

INSIEMI

L'INSIEMISTICA È LA BRANCA DELLA MATEMATICA CHE STUDIA I MODI PER RAGGRUPPARE UNA QUAISIASI COLLEZIONE DI ELEMENTI. NEL CONTESTO DEW ALGEBRA E DEWA LOGICA, SI RICHIAMANO I SEGUENTI INSIEMI FONDAMENTALI:

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ INSIEME DEI NUMERI NATURALI
- $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ INSIEME DEI NUMERI INTERI
- $\mathbb{Q} := \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \right\}$ INSIEME DEI NUMERI RAZIONALI
 - ! $\exists m \in \mathbb{N} \mid a = mb \rightarrow \frac{a}{b} = \frac{mb}{m} = m \Rightarrow \frac{a}{b} \in \mathbb{N}$
- $\mathbb{R} := \{\mathbb{N}\} \cup \{\mathbb{Z}\} \cup \{\mathbb{Q}\} \cup \{\pi, \sqrt{2}, e, \dots\}$ INSIEME DEI NUMERI REALI
- $\mathbb{C} := \{a + bi \mid (a, b \in \mathbb{R}) \wedge (i^2 = -1)\}$ INSIEME DEI NUMERI COMPLESSI

OSSERVANDO LE DEFINIZIONI NOMANO, AD ESEMPIO, CHE \mathbb{N} È SOTTOINSIEME DI \mathbb{Z} . QUESTO VIENE FORMALMENTE INDICATO CON IL SIMBOLO DI INCLUSIONE $\mathbb{N} \subseteq \mathbb{Z}$. IN CASO DI INCLUSIONE PROPRIA, OSSIA DATI DUE INSIEMI A, B $A \subseteq B \wedge A \neq \emptyset \wedge A \neq B$, SI INDICA CHE $A \subset B$.

IN GENERALE, UN INSIEME A HA DIMENSIONE INFINTA (AD ESEMPIO

QUELLI CITATI IN PRECEDENZA). IN CASO DI DIMENSIONE FINITA, INDICHIAMO CON $|A|$ LA SUA CARDINALITÀ (= NUMERO DI ELEMENTI).

AD ESEMPIO, PER L'INSIEME VUOTO \emptyset , $|\emptyset|=0$.

UN ALTRO STRUMENTO IMPORTANTE DA INTRODURRE È IL PRODOTTO CARTESIANO

DEI/INSIEME A CON L'INSIEME B DEFINITO CONE $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$. SI NOTI CHE, IN GENERALE, $A \times B \neq B \times A$ (NON VALE LA PROPRIETÀ COMMUTATIVA).

SI INTRODUCONO, INOLTRE, PER UN INSIEME A:

- L'INSIEME DEUE PARTI $A'(\mathcal{P}(A)) := \{A' \mid A' \subseteq A\}$
- DATO $A' \in \mathcal{P}(A)$, L'INSIEME COMPLEMENTARE DI A $\bar{A} = \{\alpha \in A \mid \alpha \notin A'\}$

FUNZIONI

SIANO A E B DUE INSIEMI. UNA FUNZIONE DA A IN B È UN SOTTOINSIEME $F \subseteq A \times B$ TALE CHE:

a) $(a, b_1) \in F \wedge (a, b_2) \in F \Rightarrow b_1 = b_2 \quad \forall a \in A \wedge b_1, b_2 \in B$

b) $\forall a \in A \exists b \in B \mid (a, b) \in F$

IN GENERE, LA FUNZIONE $F \subseteq A \times B$ VIENE INDICATA COME $F: A \rightarrow B$

E, SE $(a, b) \in F$, SCRIVIAMO $f(a) = b$

IN PARTICOLARE, LA FUNZIONE $I_{\text{OCA}}: A \rightarrow A$ | $I_{\text{OCA}}(\alpha) = \alpha$

VOLGA È CHIAMATA FUNZIONE IDENTITÀ SU A

DEFINIZIONI: UNA FUNZIONE $f: X \rightarrow Y$ È:

- INIETTIVA SE $f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \quad \forall x_1, x_2 \in X$
- SURIESSIVA $\text{Im}(f) = Y$, DOVE $\text{Im}(f) = \{f(x) \mid x \in X\} \subseteq Y$
- BIUNIVOLA SE INIETTIVA E SURIESSIVA

COMPOSIZIONE DI FUNZIONI SIANO $f: X \rightarrow Y$ E $g: Y \rightarrow Z$ DUE

FUNZIONI. LA FUNZIONE $g \circ f: X \rightarrow Z$ È DETTA FUNZIONE COMPOSTA

DI g CON f, DOVR $(g \circ f)(x) = g(f(x)) \quad \forall x \in X$

DEFINIZIONE: UNA FUNZIONE $f: X \rightarrow Y$ È INVERTIBILE SE ESISTE

LA FUNZIONE $g: Y \rightarrow X$, DETTA INVERSA DI f, TALIS CHE:

- $f \circ g = I_{\text{OcY}}$
- $g \circ f = I_{\text{OcX}}$

PROPOSIZIONE: UNA FUNZIONE $f: X \rightarrow Y$ È INVERTIBILE SE E SOLO SE

ESSA È BIUNIVOCA

DIM

\Rightarrow f INVERTIBILE $\Rightarrow \exists g \mid f \circ g = I_{\text{OcY}} \wedge g \circ f = I_{\text{OcX}}$, OSSIA

$f(g(y)) = y$ E $g(f(x)) = x$

- INIEZIONE FISSATO y | $g(y) = x_1 \wedge f(g(y)) = y$. ESSENDO

g UNA FUNZIONE, $g(y)$ PUÒ PRODURRE UN RISULTATO UNIVOCO

$$x_1 \Rightarrow f(x) = y \Leftrightarrow x = x_1 \quad \checkmark$$

SI RIUORDI CHE, IN GENERALE, $\exists x_1 \neq x_2, x_1, x_2 \in X$ TALI CHE

$f(x_1) = f(x_2) = y$ MA, IN QUESTO CASO, x_1 È GENERATO

DA $g(y)$, UNIVOCO PER DEFINIZIONE DI FUNZIONE

- SURIEZIONE $\forall x \in X \exists y \in Y | g(f(x)) = x$. ESSENDO UNA

FUNZIONE COMPOSTA TRA $f: X \rightarrow Y$ E $g: Y \rightarrow X$, POSSIAMO

CONCLUDERE CHE $f(x) \subseteq Y \forall x \in X$ (DEFINIZIONE DI IMMAGINE) \checkmark

\Leftarrow SFUITANDO LA SURIEZIONE, $\text{Im}(f) : \{f(x) | x \in X\}$. DAI' INIEZIONE,

$f(x_1) = y \Rightarrow f(x_2) = y \Leftrightarrow x_1 = x_2$. POICHÉ $\text{Im}(f) \subseteq Y$,

$\text{Im}(f) = Y = \{f(x_1), f(x_2) | x_1, x_2 \in X\}, y \in Y$, MA $x_1 = x_2$

$\Rightarrow \text{Im}(f) = \{f(x) | x \in X\} \Rightarrow \text{Im}(f) : Y \rightarrow X$. INOLTRE,

$f \circ \text{Im}(f) = f(\text{Im}(f)) = f(x) = \text{Id}_Y \Rightarrow g = \text{Im}(f) : Y \rightarrow X$

$| f \circ g = \text{Id}_Y \quad \checkmark$

INFINE, $g \circ f = g(f(x))$ E, RICORDANDO CHE $f(x)$ È BIUNIVOCO,

$f(x) = y \Rightarrow g \circ f = \text{Id}_X \quad \checkmark$

OPERAZIONI SU INSIEMI

DEFINIZIONE: UNA FUNZIONE $f: A \times A \rightarrow A$ È DETTA OPERAZIONE

SU A E, INVECE DI $f(a_1, a_2)$, SCRIVEREMO $a_1 * a_2$

DEFINIZIONE: UN'OPERAZIONE $*$ SU X È ASSOCIAUTIVA SE

$$x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3 \quad \forall x_1, x_2, x_3 \in X$$

DEFINIZIONE: UN'OPERAZIONE $*$ SU X È COMMUTATIVA SE

$$x_1 * x_2 = x_2 * x_1 \quad \forall x_1, x_2 \in X$$

ESEMPI:

a) $(\mathbb{P}(A))$ CON \cap È ASSOCIAUTIVA E COMMUTATIVA, COSÌ COME $(\mathbb{P}(A))$ CON \cup

- ASSOCIAUTIVA $\cap \quad A \cap B \cap C = (A \cap B) \cap C$

- COMMUTATIVA $\cap \quad A \cap B = B \cap A$

- ASSOCIAUTIVA $\cup \quad A \cup B \cup C = (A \cup B) \cup C$

- COMMUTATIVA $\cup \quad A \cup B = B \cup A$

b) $A \setminus B := A \cap \bar{B}$, DIFFERENZA INSIEMISTICA

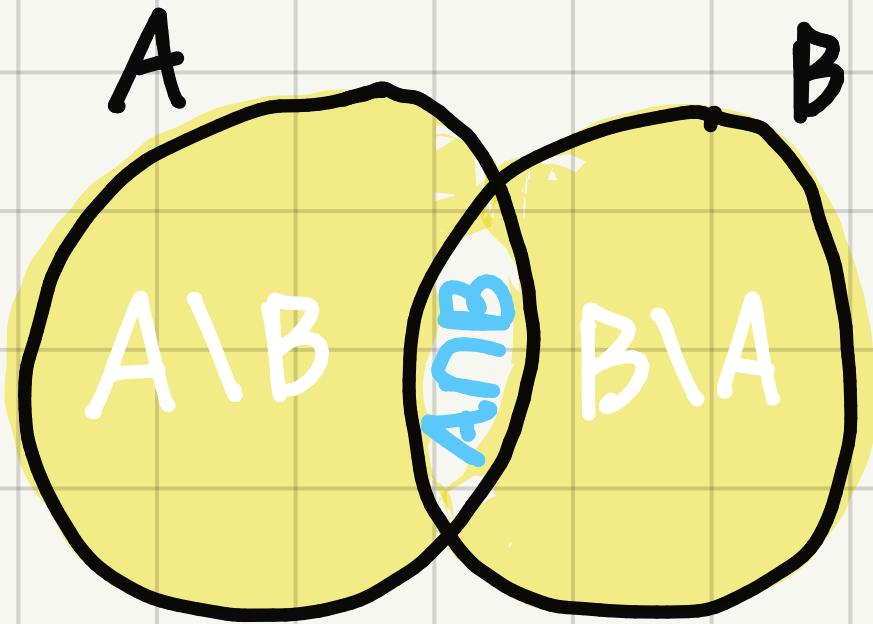
- NON ASSOCIAUTIVA, SIA $A \neq \emptyset \quad A \setminus (A \setminus A) = A \setminus \emptyset = A \neq$

$$(A \setminus A) \setminus A = \emptyset \setminus A = \emptyset$$

- NON COMMUTATIVA $A \setminus \emptyset = A \neq \emptyset \setminus A = \emptyset$

c) $A \Delta B := (A \setminus B) \cup (B \setminus A)$, DIFFERENZA SIMMETRICA

NOTAMO CHE $A \Delta B = (A \cup B) \setminus (A \cap B)$



- COMMUTATIVA \cap $A \Delta B = (A \setminus B) \cup (B \setminus A) =$

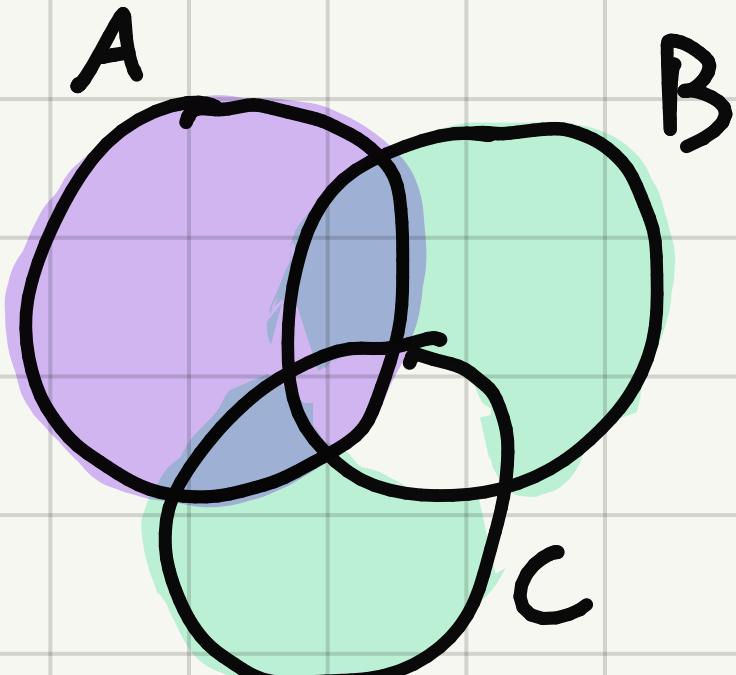
$$= (B \setminus A) \cup (A \setminus B) = B \Delta A$$

- ASSOCIAZIONE \cap $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

DIMOSTRAZIONE CON I DIAGRAMMI DI VENN

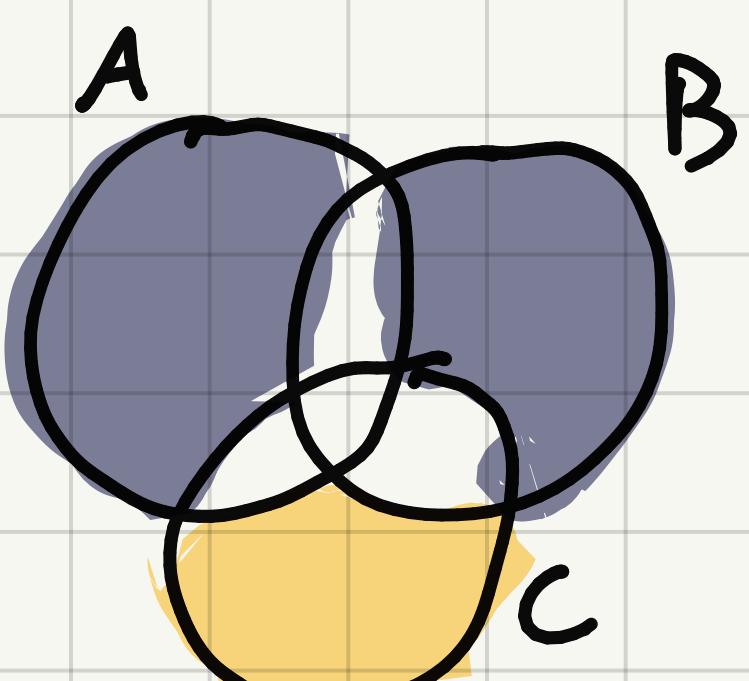
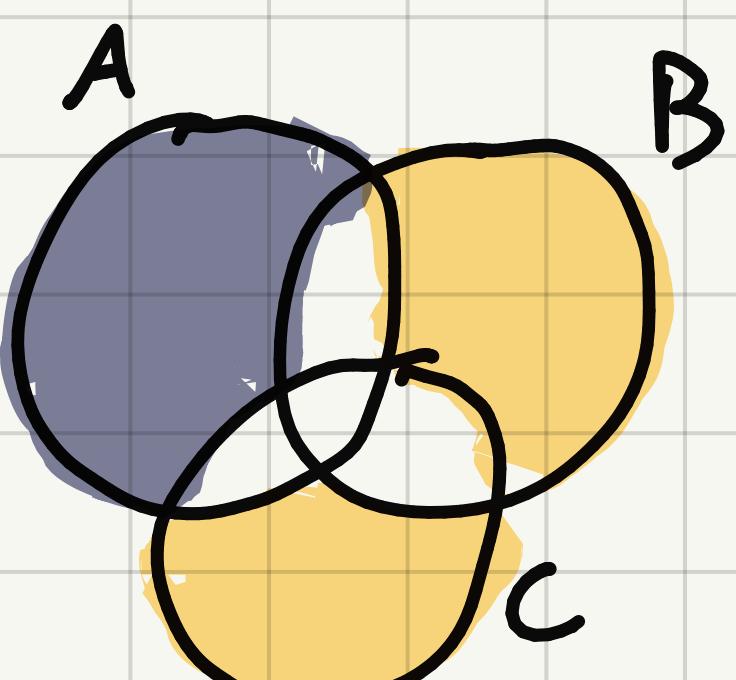
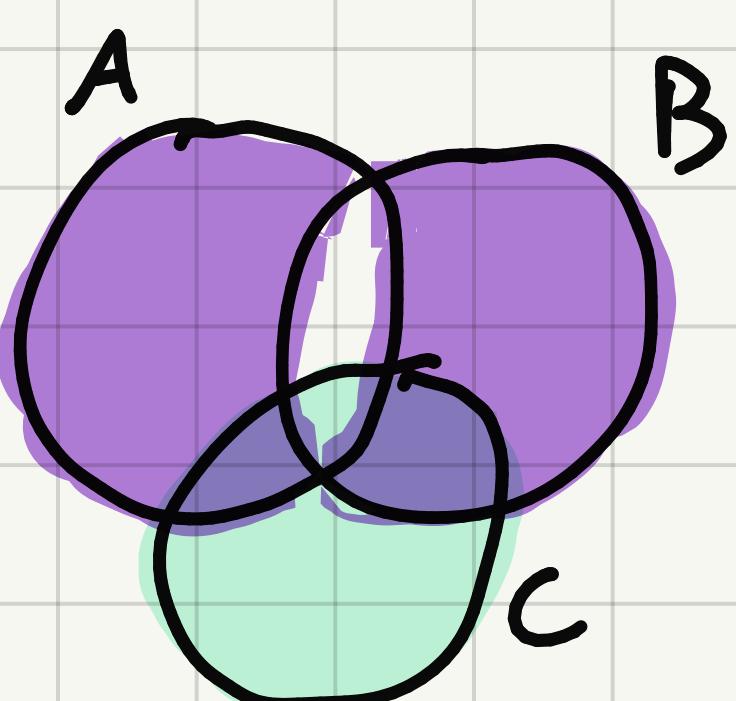
$$A \Delta (B \Delta C) =$$

$$A \setminus (B \Delta C) \cup (B \Delta C) \setminus A$$



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

$$(A \Delta B) \setminus C \cup (A \Delta B) \cap C$$



d) SIA $F(X) := \{f: X \rightarrow X\}$. LA COMPOSIZIONE È

- NON COMMUTATIVA $f_{v_1}(x) \circ f_{v_2}(x) = f_{v_1}(f_{v_2}(x)) \neq$

$$\neq f_{v_2}(x) \circ f_{v_1}(x) = f_{v_2}(f_{v_1}(x))$$

- ASSOCIAHVA $f_{v_1}(x) \circ (f_{v_2}(x) \circ f_{v_3}(x)) =$

$$= f_{v_1}(x) \circ f_{v_2}(f_{v_3}(x)) = f_{v_1}(f_{v_2}(f_{v_3}(x))) =$$

$$(f_{v_1}(x) \circ f_{v_2}(x)) \circ f_{v_3}(x) = f_{v_1}(f_{v_2}(x)) \circ f_{v_3}(x) =$$

$$f_{v_1}(f_{v_2}(f_{v_3}(x)))$$

e) $a * b = \frac{a+b}{2}$

- COMMUTATIVA $a * b = \frac{a+b}{2} = \frac{b+a}{2} = b * a$

- NON ASSOCIAHVA

$$\bullet a * (b * c) = a + \frac{b+c}{2} = \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4}$$

$$\bullet (a * b) * c = \frac{a+b}{2} + c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4}$$

DEFINIZIONE: SIA $*$ UN'OPERAZIONE SU X . L'IDENTITÀ DI X È

UN ELEMENTO $i \in X$ | $i * x = x * i = x \quad \forall x \in X$. L'IDENTITÀ È UNICA,

OSSIA $i_1, i_2 \in X \Rightarrow i_1 * i_2 = i_1 = i_2 = i$

DEFINIZIONE: UN INSIEME X CON UN'OPERAZIONE ASSOCIAHVA $*$ ED

UNA IDENTITÀ È DETTO MONOIDE

ESEMPI:

a) $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; $* = +$; $\lambda = 0$

b) $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; $* = \cdot$; $\lambda = 1$

c) $P(X)$; \cap ; $\lambda = X$

d) $P(X)$; \cup ; $\lambda = \emptyset$

e) $F(X) := \{\rho : X \rightarrow X\}$; $\lambda = I_0(x)$

In un monoido con operazione $*$, invece di $x * y$ si scrive xt

DEFINIZIONE: SIA A UN MONOIDO. UN ELEMENTO $a \in A$ È INVERIBILE

SE ESISTE $a^{-1} \in A$ | $a a^{-1} = a^{-1} a = i$ E a^{-1} È DETTO INVERSO DI a

PROPRIETÀ: L'IDENTITÀ DEL MONOIDO È SEMPRE INVERIBILE E IL SUO

INVERSO È L'IDENTITÀ STESSA

ESEMPI:

a) L'INSIEME DEGLI ELEMENTI INVERIBILI DI $(\mathbb{N}, +)$ È $\{0\}$

b) L'INSIEME DEGLI ELEMENTI INVERIBILI DI $(\mathbb{Z}, +)$ È \mathbb{Z} , DI

$(\mathbb{Q}, +)$ È \mathbb{Q} , DI $(\mathbb{R}, +)$ È \mathbb{R} , DI $(\mathbb{C}, +)$ È \mathbb{C}

c) L'INSIEME DEGLI ELEMENTI INVERIBILI DI (\mathbb{N}, \cdot) È $\{1\}$, DI

(\mathbb{Z}, \cdot) È DI $\{-1, 1\}$

- d) L'insieme degli elementi invertibili di (\mathbb{Q}, \cdot) è $\mathbb{Q} \setminus \{0\}$, di (\mathbb{R}, \cdot) è $\mathbb{R} \setminus \{0\}$, di (\mathbb{C}, \cdot) è $\mathbb{C} \setminus \{0\}$
- e) L'insieme degli elementi invertibili di $(PC(X), \cap)$ è $\mathcal{X} \setminus \{\emptyset\}$, di $(PC(X), \cup)$ è $\mathcal{X} \setminus \{\emptyset\}$

P) L'insieme degli elementi invertibili di $F(X) = \{f : X \rightarrow X\}$ è l'insieme delle funzioni invertibili, ossia delle funzioni bivincolate da X in X

DEFINIZIONE: UN MONOIDE I CUI ELEMENTI SONO TUTTI INVERTIBILI È CHIAMATO GRUPPO. SE L'OPERAZIONE * È COMMUTATIVA, IL GRUPPO È DETTO COMMUTATIVO (O ABELIANO)

ESEMPI:

- a) $(PC(X), \Delta)$. L'identità è \emptyset ; l'inverso di $A \in PC(X)$ è A stesso, in quanto $A^2 = \emptyset \quad \forall A \subseteq X$
- b) $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; $(\mathbb{C}, +)$
- c) $(\mathbb{Q} \setminus \{0\}, \cdot)$; $(\mathbb{R} \setminus \{0\}, \cdot)$; $(\mathbb{C} \setminus \{0\}, \cdot)$
- d) SIA $X = \{1, 2, \dots, n\}$. L'insieme delle funzioni invertibili $f : X \rightarrow X$ è il gruppo delle permutazioni di n elementi (o gruppo

SIMMETRICO) S_n , CON $|S_n| = n!$, NON ABELIANO $\forall n \geq 3$

DEFINIZIONE: SIA X UN MONOIDE CON IDENTITÀ i ED OPERAZIONE $*$.

UN SOTTOINSIEME $Y \subseteq X | i \in Y \wedge a * b \in Y \forall a, b \in Y$ SI DICE SOTTONOIDE.

DEFINIZIONE: SIA G UN GRUPPO CON IDENTITÀ i ED OPERAZIONE $*$.

UN SOTTOINSIEME $H \subseteq G | h^{-1} \in H \forall h \in H \rightarrow h * h^{-1} = i \wedge h_1 * h_2 \in H$

$\forall h_1, h_2 \in H$ SI DICE SOTTOGRUPPO. IN PARTICOLARE, L'INSIEME $\{i\} \subseteq G$

PRENDE IL NOME DI SOTTOGRUPPO BANALE.

ESEMPI:

a) $\{0\} \subseteq (\mathbb{N}, +)$ SOTTONOIDE

b) CATENA DI SOTTONOIDI $(\{1\}, \cdot) \subseteq (\mathbb{N}, \cdot) \subseteq (\mathbb{Z}, \cdot) \subseteq (\mathbb{Q}, \cdot) \subseteq (\mathbb{R}, \cdot) \subseteq (\mathbb{C}, \cdot)$

c) CATENA DI SOTTOGRUPPI $(\{1\}, \cdot) \subseteq (\mathbb{Q} \setminus \{0\}, \cdot) \subseteq (\mathbb{R} \setminus \{0\}, \cdot) \subseteq (\mathbb{C} \setminus \{0\}, \cdot)$

DEFINIZIONE: SIA X UN MONOIDE E $S \subseteq X$ UN SOTTOINSIEME. IL

SOTTONOIDE DI X GENERATO DA S $\langle S \rangle$ È DEFINITO COME L'

INTERSEZIONE DI TUTTI I SOTTONOIDI DI X CHE CONTENGONO S .

ANALOGAMENTE SI DEFINISCE IL SOTOGRUPO GENERATO DA $S \subseteq X$.

(SI NOTI CHE L'INTERSEZIONE DI SOTOMONOIDI È UN SOTOMONOIDE E CHE
L'INTERSEZIONE DI SOTOGRUPPI È UN SOTOGUARPO)

ESEMPI:

a) $S = \{1\} \subseteq (\mathbb{N}, +) \Rightarrow \langle S \rangle = \langle \{1\} \rangle = \{0, 1, 2, \dots\} = \mathbb{N}$

P È PRIMO

b) $S = \{p \in \mathbb{N} \mid \exists k, m \in \mathbb{N} \text{ } l.p = km\} \subseteq (\mathbb{N}, \cdot) \Rightarrow \langle S \rangle = \mathbb{N} \setminus \{0\}$

c) $S = \{0, 1\} \subseteq (\mathbb{N}, \cdot) \Rightarrow \langle S \rangle = S$

DEFINIZIONE: SIANO M_1, M_2 MONOIDI CON IDENTITÀ, RISPECTIVAMENTE,

$i_{M_1} \in i_{M_2}$. IL PRODOTTO DIRETTO DI M_1 CON M_2 È IL MONOIDE $M_1 \times M_2$ CON

IDENTITÀ (i_{M_1}, i_{M_2}) ED OPERAZIONE $(a_{M_1}, b_{M_1})(a_{M_2}, b_{M_2}) = (a_{M_1}a_{M_2}, b_{M_1}b_{M_2})$

$\forall a_{M_1}, a_{M_2} \in M_1; b_{M_1}, b_{M_2} \in M_2$. ANALOGAMENTE SI DEFINISCE IL PRODOTTO

DIRETTO DEL GRUPPO G_1 COL GRUPPO G_2 $G_1 \times G_2$ E, IN TAL CASO, DATO

$(g_1, g_2) \in G_1 \times G_2$, IL SUO INVERSO È $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$

MORFISMI

SIANO M_1, M_2 MONOIDI CON IDENTITÀ, RISPECTIVAMENTE, $i_{M_1} \in i_{M_2}$.

UNA FUNZIONE $f: M_1 \rightarrow M_2$ È UN MORFISMO DI MONOIDI SE:

- $f(i_{M_1}) = i_{M_2}$
- $f(xy) = f(x)f(y) \quad \forall x, y \in M_1$

IL NUOVO DI UN MORFISMO DI MONOIDI $f: M_1 \rightarrow M_2$ È IL SOTTONOIDE
DI M_1 DEFINITO COME $\text{Ker}(f) := \{x \in M_1 \mid f(x) = i_2\}$. ANALOGAMENTE,

UNA FUNZIONE $f: G_1 \rightarrow G_2$ È MORFISMO DI GRUPPI SE $f(x \cdot y) = f(x) f(y)$

$\forall x, y \in G_1$ IL NUOVO DI UN MORFISMO DI GRUPPI È IL SOTTOGRUPPO DI

G_2 $\text{Ker}(f) := \{x \in G_1 \mid f(x) = i_2 \in G_2\}$ E $\text{Im}(f)$ È UN SOTTOGRUPPO DI G_2 .

DEFINIZIONE: UN ISOMORFISMO DI MONOIDI / GRUPPI È UN MORFISMO

BIUNIVOCO TALE CHE LA FUNZIONE INVERSA SIA UN MORFISMO.

IN REALTÀ, LA CONDIZIONE PER CUI LA FUNZIONE INVERSA SIA UN MORFISMO
È SUPERFLUA

PROPOSIZIONE: SIA $f: M_1 \rightarrow M_2$ UN MORFISMO DI MONOIDI. SE f È

BIUNIVOCO, ALLORA È UN ISOMORFISMO

DIM

OBBIETTIVO: MOSTRARE CHE $f^{-1}: M_2 \rightarrow M_1$ È UN MORFISMO DI MONOIDI

- $f(i_{M_1}) = i_{M_2} \Rightarrow f^{-1}(i_{M_2}) = i_{M_1}$ PER BIUNIVOCITÀ
- SIANO $x_2, y_2 \in M_2 \Rightarrow \exists x_1, y_1 \in M_1 \mid f(x_1) = x_2, f(y_1) = y_2,$

$$f(x_1 \cdot y_1) = f(x_1) f(y_1) = x_2 \cdot y_2 \Rightarrow \text{PER BIUNIVOCITÀ, } f^{-1}(x_2 \cdot y_2) =$$

$$= f^{-1}(f(x_1 \cdot y_1)) = x_1 \cdot y_1 = f^{-1}(x_1) f^{-1}(y_1)$$



PROPOSIZIONE ANALOGA VALE PER I MORFISMI DI GRUPPI

ESEMPI:

a) SIANO $M_1 = (\mathcal{P}(X), \cap)$ E $M_2 = (\mathcal{P}(X), \cup)$, DOVE X È UN INSIEME.

SIA $f: M_1 \rightarrow M_2$ DEFINITA COME $f(A) = \bar{A} \forall A \subseteq X$

- $f(A_1) = \bar{A}_1 \wedge f(A_2) = \bar{A}_2 \Leftrightarrow A_1 \in A_2 \forall A_1, A_2 \subseteq X \quad \left. \begin{array}{l} \\ \\ \end{array} \right\}$ BIUNIVOC
- $f^{-1}(A) = A \forall A \subseteq X$
- $f(A \cap B) = \overline{A \cap B} = \bar{A} \cup \bar{B} = f(A) \cup f(B) \quad \checkmark$
- $i_1 = X (A \cap X = A \forall A \subseteq X)$
- $i_2 = \emptyset (A \cup \emptyset = A \forall A \subseteq X)$
- $f(X) = \bar{X} = \emptyset \quad \checkmark$

$\Rightarrow f$ È UN ISOMORFISMO

b) SIA $\mathbb{Z}_2 := \{0, 1\}$ CON L'OPERAZIONE

COSÌ DEFINITA È $X := \{1, 2, \dots, n\}, n \in \mathbb{N}$

+	0	1
0	0	1
1	1	0

LA FUNZIONE $f: \mathcal{P}(X) \rightarrow \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 = (\mathbb{Z}_2)^n$ DEFINITA DA

$f(A) = (a_1, \dots, a_n)$, CON $a_{ij} = \begin{cases} 0 & i \notin A \\ 1 & i \in A \end{cases} \forall A \subseteq X$ È

UN ISOMORFISMO DEL GRUPPO $(\mathcal{P}(X), \Delta)$ CON $(\mathbb{Z}_2)^n$

OGNI MONOIDE FINITO È ISOMORFO AD UN MONOIDE DIMATRICE QUADRATA

DOVE L'OPERATORE È IL PRODOTTO RIGHE PER COLONNE

SIA $M = \{x_1, \dots, x_n\}$ UN MONOIDE DI CARDINALITÀ $|M| = n \in \mathbb{N}$ ED

IDENITÀ $i=x_1$. PER OGNI $x \in M$ DEFINIAMO UNA MATRICE

$A(x) \in \mathbb{Z}_{n \times n}$ NEL SEGUENTE MODO: $A(x)_{ii} = \begin{cases} 1 & x \cdot x_i = x_i \\ 0 & \text{ALTRIMENTI} \end{cases}$

LA FUNZIONE $F: \begin{matrix} M \rightarrow \mathbb{Z}_{n \times n} \\ x \mapsto A(x) \end{matrix}$ È INIEZIVA POICHÉ $A(x) = A(y) \Rightarrow$

$\Rightarrow A(x)_{ii} = A(y)_{ii} \forall i \in \{1, \dots, n\}$. QUINDI $A(x)_{ii} = A(y)_{ii} \Rightarrow$

$\Rightarrow x \cdot x_i = x_i = y \cdot x_i = y$. È INOLTRE FACILE VEDERE CHE $A(xy) =$

$= A(x)A(y)$ DAL PRODOTTO RIGHE PER COLONNE $\Rightarrow F$ È UN MORFISMO

DI MONOIDI $(\mathbb{Z}_{n \times n}, \cdot)$ È UN MONOIDE CON IL PRODOTTO RIGHE PER COLONNE LA

CUI IDENITÀ È LA MATRICE $I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \Rightarrow F: \begin{matrix} M \rightarrow \mathbb{Z}_{n \times n} \\ x \mapsto A(x) \end{matrix}$ È UN

ISOMORFISMO DI MONOIDI

ESEMPIO: SIA $M = (\mathbb{Z}_2, \cdot)$ IL MONOIDE DEFINITO DA

$$\begin{array}{c|cc|c} \bullet & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \end{array}$$

COSTRUIAMO UN SOTTONOIDE DI $\mathbb{Z}_{4 \times 4}$ ISOMORFO AD $M \times M =$

$\{ (0,0), (0,1), (1,0), (1,1) \}$

•	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)^*$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)^*$	$(0,1)^*$	$(0,0)^*$	$(0,1)^*$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

$$\mathbb{Z}_4(m)_{ii} = 1 \quad \text{SE } m \cdot m_i = m_i$$

ESEMPI

$$(0,1) \cdot (0,0) \xrightarrow{\hspace{1cm}} (0,0) = (0,0) \checkmark$$

$$(0,1) \cdot (1,1) \xrightarrow{\hspace{1cm}} (0,1) \neq (1,1)$$

$$(0,0) \mapsto \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad (1,0) \mapsto \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{vmatrix}$$

$$(0,1) \mapsto \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad (1,1,0) \mapsto \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

SI PUÒ VERIFICARE DIRETTAMENTE CHE LE MATERI MANNO LA STESSA

TABELLA MOLTIPLICATIVA.

ABBIAMO VISTO CHE UN MONOIDE FINITO DI CARDINALITÀ n È ISOMORFO A UN

MOLTADE DI MATRIU $n \times n$ LE AI COLONNE MANNO UN UNICO "1" E ALTRONE SONO "0".

OGNUNA DI QUESTE MATERICI PUÒ ESSERE VISTA COME UNA FUNZIONE DA

$X = \{1, \dots, n\}$ IN X : $A_{ij} = \begin{cases} 1 & f_i(j) = i \\ 0 & f_i(j) \neq i \end{cases}$. IL PRODOTTO RIGHE

PER COLONNE CORRISPONDE ALLA COMPOSIZIONE DI FUNZIONI, QUINDI UN MONOIDE

FINITO DI CARDINALITÀ n È ISOMORFO A UN SOTTOMONOIDE DEL MONOIDE DEI

FUNZIONI f DA $\{1, \dots, n\}$ IN $\{1, \dots, n\}$ CON L'OPERAZIONE DI COMPOSIZIONE.

NOMAMO CHE UN ELEMENTO x IN UN MONOIDE FINITO M È INVERIBILE SE

E SOLO SE LA MATERICE ASSOCIAVA È INVERIBILE (UNA MATERICE $A \in \mathbb{Z}_{n \times n}$

È INVERIBILE SE E SOLO SE IL SUO DETERMINANTE È INVERIBILE SU \mathbb{Z} ,