

*Abstract* - This report presents the topics of the Seminar held in Lecce by prof. J. Szép. The purpose of the Seminar was to introduce the participants to the study of Semigroup Theory, and at the same time to provide some hints for research. In part I, after some definitions, the problems of partitions and classification of semigroup are examined. The subject of part.II is a theorem on structure of algebras with two operations; moreover some research problems are suggested. Finally part III gives an introduction to the Theory of automata, with various examples.

## I N D I C E

### Parte I - Semigrupperi

1. Relazioni .....	pag.	1
2. Semigrupperi e ideali .....	"	5
3. Esempi di semigrupperi .....	"	11
4. Osservazioni .....	"	12
5. Partizioni di semigrupperi .....	"	13
6. Osservazioni .....	"	15
7. Semigrupperi completamente regolari e completamente semplici "	"	16
8. Osservazioni .....	"	24
9. Matrici di Rees .....	"	26
10. Osservazioni .....	"	29
11. Gruppi a destra .....	"	30
12. Lateralì in un semigruppero .....	"	34

### Parte II - Algebre

13. Algebre con due operazioni .....	"	38
14. Osservazioni .....	"	42
15. Struttura di sistemi .....	"	43
16. Problemi vari .....	"	47

### Parte III - Automi

17. Teoria degli automi .....	"	49
18. Esempi di automi .....	"	53
19. Sottoautoma, automa superiore, automa inferiore .....	"	56
20. Esempio .....	"	62

## Parte I - Semigruppí

### Notazioni.

Per le applicazioni useremo la notazione destra, scriveremo cioè  $a\varphi$  e  $\varphi\psi$  per indicare rispettivamente  $\varphi(a)$  e  $\varphi\circ\psi$ . Con  $E_A$  indicheremo l'identità di  $A$ .

### 1. Relazioni.

Per relazione binaria su un insieme  $M$  intendiamo un sottoinsieme  $R$  di  $M \times M$ .

Per indicare che  $(a,b) \in R$  scriveremo anche  $a R b$  (e leggiamo "a è in relazione  $R$  con  $b$ ").

Tra relazioni binarie su uno stesso insieme assegnato si definiscono le operazioni di unione e intersezione (insiemistiche), l'operazione di complemento e il confronto per inclusione:

$$R \cup R', \quad R \cap R', \quad \bar{R} \quad (a \bar{R} b \text{ sse } (a,b) \notin R) \quad \text{e} \quad R \subseteq R'.$$

Se  $R$  ed  $S$  sono relazioni su  $M$  definiamo il prodotto  $RS$  nel modo seguente:

$$a R S b \quad \text{sse esiste } c \in M \text{ tale che } a R c \text{ e } c S b.$$

E' chiaro che, se  $R,S,T$  sono relazioni su  $M$ , allora:

$$(R S) T = R (S T) \quad (1.1)$$

mentre, generalmente,  $R S \neq S R$

Inoltre, se  $R_i$ ,  $i \in \mathcal{I}$ , è una famiglia di relazioni su  $M$ , allora, per ogni relazione  $S$  su  $M$ , valgono:

$$\left(\bigcup_{i \in \mathcal{I}} R_i\right) S = \bigcup_{i \in \mathcal{I}} R_i S \quad (1.2)$$

$$S \left(\bigcup_{i \in \mathcal{I}} R_i\right) = \bigcup_{i \in \mathcal{I}} S R_i \quad (1.3)$$

Infatti, se  $a \left[ \left(\bigcup_{i \in \mathcal{I}} R_i\right) S \right] b$ , allora esiste  $c$  tale che

$a \left(\bigcup_{i \in \mathcal{I}} R_i\right) c$  e  $c S b$ , cioè esiste  $R_i$ , tale che  $a R_i c$  e  $c S b$  e quindi  $a(R_i S) b$ , da cui segue  $a \left(\bigcup_{i \in \mathcal{I}} R_i S\right) b$ .

In maniera analoga si prova l'altra inclusione e quindi si ha la (1.2).

Allo stesso modo si prova la (1.3): osserviamo che per l'intersezione non è detto che valgano le stesse uguaglianze.

Se  $R, R', S$  sono relazioni su  $M$ , allora si ha:

$$R \subseteq R' \Rightarrow R S \subseteq R' S \quad \text{e} \quad S R \subseteq S R' \quad (1.4)$$

L'inversa  $R^{-1}$  della relazione  $R$  è definita da:

$$a R^{-1} b \quad \text{sse} \quad b R a$$

Si vede facilmente che:

$$(R^{-1})^{-1} = R \quad ; \quad R \subseteq S \Leftrightarrow R^{-1} \subseteq S^{-1} \quad (1.5)$$

$$\left(\bigcap_i R_i\right)^{-1} = \bigcap_i R_i^{-1} \quad (1.6)$$

$$\left(\bigcup_i R_i\right)^{-1} = \bigcup_i R_i^{-1} \quad (1.7)$$

$$(S T)^{-1} = T^{-1} S^{-1} \quad (1.8)$$

La relazione uguaglianza  $E$  è definita come:

$$a E b \quad \text{sse} \quad a = b.$$

E' chiaro che  $E^{-1} = E$  e  $R E = E R = R$  per ogni relazione  $R$  su  $M$ , mentre, se  $O$  indica la relazione vuoto, si ha:

$$O \subseteq R, \quad R O = O R = O \quad \text{per ogni relazione } R \text{ su } M.$$

Una relazione  $R$  si dice che gode della proprietà:

1. riflessiva sse  $a R a \quad \forall a \in M$  (cioè  $E \subseteq R$ )
2. transitiva sse  $a R b$  e  $b R c \Rightarrow a R c$  (cioè  $RR \subseteq R$ )
3. simmetrica sse  $a R b \Rightarrow b R a$  (cioè  $R^{-1} = R$ )
4. antisimmetrica sse  $a R b$  e  $b R a \Rightarrow a = b$  (cioè  $R \cap R^{-1} \subseteq E$ )

Diciamo che  $R$  è una relazione di equivalenza se essa gode delle proprietà riflessiva, simmetrica e transitiva. Una relazione  $R$  di equivalenza determina nell'insieme  $M$  una partizione disgiunta (la partizione delle classi di equivalenza modulo  $R$ ) e, viceversa, data una partizione disgiunta  $\pi$  dell'insieme  $M$ , si può definire una relazione di equivalenza  $R$  (le cui classi di equivalenza sono proprio gli elementi della partizione  $\pi$ ).

Sia data una famiglia  $R_i$ ,  $i \in J$ , di relazioni di equivalenza su  $M$ .

Anche  $\bigcap_{i \in J} R_i$  è una relazione di equivalenza (su  $M$ ): lo stesso non si può dire per  $\bigcup_{i \in J} R_i$ .

Ancora, se  $R$  ed  $S$  sono relazioni di equivalenza, si ha:

$$R S \text{ relaz. d'equ.} \iff R S = S R$$

(e si può anche provare che  $R S = R \cup S$ ). (cfr. F. Sik, Spisy vyd. prirodovade fakult. Masarykovy univ. (1954), n. 3, 97 - 102).

Dim.

$$\Rightarrow \underline{S R} = S^{-1} R^{-1} = (R S)^{-1} = \underline{R S}$$

$$\Leftarrow \underline{(R S)(R S)} = R(S R) S = R(R S) S = (R R)(S S) \subseteq \underline{R S} \quad (\text{transitività})$$

$$\underline{(R S)^{-1}} = S^{-1} R^{-1} = S R = \underline{R S} \quad (\text{simmetria})$$

$$\underline{E} \subseteq S = E S \subseteq \underline{R S} \quad (\text{riflessività})$$

Se  $R$  è una relazione di equivalenza su  $M$  indichiamo con  $[a]$  la classe degli elementi di  $M$  equivalenti ad  $a$  modulo  $R$  (classe di equivalenza) e con  $M/R$  l'insieme delle classi di equivalenza di elementi di  $M$ . Per applicazione naturale  $\varphi$  intendiamo l'applicazione da  $M$  su  $M/R$  tale che  $a\varphi = [a]$  per ogni elemento  $a$  di  $M$ .

## 2. Semigrupperi e ideali.

Sia  $S$  un insieme su cui è definita un'operazione binaria, che indichiamo con  $\cdot$  (e chiamiamo prodotto);  $S$  è allora un gruppoide. Osserviamo che un'operazione binaria su  $S$  può essere riguardata come una relazione ternaria  $R$  nel modo seguente: se  $a \cdot b = c$  allora diciamo che  $(a, b, c) \in R$ .

Un gruppoide la cui operazione binaria goda della proprietà associativa si chiama semigruppero. Un sottoinsieme  $A$  di un semigruppero  $S$  lo diciamo sottosemigruppero se è chiuso rispetto al prodotto in  $S$ . Se  $A \subseteq S$ , l'insieme dei prodotti finiti di elementi di  $A$  è un sottosemigruppero che chiamiamo sottosemigruppero generato da  $A$  e indichiamo con  $\langle A \rangle$ . Il sottosemigruppero generato da un solo elemento  $a$  di  $S$ , cioè  $\langle a \rangle$ , lo chiamiamo sottosemigruppero ciclico generato da  $a$ .

Se  $\langle a \rangle = S$  per qualche  $a \in S$ , diremo che  $S$  è un semigruppero ciclico.

Osserviamo che, se  $H_i$ ,  $i \in J$  sono i sottosemigrupperi di  $S$  includenti  $A$  (con  $A$  sottoinsieme di  $S$ ), allora certamente  $\bigcap_{i \in J} H_i \supseteq \langle A \rangle$  e anzi, poiché anche  $\langle A \rangle$  è tra i sottosemigrupperi includenti  $A$ , si ha l'eguaglianza.

Con ciò si è provato il

### Teorema 2.1

Sia  $A \subseteq S$ : allora  $\langle A \rangle$  è l'intersezione di tutti i sottosemi-

gruppi di  $S$  contenenti  $A$ .

Sia ora  $a \in S$ ; il sottosemigruppo ciclico  $\langle a \rangle$  è costituito da tutte le potenze di  $a$ . Possono presentarsi due casi:

- 1) Tutte le potenze di  $a$  sono distinte;
- 2) Esistono due interi,  $m$  ed  $n$ , con  $m < n$ , tali che  $a^m = a^n$ .

Nel primo caso  $\langle a \rangle$  ha ordine infinito, mentre nel secondo caso, come vedremo tra poco,  $\langle a \rangle$  ha ordine finito.

Fissiamo il più piccolo  $n$  tale che  $a^m = a^n$  per qualche  $m < n$ . Allora gli elementi distinti di  $\langle a \rangle$  sono  $a, a^2, \dots, a^m, \dots, a^{n-1}$ , e inoltre  $\{a^m, \dots, a^{n-1}\}$  è un gruppo ciclico di ordine  $n - m$  la cui unità è  $a^{m+k_0}$  con  $k_0 \gg 0$  e  $m + k_0 \equiv 0 (n - m)$ .

Sia  $T \subseteq S$ ; diciamo che  $T$  è un ideale sinistro (destro) di  $S$  se accade  $S t \subseteq T$  ( $t S \subseteq T$ ) per ogni  $t \in T$ . Se  $T$  è un ideale sinistro e destro si dice che  $T$  è un ideale.

Si prova facilmente che, se  $T \subseteq S$ , valgono:

- $T$  sottosemigruppo  $\Leftrightarrow T \cdot T \subseteq T$
- $T$  ideale sinistro  $\Leftrightarrow S T \subseteq T$
- $T$  ideale destro  $\Leftrightarrow T S \subseteq T$
- $T$  ideale  $\Leftrightarrow S T \subseteq T, T S \subseteq T$

### Teorema 2.2

Se  $T$  e  $V$  sono ideali sinistri (destri) di  $S$ , anche  $T \cap V$  è ideale sinistro (destro) di  $S$ .



Un teorema analogo vale anche per gli ideali.

Diamo ora alcune definizioni. Sia  $A \subseteq S$ , poniamo

$$L(A) = \bigcap L_i \quad \text{con } L_i \text{ ideale sinistro, } L_i \supseteq A$$

$$R(A) = \bigcap R_i \quad \text{con } R_i \text{ ideale destro, } R_i \supseteq A$$

$$J(A) = \bigcap J_i \quad \text{con } J_i \text{ ideale, } J_i \supseteq A$$

Chiamiamo  $L(A)$  ( $R(A)$ ) ideale sinistro (destro) generato da  $A$   
e  $J(A)$  ideale generato da  $A$ .

Si può provare che :

$$L(a) = a \cup S a$$
$$R(a) = a \cup a S$$
$$J(a) = a \cup a S \cup S a \cup S a S$$

Proviamo, ad esempio, la prima uguaglianza. Che  $a \cup S a$  sia un ideale sinistro e che contenga  $a$  è ovvio; inoltre  $a \cup S a$  è contenuto in ogni altro ideale sinistro che contiene  $a$ , da cui l'uguaglianza.

Si dice che un semigruppò  $S$  è semplice a sinistra (a destra) se non contiene ideali sinistri (destri) propri.  $S$  si dice semplice se non contiene ideali propri.

Si vede subito che:

$$S \text{ semplice a sinistra} \iff S a = S, \text{ per ogni } a \in S.$$

Osserviamo che, se  $S$  è semplice a sinistra, l'equazione  $x a = b$  ha sempre soluzioni (non è detto che la soluzione sia unica). Considerazioni analoghe si possono fare anche per i semigruppò semplici a destra.

L'intersezione di tutti gli ideali di  $S$  si chiama nucleo di  $S$ .

Evidentemente il nucleo è il minimo degli ideali di  $S$ . Vale anche:

Teorema 2.3

Se  $\mathcal{J}$  è ideale semplice di  $S$  (cioè non contiene ideali propri di  $S$ ), allora  $\mathcal{J}$  è il nucleo di  $S$ .

Un elemento  $e \in S$  si chiama unità sinistra (destra) per  $a$  se  $ea = a$  ( $ae = a$ ), e viene detto semplicemente unità per  $a$  se è sia unità destra che unità sinistra per  $a$ .

Un elemento  $e \in S$  è <sup>chiamato</sup> elemento unità sinistra (destra) o semplicemente unità di  $S$  se è una unità sinistra (destra) o una unità per ogni  $a \in S$ .

E' chiaro che, se  $S$  ha unità, questa è unica.

Poiché a volte conviene lavorare con semigrupper aventi unità, si può "ampliare" il semigrupper  $S$  immergendolo in  $S^1 = S \cup \{e\}$ , con le condizioni:  $ea = a$  e  $ae = a$  per ogni  $a \in S^1$ . E' evidente che  $S^1$  è ancora un semigrupper.

Se, considerato  $a \in S$ , esiste  $z \in S$  tale che  $az = z$  ( $za = z$ ) si dice che  $z$  è uno zero a destra (sinistra) per  $a$ . Se  $za = az = z$  per ogni elemento  $a \in S$ , si dice che  $z$  è uno zero di  $S$  (ed è allora unico).

Se  $z$  è lo zero di  $S$  ed esistono  $a, b \in S$  (non zero elementi) tali che si abbia  $ab = z$ , allora  $a$  e  $b$  si chiamano divisori dello zero.

Se  $S$  ha lo zero, questo si indica con  $0$ . Analogamente a quanto

fatto prima, si può "ampliare"  $S$  immergendolo in  $S^0 = S \cup \{0\}$  con le condizioni  $0a = a0 = 0$  per ogni  $a \in S^0$ .

Diciamo che  $S$  è un semigrupp zero a sinistra (a destra) se  $ab = a$  ( $ab = b$ ) per ogni  $a, b \in S$ . Se  $0 \in S$  e se  $ab = 0$  per ogni  $a, b \in S$ , allora diciamo che  $S$  è un semigrupp zero.

I semigrupp zero costituiscono uno dei "poli" del problema della classificazione dei semigrupp, in quanto semigrupp aventi una struttura molto semplice. L'altro "polo" è costituito, invece, dai gruppi, che possono essere riguardati come semigrupp dalla struttura molto sofisticata.

Altre definizioni utili sono:

$$C(s) = \{ a \in S \mid as = sa \} \quad (\text{centralizzatore di } s);$$

$$C = \{ a \in S \mid as = sa \text{ per ogni } s \in S \} \quad (\text{centro di } S).$$

Si vede facilmente che  $C(s)$  e  $C$  sono semigrupp; inoltre  $S$  è un semigrupp commutativo se e solo se coincide col suo centro.

Ci chiediamo ora: tra i sottosemigrupp di un semigrupp  $S$ , c'è qualche gruppo? Il teorema 2.4 darà una risposta a questa domanda.

Un elemento  $a$  di  $S$  lo diciamo idempotente se  $aa=a$ ; un semigrupp  $S$  lo diciamo idempotente se ogni suo elemento è idempotente.

Un semigrupp  $S$  idempotente e commutativo lo diciamo semi reticolo.

#### Teorema 2.4

Sia  $e$  un elemento idempotente di  $S$ . Poniamo:

$$G_e = \{ a \in S \mid a = ea = ae, e = aa' = a'a \text{ per qualche } a' \in S \}.$$

Allora  $G_e$  è un gruppo.

Dim. E' facile verificare che  $e \in G_e$  e che  $G_e$  è un semigruppò: per completare la dimostrazione basta far vedere che, fissato  $a \in G_e$ ,  $a' \in G_e$  <sup>ed</sup> è unico.

Intanto si ha:

$$a(ea') = (ae)a' = aa' = e = ee = e(a'a) = (ea')a$$

$$e(ea') = (ee)a' = ea' = e(ea') = e(a'a)a' = (ea')e$$

e quindi  $ea' \in G_e$ , inoltre  $ea' = a'e = b$  (quindi  $b \in G_e$ ).

Se ora valesse  $ab = ab' = e$ , moltiplicando a sinistra per  $a'$  si avrebbe  $eb = eb' \Rightarrow b=b'$  e pertanto l'inverso di  $a$  in  $G_e$  è determinato univocamente.

Dunque  $G_e$  è un gruppo (la cui unità è, evidentemente,  $e$ ) ed è inoltre massimale rispetto alla proprietà di avere  $e$  come unità.

Consideriamo ora, sempre nelle ipotesi che  $e$  sia un elemento idempotente di  $S$ , il sottoinsieme:

$$G'_e = \{ a \in S \mid a \in eS \cap Se, e \in aS \cap Sa \}.$$

### Teorema 2.5

Si ha:  $G'_e = G_e$

Dim. Si verifica immediatamente che  $G'_e \supseteq G_e$ ;

sia ora  $a \in G'_e$ ; si ha:

$$a = ex = ye \quad \text{con} \quad e = az = wa$$

$$e a = e(ex) = (ee)x = ex = a = ye = y(ee) = (ye)e = a e$$

$$e = a(e z e) = (e w e)a$$

$$e z e = e(e z e) = e (w a) z e = e w(a z) e = e w e$$

quindi  $e z e = e w e = a'$  e allora  $a \in G_e$ .

$$\text{Pertanto } G'_e = G_e$$

Diamo ancora alcune definizioni.

Un elemento  $a \in S$  lo diciamo regolare se  $a = a x a$  per qualche  $x \in S$ .

Un semigruppò lo diciamo regolare se è regolare ogni suo elemento.

Si dice che  $x$  è un inverso di  $a$  se accade:  $a = axa$ ,  $x = xax$ .

### Teorema 2.6

Sia  $a \in S$ ,  $a = a x a$ : allora  $x a x$  è un inverso di  $a$ .

Dim.  $xax = x(axa)x = xaxax = (xax)a (xax)$

$$a(xax)a = (axa)xa = axa = a$$

quindi  $xax$ , verificando le due proprietà, è un inverso di  $a$ .

Questo teorema ci assicura che ogni elemento regolare ha un inverso.

Un elemento  $a \in S$  lo diciamo elemento accrescitivo a sinistra (a destra) se accade  $a S' = S$  ( $S'a = S$ ), con  $S' \subset S$ .

### 3. Esempi di semigruppò.

1) Sia  $S$  un insieme non vuoto; si definisca

$$x \cdot y = \begin{cases} x & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases} \quad \text{per ogni } x, y \in S$$

$S$  è allora un semigruppò (semigruppò di Kronecker)

2) L'insieme delle matrici (reali)  $n \times n$  è un semigruppò sia rispetto all'operazione di somma che a quella di prodotto.

3) Sono semigruppò gli insiemi finiti di cui diamo qui di seguito le operazioni definite con le tavole di Cayley (con le convenzioni usuali).

	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	b	b
d	a	a	b	a

	a	b	c	d
a	a	b	a	a
b	a	b	a	b
c	a	b	a	c
d	a	b	a	d

	a	b	c	d
a	a	b	b	b
b	a	b	b	b
c	a	b	c	b
d	a	b	b	d

#### 4. Osservazioni.

Uno dei problemi di ricerca nella teoria dei semigruppò consiste nel "classificare" i semigruppò.

I due "poli", in tale classificazione, sono i semigruppò zero ed i gruppi.

Quando lo studio di un semigruppò è ricondotto a quello di certi suoi sottogruppi, il problema è risolto: lì termina la teoria dei semigruppò

ed ha inizio la teoria dei gruppi.

### 5. Partizioni di semigrupperi.

Ci proponiamo ora di costruire una partizione di semigrupperi in sottosemigrupperi disgiunti. Prima però di affrontare questo problema ci serve una nozione mediante la quale potremo "eliminare" dal nostro studio complicazioni portate da certi elementi particolari (gli annullatori).

Se  $\mathcal{I}$  è un ideale del semigruppero  $S$ , la relazione  $R$  definita da:

$$x R y \quad \text{se e solo se} \quad x, y \in \mathcal{I} \quad \text{o} \quad x = y$$

è una relazione di equivalenza. Le classi di equivalenza di  $S$  modulo  $R$  sono date da  $\mathcal{I}$  e da ogni sottoinsieme  $\{a\}$  con  $a \in S$ . Definendo, in maniera naturale, l'operazione

$$x \circ y = \begin{cases} x y & \text{se } x, y \notin \mathcal{I} \\ 0 & \text{altrimenti} \end{cases}$$

si ottiene un semigruppero in cui  $\mathcal{I}$  gioca il ruolo di elemento zero, mentre gli altri elementi ( $\notin \mathcal{I}$ ) operano tra loro come in  $S$ . Questo semigruppero si indica con  $S/\mathcal{I}$  e prende il nome di semigruppero quoziente (di Rees).

Se il semigruppero  $S$  ha annullatori (cioè elementi  $a \in S$  )'  $ax=xa=0$  per ogni  $x \in S$ ), si vede che essi costituiscono un ideale (ideale degli annullatori) e dunque, passando al semigruppero quoziente, si può ottenere un semigruppero con elemento zero ma senza annullatori.

Sia quindi  $S$  un semigruppò senza annullatori. Definiamo:

$$\begin{aligned} S_0 &= \{ a \in S \mid a x = 0, \text{ per qualche } x \neq 0 \} \\ S_1 &= \{ a \in S \setminus S_0 \mid a x = a y; x, y \in S, x \neq y \} \\ S_2 &= \{ a \in S \setminus (S_0 \cup S_1) \mid a S < S \} \\ S_3 &= \{ a \in S \setminus (S_0 \cup S_1) \mid a S = S \} \end{aligned} \quad (5.1)$$

Osserviamo che  $S_0, S_1, S_2, S_3$  sono sottosemigruppò, come anche  $S \setminus S_0$  ed  $S \setminus (S_0 \cup S_1)$ , e inoltre:

$$S = S_0 \cup S_1 \cup S_2 \cup S_3 \quad (5.2)$$

A sua volta  $S_0$  ed  $S_1$  possono decomporre in sottosemigruppò nel modo seguente:

$$S_0 = S_{00} \cup S_{01} \quad \text{ed} \quad S_1 = S_{11} \cup S_{12}$$

con

$$\begin{aligned} S_{00} &= \{ a \in S_0 \mid a S < S \} & , & & S_{01} &= \{ a \in S_0 \mid a S = S \} \\ S_{11} &= \{ a \in S_1 \mid a S < S \} & & & S_{12} &= \{ a \in S_1 \mid a S = S \} \end{aligned} \quad (5.3)$$

Se  $a \in S_{01}$  ed  $x$  è un elemento  $\neq 0$  tale che  $a x = 0$ , allora  $a(S \setminus x) = S$ .

Elementi siffatti si chiamano accrescitivi (cio: elementi tali che  $aT = S$  con  $T < S$ ).

E ancora, se  $a \in S_{12}$  e  $x, y$  sono elementi di  $S$  tali che  $ax = ay$ , allora  $a(S \setminus y) = S$ . Quindi tutti gli elementi di  $S_{01} \cup S_{12}$  sono accrescitivi. Viceversa ogni elemento accrescitivo di  $S$  sta in  $S_{01} \cup S_{12}$ .



Infatti, se  $a$  è un elemento accrescitivo, non può stare in  $S_2$  né in  $S_3$  (perché se  $a \in S_3$ , in  $aS$  troviamo gli elementi di  $S$  una sola volta), né può stare in  $S_{00}$  o  $S_{11}$ .

Dunque gli elementi di  $S_{01} \cup S_{12}$  sono tutti e soli gli elementi accrescitivi di  $S$ .

Tra i sottosemigrupperi ora visti esistono alcuni legami; più precisamente:

$$S_3 S_2 \subseteq S_2$$

$$S_2 S_3 \subseteq S_2$$

$$S_2 S_1 \subseteq S_1 \quad (\text{ma niente si può dire di } S_1 S_2)$$

$$S_{00} S \subseteq S_{00}$$

$$S_3 S_{00} \subseteq S_{00}$$

Proviamo, come esempio, la prima inclusione. Intanto è ovvio che  $S_3 S_2 \subseteq S_3 \cup S_2$  (essendo  $S_3 \cup S_2$  un sottosemigruppero) e quindi un prodotto  $s_3 s_2$  (con  $s_3 \in S_3$ ,  $s_2 \in S_2$ ) sta in  $S_2$  o in  $S_3$ ; si ha poi  $s_3 s_2 S \subseteq S$  (essendo  $s_2 S \subseteq S$ ) e quindi  $s_3 s_2 \in S_2$ .

### 6. Osservazioni.

Tra i problemi ancora aperti in teoria dei semigrupperi, notevole importanza ha quello di trovare una decomposizione disgiunta di un semigruppero  $S$  per la quale il prodotto di ogni coppia di componenti sia incluso in un'altra componente della decomposizione.

Lo scopo è sempre quello di classificare i semigrupperi.

Szep ha descritto completamente ciò che accade nel caso finito commu  
tativo.

In generale, nel caso finito, è stato provato che

$$S = S_0 \cup S_1 \cup S_3.$$

### 7. Semigrupperi completamente regolari e completamente semplici.

Sempre in riferimento alla ricerca di cui al paragrafo precedente, è  
interessante la possibilità di decomporre un semigruppero in sottosemigrupperi  
pi con una struttura "molto vicina" a quella dei gruppi. Introduciamo,  
a questo scopo, i semigrupperi completamente regolari.

Un elemento  $a \in S$  si dice completamente regolare se  $a = a x a$ ,  
 $a x = x a$ , per qualche  $x \in S$ .

Un semigruppero  $S$  lo diciamo completamente regolare se tale è ogni suo  
elemento.

Si ha una caratterizzazione degli elementi completamente regolari:

#### Teorema 7.1

Per ogni  $a \in S$  sono equivalenti:

- i)  $a$  è completamente regolare;
- ii)  $a$  ha un inverso commutativo;
- iii)  $a \in a^2 S a^2$ ;
- iv)  $a \in a^2 S \cap S a^2$ ;
- v)  $a$  è un <sup>in</sup> sottogruppo di  $S$ .

Dim.  $i) \Rightarrow ii)$ :

$$a = axa = a(xax)a$$

$$xax = x(axa)x = (xax)a(xax)$$

$$a(xax) = (axa)x = ax = xa = x(axa) = xax)a$$

quindi  $xax$  è un inverso di  $a$  ed è permutabile con  $a$ .

$$ii) \Rightarrow iii): a = aya = ayaya = ayayaya = a^2 yyya \in a^2 S a^2;$$

$$iii) \Rightarrow iv): a = a^2 za^2 \in a^2 S \cap S a^2;$$

$$iv) \Rightarrow v): a = xa^2 = a^2 y \Rightarrow xa = x(a^2 y) = (xa^2)y = ay;$$

poniamo  $e = xa = ay$ ; si ha allora:

$$ae = a^2 y = a = xa^2 = ea$$

$$e^2 = (xa)(ay) = (xa^2)y = ay = e \quad \text{ed } e \in Sa \cap aS$$

quindi  $a \in G_e$  che è un gruppo;

$v) \Rightarrow i)$ : ovvio.

Le equivalenze ora provate ci permettono di affermare che se il se  
migruppo  $S$  è completamente regolare, allora  $S = \bigcup G_e$  con  $e$   
idempotente, dove, essendo i  $G_e$  massimali, sono anche tra loro disgiunti.

Sia  $\mathcal{C}$  una classe di semigrupperi. Un semigruppo  $S$  si dice semi reti-  
colo di semigrupperi se esiste una congruenza le cui classi di equivalenza  
sono tutte in  $\mathcal{C}$ .

### Teorema 7.2

$S$  sia un semireticolato di semigrupperi,  $S = \bigcup S_\alpha, \alpha \in \mathcal{I}$ .

$S$  è completamente regolare se e solo se  $S_\alpha$  è completamente regolare, per ogni  $\alpha \in \mathcal{J}$ .

Se  $S$  è un semigruppò ed  $\mathcal{J}$  un suo ideale, diciamo che  $\mathcal{J}$  è un ideale primo se accade che:  $a S b \subseteq \mathcal{J} \Rightarrow a \in \mathcal{J} \text{ o } b \in \mathcal{J}$ .

Si dirà che  $\mathcal{J}$  è un ideale semiprimo se  $a S a \subseteq \mathcal{J} \Rightarrow a \in \mathcal{J}$ .

Si dirà che  $\mathcal{J}$  è completamente semiprimo se:  $x^2 \in \mathcal{J} \Rightarrow x \in \mathcal{J}$ .

### Teorema 7.3

Sia  $S$  un semigruppò; le seguenti proposizioni sono equivalenti:

- i)  $S$  è completamente regolare;
- ii)  $\forall a \in S: a \in a S a^2$ ; (ii')  $\forall a \in S: a \in a^2 S a$
- iii)  $S$  è unione di sottogruppi disgiunti;
- iv) Ogni ideale sinistro (o destro) di  $S$  è completamente semiprimo.

Dim. i)  $\Rightarrow$  ii)

per ipotesi  $a \in a^2 S a^2 = a(aS)a^2 \subseteq a S a^2$ ; similmente si prova che  $a \in a^2 S a$ ;

ii)  $\Rightarrow$  iii)

poiché la ii) ci dice che  $a \in S a^2$ , basta provare che  $a \in a^2 S$  e sfruttare poi il Teor. 7.1 per affermare che ogni  $a \in S$  sta in un sottogruppo di  $S$ .

Abbiamo intanto:

$a \in a S a^2 \Rightarrow$  esiste  $x \in S$   $\exists$   $a = axa^2$  e ancora  $(xa)y(xa)^2 = xa$  per qualche  $y \in S$ ; quindi:

$$\begin{aligned}
 a &= axa^2 = a(xa)a = a(xa)y(xa)^2 a = (axayx)(axa^2) = \\
 &= axayxa = axay(xa) = (axay)(xa)y(xa)^2 = ay(xa)^2 = \\
 &= (ayx)a(xa) = (ayx)(axa^2)(xa) = (ay)(xa)^2(axa) = \\
 &= a(axa) = a^2xa \quad \text{cioè} \quad a \in a^2S \quad a \subseteq a^2S;
 \end{aligned}$$

iii)  $\Rightarrow$  iv)

sia  $\mathcal{J}$  ideale sinistro di  $S$  (cioè  $S\mathcal{J} \subseteq \mathcal{J}$ ) e sia  $G_e$  uno dei gruppi la cui unione copre  $S$  tale che  $G_e \neq \emptyset$ . Esiste allora  $a \in \mathcal{J} \cap G_e$  e quindi  $G_e a \subseteq G_e \mathcal{J} \cap G_e^2 = G_e \mathcal{J} \cap G_e \subseteq \mathcal{J} \cap G_e \subseteq \mathcal{J}$  da cui:

$$G_e = G_e a \subseteq \mathcal{J}.$$

$\mathcal{J}$  è allora unione disgiunta di gruppi e dunque:

$$x^2 \in \mathcal{J} \Rightarrow x^2 \in G_e, \text{ per qualche } G_e \Rightarrow x \in G_e \Rightarrow x \in \mathcal{J}.$$

iv)  $\Rightarrow$  i)

se  $a \in S$ ,  $S a^2$  è un ideale sinistro di  $S$  e quindi

$$a^4 = a^2 a^2 \in S a^2 \Rightarrow a^2 \in S a^2 \Rightarrow a \in S a^2;$$

similmente si prova che  $a \in a^2 S$  e quindi  $S$  è completamente regolare.

Sia  $E_S$  l'insieme degli elementi idempotenti di un semigrupp  $S$ .

La seguente relazione risulta essere l'ordine (parziale) in  $E_S$ :

$$e \leq f \stackrel{\text{def}}{\iff} e = ef = fe$$

(La verifica è banale).

Un elemento idempotente si dice primitivo se è minimale (rispetto alla relazione d'ordine ora definita).

Teorema 7.4

Se  $S$  è un semigruppò regolare in cui tutti gli idempotenti sono primitivi, allora  $S$  è completamente regolare e  $G_e = a S a$ , con  $e \in E_s$ ,  $a \in G_e$ .

Dim.

$a \in S \Rightarrow a = axa$  per qualche  $x \in S \Rightarrow a^2 = a^2 ya^2$  per qualche  $y \in S$ ;

poniamo  $e = ax$ ,  $f = a^2 yax$ ;  $e$  ed  $f$  sono elementi idempotenti;

infatti:

$$e^2 = (ax)^2 = (axa)x = ax = e$$

$$\begin{aligned} f^2 &= (a^2 yax)^2 = a^2 yax a^2 yax = a^2 y(axa) ayax = (a^2 ya^2) yax = \\ &= a^2 yax = f \end{aligned}$$

inoltre:

$$ef = (ax)(a^2 yax) = (axa)(ayax) = a^2 yax = f$$

$$fe = (a^2 yax)(ax) = a^2 y(axa)x = a^2 yax = f$$

quindi  $f = ef = fe$  e, per l'ipotesi,  $e = f$ , cioè:

$$ax = a^2 yax \Rightarrow axa = a^2 yaxa \Rightarrow a = a^2 ya \in a^2 S a$$

$S$  è allora completamente regolare (e unione di gruppi disgiunti).

Siano ora  $e \in E_s$ ,  $a \in G_e$ :

$$x \in G_e \Rightarrow x = exe = a(a^{-1}x a^{-1})a \Rightarrow x \in a S a,$$

viceversa:

$$x \in a S a \Rightarrow x = aya \text{ per qualche } y \Rightarrow x \in G_f \text{ per qualche } f \in E_S;$$

ne segue

$$ef = e(x x^{-1}) = e(aya)x^{-1} = (aya)x^{-1} = x x^{-1} = f$$

similmente si prova  $fe = f$  e quindi  $e = f$ ; allora  $x \in G_e$  ed anche la seconda inclusione è provata.

Diciamo che il semigruppoo  $S$  è completamente semplice se è semplice ed ogni suo elemento idempotente è primitivo (cioè minimale in  $E_S$ ).

$S$  si dirà poi cancellabile debolmente se da  $ax = bx$  e  $xa = xb$  segue  $a = b$ .

Possiamo caratterizzare i semigruppooi completamente semplici con il seguente teorema.

### Teorema 7.5

Le proposizioni seguenti sono equivalenti:

- i)  $S$  è completamente semplice;
- ii)  $S$  è semplice e completamente regolare;
- iii)  $S$  è regolare e ogni suo idempotente è primitivo;
- iv)  $S$  è regolare e cancellabile debolmente;
- v)  $S$  è regolare e, per ogni  $a, x \in S$ , si ha:  $a = axa \Rightarrow x = xax$

Dim. i)  $\Rightarrow$  ii)

Sia  $e$  un idempotente (primitivo) ed  $a \in S$ ; poiché  $SeS = S$  (in quanto  $S$  è semplice), si ha  $a = uev$  ed  $e = x(ea^3e)y$  con opportuni  $u, v, x, y \in S$ .

Poniamo  $f = evae y ex ea ue$ ; si ha:

$$f^2 = evae y ex ea (ueev) aeyex ea ue = evae y ex ea^3 ey) ex ea ue = evae y ex ea ue = f ;$$

inoltre  $ef = fe = f$  e quindi  $f = e$ .

Pertanto  $a = uev = ufv = (uev) aeyex ea (uev) = a^2 (eyex e) a^2 \in a^2 S a^2$

e quindi  $S$  è completamente regolare.

ii)  $\Rightarrow$  iii)

siano  $e, f \in E_s$ ,  $e \leq f$ ; essendo  $S$  semplice si ha  $f = xey$  con opportuni  $x, y \in S$ ; poniamo  $a = fxf$ ,  $b = f\|f$ . Si ha allora:

$$aeb = (fxf)e(fyf) = fx(fef)yf = f(xey)f = f f f = f$$

Sia  $a'$  un elemento tale che  $a = aa'a$ ,  $aa' = a'a$ . Si ha:

$$f = aeb = aa'a eb = aa'f = a'af = a'a = aa'$$

$$f = a'a = (a'a)(a'a) = a'(aa')a = a'fa = a'(aeb)a = (a'a)(eba) = feba = eba$$

pertanto:  $e = ef = e(eba) = eba = f$



e così si è provato che ogni idempotente è primitivo.

iii)  $\Rightarrow$  iv)

Per il Teorema 7.4,  $S$  è completamente regolare; supponiamo che  $ax = bx$ ,  $xa = xb$ . Siano  $e, f$  due idempotenti tali che

$a \in G_e$ ,  $b \in G_f$ ; allora  $axa \in G_e$  e  $bxb \in G_f$ ;

$$axa = bxa = bxb \Rightarrow G_e = G_f \Rightarrow e = f ;$$

se ora poniamo  $y = exe$  si ha:  $y \in G_e$  e quindi, essendo

$$ay = aexe = (ae)xe = axe = bxe = hexe = by , \quad \text{per la legge}$$

di cancellazione in un gruppo, si ha  $a = b$ .

iv)  $\Rightarrow$  v)

$$a = axa \Rightarrow ax = a(xax) , \quad xa = (xax)a \Rightarrow x = xax$$

v)  $\Rightarrow$  i)

Siano  $e, f \in E_S$ ,  $e \leq f$ ; allora  $e = efe$  e quindi, dalla v), si ha:

$$f = fe f = efe = fe \quad \text{da cui} \quad e = f$$

Supponiamo ora che  $S$  non sia semplice e sia  $\mathcal{J}$  un ideale proprio di  $S$ . Se  $a \in \mathcal{J}$  esiste  $G_e$  tale che  $a \in \mathcal{J} \cap G_e$  e dunque:

$$G_e \mathcal{J} \cap G_e \supseteq G_e a = G_e ;$$

se ora  $f \notin \mathcal{J}$ , si ha:  $G_f = fsf \supseteq f \mathcal{J} f \supseteq \mathcal{J} : =$  contraddizione!

Allora  $S$  è semplice.

Teorema 7.6

Se  $S$  è un semigruppoo completamente semplice ed  $e, f \in E_S$ , allora valgono le seguenti proposizioni:

- i)  $a, b \in S, \quad ab \in G_e \implies a S b \subseteq G_e$  ;
- ii)  $ef = e \implies fe = f$  ;
- iii)  $fe = e \implies ef = f$ .

Dim. Proviamo la i).

Sia  $a \in G_g, \quad b \in G_h, \quad ab \in G_e$ ; allora  $aba \in G_g, \quad bab \in G_h$ ;

$a = (aba)u, \quad b = v(bab)$  con opportuni  $u, v$  in

$G_g$  e  $G_h$  rispettivamente; quindi:

$$axb = (aba)uxv(bab) = (ab)(auxvb)(ab) \in G_e$$

e dunque  $a S b \subseteq G_e$ ,

Proviamo la ii)

$ef = f \implies fe \in E_S$  e poiché  $fe = f e f \in G_f$ , si ha  $f = fe$ .

Analogamente si prova anche la iii)

8. Osservazioni.

Abbiamo visto come un semigruppoo  $S$  si può decomporre in sottosemi-gruppi:

$$S = S_0 \cup S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \tag{8.1}$$

in maniera che in  $S_1 \cup S_3$  ci sono tutti e soli gli elementi acce-

scitivi di  $S$  (facciamo notare che rispetto al par. 5, si è cambiato il modo di indicare le componenti della partizione; in particolare si indicano qui con  $S_0, S_1, S_2, S_3, S_4, S_5$  quei sottosemigrupperi indicati prima rispettivamente con  $S_{00}, S_{01}, S_{11}, S_{12}, S_2, S_3$ ).

La decomposizione (8.1) è valida in generale, a parte il fatto che sono stati "eliminati" gli eventuali annullatori col passaggio al se migruppo quoziente (di Rees).

Ci chiediamo come si presenta tale decomposizione quando  $S$  è completamente regolare. In questo caso si ha:

$$S = S_2 \cup S_5$$

Vedremo nel seguito che  $S_5$  ha una struttura "molto vicina" a quella di gruppo (ed è unione di gruppi massimali in  $S$ , come anche  $S_2$ ).

Avendo  $S_2$  una struttura "simile" ad  $S$ , si congettura di poter fare una decomposizione di  $S_2$ :

$$S_2 = S_2^{(1)} \cup S_5^{(1)}$$

e poi di scomporre ancora  $S_2^{(1)}$ , e così via.

Si possono allora presentare due casi:

i) le decomposizioni non hanno termine; allora:

$$S = ( \dots ( \dots S_2^{(2)} \cup S_2^{(1)} \cup \dots ) \cup S_5^{(2)} \cup S_5^{(1)} \dots ) \cup S_5^{(0)}$$

ii) la decomposizione ha termine dopo un numero finito  $n$  di passi:

$$S = (\dots (S_2^n \cup S_5^n) \cup S_5^{n-1} \cup \dots) \cup S_5^{(0)};$$

Comunque si può sempre provare che:

$$S_5^i \cdot S_5^j \subseteq S_5^j \quad \text{e} \quad S_5^j \cdot S_5^i \subseteq S_5^j \quad \text{se} \quad i \geq j,$$

mentre nel caso ii) si ha:  $S_5 \cdot S_2^i \subseteq S_5$

Sarebbe interessante conoscere la struttura di  $S_2^n$ , ma il problema non è facile. Si può affermare che:

$$S_2^n = \bigcup_{\beta \in B} G_{e_\beta},$$

dove, se  $a \in S_2^n$ , si ha:  $a S_2^n \subset S_2^n$ .

### 9. Matrici di Rees.

Vogliamo ora occuparci della rappresentazione di semigrupp<sub>u</sub> mediante le matrici di Rees.

Sia  $G$  un gruppo con  $0$  ed  $I, M$  insiemi i cui elementi indichiamo con  $i, j, k, \dots$  e  $\mu, \nu, \xi, \dots$  rispettivamente. Se  $P$  è una applicazione di  $M \times I$  in  $G$ , indicheremo con  $p_{\mu i}$  l'elemento di  $G$  immagine di  $(\mu, i)$ .

Osserviamo che, se è data una applicazione  $P: M \times I \rightarrow G$ , allora

l'insieme  $I \times G \times M$  assume la struttura di semigruppo con l'operazione:

$$(i, a, \mu) (j, b, \nu) = (i, a p_{\mu j} b, \nu) \quad (9.1)$$

Chiamiamo matrice di Rees su  $G$  ad indici  $M \times I$  una matrice con al più un elemento diverso da  $0$ ; sia  $S$  l'insieme delle matrici di Rees su  $G$ .

Se  $P$  è una fissata matrice su  $G$ , possiamo definire una operazione binaria su  $S$  nel modo seguente:

$$A * B = A P B \quad \text{con } A, B \in S$$

dove il prodotto al secondo membro è l'ordinario prodotto "righe per colonne" fra matrici.

È facile verificare che  $S(*)$  è un semigruppo: lo chiamiamo semigruppo delle matrici di Rees sul gruppo  $G$  con matrice "sandwich"  $P$ . Osserviamo che questa costruzione porta agli stessi risultati visi prima ed il prodotto è ancora quello definito nella (9.1).

### Teorema 9.1

Sia  $S$  un semigruppo completamente semplice e  $G$  un suo sottogruppo con unità  $g (g \in E_S)$ . Indichiamo

$$I = \{ e \in E_S \mid e g = e \}$$

$$M = \{ f \in E_S \mid g f = f \}$$

e definiamo una applicazione  $P$  da  $M \times I$  in  $G$  ponendo  $p_{fe} = f e$ .

Con  $T$  indichiamo il semigruppoo  $I \times G \times M$  con l'operazione (9.1); allora l'applicazione  $\chi : S \rightarrow T$  definita da:

$$a \longrightarrow (e, g a g, f), \quad \text{dove } a g \in G_e, \quad g a \in G_f,$$

è un isomorfismo tra  $S$  e  $T$ .

Dimostriamo il teorema in quattro "passi".

i. Dimostriamo che  $p_{fe} = fe$  è un elemento di  $G$  e che gli idempotenti  $e, f$  di  $(e, g a g, f)$  sono determinati univocamente;

sia  $(f, e) \in M \times I$ ;  $p_{fe} = fe = (g f)(e g) = g(f e)g \subset g S g = G$ ;

sia ora  $a \in S$ ; se  $a g \in G_e$  allora esiste  $u \in I$  tale che  $u(ag) = e$ ; così

$$e g = u(ag)g = u(ag) = e \quad \text{e quindi } e \in I.$$

Analogamente si prova che  $f \in M$ .

ii. Proviamo che  $\chi$  è un omomorfismo;

siano  $a, a' \in S$  tali che  $ag \in G_e, ga \in G_f, a'g \in G_{e'}, ga' \in G_{f'}$ ;

allora

$$aa'g \in G_e, \quad gaa' \in G_{f'},$$

$$\begin{aligned} (a\chi)(a'\chi) &= (e, gag, f)(e', ga'g, f') = (e, (gag)(fe')(ga'g), f') = \\ &= (e, (ga)(gf)(e'g)(a'g), f') = (e, (ga)fe'(a'g), f') = \\ &= (e, (gaf)(e'a'g), f') = (e, (ga)(a'g), f') = (e, g(aa')g, f') = \\ &= (aa')\chi. \end{aligned}$$

iii. Proviamo che  $\chi$  è iniettiva;

sia  $a\chi = a'\chi$ ; allora:

$$(e, gag, f) = (e', ga'g, f') \Rightarrow e = e', f = f', gag = ga'g \Rightarrow$$

$$\Rightarrow ga = (ga)f = (ga)(gf) = (gag)f = (ga'g)f = (ga')(gf) =$$

$$= (ga')(gf') = (ga')f' = ga' ;$$

analogamente  $ag = a'g$  e poiché  $S$  è cancellabile debolmente, si

ha:

$$a = a'.$$

iv. Proviamo che  $\chi$  è suriettiva;

sia  $(e, x, f) \in T$  ( $x \in G$ ); se  $eg = e, gf = f$  allora (Teorema 7.6)

si ha  $ge = g = fg$ . Poniamo  $a = e x f$ ; si ottiene:

$$e(ag)e = e(exf)ge = (exf)gf = (exf)g = ag$$

e quindi  $ag \in G_e$ ; analogamente si prova  $ga \in G_f$  e dunque

$$gag = g(exf)g = (ge)x(fg) = gxg = x; \quad \text{abbiamo pertanto determinato}$$

$$a \in S \text{ } \}^1 \quad a\chi = (e, x, f).$$

Si è così provato che  $\chi$  è un isomorfismo.

### 10. Osservazioni.

Se  $S$  è un semigrupp su cui non si fanno ipotesi di "completa semplicità", lo si può "rappresentare" mediante un semigrupp di matrici?

Osserviamo intanto che se  $S$  è un semigruppò del tipo  $I \times G$ , considerati i sottoinsiemi:

$$H_{i\mu} = \{ (i, a, \mu) \mid a \in G \},$$

$$L_\mu = \{ (i, a, \mu) \mid i \in I, a \in G \},$$

$$R_i = \{ (i, a, \mu) \mid a \in G, \mu \in M \}.$$

si ha che  $H_{i\mu}$  è un gruppo  $\forall i, \mu$ ,  $L_\mu$  è un ideale sinistro  $\forall \mu$ ,  $R_i$  è un ideale destro  $\forall i$  e inoltre:

$$S = \bigcup H_{i\mu} = \bigcup L_\mu = \bigcup R_i.$$

### 11. Gruppi a destra (e a sinistra).

Vogliamo ora portare l'attenzione sulla struttura del sottoinsieme  $E_s$  degli elementi idempotenti. Se  $S$  è un semigruppò regolare nulla possiamo dire di  $E_s$  mentre qualcosa si sa quando  $S$  è completamente regolare. Ancora di più si conosce sulla struttura di  $E_s$  nel caso che  $S$  sia semplice.

È interessante vedere anche cosa accade quando  $E_s$  ha la struttura di semigruppò.

#### Teorema 11.1

Le seguenti proposizioni sono equivalenti:

- i)  $E_s$  è sottosemigruppò di  $S$ ;
- ii) se  $a \overset{e}{\vee} b$  sono inversi di  $a$  e  $b$ , allora  $b'a'$  è inverso



di  $a$   $b$ ;

iii)  $a = axa, b = byb \Rightarrow ab = abyxab$ .

Se poi  $S$  è regolare le precedenti proposizioni sono equivalenti a:

iv)  $e \in E_s \Rightarrow$  l'inverso di  $e$  è un idempotente.

Dim. i)  $\Rightarrow$  ii)

$a'a, bb' \in E_s$  e quindi anche  $(a'a)(bb') \in E_s$ , cioè

$$(a'a)(bb')(a'a)(bb') = (a'a)(bb') \quad \text{da cui:}$$

$$a(a'a)(bb')(a'a)(bb')b = a(a'a)(bb')b$$

$$(aa')(ab)(b'a')(ab)b'b = (aa')(ab)(b'b)$$

$$ab(b'a')ab = ab$$

e, similmente,  $b'a'(ab)b'a' = b'a'$

ii)  $\Rightarrow$  iii)

$xax$  e  $yby$  sono inversi di  $a$  e  $b$  (Teorema 2.6)

e quindi  $(yby)(xax)$  è un inverso di  $ab$ ; perciò:

$$ab = ab(yby)(xax)ab = a(byb)yx(axa)b = abyxab$$

iii)  $\Rightarrow$  i)

siano  $e_1, e_2 \in E_s$ ; poiché  $e_1 e_1 e_1 = e_1$ ,  $e_2 e_2 e_2 = e_2$

segue, applicando la iii), che:

$$e_2 e_1 = e_2 e_1 (e_1 e_2) e_2 e_1 = e_2 (e_1 e_1) (e_2 e_2) e_1$$

cioè  $e_2 e_1 = (e_2 e_1)(e_2 e_1)$  e quindi  $e_2 e_1 \in E_s$ .

iv)  $\Rightarrow$  i) (nell'ipotesi che  $S$  è regolare)

siano  $e, f \in E_S$  e sia  $x$  un inverso di  $e$  e  $f$ . Allora

$$fxe = f(xefx)e = (fxe)(fxe) = (fxe)^2 \quad \text{quindi } (fxe) \in E_S$$

$$(ef)(fxe)(ef) = e(ff)x(ee)f = (ef)x(ef) = ef$$

$$(fxe)(ef)(fxe) = fx(ee)(ff) = e = (fxe)(fxe) = fxe$$

e per la iv), essendo  $fxe$  inverso di  $ef$ , si conclude  $ef \in E_S$ .

iii)  $\Rightarrow$  iv)

sia  $e \in E_S$  e  $x$  inverso di  $e$ : essendo allora  $e = exe$ ,  $x = xex$

segue per la iii) che  $ex = ex(xe)ex$ ; pertanto:

$$\begin{aligned} x &= xex = (xe)(ex) = [(xe)(ex)] \cdot [(ex)(xe)] \cdot [(xe)(ex)] = \\ &= xee(xex)(xex)eex = (x \ e \ x)(x \ e \ x) = (xex)^2 = x^2, \end{aligned}$$

quindi  $x \in E_S$ .

Introduciamo ora la nozione di gruppo a destra (e a sinistra) con cui ci "avviciniamo" ancora di più alla struttura di gruppo.

Un semigruppoo  $S$  è detto gruppo a destra se è semplice a destra e se da  $ax = ay$  segue  $x = y$ . In altri termini si ha  $aS = S$ ,  $\forall a \in S$ , ed i prodotti  $ax$  "riproducono" una sola volta gli elementi di  $S$ .

Osserviamo che la definizione ora data equivale a dire che: per ogni  $a, b \in S$ , esiste un unico  $x$  tale che  $ax = b$ .

Dualmente si definiscono i gruppi a sinistra.

Teorema 11.2

Le seguenti proposizioni sono equivalenti:

- i)  $S$  è un gruppo a destra;
- ii) Per ogni  $a \in S$  esiste un unico  $x \in S$   $\exists!$   $a^2x = a$ ;
- iii)  $S$  è regolare ed  $E_S$  è uno zero semigruppato destro.

Dim. i)  $\Rightarrow$  ii) : ovvia

ii)  $\Rightarrow$  iii)

sia  $a^2x = a$ , allora:

$$a = a^2x = a(ax) = a(a^2x)x = a^2(ax^2) \Rightarrow x = ax^2;$$

se poi  $x = x^2y$  similmente si conclude che  $y = xy^2$ ,

da cui segue che  $ax = ax^2y = xy$ ;

$$y = xy^2 = (xy)y = (ax)y = a(ax) = a^2x = a.$$

Pertanto  $ax = xy = xa$ ; allora  $a = axa$  ed  $S$  è completam. regolare.

Siano ora  $e, f \in E_S$ ; per la ii) esiste  $z \in S$  tale che  $fe = (fe)^2z$

Quindi  $fe = (fe)^2ez$  e, per l'unicità:  $ez = z$

$$z = (fe)z^2 = f(fe)z^2 = fz \Rightarrow fe = (fe)^2z = z$$

$$z = ez \Rightarrow fe = efe$$

$$fe = (fe)^2(fe) = (fe)^2e \Rightarrow e = fe$$

iii)  $\Rightarrow$  i)

sia  $a \in S$  ed  $x, y$  suoi inversi, cioè:  $axa = a = aya$ ,  $xax = x$ ,  
 $yay = y$ .

Allora  $(ax)(xa) = xa$  (in quanto vale la iii) e  $ax, xa$  sono idempotenti) cioè  $xa = ax^2a$  e quindi  $a^2x^2a = axa = a$  per cui  $a \in a^2S$ ;

similmente si prova:  $a \in Sa^2$  e quindi  $S$  è completamente regolare ed è unione di gruppi in ognuno dei quali c'è solo un idempotente:

$S = \bigcup G_{e_\alpha}$ , con  $e_\alpha e_\beta = e_p$  a causa della iii). Pertanto

$e_\alpha G_\beta = G_\beta$  per ogni  $G_\beta$  ed in maniera univoca, per cui

$$e_\alpha S = S$$

Se  $a \in G_{e_\alpha}$  si ha:  $a e_\alpha S = aS = s$  ( $aS \supseteq aa'S = e_\alpha S = S$ )

Si può provare ancora che se  $S$  è un gruppo a destra,  $S$  è prodotto diretto di un suo sottogruppo  $G$  e di  $E_S$ :  $S = G \times E_S$

## 12. "Laterali" in un semigruppo.

Se  $G$  è un gruppo ed  $H$  un suo sottogruppo, si può decomporre  $G$  in laterali:  $G = H + Hg_1 + Hg_2 + \dots$ . Ci chiediamo se una decomposizione di questo tipo può trovarsi anche per i semigruppi. Il problema è il seguente:

se  $S$  è un semigruppo ed  $A$  un suo sottosemigruppo, è possibile

trovare un insieme  $C \subseteq S$  tale che  $C \cap A = \emptyset$  e  $S \setminus A = AC$ ?

Vedremo tra poco che è possibile caratterizzare i semigrupp che godono di questa proprietà.

Ricordiamo intanto che un elemento  $a \in S$  genera un gruppo (quando lo genera) univocamente determinato (la dimostrazione non presenta eccessiva difficoltà). Nel seguito indicheremo con  $\langle a \rangle$  il gruppo generato dall'elemento  $a \in S$  (quando esiste) e con  $[a]$  il sottosemigrupp generato da  $a$  (evidentemente  $[a] = \{a, a^2, a^3, \dots\}$ ).

Poniamo ora:

$$S_a = \begin{cases} \langle a \rangle & \text{se esiste e se } \sqrt{a} \text{ permuta con l'elemento neutro di } \langle a \rangle \\ [a] & \text{negli altri casi} \end{cases} \quad (12.1)$$

### Teorema 12.1

Sia  $S$  un semigrupp; se  $\forall S_a (a \in S)$ , esiste  $C$ , disgiunto da  $S_a$ , tale che  $S \setminus S_a = S_a C$ , allora  $S$  è unione di gruppi disgiunti ( $S = \bigcup G_i$ ) con  $e_i e_k = e_k (e_i \in G_i)$ .  $S$  risulta quindi essere un gruppo a destra.

Dim.

Dalle ipotesi si ha:  $S \setminus S_a = S_a B$ ,  $S \setminus S_{a^2} = S_{a^2} C$  con opportuni  $B$  e  $C$  sottoinsiemi di  $S$ . Vogliamo ora provare che  $S_a$  è un gruppo; supponiamo che  $S_{a^2}$  non sia un gruppo; se  $a \in S_{a^2}$ , allora  $a = a^{2r}$

per cui  $S_a = \{a, a^2, \dots, a^{2r-1}\}$  è un gruppo ( $2r$  sia il più piccolo esponente per cui si abbia l'uguaglianza).

Se invece  $a \in S_{a^2}C$ , allora  $a = a^{2r}c$ , per un opportuno  $c \in C$ ; proviamo che  $c \in S_a$ ; se non fosse vero, cioè se fosse  $c \in S_{a^2}C$ , allora si avrebbe:

$$a \in a^{2r} S_{a^2}C \subseteq S_{a^2}C : \text{assurdo poiché } a \in S_a.$$

Quindi è  $c \in S_a$ , cioè  $c = a^t$ , da cui

$$a = a^{2r} a^t = a^{2r+t}$$

e si conclude di nuovo che  $S_a$  è un gruppo. In entrambi i casi  $S_a$  è un gruppo (e quindi è tale anche  $S_{a^2}$ ): siamo giunti ad una contraddizione e quindi  $S_{a^2}$  è un gruppo.

Esiste pertanto  $\bar{a}$  tale che  $a^{2\bar{a}} = \bar{a}a^2 = e_{a^2}$ .

Se il gruppo è finito ed il suo ordine è  $n$ , si ha  $\bar{a} = a^{2(n-1)}$

si vede subito che  $e_{a^2}$  è elemento neutro anche per  $a$  e qui  $S_a$

è un gruppo. Se invece  $S_{a^2}$  è infinito procediamo come segue:

$$ae_{a^2} = e_{a^2}a \quad (\text{per la 12.1})$$

$$a(a^2 \bar{a}) = (a^2 \bar{a})a$$

$$a^2(a \bar{a}) = a^2(\bar{a} a)$$

$$a \bar{a} = \bar{a} a$$

da cui segue:

$$e_{a^2} = (\bar{a} a)a = (a \bar{a})a = a(\bar{a} a).$$

Pertanto  $a$  è in un gruppo che, ovviamente, contiene tutte le potenze di  $a$  (cioè contiene  $S_a$ ).  $S_a$  è allora un gruppo, per ogni elemento  $a \in S$ . Quindi ogni elemento di  $S$  è in un gruppo; consideriamo quelli massimali, che saranno anche disgiunti per ovvie considerazioni, e indichiamoli con  $G_i$  (le rispettive unità siano  $e_i$ ). Si ha così

$$S = \bigcup G_i, \quad e_i e_k = e_k \quad (12.2)$$

Supponiamo ora che valgano le (12.2); è evidente allora che vale  $e_i G_k = G_k$ ; proviamo che è anche  $G_i e_k = G_k$ .

È facile verificare che  $e_k G_i e_k$  è un gruppo con unità  $e_k$  e in cui l'inverso di  $e_k g_i e_k$  è  $e_k g_i^{-1} e_k$ . Allora  $e_k G_i e_k \subseteq G_k$ , cioè

$$G_i e_k \subseteq G_k.$$

Ma si ha anche:

$$G_i = G_i e_i = G_i e_k e_i \subseteq G_k e_i \subseteq G_i$$

da cui  $G_k e_i = G_i$ .

Questo significa che si può porre:

$$S = G(e_1 \cup e_2 \cup \dots) \quad (12.3)$$

con ovvio significato dei simboli ( $G$  è uno dei gruppi  $G_i$ ).

In conclusione si è provato che tutti e soli i semigrupperi per cui vale una decomposizione del tipo (12.3) sono i gruppi a destra.

Parte II - Algebre

73. 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 semigrupperi ( $S_2$ ) 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:

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

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:

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

Pertanto  $S_2$  è un semigruppero idempotente.

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



stenza di eventuali elementi idempotenti. Se però supponiamo che ne esista 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:

$$(a \times b)c = (a^P c) \times (b^P c) \quad (13.2)$$

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 (con  $\bar{a}$  idempotente di  $S_2$ ):

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

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

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

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:

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

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

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

$$c \times 1 = c, \quad c' \times 1 = c' \Rightarrow cc' = cc' \times 1 \quad (13.4)$$

Infatti:

$$cc' \times c' = cc' \quad (\text{dalle ipotesi } (13.4))$$

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

$$cc' \times c' = cc' \times 1 \quad (\text{fruttando la } (13.4))$$

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

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

Si può ancora verificare che:

$$c \times 1 = c \Rightarrow c^{-1} \times 1 = c^{-1} \quad (13.5)$$

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:

$$G_1 = \langle \langle c_1^{S_1} \rangle, \langle c_2^{S_1} \rangle, \dots \rangle \triangleleft S_1,$$

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

Allo stesso modo, considerati gli elementi  $b$  per cui:

$$1 \times b = b \quad (13.6)$$

si può provare che:

$$G_2 = \langle \langle b_1^{S_1} \rangle, \langle b_2^{S_1} \rangle, \dots \rangle \triangleleft S_1,$$

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

$$\text{Si ha: } G_1 \cap G_2 = 1.$$

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:

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

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

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

### 14. Osservazioni.

Cosa si può dire della struttura di  $S$  quando  $S_1$  è un semigruppone 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 semigruppato e non contiene semigruppato.

Su queste strutture non si conosce niente di più; si intuisce che esiste una connessione tra semigruppato 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  $a_1, a_2, \dots, a_n$  dei simboli con i quali definiamo delle potenze formali:  $a_1^{\alpha_1}, a_2^{\alpha_2}, \dots, a_n^{\alpha_n}$  con  $\alpha_i \in \mathbb{R}$ ,  $\alpha_i > 0$ . Supponiamo che queste potenze siano permutabili e, considerati tutti i prodotti del tipo:

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

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

Introduciamo un elemento unità  $\mathcal{E}$  e definiamo  $F^+$  l'insieme costituito dal semigruppò 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:

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

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

- 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)  $\varphi(a,bb',cb',d) = \gamma(b') \varphi(a,b,c,d)$  (15.2)

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

Ci chiediamo quando una tale struttura è un semigruppò.

Si può dare una condizione necessaria, e precisamente:

Se  $F^+ \times F^+ (\odot)$  è un semigruppò, 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 semigrupp.

Imponendo

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

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:

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

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:

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

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

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

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

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

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

ancora:

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

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

$$a\alpha(a) = \mathcal{E} \quad \text{cioè} \quad \alpha(a) = a^{-1}$$

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

$$\alpha(a) = \mathcal{E}, \alpha(b) = \mathcal{E} \Rightarrow \alpha(ab) = \mathcal{E}$$

e quindi gli elementi  $a$  tali che  $\alpha(a) = \mathcal{E}$  formano semigrupp.

Ciò può aiutare nello studio del gruppo.

Continuiamo ancora a ricavare dalle conseguenze sulle funzioni  $\alpha$  e  $\gamma$ .

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:

$$\alpha(a) = \gamma(a) \quad \text{per ogni} \quad a \in F^+ \cup \mathcal{E}$$

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

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

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

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

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)  $\varphi(bb', cb') = \alpha(b') \varphi(b,c)$
- iv)  $\varphi(a, \varepsilon) = \varepsilon$

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

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

### 16. Problemi vari.

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

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

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

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 semigrupp, ma non è facile ricavare altre informazioni.

Per accostarsi all'argomento è utile la seguente bibliografia:

J.B.Kim. - Mutants in the symmetric semigroups - *Czechosl. 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 semigroup - *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:

M. Harao - S. Naguki - Toulit Idirent Cellular Automata - *Journal of Computer and systems Science* 11 (1975), 171 - 185.

Parte III - Automi

17. Teoria degli automi

Il primo lavoro completo che si conosce su questo argomento è del 1961:

V.M. Gluskov - The abstract theory of automata (testo in russo).

Successivamente sono stati pubblicati altri lavori:

S. Ginsburg - An introduction to mathematical machine theory (1962)

M.A. Arbib - Theory of abstract automata (1969)

Deusseu F - Halbgruppen und automaten (1971)

Vi sono poi lavori più recenti.

In genere, quando si parla di automa si intende parlare di un "sistema" in cui si possono immettere informazioni, segnali, ecc. che modificano lo stato del sistema, da cui, intanto, vengono emesse informazioni trasformate, segnali, dati ecc.

Da un punto di vista assiomatico intendiamo per automa (Automa MEALY) una 5-pla

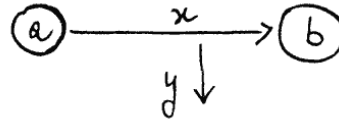
$$\mathcal{U} = (A, X, Y, \delta, \lambda)$$

dove  $A$  è l'insieme degli stati del sistema,  $X$  l'insieme dei segnali di entrata e  $Y$  l'insieme di quelli di uscita;  $\delta$  e  $\lambda$  sono funzioni:

$$\delta: A \times X \rightarrow A, \quad \lambda: A \times X \rightarrow Y$$

Ad esempio, se  $a$  e  $b$  indicano due stati di un sistema e  $x, y$  un segnale di entrata ed uno di uscita,

$\delta(a, x) = b$  e  $\lambda(a, x) = y$ , si ha

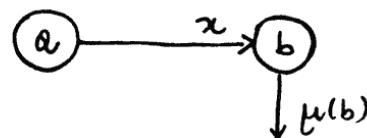


lo schema in figura.

Un automa lo diremo definito perfettamente quando  $\delta(a, x)$  è definito per ogni  $(a, x)$  e lo diremo deterministico se  $\delta$  e  $\lambda$  sono funzioni univoche. Parleremo poi di automa stocastico se è possibile dare una funzione di probabilità condizionata  $P(a', y | a, x)$ , che esprime la probabilità che l'automa assuma lo stato  $a'$  dopo il segnale  $y$  nell'ipotesi che sia nello stato  $a$  dopo il segnale  $x$ .

Un automa è poi detto di MOORE quando da  $\delta(a, x) = \delta(a', x')$  segue  $\lambda(a, x) = \lambda(a', x')$ . In questo caso il valore di  $\lambda$  dipende solo dallo stato finale  $\delta(a, x)$ , cioè

$\lambda(a, x) = \mu(\delta(a, x))$  e, ad esprimere  
re ciò, si scrive:



$$\mathcal{U} = (A, X, Y, \delta, \mu)$$

Continuiamo a dare altre definizioni.

Un automa lo diciamo iniziale quando uno dei suoi stati,  $a_0$ , è distinto dagli altri:  $\mathcal{U} = (A, a_0, X, Y, \delta, \lambda)$ ; quando  $\mathcal{U} = (A, X, \delta)$ , lo diciamo senza segnali di uscita; quando  $A$  è finito,  $\mathcal{U}$  si dice A-finito; quando sono finiti anche  $X$  e  $Y$ ,  $\mathcal{U}$  si dice finito.

Un automa  $\mathcal{U}$  con stato iniziale  $a_0$  lo diciamo di ROBIN-SCOTT quando esiste  $F \subset A$ ,  $F \not\ni a_0$ , i cui elementi sono privilegiati rispetto agli altri stati del sistema.

Un automa finito può essere descritto con una tabella del tipo delle tabelle di Cayley:

$\mathcal{U}$	a	b	c	...
x				
y				
z			$(\delta(c,z), \lambda(c,z))$	
⋮				

nel punto d'incontro tra la riga  $z$  e la colonna  $c$  è riportato la coppia di valori  $(\delta(c,z), \lambda(c,z))$ : se l'automa è senza segnale d'uscita va riportato solo il valore  $\delta(c,z)$ .

Quando l'automa è di Moore si mette in evidenza la funzione  $\mu$ , come si vede nella tabella seguente.

$\mathcal{U}$	$\mu$			
	a	b	c	...
x				
y				
z			$\delta(c,z)$	
⋮				

Un automa può essere descritto anche mediante un grafo, come vedremo in qualche esempio.

Prima di dare altre definizioni, richiamiamo il concetto di semigrupo libero.

Se  $X$  è un insieme, indichiamo con  $F(X)$  l'insieme delle "parole" formali, o sequenze finite, costituite da elementi di  $X$ . Se

$$p = x_1 x_2 \dots x_k \quad , \quad x_i \in X \quad (1 \leq i \leq k)$$

$$q = y_1 y_2 \dots y_l \quad , \quad y_i \in X \quad (1 \leq i \leq l)$$

sono due parole, definiamo il prodotto  $pq$  come segue:

$$pq = x_1 x_2 \dots x_k y_1 y_2 \dots y_l$$

Il prodotto è associativo e quindi  $F(X)$  è un semigruppo (semigrupp libero con base  $X$ ). Si può aggiungere la "parola vuota",  $e$ , e si ha allora l'elemento neutro.

Ora, se  $\mathcal{U} = (A, X, Y, \delta, \lambda)$  è un automa, possiamo considerare  $F(A)$ ,  $F(X)$ ,  $F(Y)$ , insiemi delle parole di stati, parole di entrata e parole di uscita, rispettivamente. Vogliamo prolungare  $\delta$  e  $\lambda$  a  $\bar{\delta}$ ,  $\bar{\lambda}$  in modo che:

$$\bar{\delta} : A \times F(X) \longrightarrow F(A) \quad \exists' \quad \bar{\delta}(a, e) = a$$

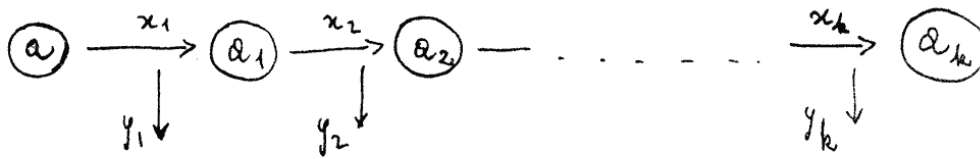
$$\bar{\lambda} : A \times F(X) \longrightarrow F(Y) \quad \exists' \quad \bar{\lambda}(a, e) = e$$

Se  $p = x_1 x_2 \dots x_k$ , definiamo  $\bar{\delta}(a, p) = a_1 a_2 \dots a_k$  e

$\bar{\lambda}(a, p) = y_1 y_2 \dots y_k$  dove:

$$a_1 = \delta(a, x_1), a_2 = \delta(a_1, x_2), \dots, a_k = \delta(a_{k-1}, x_k)$$

$$y_1 = \lambda(a, x_1), y_2 = \lambda(a_1, x_2), \dots, y_k = \lambda(a_{k-1}, x_k)$$



Per brevità indicheremo spesso con  $a_p$  lo stato finale.

Tale automa si dice sequenziale.

Si dice che un automa ha un sistema B di generatori per A ( $B \subset A$ ) quando per ogni stato  $a \in A$   $\bar{e}$  :  $a = bp$  con  $b$  e  $p$  opportuni elementi di  $B$  e  $F(X)$  rispettivamente.

$\mathcal{U}$  si dice ciclico quando esiste un sistema di generatori costituito da un solo elemento. Un automa iniziale si dice connesso inizialmente quando lo stato iniziale  $a_0$  genera  $A$ . Un automa ciclico si dice connesso fortemente quando ogni stato genera  $A$ .

Un automa  $\mathcal{U} = (A, F, \delta)$ , con  $F$  semigruppato, si dice quasi-automa quando :

$$\delta(a, fg) = \delta(\delta(a, f), g) \quad \text{per ogni } a \in A \text{ e } f, g \in F$$

### 18. Esempi di automi

1) Poniamo :  $A = \{a, b, c, d\}$  ,  $X = \{x, y\}$  ,  $Y = \{u, v\}$

$$\delta(b, x) = a$$

$$\delta(a, x) = \delta(c, x) = \delta(d, y) = b$$

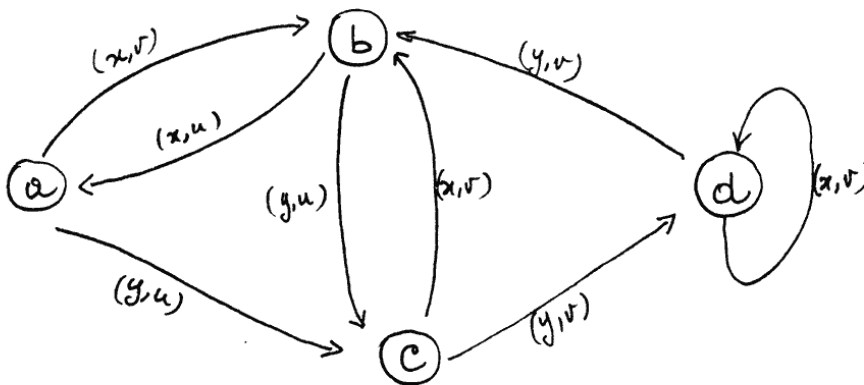
$$\delta(a,y) = \delta(b,y) = c$$

$$\delta(c,y) = \delta(d,x) = d$$

$$\lambda(a,y) = \lambda(b,x) = \lambda(b,y) = u$$

$$\lambda(a,x) = \lambda(c,x) = \lambda(c,y) = \lambda(d,x) = \lambda(d,y) = v$$

$\mathcal{U} = (A, X, Y, \delta, \lambda)$  è un automa di Moore il cui grafo è:



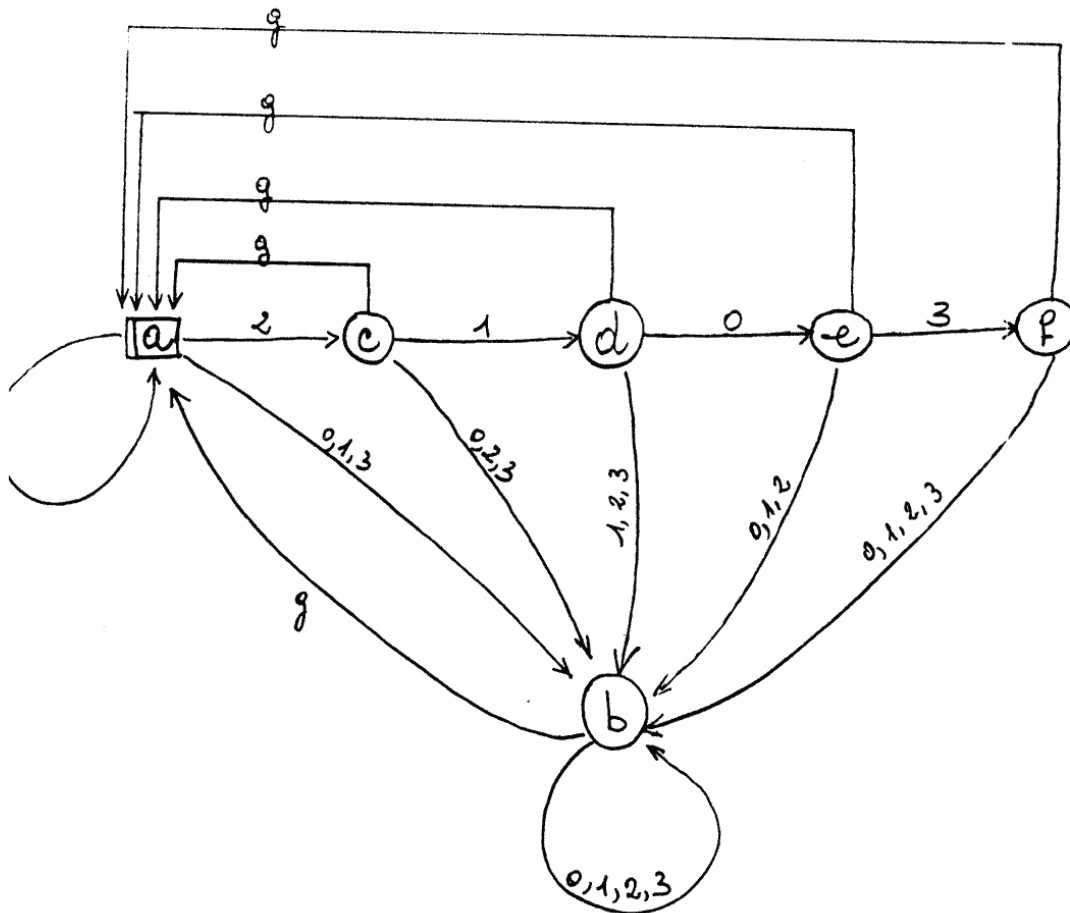
e la cui tabella è:

$\mathcal{U}$	u	v	u	v
	a	b	c	d
x	b	a	b	d
y	c	c	d	b

2) Sia  $A = \{a,b,c,d,e,f\}$  ,  $X = \{0,1,2,3,g\}$  ,  $F = \{f\}$

$\mathcal{U} = (A, a, X, \delta; F)$ , in cui  $\delta$  sarà definita mediante il grafo,  
 è un automa di Robin-Scott. Il suo grafo è:





Questo grafo rappresenta lo schema della serratura di sicurezza di una cassaforte per la quale  $f$  è l'unico stato in cui la cassaforte può essere aperta; la combinazione che sblocca la serratura è 2-1-0-3;  $g$  rappresenta il segnale "premere il pulsante".

3) Sia  $B = \{b_1, b_2, \dots, b_m\}$ ,  $X = \{x_1, x_2, \dots, x_n\}$  ed  $A$  l'insieme delle espressioni formali del tipo:

$$b_i x_{i_1} x_{i_2} \dots x_{i_k}, \quad b_i \in B, \quad x_{i_1}, \dots, x_{i_k} \in X$$

Per queste espressioni supponiamo che:

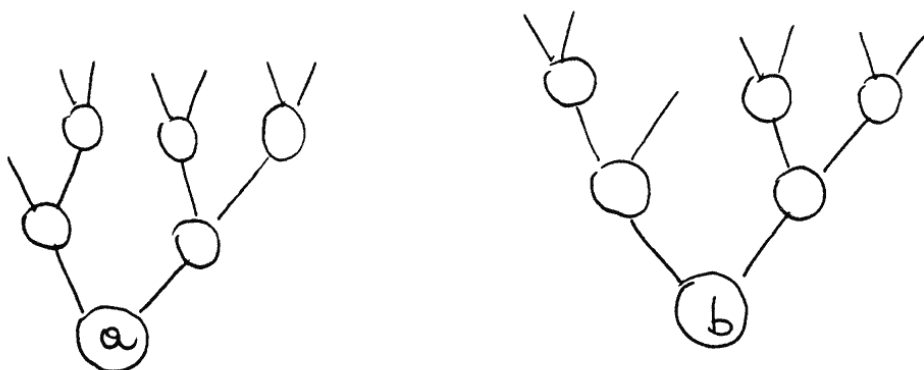
$$b_i x_{i_1} x_{i_2} \dots x_{i_k} = b_j x_{j_1} x_{j_2} \dots x_{j_\ell} \Leftrightarrow b_i = b_j, k = \ell, x_{i_1} = x_{j_1}, \dots$$

Posto  $\delta(b_i x_{i_1} x_{i_2}, \dots, x_{i_k}, x_j) = b_j x_{i_1} \dots x_{i_k} x_j$

si ha che:

$\mathcal{U} = (A, X, \delta)$  è un automa (automa libero)

Se  $B = \{a, b\}$  e  $X = \{x, y\}$ , il grafo dell'automa è del tipo detto ad albero:



19. Sottoautomi, automi superiori, automi inferiori

Per gli automi possono introdursi certi concetti usuali delle strutture algebriche.

Siano  $\mathcal{U} = (A, X, Y, \delta, \lambda)$  e  $\mathcal{U}' = (A', X', Y', \delta', \lambda')$  due automi. Si

dice che  $\mathcal{U}'$  è sottoautoma di  $\mathcal{U}$  se  $A' \subseteq A$ ,  $X' \subseteq X$ ,  $Y' \subseteq Y$  e  $\delta', \lambda'$  sono le restrizioni di  $\delta$  e  $\lambda$  rispettivamente. Se almeno uno degli insiemi  $A', X', Y'$  è incluso propriamente in  $A, X, Y$ , diciamo che  $\mathcal{U}'$  è sottoautoma proprio di  $\mathcal{U}$ . Se  $A' \subset A$ ,  $X' = X$ ,  $Y' = Y$  allora  $\mathcal{U}'$  si dice A-sottoautoma di  $\mathcal{U}$ .

Un sottoautoma  $\mathcal{U}'$  di  $\mathcal{U}$  si dice iniziale quando l'eventuale stato iniziale di  $A$  è anche stato iniziale di  $A'$ .

Sia ora  $B \subseteq A$ . chiamiamo  $A'$  l'insieme di tutti gli stati del tipo  $bp$  con  $b \in B$  e  $p \in F(X)$ ; allora  $\mathcal{U}' = (A', X, Y, \delta, \lambda)$  è un automa che viene detto sottoautoma generato da  $B$ .

Sia  $\mathcal{U} = (A, X, \delta)$  un automa senza segnali di uscita; chiamiamo centro dell'automata l'automata  $\mathcal{U}' = (A, X', \delta)$  dove:

$$X' = \{x \in X \mid axy = ayx, \quad \text{per ogni } a \text{ e per ogni } y\}$$

Introduciamo ora il concetto di omomorfismo d'automati.

Siano  $\mathcal{U} = (A, X, Y, \delta, \lambda)$ ,  $\mathcal{U}' = (A', X', Y', \delta', \lambda')$  due automati.

Diciamo che le applicazioni  $h_1: A \rightarrow A'$ ,  $h_2: X \rightarrow X'$ ,  $h_3: Y \rightarrow Y'$  costituiscono un omomorfismo da  $\mathcal{U}$  in  $\mathcal{U}'$  se accade:

$$h_1(\delta(a, x)) = \delta'(h_1(a), h_2(x))$$

$$h_3(\lambda(a, x)) = \lambda'(h_1(a), h_2(x)).$$

Evidente è la definizione di isomorfismo di automati.

Se esiste un omomorfismo da un automa  $\mathcal{U}$  su un automa  $\mathcal{U}'$ , diciamo che  $\mathcal{U}'$  è immagine omomorfa di  $\mathcal{U}$ .

Siano  $\mathcal{U}$  ed  $\mathcal{U}'$  due automi tali che  $X = X'$  e  $Y = Y'$ ; una applicazione  $h: A \rightarrow A'$  si dice A-omomorfismo da  $\mathcal{U}$  in  $\mathcal{U}'$  se accade che:

$$h(\delta(a, x)) = \delta'(h(a), x)$$

$$\lambda(a, x) = \lambda'(h(a), x)$$

(in questo caso il ruolo di  $h_2$  e  $h_3$  è svolto evidentemente dalle identità in  $X$  e  $Y$  rispettivamente).

Esempio

Siano  $\mathcal{U}$  ed  $\mathcal{U}'$  due automi le cui tabelle sono:

$\mathcal{U}$	a	b	c	d
x	(b,u)	(a,u)	(d,u)	(a,u)
y	(c,v)	(d,u)	(a,u)	(c,v)

$\mathcal{U}'$	1	2	3
x	(2,u)	(1,u)	(1,u)
y	(2,v)	(3,v)	(2,v)

e sia  $h: A \rightarrow A'$  così definita:

$$h(a)=1, \quad h(b)=h(c)=2, \quad h(d) = 3$$

Si può verificare che  $h$  è un A-omomorfismo,  $\mathcal{U}'$  è un'immagine omomorfa di  $\mathcal{U}$  ma, mentre  $\mathcal{U}$  è di Moore,  $\mathcal{U}'$  non lo è.

Come mostra l'esempio precedente, un omomorfismo tra automi non "con-

serva" la proprietà di "essere di Moore". Così, se  $\mathcal{N}$  ed  $\mathcal{U}$  sono di Moore, per mettere in evidenza questo fatto, si può far vedere che un omomorfismo "conserva" la proprietà di "essere di Moore" se accade che:

$$h_1(\delta(a, x)) = \delta'(h_1(a), h_2(x))$$

$$h_3(\mu(a)) = \mu'(h_1(a))$$

In maniera abbastanza ovvia si può parlare di endomorfismi di un automa in sè, di automorfismi, ecc..

Si può anche dimostrare che gli endomorfismi di un automa in sè formano semigruppato con la usuale operazione di prodotto.

Passiamo ora ad introdurre il concetto di automa fattoriale.

Diciamo che una relazione di equivalenza  $R$  (in  $A$ ) è una congruenza se:

$$aRb \Rightarrow \delta(a, x) R \delta(b, x) \wedge \lambda(a, x) = \lambda(b, x) \quad \text{per ogni } x \in X.$$

Se  $R$  è una congruenza, indicato con  $A_R$  l'insieme delle classi di equivalenza di elementi di  $A$ , definiamo:

$$\hat{\mathcal{U}} = (A_R, X, Y, \hat{\delta}, \hat{\lambda})$$

dove  $\hat{\delta}([a], x) = [\delta(a, x)]$

$$\hat{\lambda}([a], x) = \lambda(a, x)$$

Si può provare che la definizione è ben posta e che  $\hat{\mathcal{U}}$  è un automa, che definiamo automa fattoriale e indichiamo con  $\mathcal{U}/R$ .

A questo proposito si può provare un importante teorema.

Teorema 19.1

Sia  $\mathcal{U}$  un automa ed  $R$  una congruenza su  $A$ . Allora  $\mathcal{U}/R$  è immagine omomorfa di  $\mathcal{U}$ ; viceversa se l'automa  $\mathcal{U}'$  è immagine omomorfa di  $\mathcal{U}$ , esiste una congruenza  $R$  tale che  $\mathcal{U}' = \mathcal{U}/R$ .

(Omettiamo la dimostrazione).

Vogliamo ora introdurre il concetto di applicazione d'automa e di automa inferiore e superiore.

Sia  $p = x_1 x_2 \dots x_k \in F(X)$ ; diciamo che  $x_1 x_2 \dots x_i (i \leq k)$  è una parte iniziale di  $p$ ; se  $p = p_1 q p_2$ ,  $q$  non vuoto e  $\neq p$ , diciamo che  $q$  è una sottoparte propria di  $p$ .

Sia ora  $a \in A$ ; definiamo una applicazione  $\alpha_a: F(X) \longrightarrow F(Y)$  in modo che:  $\alpha_a(p) = \lambda(a, p)$ .

Se  $a$  è lo stato iniziale di  $\mathcal{U}$ , si scrive  $\alpha_{\mathcal{U}}$  invece di  $\alpha_a$  e si dice che è applicazione indotta da  $\mathcal{U}$ .

Una applicazione  $\alpha: F(X) \longrightarrow F(Y)$  si chiama applicazione d'automa se esiste un automa iniziale  $\mathcal{U}$  che induce  $\alpha$  (cioè tale che  $\alpha = \alpha_{\mathcal{U}}$ ).

Le applicazioni d'automa sono caratterizzate dal seguente teorema:

Teorema 19.2

Una applicazione  $\alpha: F(X) \rightarrow F(Y)$  è una applicazione d'automa se e solo se:

- i)  $\alpha$  conserva la lunghezza di ogni parola;
- ii) l'immagine di ogni parte iniziale è ancora una parte iniziale.

Omettiamo la dimostrazione del teorema, ma interessa rilevare che nella dimostrazione si usa una applicazione  $\alpha_p: F(X) \rightarrow F(Y)$  tale che  $\alpha(pq) = \alpha(p)\alpha_p(q)$ . Applicazioni di questo tipo, dette stati dell'applicazione  $\alpha$ , ci portano ad introdurre il concetto di automa inferiore nel modo seguente.

Sia  $A_\alpha$  l'insieme degli stati  $\alpha_p$  di una applicazione  $\alpha$ , al variare di  $p$  in  $F(X)$ . Si può provare allora che  $\mathcal{U}_\alpha = (A_\alpha, \alpha, X, Y, \delta_\alpha, \lambda_\alpha)$ , dove  $\delta_\alpha(\alpha_p, x) = \alpha_{px}$ ,  $\lambda_\alpha(\alpha_p, x) = \alpha_p(x)$ , è un automa, detto automa inferiore di  $\alpha$ .

Anche  $\mathcal{U}^\alpha = (F(X), \alpha, X, Y, \delta^\alpha, \lambda^\alpha)$ , dove  $\delta^\alpha(p, x) = px$ ,  $\lambda^\alpha(p, x) = \overline{\alpha(px)}$ , è un automa, detto automa superiore di  $\alpha$  (con  $\overline{\alpha(px)}$  intendiamo l'ultima lettera di  $\alpha(px)$ ).

A questo punto è possibile enunciare il

Teorema 19.3

Se  $\alpha$  è una applicazione d'automa e  $\mathcal{U}$  è connesso inizialmente, al-

lora  $\mathcal{U}_\alpha$  è immagine omomorfa di  $\mathcal{U}$  che, a sua volta, è immagine omomorfa di  $\mathcal{U}^\alpha$ .

20. Esempio

Sia  $X = \{x, y\}$ ,  $Y = \{u, v, w\}$  e  $\alpha: F(X) \longrightarrow F(Y)$  con le condizioni

- i)  $\alpha(e) = e$
- ii)  $\alpha(x^k) = u^k \quad (k \geq 1);$
- iii)  $\alpha(y^k) = v^k \quad (k \geq 1);$
- iv)  $p = x^k y^m q \implies \alpha(p) = u^k w^{m+1}$  dove  $m$  è la lunghezza di  $q$ ;
- v)  $p = y^k x^m q \implies \alpha(p) = v^k w^{m+1}$  dove  $m$  è la lunghezza di  $q$ .

Determiniamo gli stati di  $\alpha$ ; si ha:

$$\begin{aligned} \alpha(x^{k+1}) &= u^{k+1} = \alpha(x)\alpha_x(x^k) = u\alpha_x(x^k) \\ \alpha(xy^k) &= uw^k = \alpha(x)\alpha_x(y^k) = u\alpha_x(y^k) \\ \alpha(xx^k y^m q) &= u^{k+1} w^{m+1} = \alpha(x)\alpha_x(x^k y^m q) = u\alpha_x(x^k y^m q) \\ \alpha(xy^k x^m q) &= u v^{k+m+1} = \alpha(x)\alpha_x(y^k x^m q) = u\alpha_x(y^k x^m q) \end{aligned}$$

Quindi  $\alpha_x$  è definita come segue:



$$\alpha_x : \left\{ \begin{array}{l} e \longrightarrow e \\ x^k \longrightarrow u^k \\ y^k \longrightarrow w^k \\ x^k y^q \longrightarrow u^k w^{m+1} \\ y^k x^q \longrightarrow w^{k+m+1} \end{array} \right.$$

Pertanto  $\alpha_x \neq \alpha$  in quanto, ad esempio,  $\alpha(y^k) = v^k$  mentre  $\alpha_x(y^k) = w^k$ .

Facendo dei conti analoghi per  $\alpha_{x^2}$ , si vede che  $\alpha_x = \alpha_{x^2}$ .

Continuando a fare conti si prova che:

$$A_\alpha = \{\alpha, \alpha_x, \alpha_y, \alpha_{xy}\}$$

dove:

$$\alpha_y : \left\{ \begin{array}{l} e \longrightarrow e \\ x^k \longrightarrow w^k \\ y^k \longrightarrow v^k \\ x^k y^q \longrightarrow w^{k+m+1} \\ y^k x^q \longrightarrow v^k w^{m+1} \end{array} \right.$$

$$\alpha_{xy} : \begin{cases} e \longrightarrow e \\ x^k \longrightarrow w^k \\ y^k \longrightarrow w^k \\ x^k y^q \longrightarrow w^{k+m+1} \\ y^k x^q \longrightarrow w^{k+m+1} \end{cases}$$

Possiamo quindi considerare l'automa inferiore  $\mathcal{U}_\alpha$ , che risulta essere un automa di Moore.

La sua tabella è:

$\mathcal{U}_\alpha$	$\alpha$	$\alpha_x$	$\alpha_y$	$\alpha_{xy}$
x	$(\alpha_x, u)$	$(\alpha_x, u)$	$(\alpha_{xy}, w)$	$(\alpha_{xy}, w)$
y	$(\alpha_y, v)$	$(\alpha_{xy}, w)$	$(\alpha_y, v)$	$(\alpha_{xy}, w)$

Osserviamo che il grafo di  $\mathcal{U}_\alpha$  è un grafo ad albero.