16-11

DEF. DATO S INSIEME, $\perp : S \times S \to S$ E' DETTA OPERAZIONE INTERNA A S (OPPURE LEGGE DI S)
LA APPLICAZIONE

L'INSIEME DATO DALLA COPPIA $(S, \perp)$ E' DETTA STRUTTURA ALGEBRICA

~~E' UNA RELAZIONE~~

OSS. • $\perp$ E' RELAZIONE $\subseteq (S \times S) \times S$

• USEREMO LA NOTAZIONE $(x,y) \in S \to x \perp y \in S$

$\perp(x,y) = x \perp y$

• $\forall\, x,y \in S$, $x \perp y$ (IL RISULTATO DELL'OPERAZIONE) E' UNICO

ESEMPI

1) $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $\cancel{(\mathbb{N},\cdot)}$ $(\mathbb{N}_0,+)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\cdot)$,
$(\mathbb{R},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},-)$, $(\mathbb{R},\setminus)$

$$\boxed{\begin{aligned} +: \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (x,y) &\mapsto x+y \end{aligned}}$$

$$\boxed{\begin{aligned} \cdot\ \mathbb{Q} \times \mathbb{Q} &\to \mathbb{Q} \\ \left(\frac{n}{m}, \frac{l}{q}\right) &\mapsto \frac{n}{m} \cdot \frac{l}{q} = \frac{nl}{mq} \end{aligned}}$$

2) S INSIEME QUALSIASI, $(\mathcal{P}(S), \cap)$, $(\mathcal{P}(S), \cup)$,
$(\mathcal{P}(S), S\setminus)$ $\Big\}$ $S \setminus X := X^c$ (COMPLEMENTO DI X)
COMPLEMENTO A S
$S \setminus X$

$$\boxed{\begin{aligned} \cap: \mathcal{P}(S) \times \mathcal{P}(S) &\to \mathcal{P}(S) \\ (A,B) &\to (A \cap B) \end{aligned}}$$

OPERAZIONE INTERNA, BEN DEFINITA

OPERAZIONI BINARIE

$$\boxed{\begin{aligned} \cup: \mathcal{P}(S) \times \mathcal{P}(S) &\to \mathcal{P}(S) \\ (A,B) &\mapsto (A \cup B) \end{aligned}}$$

$$\boxed{\begin{aligned} C: \mathcal{P}(S) &\to \mathcal{P}(S) \\ X &\mapsto S \setminus X \end{aligned}}$$

OPERAZIONE UNARIA, NON BINARIA COME LE PRECEDENTI

ex. OP. UNARIA DI $\mathbb{R}$ = L'OPPOSTO
DI $\mathbb{R}^+$: ~~[illegible]~~ LA RADICE QUADRATA

ALTRI ESEMPI DI OPERAZIONI UNARIE

ex. $(\mathbb{R}, \sqrt[3]{x}) \to \perp : \mathbb{R} \times \mathbb{R}$
$\perp(x) = \sqrt[3]{x}$

$(\mathbb{R}, 1-x)$

$(\mathbb{R}, x^2)$

V^V INSIEME DI TUTTE LE APPLICAZIONI CHE VANNO DA V in V

$V^V = \{ f : V \to V \mid f \text{ applicazioni} \}$

ESEMPIO.
TUTTE LE f in {1,2,3,4}
INSIEME = 4^4

$$\boxed{\begin{aligned} \circ : &\ V^V \times V^V \to V^V \\ &(f,g) \mapsto g \circ f \end{aligned}}$$

COMPOSIZIONE DI FUNZIONI

COMPOSIZIONE MI RENDE L'INSIEME DELLE FUNZIONI UNA STRUTTURA ALGEBRICA

$(V^V, \circ)$

4)
$$\boxed{\begin{aligned} \perp_1 : &\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ &(x,y) \mapsto x^2 + y^2 \end{aligned}}$$

$3 \perp_1 1 = 3^2 + 1^2 = 9 + 1 = 10$

$$\boxed{\begin{aligned} \perp_2 : &\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ &(x,y) \mapsto xy + y \end{aligned}}$$

$3 \perp_2 1 = 3 \cdot 1 + 1 = 4$

5) $(L, \vee)$ L RETICOLO

OPERAZIONE DI SUP

$$\boxed{\begin{aligned} \vee : &\ L \times L \to L \\ &(x,y) \to x \vee y \end{aligned}}$$

VALE ANCHE SE E' INF.

N.B. SE L NON E' RETICOLO, $\vee$ DI x, y POTREBBE NON ESISTERE.
QUESTO DICE CHE SE L NON E' RETICOLO $\vee$ NON E' OPERAZIONE (PERCHE' NON E' FUNZIONE)

DEF. DATA $(S, \perp)$ STRUTTURA ALGEBRICA, DIREMO CHE L'OPERAZIONE E'

i) COMMUTATIVA : $x \perp y = y \perp x \quad \forall x,y \in S$ $(+, \cdot)$

ii) ASSOCIATIVA : $x \perp y \perp z = x \perp (y \perp z) \quad \forall x,y,z \in S$
$(\vee, +, \cdot)$

ESEMPIO 4 : NO COMMUTATIVA E NO ASSOCIATIVA

$1 \perp_2 3 \neq 3 \perp_2 1 \qquad (-2 \perp_2 1) \perp_2 1 = -2 \perp_2 (1 \perp_2 1)$

ANCHE LA COMPOSIZIONE NON E' COMMUTATIVA
$(V^V, \circ)$, $\circ$ NON E' COMMUTATIVA, PERO' E' ASSOCIATIVA

$(\mathbb{R}^{\mathbb{R}}, \circ)$
$f(x) = x^2 \qquad (g \circ f)(x) = g(x^2) = x^2 + 2$
$g(x) = x + 2 \qquad (f \circ g)(x) = f(x+2) = (x+2)^2$

SE DEVO DIMO-
RE CHE 2 COSE
SONO DIVERSE
E' + SEMPLICE
TROVARE UN
CHE LE REND
DIVERSE

DEF. - SE S E' FINITO $(S,\perp)$, LA TAVOLA DI MOLTIPLICATI DI $\perp$ E' DEFINITA:

$$S=\{x_1,\dots,x_n\}$$

$\perp$	x_1	x_2	...	x_n
x_1	$x_1\perp x_1$	$x_1\perp x_2$		$x_1\perp x_n$
				$x_2\perp x_n$
x_2	$x_2\perp x_1$	$x_2\perp x_2$		
⋮				$x_n\perp x_n$
x_n	$x_n\perp x_1$	$x_n\perp x_2$		

PENSANDOLA COME UN QUADRATO, PRENDENDO LA DIAGONALE TROVIAMO LE OPERAZIONI SULLE STESSE X (PER LA COMMUTATIVITA') QUESTO MI DICE ANCHE CHE LA TABELLA E' SIMMETRICA
PER CONTROLLARE SE UN'OPERAZIONE E' COMMUTATIVA CONTROLLIAMO CHE L'OPERAZIONE a[i] $\perp$ a[j] DIA LO STESSO RISULTATO DI a[j] $\perp$ a[i]

ES.
$S=\{a,b\}$ $(\mathcal{P}(S),\cup)$ $\mathcal{P}(S)=\{\emptyset,\{a\},\{b\},\{S\}\}$

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	S
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	S
$\{a\}$	$\{a\}$	$\{a\}$	S	S
$\{b\}$	$\{b\}$	S	$\{b\}$	S
S	S	S	S	S

PER VEDERE SE L'OPERAZIONE E' COMMUTATIVA CONTROLLIAMO I RISULTATI AI POSTI (3,1) e (1,3) (4,1) (1,4), (2,1), (1,2)

ES.
$S=\{a,b,c\}$

$*$	a	b	c
a	b	c	a
b	a	b	a
c	b	b	c

NON E' COMMUTATIVA
RIGA COLONNA
$a*a=b$
$b*c=a$
$c*b=b$

DEF. $(S,\perp)$ UN ELEMENTO $e\in S$ E' DETTO ELEMENTO NEUTRO PER $\perp$ SE

$$\forall x\in S \begin{cases} x\perp e=x \\ e\perp x=0 \end{cases}$$

ES. $1\cdot 1=1$ 1 x LA MOLTIPLICAZIONE
$1+0=0$ 0 x LA SOMMA

$\emptyset$ PER $(\mathcal{P}(S),\cup)$
S PER $(\mathcal{P}(S),\cap)$
0 PER $(\mathbb{R},+)$
COMPOSTO

$-: \mathbb{R}\times\mathbb{R}\to\mathbb{R}$ $x-0=x$ $\forall x\in\mathbb{R}$ E' NEUTRO A DX
$(x,y)\to x-y$ $0-x=-x$ NON E' NEUTRO A SX

DEF. SE $(S, \perp)$ HA ELEMENTO NEUTRO $e \in S$, DIREMO CHE $x \in S$ E' ~~SIMMETRIZZABILE~~
SIMMETRIZZABILE SE $\exists$ $y \in S \mid x \perp y = y \perp x = e$

4

ES $(\mathbb{Z}, +)$ $\rightarrow$ TUTTO SIMMETRIZZABILE POICHE' IN $\mathbb{Z}$ ESISTE L'OPPOSTO
QUESTI ELEMENTI SONO DETTI SIMMETRIZZABILI

$(\mathbb{N}, +)$ $\rightarrow$ NESSUN ELEMENTO E' SIMMETRIZZABILE
SOLO 0 E' SIMMETRIZZABILE

$(\mathbb{Z}, \cdot)$ $\rightarrow$ SOLO 1 e -1
$e = 1$ $\quad 1 \cdot 1 = 1$
$(-1)(-1) = 1$

L'ELEMENTO 0 E' DETTO UNITA' QUANDO E' ~~DETTA~~ RIFERITO AD UNA MOLTIPLICAZIONE

$(\mathbb{Q}, \cdot)$ $\rightarrow$ $e = 1$ $\quad \frac{n}{m} \cdot = 1$

$$\underbrace{\frac{n}{m} \cdot \frac{m}{n} = 1}_{q \cdot \frac{1}{q} = 1}$$

$\mathbb{Q} \setminus \{0\}$ SONO SIMMETRIZZABILI

$\uparrow$

$\rightarrow$ QUINDI NON POSSO SIMMETRIZZARE LO 0

DEF. DATO $(S, \perp)$ DIREMO CHE $a \in S$ E' CANCELLABILE (O REGOLARE) SE
1 $a \perp x = a \perp y \Rightarrow x = y$
2 $x \perp a = y \perp a \Rightarrow x = y$

1 CANCELLABILE A SX
2 CANCELLABILE A DX

$(\mathbb{Z}, +)$ $\quad \cancel{3} + x = \cancel{3} + y \Rightarrow x = y$
$3 + x = 3 + y \Rightarrow$ MA $x \neq y$

$(\mathbb{Z}, \perp_1)$ $\quad x \perp_1 y = x^2 + y^2$
$x \perp_1 y = x \perp_1 z$ $\quad \cancel{x^2} + y^2 = \cancel{x^2} + z^2 \Rightarrow y^2 = z^2$ MA NON $y = z$ POICHE' POTREBBERO ESSERE OPPOSTI

$(S, \perp)$ E' TALE CHE $\perp$ E' ASSOCIATIVA E HO L'ELEMENTO NEUTRO
$\Rightarrow$ OGNI ELEMENTO E' CANCELLABILE

DEF. DATI Ω, S INSIEMI, UN'OPERAZIONE ESTERNA SU S E'

ES - $\quad \star : \Omega \times S \rightarrow S$
$(\alpha, x) \mapsto \alpha \star x \in S$

$\star : \mathbb{R} \times \mathbb{R}^{\mathbb{R}} \rightarrow \mathbb{R}^{\mathbb{R}}$
$(\alpha, f) \rightarrow \alpha f$

$f(x) = x + 3x$ $\quad (\alpha f)(x) = 7f(x) = 7(x + 3x)$
$\alpha = 7$

ES - $\quad \cdot : \mathbb{Q} \times \mathbb{R} \rightarrow \mathbb{R}$
$\left(\frac{n}{m}, \alpha\right) \rightarrow \frac{n\alpha}{m}$

ALCUNE STRUTTURE NOTEVOLI $(S, \perp)$ STRUTTURA ALGEBRICA E' DETTA:

- SEMIGRUPPO SE $\perp$ E' ASSOCIATIVA $(\mathbb{N}, +)$
- MONOIDE SE $\perp$ E' ASSOCIATIVA E DESISTE L'ELEMENTO NEUTRO $(\mathbb{N}_0, +)$
- GRUPPO SE $\perp$ E' ASSOCIATIVA, ESISTE L'ELEMENTO NEUTRO E OGNI ELEMENTO E' SIMMETRIZZABILE $(\mathbb{R}^{\mathbb{R}}, \circ)$ (non e' tutto, solo f bietiive)
- GRUPPO ABELIANO SE E' UN GRUPPO E $\perp$ E' COMMUTATIVA $(\mathbb{Z}, +)$

CONSIDERO $(S, \perp, T)$ (2 OPERAZIONI BINARIE) S CON DUE OPERAZIONI ~~BINARIE~~ INTERNE:

$(S, \perp, T)$ E' DETTO

1) ANELLO SE $(S, \perp)$ E' UN GRUPPO ABELIANO (UNA DELLE 2 OP. E' COMMUTATIVA) L'ALTRA E' ASSOCIATIVA E DEVE DISTRIBUIRE SULLA PRIMA)

$$a\,T\,(b \perp c) = (a\,T\,b) \perp (a\,T\,c) \quad \forall a,b \in S$$

<u>es</u> $(\mathbb{Z}, +, \cdot)$

2) ANELLO UNITARIO SE $\exists$ ELEMENTO NEUTRO PER T.

3) ANELLO COMMUTATIVO SE T E' COMMUTATIVO

4) CAMPO (CORPO) SE E' UN ANELLO (NON COMMUTATIVO) COMMUTATIVO | OGNI ELEMENTO (ECCETTO L'ELEMENTO ~~DELLA~~ NEUTRO PER $\perp$) E' SIMMETRIZZABILE RISPETTO T

$(\mathbb{Z}, +, \cdot)$ E' ANELLO COMMUTATIVO UNITARIO, MA NON E' CAMPO

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ SONO CAMPI

2 - 11 - 2021

DEF - DATO $(S, \perp)$, $X \subseteq S$. X E' DETTO PARTE STABILE (o CHIUSO) RISPETTO A $\perp$
SE $\forall\, x,y \in X \Rightarrow x \perp y \in X$

$(X, \perp)$ E' DETTO SOTTOSTRUTTURA DI S ~~[illegible] OPERAZIONE~~

↳ $\perp' : X \times X \to X$
$(x,y) \mapsto x \perp y$

es. $(\mathbb{R}, +)$ COME GRUPPO: $(\mathbb{Z}, +)$ E' SOTTOGRUPPO
$(\mathbb{Q}, +)$ E' SOTTOGRUPPO } GLI ELEMENTI SIMMETRIZZABILI DI $\mathbb{Z}$ STANNO IN $\mathbb{Z}$

ex. $(\mathbb{N}, +)$ SEMIGRUPPO:

$X = \{x \in \mathbb{N} \mid x \geq 5\}$ E' UN SOTTOSEMIGRUPPO
$(X, +)$
↳ L'OPERAZIONE MANTIENE LE SUE PROPRIETÀ

$\forall\, a,b \in X$ $\underline{a+b \in X}$: SE $a \geq 5$ e $b \geq 5 \Rightarrow a+b \geq 10 > 5$
↳ HO PRESO L'OPERAZIONE E HO CERCATO DI VERIFICARE LA CONDIZIONE DELLA X

ex. $(\mathbb{N}, \cdot)$ E' UN MONOIDE (1 ELEMENTO NEUTRO E' NELL'INSIEME)

$X = \{x \in \mathbb{N} \mid x \geq 5\}$ NON E' SOTTOMONOIDE POICHE' $1 \notin X$, MA E' SICURAMENTE UN SOTTOSEMIGRUPPO

$(\mathbb{N}, \cdot)$ E' LUI STESSO SOTTOMONOIDE DI $(\mathbb{N}_0, \cdot)$

$(\mathbb{N}, +)$ $(\mathbb{N}_d, +)$ → LA SOMMA DEI 2 NUMERI DISPARI E' PARI, QUINDI E' QUESTA ~~[illegible]~~ CHE NON E' PARTE STABILE

$(\mathbb{N}, \cdot)$ $(\mathbb{N}_d, \cdot)$ → IL PRODOTTO DI DISPARI E' DISPARI, SARÀ QUINDI PARTE STABILE

OSSERVAZIONI

DATA $(S, \perp)$ e $(X, \perp)$ PARTE STABILE DI S:

- SE L'OPERAZIONE E' ASSOCIATIVA IN S, LO E' ANCHE IN X
- SE $\perp$ E' COMMUTATIVA IN S, LO E' ANCHE IN X
- SE ESISTE $e \in S$ ELEMENTO NEUTRO PER $\perp$ $\Rightarrow$ SE $e \in X$ ALLORA E' ELEMENTO NEUTRO ANCHE IN X
- SE x' E' SIMMETRICO DI x RISPETTO A $\perp$ e $x', x \in X \Rightarrow$ x' E' SIMMETRICO DI X ANCHE IN S

<u>NOTA</u> - SE $\perp$ E' ASSOCIATIVO, IL SIMMETRICO DI $(x \perp y)$ E' $y' \perp$
* y' E' SIMMETRICO DI y E x' E' SIMMETRICO DI x

ex $-(2+3) = (-3) + (-2)$

$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

TEOREMA

SIA $(S, \perp)$ MONOIDE, DEFINIAMO $U(S) = \{x \in S \mid x \text{ E' SIMMETRIZZABILE}\}$
ALLORA $U(S)$ E' PARTE STABILE DI S ED E' UN GRUPPO, DETTO GRUPPO DEGLI ELEMENTI INVERTIBILI

DIM.

SIANO $x, y \in U(S) \Rightarrow$ ESISTONO x' e y' LORO INVERSI.
OSSERVIAMO CHE x E' INVERSO DI x' e y E' INVERSO DI y' $\Rightarrow$
y' e $x' \in U(S)$ POICHE' LORO STESSI ELEMENTI INVERTIBILI (HANNO INVERSI)
MA ALLORA, $U(S)$ CONTIENE GLI ELEMENTI SIMMETRIZZABILI E I LORO INVERSI (PERCHE' SONO SIMMETRIZZABILI)

QUINDI $\forall x, y \in U(S)$, $x \perp y \stackrel{?}{=} (y' \perp x')'$ (DALLA NOTA DI PRIMA) E QUINDI
$x \perp y$ E' INVERTIBILE E APPARTIENE A $U(S)$

VEDIAMO CHE $(x \perp y)(y' \perp x')^{*} = e$:

$(x \perp y) \perp (y' \perp x')^{*} = x \perp (y \perp y') \perp x' = \underbrace{x \perp e}_{} \perp x' = x \perp x' = e$

$\Rightarrow U(S)$ E' GRUPPO (ABELIANO SE L'OP. ERA ANCHE COMMUTATIVA)^{x}

$\square$

ex. $(\mathbb{Z}, \cdot)$, $U(\mathbb{Z}) = \{-1, 1\}$

DEF. {DATO $(S, \perp)$ STRUTTURA ALGEBRICA. $\mathcal{R} \subseteq S \times S$ RELAZIONE DI EQUIVALENZA
$\mathcal{R}$ E' CONGRUENZA SE E' COMPATIBILE CON $\perp$, CIOE': $\left.\begin{array}{l} x_1 R x_2 \\ y_1 R y_2 \end{array}\right\} \begin{array}{l} x_1 \perp x_2 R \\ y_1 \perp y_2. \end{array}$

L'INSIEME QUOZIENTE $S/_R$ EREDITA LA STRUTTURA ALGEBRICA DI S

DEFINISCO $\perp' : S/_R \times S/_R \to S/_R$

$$[x]_R \perp' [y]_R =: [x \perp y]_R$$

↳ QUELLA INIZIALE

LA STRUTTURA $(S/_R, \perp')$ E' DETTA STRUTTURA QUOZIENTE ex. $(\mathbb{Z}, +, \cdot)$ ANELLO, $(\mathbb{Z}_m, +, \cdot)$ E' ANELLO QUOZIENTE:

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

$[1]_4 + [3]_4 = [4]_4 = \cancel{[5]_4}$

$[5]_4 + [3]_4 = [8]_4 = [0]_4$

$[1]_m \to$ ELEMENTO NEUTRO PER $\cdot$

$[0]_m \to$ ELEMENTO NEUTRO PER $+$

DEF. $(S, \perp_S)$ $(V, \perp_V)$ DUE STRUTTURE ALGEBRICHE.

LA STRUTTURA PRODOTTO $(S \times V, \perp)$ E' OTTENUTA IN QUESTO MODO:

1) $S \times V$ E' IL PRODOTTO CARTESIANO

ii) $(x,y), (z,w) \in S \times V$

$$(x,y) \perp (z,w) := (x \perp_S z, y \perp_V w)$$

ex. $(\mathbb{R}^2, +)$ PRODOTTO DI $(\mathbb{R}, +)$ e $(\mathbb{R}, +)$

$(x,y) + (z,w) = (x+z, y+w)$ APPLICO L'OPERAZIONE COMPONENTE x COMPONENTE

$1,3 + 5,-6 = (1+5, 3-6) = (6,-3)$

$\mathbb{R}^5, +$

$(1,3,7,4,-1) \in \mathbb{R}^5$ $(R \times R \times R \times R \times R)$

$(2,0,7,0,1) \in \mathbb{R}^5$ (

$(1,3,7,4,-1) + (2,0,7,0,1) = (1+2, 3+0, 7+7, 0+4, 1-1) =$
$= (3, 3, 14, 4, 0)$

DEF. ~~SPAZ~~ SPAZIO VETTORIALE

$(\Omega, +, \cdot)$ CAMPO

$(S, \perp, *)$ GRUPPO ABELIANO RISPETTO A $(S, \perp)$

$* : \Omega \times S \to S$ OPERAZIONE ESTERNA.

S E' SPAZIO VETTORIALE SU Ω

S E' SPAZIO VETTORIALE SU Ω SE:

1) $(\alpha+\beta) * x = \alpha * x \perp \beta * x$ $\quad \forall x \in S$ e $\alpha, \beta \in \Omega$

2) $\alpha * (x \perp y) = (\alpha * x) \perp (\alpha * y)$ $\quad \forall x, y \in S$ $\alpha \in \Omega$

3) $(\alpha \cdot \beta) * x = \alpha * (\beta * x)$ $\quad \forall x \in S, \forall \alpha, \beta \in \Omega$

4) $1 * x = x$ $\quad \forall x \in S$ e 1 ELEMENTO NEUTRO PER $\cdot$ IN Ω

ES. $(\mathbb{R}^2, +, *)$ $\quad * : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$

$(\alpha, (x,y)) \to (\alpha x, \alpha y)$

$\mathbb{R}^2$ E' SPAZIO VETTORIALE SE $\quad (x,y) + (z,w) = (x+z, y+w)$

$\alpha(x,y) = (\alpha x, \alpha y) \to 3(1,2) = (3,6)$

DEF. $(S, *_S)$ e $(T, *_T)$ 2 STRUTTURE ALGEBRICHE

$f: S \to T$ funzione E' DETTA OMOMORFISMO SE $f(x *_S y) = f(x) *_T f(y)$ "COMMUTA CON L'OPERAZIONE"

OMOMORFISMO INIETTIVO $\to$ MONOMORFISMO $\to$ SOTTOSTRUTTURA DELLA SECONDA

" SURIETTIVO $\to$ EPIMORFISMO $\to$ CODOMINIO QUOZIENTE DEL DOMINIO

" BIETTIVO $\to$ ISOMORFISMO — HANNO LA STESSA OPERAZIONE — AUTOMORFISMO DI UN INSIEME IN SE' STESSO

OMOMORFISMO $f: (S, *) \to (S, *)$ E' DETTO ENDOMORFISMO (QUANDO SURIETTIVA)

AUTOMORFISMO (QUANDO E' BIETTIVA)

(QUANDO E' BIETTIVO)

ES. $g: (\mathbb{N}_0, +) \to (\mathbb{N}_0, \cdot)$ $\qquad g(n) = 2^n$

$n \mapsto 2^n$ $\qquad$ E' MONOMORFISMO

SE $n \neq m \Rightarrow 2^n \neq 2^m$

ABBIAMO + NEL DOMINIO

$g(n+m) = g(n) \cdot g(m)$

$2^{n+m} = 2^n \cdot 2^m \to$ E' VERO x PROP DELLE POTENZE

PRENDIAMO LA STESSA FUNZIONE, CAMBIAMO IL DOMINIO E IL CODOMINIO

$g: (\mathbb{N}_0, \cdot) \to (\mathbb{N}_0, \cdot)$ E' FUNZIONE INIETTIVA MA NON E' OMOMORFISMO!

$g(n \cdot m) = g(n) \cdot g(m)$

$2^{n \cdot m} = 2^n \cdot 2^m$

$g(1 \cdot 1) \neq g(1) \cdot g(1)$

$2^1 \neq 2 \cdot 2$

DEF. $(S, \perp)$, R CONGRUENZA SU S

$$\pi : S \to S/R \qquad x \mapsto [x]_R$$

E' EPIMORFISMO, DETTO PROIEZIONE CANONICA (NEL QUOZIENTE)

ex. $\pi : \mathbb{Z} \to \mathbb{Z}_m$
$a \mapsto [a]_m$

$$\underbrace{\pi(a \cdot b)}_{\mathbb{Z}} = [a \cdot b]_m = [a]_m \cdot [b]_m = \pi(a) \overset{\mathbb{Z}_m}{\cdot} \pi(b)$$

$$\underbrace{\pi(a+b)}_{\mathbb{Z}} = [a+b]_m = [a]_m + [b]_m = \pi(a) \underset{\mathbb{Z}_m}{+} \pi(b)$$

ESERCIZIO:

$(\mathbb{Z}, \perp)$

$n \perp m =: n + m - 5$

SI STUDI $(\mathbb{Z}, \perp)$ E SI DIMOSTRI CHE $f : x \in \mathbb{Z} \mapsto 5 - \mathbb{Z}$ E' ISOMORFISMO $(\mathbb{Z}, +)$ in $(\mathbb{Z}, \perp)$

1) E' ASSOCIATIVA? DEVE COMPORTARSI COME IL +

$(n \perp m) \perp \ell = (n + m - 5) \perp \ell = (n + m - 5 + \ell) - 5 = n + m + \ell - 10$

$n \perp (m \perp \ell) = n \perp (m + \ell - 5) = (n + m + \ell - 5) - 5 = n + m + \ell - 10$

2) E' COMMUTATIVA?

$n \perp m = n + m - 5 = m + n - 5 = m \perp n$

3) ESISTE UN ELEMENTO NEUTRO? $e \perp n$ NON L'HO SCRIVO POICHE' HO GIA' VISTO CHE $\perp$ E' COMMUTATIVA

$n \perp e = n \iff$

$\cancel{n} + e - 5 = \cancel{n} \iff e = 5$

4) OPPOSTI? ESISTE m |

$n \perp m = e \iff n + m - 5 = \overset{\text{L'ABBIAMO DETTO PRIMA}}{5} \iff n + m = 10 \iff m = 10 - n$

$n' = 10 - n$

L'ULTIMA COSA DA VEDERE E' CHE f SIA BIETTIVA E ...