

## Oeomorfismi di strutture algebriche

(163)

OMO : uguale MORFÉ : forma

Siano  $(X, *)$  e  $(Y, \square)$  due strutture algebriche (con 1 sola operazione interna binaria, per ora) e sia  $f: X \rightarrow Y$  un'applicazione tra  $X$  e  $Y$

DEF. Dico che l'applicazione  $f$  è un omomorfismo se per ogni coppia di elementi  $a, b \in X$  si ha

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

## Attenzione:

$$a * b \in X, f(a * b) \in Y, f(a) \sqcap f(b) \in Y.$$

N.B. Se  $(X, *)$  ha neutro  $a_X \in (Y, \square)$  ha neutro  $a_Y$  si vuole anche che  $f(a_X) = a_Y$

Nomi particolari : MONO - morfismo  $\Leftrightarrow$  f è iniettiva

EPI-morfismo  $\Leftrightarrow$  f è suriettiva

iso-morfismo  $\Leftrightarrow$  f è bimivoca

ENDO-morfismo  $\Leftrightarrow X = Y$  e  $* = \square$

AUTO-morfismo  $\Leftrightarrow$  ENDO e ISO

AUTO-morfismo  $\Leftrightarrow$  ENDO e ISO

Il fatto che un'applicazione sia un onto-morfismo dipende dall'applicazione e dalle operazioni definite in  $X$  e  $Y$ .

Esempio. Sia  $X = \mathbb{N}$  e l'operazione def. in  $X$  sia +

la corrispondenza  $f: X \rightarrow Y$  definita da

$$f(x) = 2^x \quad \text{per ogni } x \in \mathbb{N}$$

- a) è una applicazione
  - b) è iniettiva (ma non suriettiva)
  - c) è un monomorfismo da  $(X, +)$  a  $(Y, \cdot)$   
 $f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$ .

ESEMPIO 2 Se come operazione nell'esempio precedente (164)

scelgo la somma tanto in  $X = \mathbb{N}$  che in  $Y = \mathbb{N}$ , la applicazione  $f: \mathbb{N} \rightarrow \mathbb{N}$  definita da  $f(x) = 2^x$

NON è un OMOMORFISMO, poiché

$$f(a+b) = 2^{a+b} \neq 2^a + 2^b = f(a) + f(b)$$

(ad es. se  $a=0, b=1$ :  $f(0+1)=2$ ,  $f(0)+f(1)=1+2$ )

ESEMPIO 3. Sia  $X=Y=\mathbb{Z}$  e consideriamo le 3 applicazioni di  $\mathbb{Z}$  in sé così definite

$$f(x) = -x, \quad g(x) = 1, \quad h(x) = x^2$$

Se in  $X$  e  $Y$  prendo l'operazione di somma:

AUTOMORF.  $f(a+b) = -(a+b) = -a-b = f(a) + f(b)$  : OMO: SI, dopp

$$g(a+b) = 1 \quad g(a) + g(b) = 1+1=2 : NO$$

$$h(a+b) = (a+b)^2 \quad h(a) + h(b) = a^2 + b^2 : NO$$

Se in  $X$  prendo la somma e in  $Y$  il prodotto:

$$f(a+b) = -a-b \quad f(a) \cdot f(b) = (-a)(-b) = ab$$

$$g(a+b) = 1 = 1 \cdot 1 = g(a) \cdot g(b)$$

$$h(a+b) = (a+b)^2 \quad h(a) \cdot h(b) = a^2 b^2$$

OMO:

NO

SI, di MONOIDI

NO

Se in  $X$  prendo il prodotto e in  $Y$  la somma:

$$f(ab) = -ab \quad f(a) + f(b) = -a-b$$

$$g(ab) = 1 \quad g(a) + g(b) = 2$$

$$h(ab) = (ab)^2 \quad h(a) + h(b) = a^2 + b^2$$

OMO:

NO

NO

NO

Se in  $X$  e  $Y$  prendo l'operazione di prodotto:

$$f(ab) = -ab \quad f(a)f(b) = ab$$

$$g(ab) = 1 = 1 \cdot 1 = g(a)g(b)$$

$$h(ab) = (ab)^2 = a^2 b^2 = h(a)h(b)$$

OMO:

NO

SI, di MONOIDI

SI, di KENOIDI

ESEMPIO 4.  $X = M_2(\mathbb{R})$ ,  $\circ$ : prodotto di matrici  
 $Y = \mathbb{R}$ ,  $\circ$ : prodotto in  $\mathbb{R}$

Considero la corrispondenza

$$\det: X \rightarrow Y$$

definita da  $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ .

È un omomorfismo da  $(X, \circ)$  a  $(Y, \circ)$ ?

- È un'applicazione? sì

$$-\det \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} ?$$

$$\begin{aligned} \det \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} &= (\underline{aa'} + \underline{bc'}) (\underline{cb'} + \underline{dd'}) + \\ &\quad - (\underline{ab'} + \underline{bd'}) (\underline{ca'} + \underline{dc'}) = \\ &= aa'dd' + bb'cc' - adb'c' - bca'd' \end{aligned}$$

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = (ad - bc)(a'd' - b'c') =$$

$$= aa'dd' + bb'cc' - adb'c' - bca'd'$$

È un EPIMORFISMO?  $\forall a \in \mathbb{R}$  la matrice  $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$  ha det. = a: sì

E se invece facendo la somma tutto in  $M_2(\mathbb{R})$  che in  $\mathbb{R}$ ?

$$\det \left( \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \right) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} ?$$

No:

$$\text{Provare con } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}: \det \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 4$$

$$\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1+1=2$$

ESEMPIO 5 sia  $X = \mathbb{Z}_3$  con l'operazione di  $+_3$   
e  $Y = S_3$  con l'operazione di composizione.

La corrispondenza  $\begin{pmatrix} [0]_3 & [1]_3 & [2]_3 \\ id & (123) & (132) \end{pmatrix}$  è un  
omomorfismo da  $(\mathbb{Z}_3, +)$  a  $(S_3, \circ)$ ?  
Qual è la sua immagine?

1) la corrisp.  $f$  è un'applicazione  $\mathbb{Z}_3 \rightarrow S_3$

2)  $f([a]_3 + [b]_3) = f([a]_3) \circ f([b]_3)$

Osservo che  $(\mathbb{Z}_3, +) = \langle [1]_3 \rangle := \{ n[1]_3, n \in \mathbb{Z} \}$

" che  $\{ \text{id}, (123), (132) \} := \langle (123) \rangle$

$$\text{infatti } (123)^1 = (123)$$

$$(123)^0 = \text{id}$$

$$(123)^2 = (132)$$



allora la  $f$  è così descritta

$$f(n[1]_3) = (123)^n \quad n=0,1,2$$

ed è un omomorfismo poiché

$$f(n[1]_3 + m[1]_3) = f((n+m)[1]_3) = (123)^{n+m}$$

$$f(n[1]_3) \circ f(m[1]_3) = (123)^n \circ (123)^m$$

$$= (123)^{n+m} \quad \xleftarrow{\text{uguali}} \Rightarrow \text{SI}$$

3) monomorfismo?

Sì poiché  $\langle (123) \rangle$  ha ordine 3 come  $\mathbb{Z}_3$  e viceversa.

che  $f: \mathbb{Z}_3 \rightarrow \langle (123) \rangle$  è suriettiva è anche l'iniezione.

4) l'immagine è  $\langle (123) \rangle$

ESEMPIO 6 Considero  $(S_3, \circ_3)$  e  $(S_2, \circ_2)$  e la

$$\text{corrispondenza } f = \begin{pmatrix} \text{id}_3 & (123) & (132) & (12)_3 & (23)_3 & (13)_3 \\ & (123) & \text{id}_2 & \text{id}_2 & (12)_2 & (12)_2 \end{pmatrix}$$

tra  $S_3$  e  $S_2$ , ove i pedici indicano in quale dei due insiemi di permutazioni devo prendere l'elemento denotato con id o con  $(12)$ . E' un EPIMorfismo?

Certamente: applicazione suriettiva. Per provare che  $f(a \circ_3 b) = f(a) \circ_2 f(b)$  conviene riprendere le tavole di composizione di  $S_3$  e quelle di  $S_2$

$\circ$	$\text{id}$	$(123)$	$(132)$	$(12)$	$(23)$	$(13)$
$\text{id}$	$\text{id}$	$(123)$	$(132)$	$(12)$	$(23)$	$(13)$
$(123)$	$(123)$	$(132)$	$\text{id}$	$(13)$	$(12)$	$(23)$
$(132)$	$(132)$	$\text{id}$	$(123)$	$(23)$	$(13)$	$(12)$
$(12)$	$(12)$	$(23)$	$(13)$	$\text{id}$	$(123)$	$(132)$
$(23)$	$(23)$	$(13)$	$(12)$	$(132)$	$\text{id}$	$(123)$
$(13)$	$(13)$	$(12)$	$(23)$	$(123)$	$(132)$	$\text{id}$

$\circ$	$\text{id}$	$(12)$
$\text{id}$	$\text{id}$	$(12)$
$(12)$	$(12)$	$\text{id}$

e osservare che i primi 3 elementi, costituiscono un sottoinsieme  $A_3$  di  $S_3$  chiuso rispetto a  $\circ_3$  e hanno ciascuno come immagine  $\text{id}_2$ , che composta con se stessa da  $\text{id}_2 \Rightarrow$  se  $a, b \in \{\text{id}, (123), (132)\}$  vale

$$(*) \quad f(a \circ_3 b) = f(a) \circ_2 f(b)$$

I secondi 3, che hanno per immagine  $(12)_2$ ,

moltiplicati tra loro da un elemento di  $A_3$  e

dato che  $(12)_2 \cdot (12)_2 = \text{id}_2$  vale  $(*)$  se  $(a, b) \in S_3 \setminus A_3$

Se poi si fa il prodotto di un elemento che sta in  $A_3$  (che ha per immagine  $\text{id}_2$ ) per uno che

sta in  $S_3 \setminus A_3$  (che ha per immagine  $(12)_2$ ),

ovvero, il prodotto sta in  $S_3 \setminus A_3$  e quindi ha l'immagine  $(12)$  e quindi vale ancora  $(*)$ .

OSS. 1 Se  $f: (X, *) \rightarrow (Y, \square)$  è un omomorfismo di strutture algebriche, l'immagine  $f(X)$  è un sottinsieme di Y chiuso rispetto a  $\square$ .

Dim. Siano  $c, d \in f(X)$ . Allora esistono

$$a, b \in X \text{ t.c. } f(a) = c, f(b) = d \Rightarrow \\ c \square d = f(a) \square f(b) = \underset{\substack{\uparrow \\ f \text{ omo}}}{f(a * b)} \in f(X).$$

OSS. 2 Se  $(X, *) \xrightarrow{f} (Y, \square) \xrightarrow{g} (Z, \triangleright)$

sono 2 omomorfismi di strutture algebriche, l'applicazione  $g \circ f : (X, *) \rightarrow (Z, \triangleright)$  è un omomorfismo di str. alg.

In particolare se sono due isomorfismi, la composta è un isomorfismo.

OSS. 3 Se  $(X, *) \xrightarrow{f} (Y, \square)$  è un isomorfismo (e quindi esiste  $f^{-1}$ ) anche  $f^{-1}: (Y, \square) \rightarrow (X, *)$  è un isomorfismo.

Dim. Siano  $c, d \in Y$  e sia  $f^{-1}(c) = a, f^{-1}(d) = b$ .

Allora  $c = f(a)$  e  $d = f(b)$  (per def. di inverso)

$$\begin{aligned} \text{e } f^{-1}(c \square d) &= f^{-1}(f(a) \square f(b)) = \text{fornito} \\ &= f^{-1}(f(a * b)) = a * b \text{ per def. inverso} \\ &= f^{-1}(c) * f^{-1}(d). \end{aligned}$$

Da tutto ciò si deduce che l'insieme degli automorfismi di  $X$ , Aut  $X$ , rispetto alla composizione non solo è chiuso (OSS 2) ma, visto che la composizione è sempre ASSOCIAUTIVA e visto che l'identità (neutro rispetto alla composizione) è un automorfismo e che l'inverso è un automorfismo, è un GRUPPO.

OSSI. Integrazione.

$(X, *)$  monoido,  $(Y, \square)$  semigruppo

(167)  
bis

$f: (X, *) \rightarrow (Y, \square)$  omomorfismo di semigruppi cioè

$$f(a * b) = f(a) \square f(b) \quad \forall a, b \in X$$

faccia la restrizione

$$f|_{f(X)} : (X, *) \rightarrow (f(X), \square)$$

Semigruppo  
è anche un monoido?

è un monoido  
cioè  $\exists u \in X$  t.c.

$$\forall x \in X : x * u = u * x = x$$

Considero  $u' = f(u)$  e un presunzione che  
 $y \in f(X)$  : cioè  $\exists x \in X$  t.c.

$$f(x) = y$$

$$y \square f(u) = f(x) \square f(u) \underset{\text{ono}}{=} f(x * u) = f(x) = y$$

$$f(u) \square y = f(u) \square f(x) \underset{\text{ono}}{=} f(u * x) = f(x) = y$$

$\Rightarrow f(u)$  risulta neutro in  
 $(f(X), \square)$

gof è una applicazione (oss 2) 167  
Ter

Dico provare che  $\forall a, b \in X$  risulta

$$g \circ f(a * b) = g \circ f(a) * g \circ f(b)$$

Osserviamo:  $g \circ f(z) = g(f(z)) \Rightarrow$

$$\begin{aligned} g \circ f(a * b) &= g(f(a * b)) = f \circ g \\ &= g(f(a) * f(b)) = g \circ f \\ &= g(f(a)) * g(f(b)) = \\ &= g \circ f(a) * g \circ f(b). \end{aligned}$$

Se  $f$  e  $g$  sono bimorpiche anche  $g \circ f$  lo è  
se  $f$  e  $g$  sono 2 ISO  $\Rightarrow g \circ f$  ISO  
conseguenze dell'oss. 2.

Suppongo  $f, g, h, \dots$  siano omomorfismi  
di  $(X, *)$  in  $(X, *)$  (ENDO " )

$(\text{End}(X, *), \circ)$  è un semigruppo?

" $\circ$ " è chiuso

" $\circ$ " è associativa già per le proprietà di  $X$   
Sì lo è

E' un monoido?  $\text{id}: (X, *) \rightarrow (X, *)$

è un omomorfismo

$$\text{e } \text{id} \circ f(x) = f \circ \text{id}(x) = f(x)$$

Sì lo è

Il sostanzia se due strutture algebriche sono (168)  
 isomorfe può cambiare: l'insieme soggiacente,  
 il nome degli elementi,  
 il nome dell'operazione  
 ma non cambia il modo  
 in cui l'operazione lavora su coppie di elementi corri-  
 sppondenti.

Esempio. Consideriamo  $(\mathbb{Z}_4, +)$  e le radici  
 complesse quarte dell'unità  $Y = \{1, -1, i, -i\}$   
 con l'operazione di prodotto e consideriamo  
 $f : (\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_4, +)$        $f([x]_4) = [3]_4 [x]_4$ ,  
 $g : (\mathbb{Z}_4, +) \rightarrow (Y, \cdot)$        $g([x]_4) = i^x \quad (x \in \mathbb{Z}_4^{0,1,2,3})$

Entrambe queste applicazioni sono:

- bimorfiche (nel primo caso notare che, essendo  $\text{MCD}(3,4)=1$ ,  $[3]_4 [x]_4$  descrive tutte le possibili classi di resto mod 4; essendo  $f$  suriettiva è anche iniettiva, poiché l'insieme è finito)
- omomorfismi

$$\begin{aligned} f([a]_4 + [b]_4) &= f([a+b]_4) = [3]_4 [a+b]_4 = \\ &= [3a+3b]_4 = [3a]_4 + [3b]_4 = \\ &= [3]_4 [a]_4 + [3]_4 [b]_4 = f([a]_4) + f([b]_4) \\ g([a]_4 + [b]_4) &= g([a+b]_4) = i^{a+b} = i^a \cdot i^b = \\ &= g([a]_4) + g([b]_4) \end{aligned}$$

Nel primo caso insieme e operazione sono rimasta  
 uguali ma sono stati cambiati i nomi di alcuni el.  
 ( $a [0], [1], [2], [3]$  sono stati sostituiti rispettivamente  
 $[0], [3], [2], [1]$ ). Nel secondo caso l'insieme e la natura  
 degli elementi nonché l'operazione sono cambiati,  
 ma resta sempre il comportamento MODULARE dell'o-  
 perazione.

Ditremo proprietà algebriche quelle che difendono solo dal modo di operare dell'operazione e non delle nature o del nome degli elementi o dell'operazione, cioè le proprie. "invarianti per isomorfismi", vale a dire possedute da tutte e sole le strutture tra le quali esiste un isomorfismo. Si possono studiare le proprietà algebriche di una struttura su una qualunque delle strutture tra loro isomorfe (isomorfismo = relazione di equivalenza; la singola struttura appartenente a una classe di equivalenza può essere presa come rappresentante o "modello" di tutta quella nella sua classe e su quest' studiare le pr. alg.)

Esempi di pr. algebriche: le 7 che abbiamo elencato prima di parlare di str. algebriche. Ma anche l'ordine dell'sistema (se finito) o la sua cardinalità (se infinito).

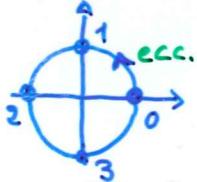
Come stabilire se due strutture sono isomorfe?

... bisogna trovare gli isomorfismi tra le due.

Non sempre è facile. Ci sono teoremi che a volte,

Le voci per verificare che non sono isomorfe bastano trovare una proprietà posseduta da una e non dall'altra; ad es. non sono isomorfi i gruppi  $\mathbb{Z}_2$ ,  $\mathbb{Z}_3$  e  $\mathbb{Z}_4$ .

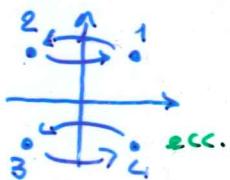
$(\mathbb{Z}_4, +)$	+	0	1	2	3
0	0	1	2	3	0
1	1	2	3	0	1
2	2	3	0	1	2
3	3	0	1	2	3



Solo [ɔ] e [ɛ] sono  
invertiti se  
stessi

$$T_4 = \{ \text{id}, (12)(34), (14)(23), (13)(24) \}$$

o	id	a	b	c
id	id	a	b	c
a	a	id	c	b
b	b	c	id	a
c	c	b	a	id



oggi eleon. è inverso  
di se stesso.