

OMOMORFISMI di SEMIGRUPPO e di GRUPPO. (170)

Siano $(X, *)$ e (Y, \square) due semigruppi (in particolare due semireticoli). Per l' OSS. 1 pag 167 si ha

OSS.1. Se $f: (X, *) \rightarrow (Y, \square)$ è un omomorfismo e S è un sottosemigruppo di $(X, *)$, anche l'immagine $f(S)$ è un sottosemigruppo di (Y, \square) .

Se poi $(X, *)$ e (Y, \square) sono monoidi e $f: X \rightarrow Y$ è un omomorfismo di monoidi, cioè $\forall a, b \in X$

$$f(a * b) = f(a) \square f(b) \quad e \quad f(u_X) = u_Y$$

l'immagine di un sottomonide di X è un sottomonide di Y . Se $(X, *)$ e (Y, \square) sono gruppi, la seconda condizione è garantita dalla prima. Infatti:

OSS.2 Se $(X, *)$ e (Y, \square) sono gruppi e $f: X \rightarrow Y$ è un omomorfismo di semigruppi, allora l'immagine $f(S)$ di ogni sottogruppo S di $(X, *)$ è un sgr. di (Y, \square) . In particolare $f(X)$ è un sgr. di (Y, \square) .

Dim. Osserviamo che

1) $u_X * u_X = u_X \Rightarrow f(u_X) = f(u_X * u_X) = f(u_X) \square f(u_X)$
 cioè l'elem. $f(u_X)$ è idempotente nel gruppo $(Y, \square) \Rightarrow f(u_X) = u_Y$ poiché il neutro è l'unico idempotente di Y .

2) $\forall a \in X : u_Y = f(u_X) = f(a * a^{-1}) = f(a) \square f(a^{-1}) = f(a^{-1} * a) = f(a^{-1}) \square f(a)$
 cioè $f(a^{-1})$ è l'inverso in Y di $f(a)$: $(f(a))^{-1} = f(a^{-1})$.

Dunque $\forall b_1, b_2 \in f(S)$, cioè t.c. esistono $a_1, a_2 \in S$ con $b_1 = f(a_1)$ e $b_2 = f(a_2)$ si ha

$$b_1 \square b_2^{-1} = f(a_1) \square [f(a_2)]^{-1} \stackrel{\text{per (2)}}{=} f(a_1) \square f(a_2^{-1}) = f(a_1 * a_2^{-1}) \in f(S)$$

c.v.d.

OSS. 3 Siano $(X, *)$ e (Y, \square) due gruppi e sia (171)
 $f: X \rightarrow Y$ un omomorfismo. L'insieme
 $f^{-1}(u_Y) = \{a \in X \mid f(a) = u_Y\}$

è un sottogruppo di $(X, *)$ che viene detto
nucleo di f e denotato con $\ker f$. VEDI pag 01

Dim. $\forall a, b \in \ker f \subseteq X$ si ha

$$f(a * b^{-1}) = f(a) \square f(b^{-1}) = f(a) \square (f(b))^{-1} = u_Y \square (u_Y)^{-1} = u_Y$$

cioè $a * b^{-1} \in \ker f$. c.v.d.

Notiamo che $\ker f$ contiene certamente il neutro u_X di X
ma può contenere anche altri elementi. Per vedere
quando $\ker f$ si riduce a $\{u_X\}$ serve la

OSS. 4. Siano $(X, *)$ e (Y, \square) due gruppi e sia

$f: X \rightarrow Y$ un omomorfismo. Se $a, b \in X$, si ha

$$f(a) = f(b) \Leftrightarrow a * b^{-1} \in \ker f,$$

(o alternativamente) $b^{-1} * a \in \ker f$.

$$\begin{aligned} \text{Dim. } f(a) = f(b) &\Leftrightarrow f(a) \square (f(b))^{-1} = u_Y \Leftrightarrow \\ &\Leftrightarrow f(a) \square f(b^{-1}) = u_Y \Leftrightarrow \\ &\Leftrightarrow f(a * b^{-1}) = u_Y \Leftrightarrow \\ &\Leftrightarrow a * b^{-1} \in \ker f \end{aligned}$$

L'altra formula si ricava partendo da

$$f(a) = f(b) \Leftrightarrow (f(b))^{-1} \square f(a) = u_Y.$$

Nota: ciò vale in particolare per le applicazioni lin. tra sp. vett.¹ VEDI O2 c.v.d.

COROLLARIO 5. Siano $(X, *)$ e (Y, \square) due gruppi.

$f: X \rightarrow Y$ è un monomorfismo $\Leftrightarrow \ker f = \{u_X\}$.

Dim. monomorfismo significa che f è iniettivo.

Sia f iniettiva: poiché $\ker f = u_X$ e ci deve essere 1 solo $a \in X$
t.c. $f(a) = u_Y$ si ha $\ker f = \{u_X\}$. Viceversa, se $\ker f = \{u_X\}$
e $f(a) = f(b)$ si deve avere $a * b^{-1} \in \ker f$ cioè $a * b^{-1} = u_X$
cioè $a = b$. c.v.d.

Dall'oss. 4 ricavo qual è la forma degli elem.^b di X che hanno la stessa immagine $f(a)$: (172)

$$\begin{aligned} f(b) = f(a) &\Leftrightarrow b * a^{-1} \in \ker f \Leftrightarrow \exists k \in \ker f \mid b * a^{-1} = k \\ &\Leftrightarrow \exists k \in \ker f \text{ t.c. } b = k * a. \end{aligned}$$

Denoto questo insieme di elementi (preimmagini di $f(a)$) con $(\ker f) * a$ e lo chiamo laterale destro di $\ker f$ individuato da a .

Tale insieme coincide con l'insieme

$$a * (\ker f) = \{ a * k, k \in \ker f \}$$

che chiamerò laterale sinistro di $\ker f$ individuato da a .

Inoltre la seconda formulazione dell'oss. 4 dice:

$$\begin{aligned} f(b) = f(a) &\Leftrightarrow a^{-1} * b \in \ker f \Leftrightarrow \exists k \in \ker f \mid a^{-1} * b = k \\ &\Leftrightarrow \exists k \in \ker f \text{ t.c. } b = a * k. \end{aligned}$$

Più in generale, se H è un sottogruppo di $(X, *)$ definisco

laterale destro di H mediante $a \in X$ l'insieme

$$H * a = \{ h * a, h \in H \}$$

laterale sinistro di H mediante $a \in X$ l'insieme

$$a * H = \{ a * h, h \in H \}.$$

Se $(X, *)$ è un gruppo abeliano $h * a = a * h$, $\forall a, h$ e quindi

$$H * a = a * H.$$

Se $(X, *)$ non è abeliano questa situazione può verificarsi (ad es. per sgr. che sono nuclei di un omomorfismo) oppure no.

$$\text{Si ha } H * a = a * H \Leftrightarrow \forall h_1 \in H \quad \exists h_2 \in H \mid h_1 * a = a * h_2$$

$$\text{cioè } a^{-1} * h_1 * a = h_2 \in H$$

$$\text{e } a * h_1 a^{-1} = h_2 \in H$$

$$H * a \subseteq a * H$$

$$\text{e } \forall h_1 \in H \quad \exists h_2 \in H \mid a * h_1 = h_2 * a$$

$$a * H \subseteq H * a$$

Esempio di sottogruppo avente laterali destri e sinistri (mediante uno stesso elemento a) diversi:

In (S_3, \circ) considero il sgr. $H = \{ \text{id}, (12) \}$

Si ha

$$H \circ (13) = \{ (13), (132) \} = H \circ (132)$$

$$H \circ (23) = \{ (23), (123) \} = H \circ (123)$$

$$H \circ (12) = \{ (12), \text{id} \} = H \circ \text{id} = H$$

123
321 ↓ (13)
312 ↓ (12)

Dettaglia
pag 03

Quindi

$$(13) \circ H = \{ (13), (123) \} = (123) \circ H$$

$$(23) \circ H = \{ (23), (132) \} = (132) \circ H$$

$$(12) \circ H = \{ (12), \text{id} \} = H$$

$$\Rightarrow H \circ (13) \neq (13) \circ H \quad \& \quad H \circ (23) \neq (23) \circ H.$$

Questo dice che H non può essere il nucleo di un omomorfismo da (S_3, \circ) a un altro gruppo. La stessa cosa succede con i sottogruppi $\{ \text{id}, (13) \}$ e $\{ \text{id}, (23) \}$.

Quindi $K = \{ \text{id}, (123), (132) \}$ ha due laterali destri:

$$K \circ (12) = \{ (12), (13), (23) \} = K \circ (13) = K \circ (23)$$

$$\& \quad K \circ \text{id} = K \circ (123) = K \circ (132)$$

che coincidono rispettivamente con i laterali sinistri $(12) \circ K$ e $\text{id} \circ K = K$.

Quindi K può essere il nucleo di un omomorfismo; è quello che abbiamo dato con l'applicazione

$$f: (S_3, \circ) \rightarrow (S_2, \circ)$$

definita da

$$f(k) = \text{id}_{S_2} \quad \forall k \in K$$

$$f(x) = (12) \quad \forall x \in S_3 \setminus K$$

OSS6. Sia H un sottogruppo di un gruppo $(X, *)$. (174)

L'insieme dei laterali destri di H è una partizione di X .

Dim. Ogni $a \in X$ appartiene ad un laterale destro poiché $a = u_x * a \in H * a$.

Se $a \in (H * b) \cap (H * c)$ esistono $h_1, h_2 \in H$ t.c.

$$a = h_1 * b = h_2 * c$$

$$\Rightarrow h_1^{-1} * h_1 * b = h_1^{-1} * h_2 * c \Rightarrow b = h_1^{-1} * h_2 * c \in H * c$$

$$\Rightarrow H * b \subseteq H * c.$$

$$\text{Similmente: } \dots c \in H * b \Rightarrow H * c \subseteq H * b$$

E quindi i due laterali coincidono. C.V.d.

Quindi si può definire una relazione di equivalenza legata ad H :

$$a R_d b \iff a \in H * b \iff a * b^{-1} \in H$$

L'OSS6 vale anche per i laterali sinistri e quindi si può definire un'altra relazione di equivalenza legata a H

$$a R_s b \iff a \in b * H \iff b^{-1} * a \in H$$

Se laterali destri e sinistri individuati da ciascun elemento non coincidono, queste sono due relazioni diverse.

I laterali destri sono le classi di equivalenza risp.

$a R_d$ cioè gli elementi dell'insieme quoziente $\frac{X}{R_d}$;

i laterali sinistri sono gli elementi di $\frac{X}{R_s}$.

Domanda: Si può introdurre in $\frac{X}{R_d}$ o $\frac{X}{R_s}$ un'operazione legata a $*$ che li stentanti a gruppo?

PROP. 1 Se H è un sottogruppo di $(X, *)$ tale che

$$\forall a : H * a = a * H$$

Si può introdurre in $\frac{X}{H}$ l'operazione

$$(H * a) \square (H * b) = H * (a * b)$$

e rispetto a questa operazione $\frac{X}{H}$ è un gruppo, che viene detto gruppo quoziante di X mediante H e denotato con $\frac{X}{H}$. La corrispondenza $f: X \rightarrow \frac{X}{H}$ definita da $f(a) = H * a$ è un omomorfismo di gruppi di nucleo H .

Dim. Mostriamo solo che l'operazione* è compatibile con la relazione di equivalenza, cioè che se cambio rappresentanti il "prodotto" non cambia. Le altre verifiche sono lasciate per esercizio.

sia $a' \in H * a$ e $b' \in H * b$: allora $H * a' = H * a$ e $H * b' = H * b$

dovendo provare che

$$(H * a') \square (H * b') = (H * a) \square (H * b)$$

Sarà $a' = h_1 * a$ e $b' = h_2 * b$ per opportuni $h_1, h_2 \in H$.

Quindi

$$H * (a' * b') = H * (h_1 * a * h_2 * b)$$

poiché $a * H = H * a, \exists h_3 \in H$ t.c.

$a * h_2 = h_3 * a$ e quindi

$$H * (a' * b') = H * (h_1 * h_3) * (a * b) \subseteq H * (a * b)$$

Lavorando con h_1^{-1} e h_2^{-1} si prova anche

$$H * (a * b) \subseteq H * (a' * b')$$

e quindi i due laterali sono uguali, cioè il "prodotto" non dipende dal rappresentante scelto.

C.Q.d.

Notiamo che l'elemento neutro in $(\frac{X}{H}, \square)$ è $H * u_x = H$ e l'inverso di $H * a$ è $H * a^{-1}$.

Prop. 2 Sia $(X, *)$ un gruppo e H un suo sottogruppo
Affinché l'operazione $*$ sia compatibile con la relazione R_d :

$$a R_d b \Leftrightarrow a * b^{-1} \in H$$

cioè affinché $\forall a, a', b, b' \in H$ se $a R_d a'$ e $b R_d b'$ anche

$(a * b) R_d (a' * b')$ è NECESSARIO che $\forall a \in X$ si abbia $H * a = a * H$.

Dim. Voglio provare che se $\forall a, b \in X$ e $\forall a' = h_1 * a \in H * a$

e $\forall b' = h_2 * b \in H * b$ si ha

$$(1) \quad H * (a * b) = H * (a' * b')$$

allora risulta $\forall a \in X$: $H * a = a * H$.

$$\text{La (1) equivale a } (a' * b') * (a * b)^{-1} \in H$$

Sostituendo e ricordando che l'inverso del prodotto...
+ prop. associativa

$$\Leftrightarrow (h_1 * a * h_2 * b) * (b^{-1} * a^{-1}) \in H$$

$$\Leftrightarrow h_1 * a * h_2 * b * \underbrace{b^{-1} * a^{-1}}_{\text{def di inverso}} = h_1 * a * h_2 * b \in H$$

$$\Leftrightarrow \exists h_3 \text{ t.c. } h_1 * a * h_2 * a^{-1} = h_3 \text{ cioè} \\ a * h_2 * a^{-1} = h_1^{-1} * h_3 = h$$

$$\Leftrightarrow \exists h \text{ t.c. } a * h_2 = h * a \quad (2)$$

$$\Leftrightarrow a * H \subseteq H * a, \text{ poiché la (2) vale } \forall h_2 \in H.$$

La (2) si può anche rileggere:

$$h_1^{-1}, \forall h_2^{-1}, \exists h^{-1} \text{ t.c. } h_2^{-1} * a^{-1} = a^{-1} * h^{-1}$$

e dato che ogni elemento di X si può leggere come
l'inverso a^{-1} di un el. di X e analogamente per gli
elementi di H si vede che vale anche $H * a \subseteq a * H$
e quindi le tesi. C.V.O.

Se fatto che laterali destri e sinistri coincidono è così

importante che un sottogruppo H b.c. $\forall a \in X$

si abbia $H * a = a * H$ ha un nome speciale:

Sottogruppo NORMALE di $(X, *)$.

Keif è un sgr. normale. I sgr. di un gr. abeliano sono
normali.

In un gruppo abeliano tutti i sottogruppi sono normali e quindi la relazione di equivalenza è compatibile con l'operazione introdotta nel gruppo.

Esempio. Considero $G = \mathbb{R}^2$ e come operazione la somma. L'insieme $H = \{(3k, 2k), k \in \mathbb{R}\}$ è un sottogruppo - ovviamente normale - di G .

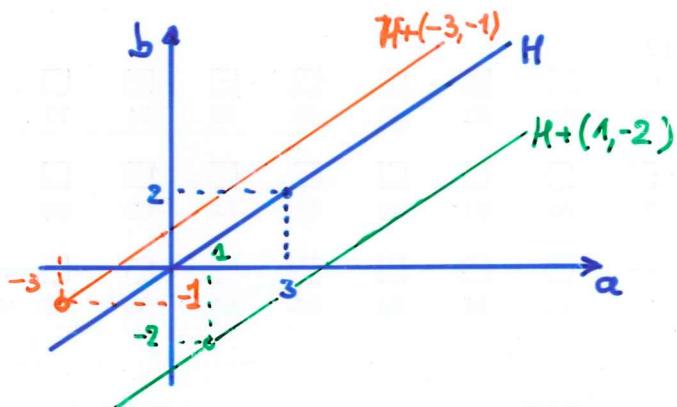
Come sono fatti i laterali destri (e sinistri) di H ? Possono essere considerati come le preimmagini in un omomorfismo $f: (G, +) \rightarrow (\mathbb{R}, +)$?

Svolg.: H è un sottogruppo poiché $\forall k_1, k_2 \in \mathbb{R}$

$$\begin{aligned}(3k_1, 2k_1) + (3k_2, 2k_2) &= (3(k_1+k_2), 2(k_1+k_2)) \in H \\ -(3k, 2k) &= (3(-k), 2(-k)) \in H\end{aligned}$$

I suoi laterali destri avranno la forma

$$H + (a, b) = \{(3k+a, 2k+b), k \in \mathbb{R}\} \quad \forall (a, b) \in \mathbb{R}^2 \text{ fissato}$$



per ogni punto $(a, b) \in \mathbb{R}^2$ c'è un laterale di H che lo contiene cioè una retta // a quella di eq. $2y = 3x$ che lo contiene

H è normale in G e quindi può essere il nucleo di un omomorfismo. Ogni laterale può essere individuato dall'intercetta sull'asse y: $3k+a=0 \Rightarrow k=-a/3 \Rightarrow y=-\frac{2}{3}a+b$. Allora definisco $f(a, b) = -\frac{2}{3}a+b$

Verificare che $f: (\mathbb{R}^2, +) \rightarrow (\mathbb{R}, +)$ è un omom. di gruppi con nucleo H e che $\forall c \in \mathbb{R}$ si ha $f^T(c) = H + (0, c)$.

N.B. Ogni classe laterale di un sgr H può essere posta in corrispondenza 1-1 con H . Il discorso vale per classi destre o sinistre o bilaterali. Vediamolo per le destre

$$f: H \rightarrow H * g \\ h \mapsto h * g$$

definita da
è applicazione su
e in ($h_1 * g = h_2 * g \Leftrightarrow$
 $h_1 * g * g^{-1} = h_2 * g * g^{-1} \Leftrightarrow$
 $h_1 = h_2$)

- Ne segue che se G è finito è ripartito in classi laterali (ad es. destre) Hg_i che hanno tutte lo stesso numero di elementi di H

$$|G| = |H \cup Hg_1 \cup \dots \cup Hg_n| = (n+1)|H|$$

\Rightarrow l'ordine di H divide l'ordine di G (teor. di LAGRANGE)

Ad es. $(\mathbb{Z}_6, +)$ non può avere sottogruppi di ordine 4. Non è comunque detto che se $n \mid |G|$ ci sia in G un sottogruppo di ordine n ma che ce ne sia 1 solo.

Mostrare che nel gruppo $T = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ ci sono 3 sgr. di ordine 2.

- Ne segue anche che una partizione di un gruppo in sottoinsiemi disgiunti ma non "equipotenti" non può essere una partizione in classi laterali.
E, visto che le preimmagini mediante un omomorfismo $f: G \rightarrow G'$ degli elem. di un gruppo G' sono laterali di $\ker f$, se le preimmagini in una corrispondenza $F: G \rightarrow G'$ di el. di G' non sono equipotenti, F non è unomorf.