

DEF X insieme, un'operazione su X è ARIELTA' se $\forall n \in \mathbb{N}$, $x_1, \dots, x_n \in X$ esiste $\star : X^n \rightarrow X$

$\star : \underbrace{X \times \dots \times X}_{n \text{ volte}} \rightarrow X$ (n volte X , su quanti elementi si applica per volta)

$$(x_1, \dots, x_n) \mapsto \star(x_1, \dots, x_n) = x_1 \star \dots \star x_n$$

se $n=2$ l'operazione si dice BINARIA

Ese $X = \mathbb{Z}$ $\star = \text{somma}$

ARIELTA' 1

$\star : \mathbb{Z} \rightarrow \mathbb{Z}$
 $x \mapsto -x$

Ese $\star = \text{somma}$ ARIELTA' 2

$\star : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$
 $(x, y) \mapsto + (x, y) =: x+y$

Ese $\star : \mathbb{Z}^2 \rightarrow \mathbb{Z}$
 $(a, b) \mapsto 2a + 3b$

ARIELTA' 2

Ese $X = \mathbb{R}$ $\star : \mathbb{R}^2 \rightarrow \mathbb{R}$
 $(a, b) \mapsto \sqrt[3]{a+b}$

Consideriamo operazioni binarie

Proprietà di \star

1) Commutativa $\forall a, b \in X \quad a \star b = b \star a$

2) Associativa $\forall a, b, c \in X \quad a \star (b \star c) = (a \star b) \star c$

3) Elemento neutro $u \in X$ è elemento neutro di \star se $\forall a \in X \quad u \star a = a \star u = a$
(overo non cambia)

4) Elemento inverso di $a \in X$ rispetto a \star

$a \star b = u$ \nearrow elemento neutro

Si dice che a è inverso sinistro di b

b è inverso destro di a

→ differenti quando \star non commutativa

Domanda: $\star : \mathbb{Z}^2 \rightarrow \mathbb{Z}$
 $(a, b) \mapsto 2a + 3b$

commutativa?
associativa?
elemento neutro?

• Comutativa: $\forall a, b \in \mathbb{Z}^2 \rightarrow a \star b = +(2 \cdot a, 3 \cdot b) = +(2 \cdot b, 3 \cdot a) = b \star a$

 $2a+3b = ?$
 $? = 2b+3a$

Ese. $1 \star 0 = 2 \cdot 1 + 3 \cdot 0 = 2 \neq 3 = 0 \star 1$

→ non vale $a, b \in \mathbb{Z}^2$, es: $a=2, b=3$:

$$\begin{array}{rcl} 4+3 & \neq & 6+6 \\ 13 & & 12 \end{array}$$

• Associativa: $\forall a, b, c \in \mathbb{Z} \rightarrow (a \star b) \star c = a \star (b \star c) = \dots$

• **Associativa**: $\forall a, b, c \in \mathbb{Z} \rightarrow (a * b) * c = a * (b * c)$

$$1 * (0 * 3) = 1 * 3 = 1 + 3 = 4$$

NO ASSOCIAZIONE

• **Elemento neutro**: λ è neutro se $\forall a \quad a * \lambda = \lambda * a = a$

$$2a + 3\lambda = a$$

$$\rightarrow a + 3\lambda = 0$$

scelgo $a = 0$ $0 + 3\lambda = 0 \rightarrow \lambda = 0$
 $a = 3$ $3 + 3\lambda = 0 \rightarrow \lambda = -1$

↓
I assieme valori
differenti per i diverse

↳ non vale la commutatività

Monoidi

Def. Un **semigruppo** è una coppia $(M, *)$ dove l'operazione è $*$: $M \times M \rightarrow M$
è un'operazione binaria **associativa**. Se $*$ è anche **comutativa** il semigruppo
si dice **comutativo** (l'esponente non è un semigruppo) (\Rightarrow **ABELIANO**).

Ese. $(\mathbb{N}, +)$ semigruppo comutativo

Ese. $(\mathbb{N} \setminus \{1\}, +)$ semigruppo comutativo
 $\hookrightarrow = \{2, 3, 4, 5, \dots\}$

"semigruppo numerico"
 \hookrightarrow solo x sottoinsieme dei naturali

Ese. $(\mathbb{N} \setminus \{2\} = \{1, 3, 4, 5, \dots\}, +)$ non è un semigruppo, + non è un'operazione su
 $\mathbb{N} \setminus \{2\}$
perché $1+1=2 \notin \mathbb{N} \setminus \{2\}$

$$+ : \mathbb{N} \setminus \{2\} \times \mathbb{N} \setminus \{2\} \rightarrow \mathbb{N} \setminus \{2\}$$

non è un'operazione

Def. Un **monide** è una tripla $(M, *, \lambda)$, dove $(M, *)$ è un semigruppo e $\lambda \in M$
è un elemento neutro, cioè $\forall x \in M \quad x = \lambda * x = x * \lambda$
Se l'operazione è comutativa, il monide si dice **comutativo** (\Rightarrow ABELIANO).

Prop. L'elemento neutro è unico

Dm Supponiamo esista $\mu \in M$ elemento neutro, $\forall x \in M \quad x = \mu * x = x * \mu$

Considero $\lambda \in M$, quindi $\lambda = \mu * \lambda = \lambda * \mu$ stesso elemento

Considero $\lambda \in M$,

quindi

$$\lambda = \mu + \lambda = \mu$$

e' neutro e' neutro

stesso elemento

□

Ese $(N, +, 0)$ monoide commutativo

Ese $(N, \cdot, 1)$ monoide commutativo

Ese $(N^*, \cdot, 1)$ monoide commutativo

Ese $(N^*, +)$ semi-gruppo commutativo, ma non un monoide (non ha el. neutro)

Ese $(Q, +, 0)$ monoide commutativo

Ese $(Q, \cdot, 1)$ " "

Ese $(Q_+, \cdot, 1)$ " "

Ese $(R \setminus Q, +)$ non sono un semi-gruppo $\rightarrow +: R \setminus Q \times R \setminus Q \rightarrow R \setminus Q$ non e'

Ese $(R \setminus Q, \cdot)$ " "

la stessa e' vero
con R el posto
di Q

ma $\sqrt{2} + (-\sqrt{2}) = 0 \notin R \setminus Q$

$\sqrt{2}, -\sqrt{2} \in R \setminus Q$

ma $\sqrt{2} + (-\sqrt{2}) = 0 \notin R \setminus Q$

Ese X insieme, $X \neq \emptyset \bullet (P(X), \cap)$ e' un semi-gruppo

$\cap: P(X) \times P(X) \rightarrow P(X)$

$$(A, B) \xrightarrow{\quad} A \cap B$$

ASSOCIAZIONE (per le proprietà di \cap):

$$(A \cap B) \cap C = A \cap (B \cap C)$$

COMMUTATIVO $A \cap B = B \cap A$

e' un monoide
(commutativo)

X e' el. neutro:

$$A \cap X = A = X \cap A$$

$$\begin{array}{l} A \in P(X) \\ A \subseteq X \end{array}$$

$\bullet (P(X), \cup)$ monoide commutativo

l'el. neutro e' il \emptyset

\cup e' associativa e commutativa

$\emptyset \cup A = \emptyset \cup A = A \quad \forall A \in P(X)$

Ese X insieme, $X \neq \emptyset$ $X^* := \{f: X \rightarrow X \text{ funzione}\}$

$$f \circ g: X^* \times X^* \rightarrow X^*$$

$$(f, g) \mapsto f \circ g$$

$(X^*, \circ, \text{Id}_X)$ e' un monoide

$$\begin{array}{c} \text{Id}: X \rightarrow X \\ x \mapsto x \end{array}$$

In generale non e' commutativo (comme $f \circ g \neq g \circ f$)
lo se $\exists X > 1$ ($f \neq g$)

$$X = N$$

$$(N^*, \circ, \text{Id}_N)$$
 non e' commutativo

$$f(x) = x+1$$

$$g(x) = 2x$$

$$f(x) = x+1 \quad g(x) = 2x$$

$$(f \circ g)(x) = 2x+1 \quad \text{ed esempio} \quad (g \circ f)(x) = 2x+2 \quad (f \circ g)(x) = 1 \neq x = (g \circ f)(x)$$

• Se $X = \{*\}$ singoloetto (X^*, \circ, Id) è monoido commutativo

$$X^* = \{(\leftarrow \rightarrow *)\} = \{\text{Id}_*\}$$

l'unica funzione che soddisfa il singoloetto è se stesso

B5 N definiamo un'operazione (dei ora binaria) $\sqcap : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$$a \sqcap b := \begin{cases} \text{lcm}(a, b) & \text{se } a \neq 0, b \neq 0 \\ a & \text{se } b = 0 \\ b & \text{se } a = 0 \end{cases}$$

$$\sqcap \text{ e' associativa} \quad a \neq 0, b \neq 0, c \neq 0 \quad \text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(\text{lcm}(a, b), c)$$

$$\text{se } (a=0) \vee (b=0) \vee (c=0) \quad a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$$

\sqcap è commutativa

$\rightarrow (\mathbb{N}, \sqcap, 0)$ monoido commutativo

Def $(M, *, \lambda)$ monoido, ip **monoido opposto** $(M, \bar{*}, \lambda)$ dove $x \bar{*} y = y * x$

B6 Se $(M, *, \lambda)$ è commutativo, $\bar{*} = *$. Quindi $(M, \bar{*}, \lambda) = (M, *, \lambda)$

Def $(M, *, \lambda)$ monoido, $a, b \in M$. Se

$$a * b = \lambda$$

Diciamo che a è **inverso sinistro** di b \rightarrow moltiplicando b a sinistra di b ottengo λ .

b è **inverso destro** di a \rightarrow " a a destra di a ".

Un elemento che ha un **inverso sinistro** (\neq **destro**) si dice **INVERTIBILE A SINISTRA** (\neq **A DESTRA**) rispettivamente

Se a ha sia inverso sx che inverso dx si dice **INVERTIBILE**.

Prop $(M, *, \lambda)$ monoido. Allora

1) λ è inverso sx e dx di se stesso

2) a è inverso sx di b , c inverso dx di b , allora $a=c$

[PROPRIETÀ]

(Quindi se un elemento ha un inverso allora l'inverso è unico: Indichiamo con a^{-1} l'inverso di a)

- 3) a è inverso sx di b , c inverso sx di d , allora $(c * a)$ è inverso sx di $(b * d)$
- 4) " " dx di b , c " dx di d , " $(c * a)$ è inverso dx di $(b * d)$
- 5) $(M, *, \lambda)$ è commutativo, $a \in M$, allora a ha inverso sx $\Leftrightarrow a$ ha inverso dx.
↳ quindi si parla in generale di "inverso".

Dim

- 1] $\lambda * \lambda = \lambda$
- 2] $a * b = \lambda$ $b * c = \lambda$ Tesi $a = c$
 $a = a * \lambda = a * (b * c) = (a * b) * c = \lambda * c = c$
 \downarrow
 prop. assoc. invert.

- 3] $a * b = \lambda$, $c * d = \lambda$ Tesi, $(c * a) * (b * d) = \lambda$

$$(c * a) * (b * d) = c * (a * b) * d = c * \lambda * d = (c * \lambda) * d = c * d$$

$\cancel{a * c}$ prop. associativa $= \lambda$

\downarrow
 non ha inverso
 specificare
 che sia commutativa

4) Analogamente alla 3]:

$$b * a = \lambda, d * c = \lambda \quad \text{tesi: } (b * d) * (c * a) = \lambda$$

$$(b * d) * (c * a) = b * (d * c) * a = b * \lambda * a = (b * \lambda) * a = b * a = \lambda$$

5) Sia $(M, *, \lambda)$ commutativo

$$\begin{aligned} &\text{se } a * b = \lambda \text{ allora } b * a = \lambda \quad a \text{ ha inverso } \cancel{\text{sx}} \quad \cancel{a \text{ ha inverso dx}} \\ &\text{se } b * a = \lambda \text{ allora } a * b = \lambda \end{aligned}$$

Ese • $(\mathbb{N}, +, 0)$ $\circ \circ$ l'unico elemento con inverso (non è commutativo, non specifica se inverso dx o sx)

1) $\exists c \in \mathbb{N}, c \neq 0$ allora $\nexists y \in \mathbb{N} \text{ t.c. } y + c = 0$

• $(\mathbb{Z}, +, 0)$ monoidre commutativo, ogni elemento ha inverso

2) • $(\mathbb{Q}, +, 0)$ " " " "
 • $(\mathbb{D}, +, 0)$ " " " "

$\exists \{ (\mathbb{Z}, \cdot, 1)$ monoidi commutativi. Gli unici elementi invertibili sono 1 e -1
 $(\mathbb{N}, \cdot, 1)$ " . L'unico el. invertibile e' 1

$\{ (\mathbb{Q}, \cdot, 1), (\mathbb{R}, \cdot, 1), (\mathbb{C}, \cdot, 1)$ monoidi commutativi, tutti gli elementi $\neq 0$
 hanno l'inverso

$\{ X$ insieme, $X \neq \emptyset$

INVERTIBILI $\Rightarrow (\mathcal{P}(X), \cap, X)$? non-commutativo

$A \in \mathcal{P}(X), A \subseteq X$

A ha inverso se $\exists B \in \mathcal{P}(X)$ t.c. $A \cap B = X = B \cap A$

• se $A \neq X$, coe' $A \not\subseteq X$ allora $\forall B \in \mathcal{P}(X) A \cap B \subseteq A \not\subseteq X \rightarrow A \cap B \neq X$

• se $A = X$ el. neutro, che ha inverso (ed e' se stesso)

INVERSO di $(\mathcal{P}(X), \cup, \emptyset)$?

$A \in \mathcal{P}(X)$

A ha inverso se $\exists B$ t.c. $A \cup B = \emptyset = B \cup A$

• se $A \neq \emptyset \rightarrow \exists a \in A, \forall b \in A \subseteq A \cup B \rightarrow A \cup B \neq \emptyset$

• unica possibilità e' che $A = \emptyset$ e solo \emptyset ha un inverso che e' se stesso

$\{ (\mathbb{N}, \sqcap, \sqcup)$ monoidi commutativi

$$a \sqcap b = \begin{cases} \text{HCD}(a, b) & \text{se } a \neq 0, b \neq 0 \\ a & \text{se } b = 0 \end{cases}$$

Quali el. hanno inverso?

- 0 perde verso

- $a \in \mathbb{N}, a \neq 0$ a ha inverso b se $a \sqcap b = 0$

- se $b = 0$ allora $a \sqcap b = a \neq 0$

- se $b \neq 0$ allora $a \sqcap b = \text{HCD}(a, b) \rightarrow$ l'el. che divide entrambi al peggior dei cost e' 1
 $\text{HCD}(a, b) \geq 1$

In particolare $a \sqcap b \neq 0$

$\rightarrow a$ non ha inverso (non riesco a ottenere l'el. neutro)

e . e . e . e . e . e . e

Dato l'invertibilità del monoide: $(\mathbb{N}, +, \lambda)$ $a, b \in \mathbb{N}$ t.c. $a + b = \lambda$

Dato $\text{set } M$, se a ha inverso Δx e Δy ,
questi coincidono e vengono detti
INVERSO DI A

$$\begin{aligned} & \text{inverso de } b \\ & \underline{\text{inverso de } b} \\ & \text{inverso de } a = b \quad | \rightarrow b = c \quad \Rightarrow \text{denote} \\ & \underline{a \times c = 1} \quad \text{on } a^{-1} \\ & \text{inverso de } x \end{aligned}$$

Teorema X insieme, $|X| \geq 2$, (X, \circ, Id_X) conosce, fissiamo $y \in X^{\times}$. Allora:

- i) f ha inverso $\Leftrightarrow f$ è iniettiva
 - ii) f ha inverso $\Leftrightarrow f$ è surgettiva
 - iii) f ha inverso $\Leftrightarrow f$ è bisettiva

Dim

i) f: X → X

$$= f(f(x)) = x \quad \forall x \in X$$

" \rightarrow " Significava che f obbliga inverso su $\rightarrow \exists g: X \rightarrow X$ t.c. $g \circ f = Id_X$

Sígueme $x, x' \in X$ d.c. $f(x) = f(x')$ GOAL: $x = x'$

$$f(x) = f(x') \xrightarrow{\text{apply } g} g(f(x)) = g(f(x')) \xrightarrow{\quad} x = x' \quad \underline{g \text{ is invertible}}$$

" " " " " "

 $\bar{x} \quad \bar{x}'$

" " " "

 $x \quad x'$

\rightarrow provides g is inv. \propto

" \leftarrow " suggestions of nine Hives

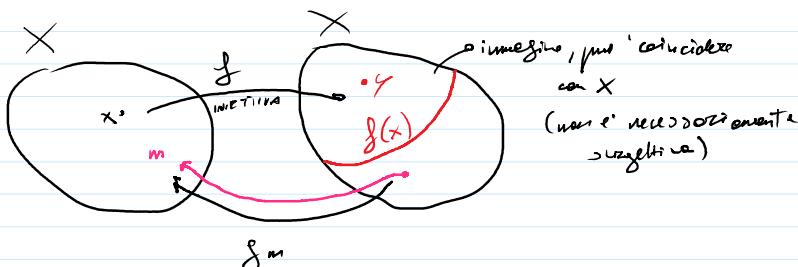
tesi: $\exists g \in X^*$ inverso \gg di f

Fusions $w \in X$

Definitions $f_m : X \rightarrow X$

$$g_m(y) = \begin{cases} x \in y \in f(x) & \rightarrow y \in f(x) \rightarrow \exists! x \in X \\ m \in y \notin f(x) & \text{i.e. } f(x) = y \end{cases}$$

! perde' l'iniezione



Verificazione che g_m è inversa su \mathcal{G}

$$x \in X \quad (g_m \circ f)(x) = g_m(f(x)) = x \quad g_m \circ f = \text{Id}_X$$

*Elements of f ,
not X*

well imagine $f(x)$

ii] " \rightarrow " supposons que f a une inverse $\Rightarrow \exists g \in X^*$ t.c. $f \circ g = \text{Id}_X$

Test : of suggestive

$f: X \rightarrow X$ $\exists x \in X \quad \forall y \in X \text{ d.c. } f(y) = x?$

Selego $y = g(x)$

$$g(\gamma) = g(g(x)) = \text{Id}_X(x) = x \quad \rightarrow \quad g \text{ surgettiva}$$

$$\leftarrow \text{ suggestion} \rightarrow \forall x \in X \quad g^{-1}(x) \neq \emptyset$$

$$\{y \in X \mid f(y) = x\}$$

→ per l'assunzione della scelta, scelgo $\forall x \in X$ un elemento $y_x \in f^{-1}(x)$

outra definição $g: X \rightarrow X$ t.e. $g(x) = y \in g^{-1}(x) \subseteq X$

g e' inversa da q

$$(f \circ g)(x) = f(g(x)) = f(y_x) = x \quad \forall x \in X$$

$\hookrightarrow y_x \in f^{-1}(x)$

$$ii] i) + ii) \quad \square$$

Def (M, \cdot, λ) monoid, $n \in \mathbb{N}$, $x \in M$, la potenza n -esima di x è:

$$x^n := \begin{cases} \lambda & n = 0 \\ \underbrace{x * \dots * x}_{n \text{ volte}} & n > 0 \end{cases} \quad \rightarrow \text{andamento ai numeri naturali: } z^0 = s^0 = 1 \text{ dove } z \text{ è neutro di } N$$

$$\underline{\text{Es}} \quad (X^*, o, \overline{\partial}d_n) \quad g \in X^*, \quad g^n = \underbrace{g \circ \dots \circ g}_{n \text{ malte}}$$

DFF Se $x \in M$ è invertibile, $n \in \mathbb{Z}$, $n < 0$

$$x^n := (x^{-1})^{ln} \quad \text{l'inverso di } x, \text{ elevato alle } n$$

! se $(M, +, \lambda)$ non è commutativo $(x+y)^n \neq x^n + y^n$

$$x+y \neq x+y + \dots + y \neq xy$$

$$\begin{aligned} \text{Vero! e vero} & \left\{ \begin{array}{l} x^n * x^m = x^{n+m} \\ (x^n)^m = x^{n \cdot m} \end{array} \right. \quad \text{se } x \text{ e' stesso elemento} \quad \} \text{ per qualunque monoide} \\ & \quad (\text{anche non commutativo}) \end{aligned}$$

Ese $(\mathbb{Q}, \cdot, 1)$

$$\mathbb{Q}^n = \mathbb{Q} \cdot \dots \cdot \mathbb{Q} \quad n > 0$$

$$\mathbb{Q}^0 = 1 \quad n = 0$$

$$\mathbb{Q}^n = (\mathbb{Q}^{-1})^{-n} = \left(\frac{1}{\mathbb{Q}}\right)^{\text{int}} \quad n < 0$$

$$\mathbb{Q}^{n+m} = \mathbb{Q}^n \cdot \mathbb{Q}^m$$

$(\mathbb{M}, *, \lambda)$

$$x^n := x * \dots * x \quad n > 0$$

$$x^0 := \lambda \quad n = 0$$

$$x^n := (x^{-1})^{\text{int}} \quad n < 0$$

$$x^{n+m} = x^n * x^m \quad n, m \geq 0$$

$$\underbrace{x * \dots * x}_{n+m \text{ volte}} \quad \underbrace{x * \dots * x}_{n \text{ volte}} * \underbrace{x * \dots * x}_{m \text{ volte}}$$

$$\begin{aligned} &\text{Se } n < 0, m > 0 \\ &x^m * x^n = x^{\underbrace{n + m}_{= -n} - 1} = x^{\underbrace{-n}_{= n \text{ volte}}} * x^m = x^m \end{aligned}$$

$$\begin{aligned} &\text{Se abbiano più } x \text{ che } x^{-1} \rightarrow = x^{\underbrace{m - (-n)}_{= m + n} - 1} \\ &\text{velte} \end{aligned}$$

Def $(\mathbb{M}, *, \lambda)$ monoidre, $M(\mathbb{M}) = \{m \in \mathbb{M} \mid \text{"m ha inverso}\} \subseteq \mathbb{M}$
(m è invertibile)

Ese $M(\mathbb{Z}) = \mathbb{Z}$ se intendo $(\mathbb{Z}, +, 0)$

$\Rightarrow \{-1, 1\}$ se intendo $(\mathbb{Z}, \cdot, 1)$

Def Un monoidre (abeliano) $(\mathbb{M}, *, \lambda)$ tale che ogni elemento ha inverso si dice:
gruppo (abeliano).

Ese $(\mathbb{Z}, +, 0)$ gruppo abeliano

$(\mathbb{Z}, \cdot, 1)$ non è un gruppo perché es. 2 non ha inverso ($\exists n \text{ t.c. } n \cdot 2 = 1$)

C, R $(\mathbb{Q}, +, 0)$ gruppo abeliano

C, R $(\mathbb{Q}, \cdot, 1)$ gruppo? no, perché 0 ∈ Q non è invertibile, $\exists c \in \mathbb{Q} \text{ t.c. } c \cdot 0 = 1$

C, R $(\mathbb{Q}^*, \cdot, 1)$ gruppo abeliano $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ || $(\mathbb{Q}^*, \cdot, 1)$ gruppo

Ese (X, \circ, Id_X) gruppo? In generale no (\circ $|X| = 1$ si), dipende da X .

$$\text{Bis}(X) := \{f: X \rightarrow X \text{ INVERSA}\}$$

$(\text{Bis}(X), \circ, \text{Id}_X)$ gruppo
(non abeliano)