Parte I - Semigruppi

Notazioni.

Per le applicazioni useremo la notazione destra, scriveremo cioè $a\varphi$ e $\varphi\psi$ per indicare rispettivamente $\varphi(a)$ e $\psi\circ\varphi$. Con ε_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:

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

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

$a\ R\ S\ b$ sse esiste $c \in M$ tale che $a\ R\ c$ e $c\ S\ b$.

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

$$(R\ S)\ T = R(S\ T) \tag{1.1}$$

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

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

$$(\bigcup_{i\in\mathfrak{J}} R_i)\ S = \bigcup_{i\in\mathfrak{J}} R_i\ S \qquad (1.2)$$

$$S(\bigcup_{i\in\mathfrak{J}} R_i) = \bigcup_{i\in\mathfrak{J}} S\ R_i \qquad (1.3)$$

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

$a\ (\bigcup_{i\in\mathfrak{J}} R_i)\ c$ *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* $a(\bigcup_{i\in\mathfrak{J}} R_i\ S)\ b$.

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:*

$$R \subseteq R' \Rightarrow R\ S \subseteq R'S \quad e \quad S\ R \subseteq S\ R' \qquad (1.4)$$

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

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

Si vede facilmente che:

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

$$(\bigcap_i R_i)^{-1} = \bigcap_i R_i^{-1} \tag{1.6}$$

$$(\bigcup_i R_i)^{-1} = \bigcup_i R_i^{-1} \tag{1.7}$$

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

La *relazione* <u>uguaglianza</u> E è definita come:

$$a\ E\ b \quad sse \quad a = b.$$

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

$O \subseteq R$, $R\ O = O\ R = O$ per ogni relazione R su M.

Una relazione R si dice che gode della proprietà:

1. <u>riflessiva</u> sse $a\ R\ a \quad \forall a \in M$ (cioè $E \subseteq R$)
2. <u>transitiva</u> sse $a\ R\ b$ e $b\ R\ c \Rightarrow a\ R\ c$ (cioè $RR \subseteq R$)
3. <u>simmetrica</u> sse $a\ R\ b \Rightarrow b\ R\ a$ (cioè $R^{-1} = R$)
4. <u>antisimmetrica</u> 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 <u>equivalenza</u> 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 π dell'insieme M, si può definire una relazione di equivalenza R (le cui classi di equivalenza sono proprio gli elementi della partizione π).

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 relaz. d'equ.za sse R S = S R

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

Dim.

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

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

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

$\underline{E} \subseteq S = E\ S \subseteq \underline{R\ S}$ (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 <u>applicazione naturale</u> φ intendiamo l'applicazione da M su M/R tale che $a\varphi = [a]$ per ogni elemento a di M.

2. Semigruppi 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 semigruppo. Un sottoinsieme A di un semigruppo S lo diciamo sottosemigruppo se è chiuso rispetto al prodotto in S. Se $A \subseteq S$, l'insieme dei prodotti finiti di elementi di A è un sottosemigruppo che chiamiamo sottosemigruppo generato da A e indichiamo con $< A >$. Il sottosemigruppo generato da un solo elemento a di S, cioè $< a >$, lo chiamiamo sottosemigruppo ciclico generato da a.

Se $< a > = S$ per qualche $a \in S$, diremo che S è un semigruppo ciclico.

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

Con ciò si è provato il

Teorema 2.1

Sia $A \subseteq S$: allora $< A >$ 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 $a, a^2, \ldots\ldots a^m, \ldots a^{n-1}$, e inoltre $\{ a^m, \ldots\ldots a^{n-1} \}$ è un gruppo ciclico di ordine $n - m$ la cui unità è a^{m+k_o} con $k_o \geq 0$ e $m + k_o \equiv 0 (n - m)$.

Sia $T \subseteq S$: diciamo che T è un <u>ideale sinistro</u> (<u>destro</u>) 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 <u>ideale</u>.

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 $\Leftrightarrow$ $S\,T \subseteq T$, $T\,S \subseteq T$

<u>Teorema 2.2</u>

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

$L(A) = \bigcap L_i$ con L_i ideale sinistro, $L_i \supseteq A$

$R(A) = \bigcap R_i$ con R_i ideale destro , $R_i \supseteq A$

$J(A) = \bigcap J_i$ con J_i ideale , $J_i \supseteq A$

Chiamiamo $L(A)$ ($R(A)$) <u>ideale sinistro</u> (<u>destro</u>) <u>generato da A</u> e $J(A)$ <u>ideale generato da A</u>.

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 semigruppo S è <u>semplice a sinistra</u> (<u>a destra</u>) se non contiene ideali sinistri (destri) propri. S si dice <u>semplice</u> se non contiene ideali propri.

Si vede subito che:

S semplice a sinistra $\iff S\,a = S$, 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 semigruppi semplici a destra.

L'intersezione di tutti gli ideali di S si chiama <u>nucleo</u> di S.

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

Teorema 2.3

Se J è ideale semplice di S (cioè non contiene ideali propri di S), allora J è il nucleo di S.

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

Un elemento $e \in S$ è chiamato 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.

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

Se, considerato $a \in S$, esiste $z \in S$ tale che $a\,z = z$ ($za = z$) 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 $a\,b = z$, 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 $S^\bullet = S \cup \{0\}$ con le condizioni $0\,a = a\,0 = 0$ per ogni $a \in S^\bullet$.

Diciamo che S è un <u>semigruppo zero a sinistra</u> (<u>a destra</u>) se $a\,b = a$ $(a\,b = b)$ per ogni $a,b \in S$. Se $0 \in S$ e se $a\,b = 0$ per ogni $a,b \in S$, allora diciamo che S è un <u>semigruppo zero.</u>

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

Altre definizioni utili sono:

$C(s) = \{ a \in S \mid a\,s = s\,a \}$ (<u>centralizzatore di s</u>);

$C = \{ a \in S \mid a\,s = s\,a$ per ogni $s \in S\}$ (<u>centro di S</u>).

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

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

Un elemento a di S lo diciamo <u>idempotente</u> se $aa=a$; un semigruppo S lo diciamo <u>idempotente</u> se ogni suo elemento è idempotente.

Un semigruppo S idempotente e commutativo lo diciamo <u>semi reticolo</u>.

<u>Teorema 2.4</u>

Sia e un elemento idempotente di S. Poniamo:

$G_e = \{ a \in S \mid a = ea = ae\ ,\ e = aa' = a'a$ 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 semigruppo; per completare la dimostrazione basta far vedere che, fissato $a \in G_e$ $a' \in G_e$ ed 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:

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

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:

$$a = e x = y e \qquad \text{con} \qquad e = a z = w a$$

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.

Pertanto $G'_e = G_e$

Diamo ancora alcune definizioni.

Un elemento a $\in$ S *lo diciamo* <u>regolare</u> *se* a = a x a *per qualche* x $\in$ S.

Un semigruppo lo diciamo <u>regolare</u> *se è regolare ogni suo elemento.*

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

<u>Teorema 2.6</u>

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

<u>Dim.</u> 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* <u>accrescitivo a sinistra</u> (<u>a destra</u>) *se accade* a S' = S (S'a = S), *con* S' $\subset$ S.

3. Esempi di semigruppi.

1) *Sia* S *un insieme non vuoto: si definisca*

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

S è allora un semigruppo (semigruppo di Kronecker)

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

3) Sono semigruppi 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 semigruppi consiste nel "classificare" i semigruppi.

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

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

ed ha inizio la teoria dei gruppi.

5. Partizioni di semigruppi.

Ci proponiamo ora di costruire una partizione di semigruppi in sottosemigruppi 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 $\mathcal{J}$ è un ideale del semigruppo S, la relazione R definita da:

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

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

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

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

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

Sia quindi S *un semigruppo senza annullatori. Definiamo:*

$$S_0 = \{ a \in S \mid a\,x = 0 \text{ , per qualche } x \neq 0\}$$

$$S_1 = \{ a \in S \setminus S_0 \mid a\,x = a\,y;\ x,y \in S,\ x \neq y\}$$

$$S_2 = \{ a \in S \setminus (S_0 \cup S_1) \mid a\,S \subset S \} \tag{5.1}$$

$$S_3 = \{ a \in S \setminus (S_0 \cup S_1) \mid a\,S = S\}$$

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

$$S = S_0 \cup S_1 \cup S_2 \cup S_3 \tag{5.2}$$

A sua volta S_0 *ed* S_1 *possono decomporsi in sottosemigruppi nel modo seguente:*

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

con

$$S_{00} = \{a \in S_0 \mid a\,S \subset S\} \quad , \quad S_{01} = \{a \in S_0 \mid a\,S = S\}$$

$$S_{11} = \{a \in S_1 \mid a\,S \subset S\} \qquad S_{12} = \{a \in S_1 \mid a\,S = S\} \tag{5.3}$$

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 *(cioè: elementi tali che* $aT = S$ *con* $T \subset S$).

E ancora, se $a \in S_{12}$ *e* x,y *sono elementi distinti 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 a S 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 sottosemigruppi ora visti esistono alcuni legami; più precisamente:

$S_3 S_2 \subseteq S_2$ $\qquad$ $S_2 S_3 \subseteq S_2$

$S_2 S_1 \subseteq S_1$ (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 sottosemigruppo) 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 $s_3 s_2 S \subset S$ (essendo $s_2 S \subset S$) e quindi $s_3 s_2 \in S_2$.

6. Osservazioni.

Tra i problemi ancora aperti in teoria dei semigruppi, notevole importanza ha quello di trovare una decomposizione disgiunta di un semigruppo 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 semigruppi.

Szep ha descritto completamente ciò che accade nel caso finito commutativo.

In generale, nel caso finito, è stato provato che

$$S = S_{00} \cup S_{11} \cup S_3 .$$

7. Semigruppi completamente regolari e completamente semplici.

Sempre in riferimento alla ricerca di cui al paragrafo precedente, è interessante la possibilità di decomporre un semigruppo in sottosemigruppi con una struttura "molto vicina" a quella dei gruppi. Introduciamo, a questo scopo, i semigruppi 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 semigruppo 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 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.

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

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

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

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

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

$$e^2 = (xa)(ay) = (xa^2)y = ay = e \quad ed \quad e \in Sa \cap a S$$

quindi $a \in G_e$ *che è un gruppo;*

$v) \Rightarrow i)$: *ovvio.*

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

Sia $\mathcal{C}$ *una classe di semigruppi. Un semigruppo* S *si dice* <u>semi reticolo di semigruppi</u> *se esiste una congruenza le cui classi di equivalenza sono tutte in* $\mathcal{C}$.

<u>Teorema 7.2</u>

S *sia un semireticolo di semigruppi,* $S = \bigcup S_\alpha$, $\alpha \in \mathcal{J}$.

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

Se S è un semigruppo ed $\mathcal{J}$ un suo ideale, diciamo che $\mathcal{J}$ è un <u>ideale primo</u> se accade che: $a\,S\,b \subseteq \mathcal{J} \Rightarrow a \in \mathcal{J}$ o $b \in \mathcal{J}$.

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

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

<u>Teorema 7.3</u>

Sia S un semigruppo; 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.

<u>Dim.</u> 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)

poichè 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 $x \in S$ t.c. $a = axa^2$ e ancora $(xa)y(xa)^2 = xa$

per qualche $y \in S$; quindi:

$$a = axa^2 = a(xa)a = a(xa)y(xa)^2a = (axayx)(axa^2) =$$

$$= axayxa = axay(xa) = (axay)(xa)y(xa)^2 = ay(xa)^2 =$$

$$= (ayx)a(xa) = (ayx)(axa^2)(xa) = (ay)(xa)^2(axa) =$$

$$= a(axa) = a^2xa \qquad \textit{cioè} \quad a \in a^2S \; a \subseteq a^2S;$$

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:

$x^2 \in \mathcal{J} \Rightarrow x^2 \in G_e$, *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*

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

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 semigruppo* S.

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

$$e \leq f \iff e = ef = fe$$

(La verifica è banale).

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

<u>Teorema 7.4</u>

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

<u>Dim.</u>

$a \in S \Rightarrow a = axa$ per qualche $x \in S \Rightarrow a^2 = a^2ya^2$ per qualche $y \in S$; poniamo $e = ax$, $f = a^2yax$; e ed f sono elementi idempotenti; infatti:

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

$$f^2 = (a^2yax)^2 = a^2yaxa^2yax = a^2y(axa)ayax = (a^2ya^2)yax =$$

$$= a^2yax = f$$

inoltre:

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

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

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

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

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:

$x \in a\ S\ a \Rightarrow x = aya$ *per qualche* $y \Rightarrow x \in G_f$ *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 semigruppo S *è* <u>completamente semplice</u> *se è semplice ed ogni suo elemento idempotente è primitivo (cioè minimale in* E_s*).*

S *si dirà poi* <u>cancellabile debolmente</u> *se da* $ax = bx$ *e* $xa = xb$ *segue* $a = b$.

Possiamo caratterizzare i semigruppi completamente semplici con il seguente teorema.

<u>*Teorema 7.5*</u>

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) ⇒ ii)*

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

Poniamo $f = evaeyexeaue$; *si ha:*

$f^2 = evaeyexea(ueev)aeyexeaue = evaeye(xea^3ey)exeaue =$

$= evaeyexeaue = f$;

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

Pertanto $a = uev = ufv = (uev)aeyexea(uev) =$

$= a^2(eyexe)a^2 \in a^2 S a^2$

e quindi S *è completamente regolare.*

ii) ⇒ iii)

siano $e, f \in E_S$, $e \leq f$; *essendo* S *semplice si ha* $f = xey$ *con opportuni* $x,y \in S$; *poniamo* $a = fxf$, $b = fyf$. *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) $\Longrightarrow$ 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

$$ay = aexe = (ae)xe = axe = bxe = bexe = by \ ,$$

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

iv) $\Longrightarrow$ v)

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

v) $\Longrightarrow$ i)

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

$$f = fef = ef = fe \qquad \text{da cui} \qquad e = f$$

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 semigruppo completamente semplice ed* $e, f \in E_S$, *allora valgono le seguenti proposizioni:*

i) $a, b \in S, \quad ab \in G_e \Rightarrow a\,S\,b \subseteq G_e$;

ii) $e\,f = e \Rightarrow f\,e = f$;

iii) $f\,e = e \Rightarrow e\,f = f$.

Dim. Proviamo la i).

Sia $a \in G_g$, $b \in G_h$, $a\,b \in G_e$; *allora* $a\,b\,a \in G_g$, $b\,a\,b \in G_h$;

$a = (aba)u$, $b = v(bab)$ *con opportuni* u e 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)

$e\,f = f \Rightarrow f\,e \in E_S$ *e poichè* $f\,e = f\,e\,f \in G_f$, *si ha* $f = f\,e$.

Analogamente si prova anche la iii)

8. Osservazioni.

Abbiamo visto come un semigruppo S *si può decomporre in sottosemigruppi :*

$$S = S_0 \cup S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \qquad (8.1)$$

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

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 sottosemigruppi 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 semigruppo 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:

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

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

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

Comunque si può sempre provare che:

$$S_5^i \cdot S_5^j \subseteq S_5^j \qquad e \quad S_5^j \cdot S_5^i \subseteq S_5^j \qquad se \quad i \geqslant j ,$$

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:*

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

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 semigruppi mediante le matrici di Rees.

Sia G *un gruppo con* O *ed* I,M *insiemi i cui elementi indichiamo con* i,j,k..... *e* $\mu, \nu, \varepsilon, \ldots\ldots$ *rispettivamente. Se* P *è una applicazione di* M x I *in* G, *indicheremo con* $p_{\mu i}$ *l'elemento di* G *f.* immagine di (μ, i).

Osserviamo che, se è data una applicazione P: M x I ⟶ G, *allora*

l'insieme I x G x M *assume la struttura di semigruppo con l'opera-*
zione:

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

Chiamiamo matrice di Rees su G ad indici M x 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:*

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

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

E' 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 visti 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 x I *in* G *ponendo* p_{fe} = f e.

Con T *indichiamo il semigruppo* I x G x M *con l'operazione (9.1);*
allora l'applicazione $\chi : S \longrightarrow T$ *definita da:*

$a \longrightarrow (e, g\,a\,g, f)$, *dove* $a\,g \in G_e$, $g\,a \in G_f$,

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* $u \ni' u(ag) = e$; *così*

$e\,g = u(ag)g = u(ag) = e$ *e quindi* $e \in I$.

Analogamente si prova che $f \in M$.

ii. Proviamo che χ *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

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

$(a\chi)(a'\chi) = (e,gag,f)(e',ga'g,f') = (e,(gag)(fe')(ga'g),f') =$

$= (e,(ga)(gf)(e'g)(a'g),f') = (e,(ga)fe'(a'g),f') =$

$= (e,(gaf)(e'a'g),f') = (e,(ga)(a'g),f') = (e,g(aa')g,f') =$

$= (aa')\chi$.

iii. Proviamo che χ 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 poichè S è cancellabile debolmente, si ha:

$a = a'$.

iv. Proviamo che χ 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

$gag = g(exf)g = (ge)x(fg) = gxg = x$; abbiamo pertanto determinato

$a \in S$ $\exists'$ $a\chi = (e,x,f)$.

Si è così provato che χ è un isomorfismo.

10. Osservazioni.

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

Osserviamo intanto che se S *è un semigruppo del tipo* IxG. *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_{μ} *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 semigruppo 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.*

E' interessante vedere anche cosa accade quando E_S *ha la struttura di semigruppo.*

Teorema 11.1

Le seguenti proposizioni sono equivalenti:

i) E_S *è sottosemigruppo di* S;

ii) se a' *e* 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*

$(a'a)(bb')(a'a)(bb') = (a'a)(bb')$ *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 $e_1, e_2 \in E_s$; *poichè* $e_1 e_1 e_1 = e_1$, $e_2 e_2 e_2 = e_2$

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 f. *Allora*

$fxe = f(xefx)e = (fxe)(fxe) = (fxe)^2$ *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:*

$$x = xex = (xe)(ex) = \big[(xe)(ex)\big] \cdot \big[(ex)(xe)\big] \cdot \big[(xe)(ex)\big] =$$

$$= xee(xex)(xex)eex = (x\ e\ x)(x\ e\ x) = (xex)^2 = x^2,$$

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 semigruppo S *è detto* <u>*gruppo a destra*</u> *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 <u>*gruppi a sinistra*</u>.

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 semigruppo destro.*

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

ii) $\Rightarrow$ *iii)*

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

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

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 $fe = (fe)^2e\ z$ *e, per l'unicità:* $e\ z = z$

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

$z = e\ z \implies fe = e\ fe$

$fe = (fe)^2(fe) = (fe)^2e \implies e = f\ e$

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 idem*potenti) *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_β *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:* $G = H + Hg_1 + Hg_2 + \ldots\ldots$. *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 semigruppi 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 sottosemigruppo generato da a (evidentemente $[a] = \{a, a^2, a^3 \ldots\}$).

Poniamo ora:

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

Teorema 12.1

Sia S un semigruppo; 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 $S_a = \{a, a^2, \ldots, a^{2r-1}\}$ 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 $c \in S_a C$, allora si avrebbe:

$a \in a^{2r} S_a C \subseteq S_a C$: assurdo poichè $a \in S_a$.

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:

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

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

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

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

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

$$S = \bigcup G_i \quad , \qquad e_i e_k = e_k \tag{12.2}$$

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

E' 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:

$$S = G(e_1 \cup e_2 \cup \ldots\ldots) \tag{12.3}$$

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

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