Parte II - Algebre

§3. Algebre con due operazioni.

Vogliamo ora esaminare alcuni problemi connessi con lo studio di una particolare struttura con due operazioni.

Sia S un insieme su cui sono definite due operazioni: l'operazione "$\times$" definisce su S una struttura di semigruppi (S_2) e l'operazione "$\cdot$" definisce su S una struttura di gruppo (S_1) (nel seguito invece di $a \cdot b$ scriveremo ab). Queste due operazioni sono collegate dalla seguente legge distributiva:

$$\begin{aligned} (a \times b)c &= (ac) \times (bc) \\ c(a \times b) &= (ca) \times (cb) \end{aligned} \qquad (13.1)$$

Supponiamo inoltre che S sia finito.

In queste ipotesi esiste in S_2 un elemento idempotente (le potenze di un fissato elemento non sono tutte distinte e tra esse si può quindi individuare un gruppo ciclico la cui unità è, evidentemente, idempotente); quindi esiste $a \in S_2$ $a \times a = a$ da cui, moltiplicando per a^{-1}, si ricava $1 \times 1 = 1$ e, ancora:

$$b \times b = b \,, \qquad \text{per ogni } b \in S_2.$$

Pertanto S_2 è un semigruppo idempotente.

Osserviamo che se S è infinito non possiamo dire nulla nella esi-

stenza di eventuali elementi idempotenti. Se però supponiamo che ne esiste almeno uno, la situazione è analoga a quella del caso finito.

Allora si può pensare di risolvere il problema: "Caratterizzare i semigruppi che non hanno elementi idempotenti".

Prima di procedere ad un esame più dettagliato di S osserviamo che, se avessimo posto:

$$(a \times b)c = (a^p c) \times (b^p c) \qquad (13.2)$$

al posto delle (13.1), contrariamente a quanto si può pensare, non avremmo avuto un caso più generale, ma un caso particolare di struttura con due operazioni. Infatti, sempre nel caso in cui S è finito, avremmo avuto $\bar{a}$ (con $\bar{a}$ idempotente di S_2):

$\bar{a} \times \bar{a} = \bar{a} \Rightarrow (1 \times 1)\,\bar{a} = \bar{a} \Rightarrow 1 \times 1 = 1$ e quindi, ancora,

$b \times b = b$ per ogni $b \in S_2$. Da ciò segue, per ogni $a \in S_2$:

$a = a \cdot 1 = (a \times a)\,1 = a^p \times a^p = a^p \Rightarrow a = a^p \Rightarrow a^{p-1} = 1$

Pertanto ogni elemento del gruppo ha ordine divisore di $p - 1$; invece di a^p, in (13.2), possiamo allora scrivere solo a; otteniamo quindi la (13.1) ma con una condizione in più.

Torniamo alla nostra struttura (supponendo sempre S finito).

Consideriamo gli elementi c tali che:

$$c \times 1 = c \qquad (13.3)$$

(elementi siffatti esistono perchè, fissato $a \in S$ e posto $b = a \times 1$,

si ha che $b \times 1 = b$). Vale :

$$c \times 1 = c \ , \quad c' \times 1 = c' \implies cc' = cc' \times 1 \tag{13.4}$$

Infatti:

$cc' \times c' = cc'$ (dalle ipotesi (13.4)

$cc' \times c' \times 1 = cc' \times 1$

$cc' \times c' = cc' \times 1$ (sfruttando la (13.4)

$(c \times 1)c' = cc' \times 1$

$cc' = cc' \times 1$

Si può ancora verificare che:

$$c \times 1 = c \implies c^{-1} \times 1 = c^{-1} \tag{13.5}$$

Sia $s \in S_1$. se c verifica la (13.3), anche $s^{-1} c\, s$ la verifica; analogamente per ogni coniugato di c in S_1. Allora $\langle c^{S_1} \rangle$ (sottogruppo generato da tutti i coniugati di c in S_1) è normale in S_1 e anche:

$$G_1 = \left\langle \langle c_1^{S_1} \rangle \ , \ \langle c_2^{S_1} \rangle \ , \ \ldots\ldots \right\rangle \triangleleft S_1 \ ,$$

dove i $c_i (i = 1, 2, \ldots\ldots)$ sono tutti gli elementi per cui vale (13.3).

Allo stesso modo, considerati gli elementi b per cui:

$$1 \times b = b \tag{13.6}$$

si può provare che:

$$G_2 = \left\langle \langle b_1^{S_1} \rangle \ , \ \langle b_2^{S_1} \rangle, \ \ldots\ldots \right\rangle \triangleleft S_1 \ ,$$

dove i $b_i (i = 1,2, ...)$ sono tutti gli elementi per cui vale (13.6).

Si ha: $G_1 \cap G_2 = 1$.

infatti da $c \times 1 = c$ segue $1 \times c = 1$ e, se deve essere anche $1 \times c = c$, si ottiene $c = 1$.

Segue che gli elementi di G_1 e G_2 permutano tra loro: $g_1 g_2 = g_2 g_1$.

Vogliamo provare che $S_1 = G_1 \otimes G_2$ (dove $\otimes$ indica il prodotto diretto di G_1 e G_2).

Dopo quanto visto prima, basterà provare che $S_1 = G_1 G_2$.

Sia $a \in S_1$; vale:

$$G_1 \ni a^{-1} \times 1 = (1 \times a)\, a^{-1} \quad e, \text{ posto } c = (1 \times a)a^{-1}, \text{ si ha:}$$

$$1 \times a = c \quad a \in G_1 a \quad \text{dove inoltre} \quad c\, a = 1 \times a \in G_2.$$

Allora $a \in c^{-1} G_2 \subseteq G_1 G_2$ come volevamo.

Si prova inoltre che $1 \times g_1 g_2 = g_2$ $(g_1 g_2 \times 1 = g_1)$.

Infatti:

$$g_1 g_2 (g_1^{-1}\ g_2^{-1} \times 1) = 1 \times g_1 g_2 \in G_2$$

$$g_1^{-1} g_2^{-1} \times 1 \in g_1^{-1}\ G_2$$

ma è anche $g_1^{-1} g_2^{-1} \times 1 \in G_1$ e, essendo $g_1^{-1}\ G_2 \cap G_1 = g_1^{-1}$,

segue:

$$g_1^{-1} g_2^{-1} \times 1 = g_1^{-1}$$

e anche : $g_1 g_2 \times 1 = g_1$. analogamente $1 \times g_1 g_2 = g_2$.

Si prova inoltre che: $g_1 g_2 \times g_1' g_2' = g_2' g_1$

Abbiamo così dimostrato il seguente

Teorema 13.1

L'algebra finita $S(X, \cdot)$ con la legge (13.1), ha la seguente struttura:

i) $S_1 = G_1 \otimes G_2$

ii) $g_1 g_2 \times g_1' g_2' = g_2' g_1$ $\quad (g_1, g_1' \in G_1, \quad g_2, g_2' \in G_2)$

14. Osservazioni.

Cosa si può dire della struttura di S quando S_1 è un semigruppo unione di gruppi? O nel caso speciale in cui S_1 è un gruppo con zero?

Questi problemi non hanno ancora soluzione, come non è ancora risolto il caso in cui S è infinito.

Se $S_1 = 0 \cup G$ (gruppo con zero) ed S finito, si può provare che G è abeliano, analogamente a quanto accade per un corpo finito? (cfr. Teorema di Wedderburn.)

Risolvere questo problema sarebbe utilissimo nello studio di questa

teoria.

Vediamo un altro problema; fissato p intero positivo, si può definire: $(a \times b)c = ac^p \times bc^p$. Se S_1 ha ordine k e se $a \times a = a$, allora: $a^{kp+1} \times a^{kp+1} = a^{k+1} = a$. Fissato p si ha allora che il gruppo non contiene alcun elemento di ordine p e quindi, ad esempio, se $p = 2$ ogni elemento ha ordine dispari.

Se accade che $1 \times 1 = a$ allora $a \in Z(S_1)$; se S_1 non ha centro si ha $a = 1$ e si può provare in tal caso che 1 è l'unico idempotente di S_2. La struttura di S_2 si può descrivere: $S_2 = G \cup S'$ dove S' non è semigruppo e non contiene semigruppi.

Su queste strutture non si conosce niente di più; si intuisce che esiste una connessione tra semigruppi e gruppi finiti ma ancora non si sa qual'è.

15. Struttura di sistemi.

Passiamo ora a considerare un altro tipo di struttura, scaturito dall'esigenza di descrivere certi fenomeni chimici.

Siano $a_1, a_2, \ldots\ldots, a_n$ dei simboli con i quali definiamo delle potenze formali: $a_1^{\alpha_1}, a_2^{\alpha_2}, \ldots\ldots a_n^{\alpha_n}$ con $\alpha_i \in \mathbb{R}$, $\alpha_i > 0$. Supponiamo che queste potenze siano permutabili e, considerati tutti i prodotti del tipo:

$$a_{i_1}^{\beta_1} a_{i_2}^{\beta_2} \ldots\ldots a_{i_r}^{\beta_r} \quad \text{con} \quad 1 \leq r \leq n \,, \tag{15.1}$$

supponiamo che ognuno di questi elementi sia esprimibile in un unico modo. Si ottiene così una struttura di semigruppo commutativo infinito.

Introduciamo un elemento unità $\mathcal{E}$ e definiamo F^+ l'insieme costituito dal semigruppo più $\mathcal{E}$. Con F^- indicheremo poi l'insieme degli elementi del tipo (15.1) ad esponente negativo (con $\mathcal{E}$ unità).

$F = F^+ \cup F^-$ è allora un gruppo abeliano (imponendo la legge commutativa)

Consideriamo ora, tra le coppie (a,b) di $F^+ \times F^+$, una operazione così definita:

$$(a,b) \odot (c,d) = \left(ac\,\varphi(a,b,c,d)\ ,\ bd\,\varphi(a,b,c,d)\right)$$

dove supponiamo che $ac\,\varphi(a,b,c,d) \in F^+$ è ancora:

$$\begin{aligned}
&i)\ \varphi(a,b,c,d) \in F \\
&ii)\ \varphi(aa',ba',c,d) = \alpha(a')\varphi(a,b,c,d)\ ,\ \varphi(a,b,cc',dc') = \beta(c')\varphi(a,b,c,d) \\
&iii)\ \varphi(a,b,c,d) = \varphi(c,d,a,b) \\
&iv)\ \varphi(a,bb',cb',d) = \gamma(b')\varphi(a,b,c,d) \qquad (15.2)
\end{aligned}$$

con $\alpha(a')$, $\beta(c')$, $\gamma(b') \in F$

Ci chiediamo quando una tale struttura è un semigruppo.

Si può dare una condizione necessaria, e precisamente:

Se $F^+ \times F^+(\odot)$ è un semigruppo, allora:

$$\varphi(a,b,c,d)\,\alpha(\varphi(a,b,c,d))\,\varphi(ac,bd,e,f) = \varphi(c,d,e,f)\,\beta(\varphi(c,d,e,f))\,\varphi(a,b,ce,d$$

Non si sa ancora se questa condizione è anche sufficiente.

Vediamo ora di ricavare altre condizioni sulle funzioni $\varphi, \alpha, \beta, \gamma$, nelle ipotesi che $F^+ \times F^+$ sia un semigruppo.

Imponendo

$$\left[(a,b) \odot (c,d) \right] \odot (e,f) = (a,b) \odot \left[(c,d) \odot (e,f) \right]$$

si ottiene, con ovvii calcoli

$$\varphi(aa',ba',c,d) = \varphi(c,d,aa'ba')$$

$$\alpha(a')\varphi(a,b,c,d) = \beta(a')\varphi(c,d,a,b) = \beta(a')\varphi(a,b,c,d)$$

da cui si ricava:

$$\alpha(a') = \beta(a') \qquad \text{per ogni } a' \in F^+ \cup \mathcal{E} \tag{15.3}$$

Dalla i) delle (15.2) si ottiene poi:

$$\alpha(a'a'') = \alpha(a')\alpha(a'')$$

Sempre nelle ipotesi che valga la proprietà associativa, posto

$\varphi_0 = \varphi(\mathcal{E},\mathcal{E},\mathcal{E},\mathcal{E})$ e se $a = b$, $c = d = e = f = \mathcal{E}$, si ricava:

$$\varphi(a,a,\mathcal{E},\mathcal{E})\,\varphi\left[a\varphi(a,a,\mathcal{E},\mathcal{E}),\ a\varphi(a,a,\mathcal{E},\mathcal{E}),\ \mathcal{E},\mathcal{E}\right] =$$

$$= \varphi(\mathcal{E},\mathcal{E},\mathcal{E},\mathcal{E})\,\varphi\left[a, a, \varphi(\mathcal{E},\mathcal{E},\mathcal{E},\mathcal{E}), \varphi(\mathcal{E},\mathcal{E},\mathcal{E},\mathcal{E})\right]$$

da cui: $\varphi_0\,\alpha(a)\,\varphi\left[a\alpha(a)\varphi_0, a\alpha(a)\varphi_0, \mathcal{E},\mathcal{E}\right] = \alpha(a)\varphi_0\varphi(\mathcal{E},\mathcal{E},\varphi_0,\varphi_0)$

$$\alpha(a\alpha(a))\,\varphi(\varphi_0,\varphi_0,\mathcal{E},\mathcal{E}) = \varphi(\mathcal{E},\mathcal{E},\varphi_0,\varphi_0)$$

$$\alpha(a(\alpha(a))) = \mathcal{E}$$

se a questo punto supponiamo che $\alpha(a) = \mathcal{E} \Leftrightarrow a = \mathcal{E}$ (*) (l'implicazione verso sinistra è vera nelle ipotesi in cui lavoriamo), si ottiene

ancora:

$$\alpha(a\alpha(a))\,\alpha(\varphi_s) = \alpha(\varphi_0)$$

$$\alpha(a\alpha(a)) = \varepsilon$$

$$a\alpha(a) = \varepsilon \qquad cioè \qquad \alpha(a) = a^{-1}$$

Con la condizione $^{(*)}$ è evidente come sia più semplice descrivere la struttura del gruppo. Senza la condizione $^{(*)}$, si può comunque osservare quanto segue:

$$\alpha(a) = \varepsilon\,,\ \alpha(b) = \varepsilon \Rightarrow \alpha(ab) = \varepsilon$$

e quindi gli elementi a tali che $\alpha(a) = \varepsilon$ formano semigruppo.

Ciò può aiutare nello studio del gruppo.

Continuiamo ancora a ricavare dalle conseguenze sulle funzioni α e γ.

Si ha:

$$\alpha^2(a)\varphi_0 = \varphi(a,a,a,a) = \gamma^2(a)\varphi_0$$

$$\alpha^2(a) = \gamma^2(a)$$

e, dall'ipotesi che ogni potenza sia esprimibile in unico modo, segue:

$$\alpha(a) = \gamma(a) \quad per\ ogni \quad a \in F^+ \cup \varepsilon$$

In conclusione si è provato che, in generale, vale:

1) $\alpha \equiv \beta$, $\alpha \equiv \gamma$

2) $\alpha(aa') = \alpha(a)\,\alpha(a')$

3) $\alpha(a)\,\alpha(\alpha(a)) = \varepsilon$ (cioè $\alpha(\alpha(a)) = \alpha(a)^{-1}$

Definiamo ora, in $F^+ \times F^+$, le operazioni unarie $\Uparrow$ e $\hat{\Uparrow}$ nel modo seguente:

$$\Uparrow(a,b) = (a.b) \odot (\varepsilon, \varepsilon) \quad , \quad \hat{\Uparrow}(a,b) = (a,b) \odot (\varphi_0, \varphi_0)$$

Si può allora provare che:

$\hat{\Uparrow}(a,b) = \Uparrow(a,b)$ e $\hat{\Uparrow}(F^+, F^+)$ è un gruppo commutativo in cui l'unità è (φ_0, φ_0).

Introduciamo ancora un'altra operazione, così definita:

$$(a,b) \otimes (c,d) = (ac\ \varphi(b,c),\ bd\ \varphi(b,c))$$

con le condizioni:

i) $\varphi(b,c) \in F$

ii) $\varphi(b.c) = \varphi(c,b)$

iii) $\varphi(hb',cb') = \alpha(b')\varphi(b,c)$

iv) $\varphi(a,\varepsilon) = \varepsilon$

Il semiaruppo non è più commutativo rispetto a quest'ultima operazione, ma accade ancora che :

$$\alpha(b\alpha(b)) = \varepsilon .$$

14. Problemi vari.

Parleremo ora di alcuni problemi connessi con la teoria dei semigruppi.

1) Sia S un semigruppo, M un suo sottoinsieme ed m,n interi distinti.

Con M^n ed M^m indichiamo gli insiemi costituiti da "parole" di lunghezza n ed m rispettivamente, costituite da elementi di M.

Ci chiediamo come determinare M affinché sia un (n,m)-mutante, cioè:

$$M^n \cap M^m = \emptyset \quad \text{o anche} \quad M^n \subseteq S \setminus M^m.$$

E' chiaro intanto che M non può essere un semiaruppo, ma non è facile ricavare altre informazioni.

Per accostarsi all'argomento è utile la seguente bibliografia:

J.B.Kim. - Mutants in the simetric seminroups - Chechosl. Math. J. 21 (1971), 355 - 363.

J.B.Kim. - No semigroup is a finite union of mutants - Semigroup forum 6 (1973), 360 - 361

K. Iseki - On (m,n)-mutants in semiaroup - Proc. Japan Ac. 38 (1962), 269 - 270.

2) Un altro problema è legato allo studio dei grafi su un gruppo.

Sia G un gruppo e K un suo sottoinsieme. Diciamo allora che $\mathcal{G}_K = (G, E_K)$ è un grafo diretto, dove:

$$(g_i, g_j) \in E_K \iff g_i^{-1} g_j \in K, \quad \text{con } g_i, g_j \in G.$$

Lo studio dei grafi diretti ha dato buoni risultati quando K è un sottogruppo· si conosce molto poco se manca questa condizione. Un lavoro interessante, sull'argomento è:

H. Harao - S. Naguki - Toult Idirent Cellular Automata - Journal of Computer and systems Science II (1975), 171 - 185.