rispetto alla moltiplicazione n-aria in esso definita mediante la* (47). *Inoltre, la corrispondenza ν, definita dalla* (48), *è un isomorfismo dell'n-semigruppo S_n su un sotto-n-semigruppo $\overline{S}_n = S_n\nu$ di $\overline{G}_n$. Infine, $\overline{G}_n$ è un n-gruppo dei quozienti di questo n-semigruppo $S_n\nu$* (n. 11), *secondo la* (49).

BIBLIOGRAFIA

[1] Bourbaki, N.: *Algèbre Chap. I*, Hermann (1951).
[2] Bruck, R. H.: *A survey of binary systems*, Springer (1958).
[3] Dörnte, W.: *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeitschrift, vol. 29 (1929), pp. 1-19.
[4] Dubreil, P.; Dubreil-Jacotin, M. L.: *Leçon d'algèbre moderne*, Dunod (1961).
[5] Post. E. L.: *Polyadic groups*, Trans. Amer. Math. Soc., vol. 48 (1940), pp. 208-350.
[6] Tvermoes, H.: *Uber eine Verallgemeinerung des Gruppenbegriffs*, Math. Scandinavica, vol. 1 (1953), pp. 18-30.
[7] Zassenhaus, H. J.: *The theory of groups*, Chelsea (1958).