||mat. discreta||

num. telefono: ~~06725960~~
067259467

email:

brenti@mat.uniroma2

ricev. studenti: mer. 16-18
o
su appuntamento

|TESTO|: online gratuito

OCW.MIT.EDU/COURSES/ELECTRICAL-
-ENGINEERING-AND-COMPUTER-SCIENCE/
/6_042J_MATHEMATICS_FOR_COMPUTER_
_SCIENCE_SPRING_2015/MIT6_042JS15_
-textbook.pdf

|ESAME|: Orale

ammissione all'orale → Test a scelta multipla
(12 domande x 5 risposte)
(+4 = RISPOSTA CORRETTA,
-1 = " ERRATA)

↓

punteggio ≥ 24 ammissione

+10 punti se studente
è nel top 25%

|ESERCIZI|: [1], [2], [3]

[1]: 10-20 min

[2]: 20-60 min

[3]: 1-4 ore

PREAMBOLO: COS'È LA MATEMATICA?

Esempio: Wimbledon: 128 giocatori

quesito: quante ~~pa~~ partite vengono giocate in totale?

$$\underset{1^\circ \text{ turno}}{64} + \underset{2^\circ \text{ turno}}{32} + \dots + 2 + 1$$

D'altraparte → tutti perdono una partita

⇓

Ogni ~~partita~~ partita ha esattamente un perdente e ogni giocatore perde esattamente una partita (tranne il vincitore)

⇓

\# partite giocate = # giocatori sconfitti =

= 128 - 1

CAPITOLO 1: Il linguaggio degli insiemi

1.1. Insiemi

Tutto in matematica è un insieme.

Concetti primitivi → insieme
elemento
appartenenza

def. di insieme (intuitivamente) → è una collezione di oggetti, detti elementi, appartenenti all'insieme

Scrittura di un insieme → elenco degli elementi, separati da virgola, racchiusi in una parentesi graffe

esempio: $A = \{\text{linea}, 3, \text{sedia}\}$

OSSERVAZIONI:
- In un insieme, l'ordine NON conta
  → infatti
  $$\{1,2\} = \{2,1\}$$
  Due insiemi sono uguali (=) se contengono gli stessi elementi
- In un insieme, non ci sono ripetizioni
  esempio: $\{1,2,2\}$ NON È UN INSIEME

L'insieme vuoto $\longrightarrow$ insieme che non ha elementi

$$\emptyset$$

$$\emptyset = \{\ \}$$

Notazione:

$$\mathbb{N} \overset{def}{=} \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} \overset{def}{=} \{0, -1, 1, -2, \dots\}$$

$$\mathbb{Q} \overset{def}{=} \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

se $a \in \mathbb{N}$ allora:

$$[a] \overset{def}{=} \{0, 1, 2 \dots a\}$$

Notazione:

$A \overset{def}{=} \{\ \}$ oppure $A := \{\ \}$

significa che A è, per definizione, l'insieme sulla destra

Sia P una proprietà che un elemento può avere o no. Allora:

$$A \overset{\text{def.}}{=} \left\{ x \overset{\text{"tale che"}}{:} \underbrace{x \text{ ha } P}_{\text{proprietà}} \right\}$$

(esempio: tutti i numeri ~~...~~ sono pari)

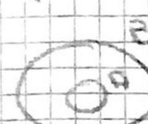
Significa che A è l'insieme che hanno la proprietà P

1.2. Operazioni tra insiemi

Siano A, B insiemi:

Definizione → Si dice che A è un sottoinsieme di B ($\text{scritto } A \subseteq B$) se ogni elemento di A è anche a B

↓
graficamente

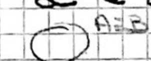


A è sottoinsieme di B

$A \overset{\subset}{\neq} B$ per dire che $A \subseteq B$ e $A \neq B$
A è sottoinsieme di B ma gli elementi di A non appartengono all'insieme B

Osservazione: $A \subseteq B$ e $B \subseteq C \Rightarrow A \subseteq C$

Osservazione: $A = B$ se e solo se $A \subseteq B$ e $B \subseteq A$



Defi. → L'insieme di A e B è l'insieme

$$A \cup B \overset{\text{def}}{=} \{x : x \in A \text{ o } x \in B\}$$

unione dei due insiemi con elementi non in comune

Def. → Intersezione:

$$A \cap B \overset{\text{def}}{=} \{x \in A : x \in B\}$$

unione dei due insiemi con elementi in comune

Esercizio [1]

- È sempre vero che $A = B$ se e solo se $A \cup B = A \cap B$?

Siano A, B, C insiemi. Allora:

1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

(Proprietà Distributiva)

3) $(A \cup B) \cup C = A \cup (B \cup C)$;
4) $(A \cap B) \cap C = A \cap (B \cap C)$;

(Proprietà Associativa)

Dimostrazione:

è un sottoinsieme

1) Dimostriamo che $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ (1)
e che $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$ (2)

(1)
Sia $x \in A \cap (B \cup C)$. Allora $x \in A$ e $x \in \underbrace{B \cup C}_{\substack{\text{non so} \\ \text{se } x \in B \\ \text{o } C}}$

$\Rightarrow x \in A$ e $(x \in B$ o $x \in C)$

essendo $A \cap (B \cup C)$

Se
- $x \in B \Rightarrow x \in A \cap B \Rightarrow x \in (A \cap B) \cup (A \cap C) \Rightarrow$ O.K

- Se $x \in C \Rightarrow x \in A \cap C \Rightarrow x \in (A \cap B) \cup (A \cap C) \Rightarrow$ O.K

(2)

Sia $x \in (A \cap B) \cup (A \cap C) \Rightarrow$ o $x \in A \cap B$ o
$x \in A \cap C$

↳ essendo che [illegible]

Supponiamo che:

- $x \in A \cap B \Rightarrow x \in A$ e $x \in B \Rightarrow x \in A$ e ~~$x \in B$~~ e $x \in B \cup C \Rightarrow x \in A \cap (B \cup C) \Rightarrow$ OK

- $x \in A \cap C \Rightarrow x \in A$ e $x \in C \Rightarrow x \in A$ e $x \in B \cup C \Rightarrow$
$\Rightarrow x \in A \cap (B \cup C) \Rightarrow$ OK

Similmente 2), 3), 4)

Sia

$$\mathcal{R} \overset{def}{=} \{ A : A \notin A \} \quad (*)$$

esempio:
$\mathbb{N} \in \mathcal{R}$ (perché $\mathbb{N} \notin \mathbb{N}$)

<u>Domanda</u>: $\mathcal{R} \in \mathcal{R}$?

↳ - se $\mathcal{R} \in \mathcal{R} \underset{(*)}{\Rightarrow} \mathcal{R} \notin \mathcal{R}$ ↳ assurdo

- se $\mathcal{R} \notin \mathcal{R} \underset{(*)}{\Rightarrow} \mathcal{R} \in \mathcal{R}$ ↳ assurdo!

Per evitare paradossi si assume l'esistenza di un <u>INSIEME UNIVERSO $\mathcal{U}$</u> di cui tutti gli insiemi sono sottoinsiemi

Sia A un <u>insieme</u>.

<u>Def.</u> → Il <u>complementare</u> di A è l'insieme
$$A' \overset{def}{=} \{ x \in \mathcal{U} : x \notin A \}$$
(si scrive anche $C A$)

Siano A, B insiemi, allora

$$(A \cup B)' = (A') \cap (B')$$

e

$$(A \cap B) = (A') \cup (B')$$

LEGGI DI DE MORGAN

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

1ª legge

Dim. : Sia $x \in \overline{(A \cup B)}' \Rightarrow \underline{x \notin A \cup B} \Rightarrow$

essendo complementare, ha come proprietà

$\Rightarrow x \notin A$ e $x \notin B$

(se $x \in A \Rightarrow x \in A \cup B$, assurdo) $\Rightarrow$

nel caso in cui $x \in A$, si arriva ad un assurdo in quanto x non deve appartenere a $A \cup B$

$\Rightarrow x \in A'$ e $x \in B' \Rightarrow x \in A' \cap B'$

Viceversa. Sia $x \in (A') \cap (B') \Rightarrow x \in A'$ e
e $x \in B' \Rightarrow x \notin A$ e $x \notin B \Rightarrow$
$\Rightarrow x \notin A \cup B$

($x \in A \cup B \Rightarrow x \in A$ o $x \in B$, assurdo) $\Rightarrow$
$\Rightarrow x \in (A \cup B)'$

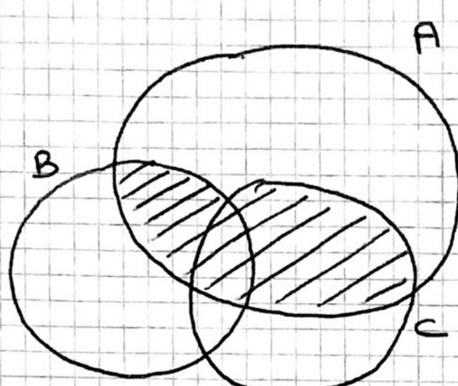
Def $\rightarrow$ La differenza di A e B è
$$A \setminus B \overset{def}{=} \{x \in A : x \notin B\}$$

Def $\rightarrow$ La differenza simmetrica è
$$A \Delta B \overset{def}{=} (A \setminus B) \cup (B \setminus A)$$

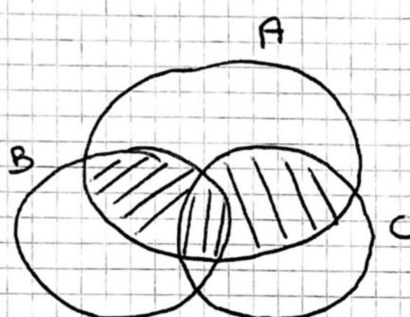
DIAGRAMMI DI VENN

Si rappresenta ogni insieme coi i punti racchiusi da una curva chiusa

esempio:

1) 

$A \cap (B \cup C)$

2) 

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

METODO DELLE TAVOLE DI VERITÀ

prendo $x \in U$. Allora:

o $x \in A$ o $x \notin A$

o $x \in B$ o $x \notin B$

o $x \in C$ o $x \notin C$

A	B	C	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1
1	1	0	1	0	1
1	0	1	0	1	1
1	0	0	0	0	0
0	1	1	0	0	0
0	1	0	0	0	0
0	0	1	0	0	0
0	0	0	0	0	0

$B \cup C$	$A \cap (B \cup C)$
1	1
1	1
1	1
0	0
1	0
1	0
1	0
0	0

legenda:
1 = si
0 = no

considerazioni: $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$

E' importante notare che:

- Tavola di verità dimostra, non aiuta l'intuizione
- Diagramma di Venn aiuta l'intuizione, ma non dimostra
- Ragionamento dimostra ma ha bisogno dell'intuizione

Esercizio [1]: Dimostra che le leggi di de morgan, usando le tavole di verità.

Siano A, B insiemi

<u>DEF</u>: Il PRODOTTO CARTESIANO DI A e B è l'insieme

$$A \times B \overset{def}{:=} \{ (a,b) : a \in A, b \in B \}$$

coppie ordinate

$$= \{\{a\}, \{a,b\}\}$$

<u>OSS</u>: $(1,2) \neq (2,1)$

esempio:

$$[2] \times [3] = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$$

Similmente

$$A \times B \times C \overset{def}{:=} \{(a,b,c) : a \in A, b \in B, c \in C\}$$

INFINE $A^2 \overset{def}{:=} A \times A$, $A^3 \overset{def}{:=} A \times A \times A$

esercizio [2-]: Siano A, B, X insiemi, è vero che
$$X \setminus (A \cup B) = (X \setminus A) \cup (X \setminus B) ?$$

esercizio [2]: A, B insiemi. È vero che
$$A = B \overset{?}{\Longleftrightarrow} A' \cap B = \emptyset \text{ e } A \cap B' = \emptyset ?$$

esercizio [1+]: A, B, C insiemi. È vero che
$$C \subseteq A \Rightarrow (A \cap B) \cup C = A \cap (B \cup C) ?$$

proprietà 1.2.3. : A, B, C insiemi. Allora :

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

Dimostrazione:

Sia $(x,y) \in A \times (B \cap C) \Rightarrow x \in A$ e $y \in B \cap C \Rightarrow$

$\Rightarrow x \in A$ e $y \in B$ e $y \in C \Rightarrow$

$\Rightarrow (x,y) \in A \times B$ e $(x,y) \in A \times C \Rightarrow$

$\Rightarrow (x,y) \in (A \times B) \cap (A \times C)$

Viceversa:

Sia $(x,y) \in (A \times B) \cap (A \times C) \Rightarrow$

$\Rightarrow (x,y) \in A \times B$ e $(x,y) \in A \times C \Rightarrow$

$\Rightarrow x \in A$ e $y \in B$ e $y \in C \Rightarrow$

$\Rightarrow x \in A$ e $y \in B \cap C \Rightarrow$

$\Rightarrow (x,y) \in A \times (B \cap C)$

Esercizio [2]: chi è

$$(\mathbb{N}\times\mathbb{Z})\cap(\mathbb{Z}\times\mathbb{P}) \text{ ?}$$

notazione:

$$\mathbb{P} \overset{\text{def}}{:=} \{1, 2, 3, \dots\}$$

Sia A un insieme:

DEF: L'insieme delle parti di A (o insieme potenza) è l'insieme

$$\mathcal{P}(A) \overset{\text{def}}{:=} \{B : B \subseteq A\}$$

esempio:

$$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$$

APPROFONDIMENTO SU CAP. 1

Paul Halmos "Teoria elementare degli insiemi"
FELTRINELLI

MATEMATICA 0

FRAZIONI

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad b, d \neq 0$$

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd} \qquad b, d \neq 0$$

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc} \qquad c, b, d \neq 0$$

EQ. DI 2° GRADO

$$ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$x^2 - 1 = 0 \Rightarrow x = \pm 1$

$x^2 + 1 = 0$ impossibile
$\nexists x \in \mathbb{R}$

LOGARITMI ed ESPONENZIALI

se $x \in \mathbb{R}$, $x > 0$

DEF. : Il logaritmo naturale di x è

$$\ln(x) \overset{def}{:=} \int_1^x \frac{1}{t}\, dt$$

PROPRIETÀ: $\ln(1) = 0$
$\ln(ab) = \ln(a) + \ln(b)$
$(a, b > 0)$

esiste un solo numero $e \in \mathbb{R}$ tale che

$$\ln(e) = 1 \qquad (e = 2,71828\ldots$$

LA FUNZIONE ESPONENZIALE

è l'inversa del logaritmo

$$e^{\ln(x)} = x \qquad \forall x > 0$$

$$\ln(e^x) = x \qquad \forall x \in \mathbb{R}$$

si scrive anche $\exp(x)$ al posto di e^x

PROPRIETÀ: $e^0 = 1$

$e^{a+b} = e^a \cdot e^b \qquad (a, b \in \mathbb{R})$

Siano $a, b > 0$, $b \neq 1$:

DEF: Il logaritmo di a in base b:

$$\log_b(a) \overset{def}{:=} \cancel{\log(a)} \frac{\ln(a)}{\ln(b)}$$

PROPRIETÀ: $\log_e(a) = \ln(a)$

$\log_a(a) = 1 \qquad (a \neq 1)$

Siano $a, x \in \mathbb{R}$, $x > 0$. allora:

$$x^a \overset{def}{:=} e^{a \cdot \ln(x)}$$

PROPRIETÀ: $1^a = 1$

$x^{a+b} = x^a \cdot x^b \quad (x > 0)$

$x^a = y$

$\ln x^a = \ln y$

$a \ln x = \ln y$

$a = \frac{\ln y}{\ln x}$

INFINE

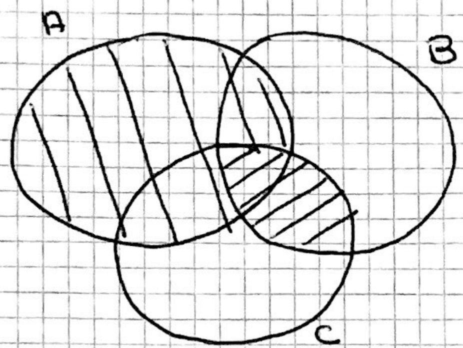
$$x^a = y \iff a \cdot \ln(x) = \ln(y)$$

$$\iff a = \frac{\ln(y)}{\ln(x)} \iff \log_x(y)$$

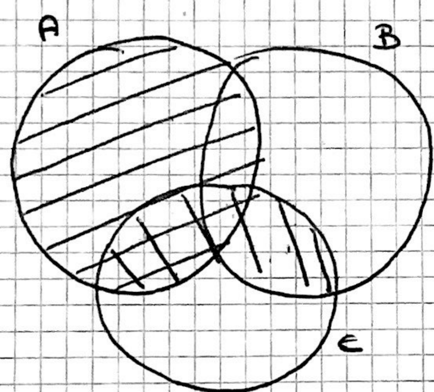
es. 1 : Siano A, B, C insiemi. È vero che:

$$A \cup ((A \cup B) \cap C) \overset{?}{=} A \cup (B \cap C) \ ?$$

1) Diagramma di Venn



$A \cup (B \cap C)$



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

2) Sia $x \in A \cup ((A \cup B) \cap C) \Rightarrow$

$\Rightarrow$ o $x \in A$ o $x \in (A \cup B) \cap C$

- Se $x \in A \Rightarrow x \in A \cup (B \cap C)$
- Se $x \in (A \cup B) \cap C \Rightarrow x \in A \cup B$ e $x \in C \Rightarrow$

$\Rightarrow \underbrace{x \in A \text{ o } x \in B \text{ e } x \in C}$

$\Downarrow$

- se $x \in A \Rightarrow x \in A \cup (B \cap C)$
- se $x \in B \Rightarrow x \in B \cap C \Rightarrow x \in A \cup (B \cap C)$

Viceversa:

Sia $x \in A \cup (B \cap C) \Rightarrow$

$\Rightarrow$ o $x \in A$ o $x \in B \cap C$

- se $x \in A \Rightarrow x \in A \cup ((A \cup B) \cap C)$

- se $x \in B \cap C \Rightarrow x \in B$ e $x \in C \Rightarrow$

  $\Rightarrow x \in A \cup B$ e $x \in C \Rightarrow$

  $\Rightarrow x \in (A \cup B) \cap C \Rightarrow x \in A \cup ((A \cup B) \cap C)$

3) Tavola della verità

A	B	C	$B \cap C$	$A \cup B$	$(A \cup B) \cap C$
1	1	1	1	1	1
1	1	0	0	1	0
1	0	1	0	1	1
1	0	0	0	1	0
0	1	1	1	1	1
0	1	0	0	1	0
0	0	1	0	0	0
0	0	0	0	0	0

$A \cup (B \cap C)$	$A \cup ((A \cup B) \cap C)$
1	1
1	1
1	1
1	1
1	1
0	0
0	0
0	0

PROBLEMA SAT

Dati n insiemi e due formule composte da questi insiemi, $\cap$, $\cup$, $\complement$ e (,) ~~decidono~~ decidere, in un tempo "ragionevole", se sono sempre uguali

1.3 FUNZIONI

Siano A, B insiemi.

DEF Una funzione (o applicazione } o mappa) f da A in B ($f\ A \to B$) è un sottoinsieme $f \subseteq A \times B$ tale che $\forall a \in A \Rightarrow \exists!\ b \in B$ tale che $(a,b) \in f$, Scriviamo allora $f(a) = b$

Intuitivamente → è una legge che ad ogni elemento di A associa uno e un solo elemento di B

NOTAZIONE

"$\forall$" → "per ogni"

"$\exists$" → "esiste"

"$\exists!$" → "esiste un unico"

Sia $f\ A \to B$

DEF f è iniettiva se

$$\begin{matrix} x, y \in A \\ x \neq y \end{matrix} \Rightarrow f(x) \neq f(y)$$

DEF f è <u>suriettiva</u>, se per $\forall\, b \in B \Rightarrow \exists\, a \in A$ tale che $f(a) = b$

DEF f è <u>biunivoca</u>, se f è iniettiva e surriettiva

SIA $X \subseteq A$

DEF <u>l'immagine</u> di X tramite f è

$$f(X) \overset{def}{:=} \{f(a) : a \in X\}$$

SIA $Y \subseteq B$

DEF <u>la controimmagine</u> (o retroimmagine) di Y tramite f è

$$f^{-1}(Y) \overset{def}{:=} \{a \in A : f(a) \in Y\}$$

OSS. $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$

Siano A, B, C insiemi e

$$f : A \to B \quad e \quad g : B \to C$$

DEF la <u>composizione</u> di f e g è la funzione $g \circ f : A \to C$ definita ponendo

$$(g \circ f)(a) \overset{def}{:=} g(f(a))$$

per $\forall a \in A$

PROP. 1.3.1

Siano A, B, C, f e g come sopra. Allora:

1) f e g iniettive $\Rightarrow$ $g \circ f$ è iniettiva

2) f e g surriettive $\Rightarrow$ $g \circ f$ è surriettiva

3) f e g biunivoche $\Rightarrow$ $g \circ f$ è biunivoca

DIMOSTRAZIONE

1) Siano $x, y \in A$, $x \neq y$.

poiché f è iniettiva $\Rightarrow f(x) \neq f(y)$

ma

g è iniettiva $\Rightarrow g(f(x)) \neq g(f(y))$

ma allora

$(g \circ f)(x) \neq (g \circ f)(y)$

quindi

$g \circ f$ è iniettiva

2) Sia $z \in C$.

poiché g è suriettiva $\Rightarrow \exists\, y \in B$ tale che $g(y) = z$

ma

f è suriettiva $\Rightarrow \exists\, x \in A$ tale che $f(x) = y$

quindi

$(g \circ f)(x) = g(f(x)) = g(y) = z$

pertanto $g \circ f$ è suriettiva

3) ~~Stesso~~ Segue da 1) e 2)

DEF L'identità su un insieme A è la funzione:

$$Id_A : A \to A$$

definita ponendo $Id_A(a) \overset{def}{:=} a$
$\forall a \in A$

(si scrive anche 1_a)

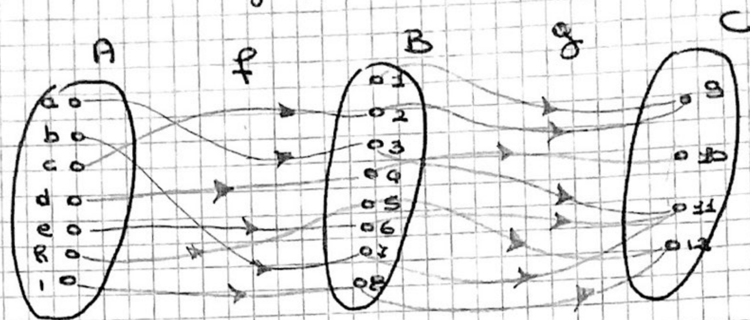
NOTAZIONE: A insieme, allora:

$$\overline{A} \overset{def}{:=} A'$$

esercizio: siano $f: A \to B$ e $g: B \to C$ tali che f è iniettiva e g è suriettiva. È vero che:

$g \circ f$ è iniettiva ?

$g \circ f$ è suriettiva ?



$\Rightarrow$ NO, $g \circ f$ non è iniettiva

Sembra che $g \circ f$ sia suriettiva

In effetti, siano

$$A \overset{def}{:=} \{a, b, c, d, e, h, i\}$$

$$B \overset{def}{:=} \{1, 2, 3, 4, 5, 6, 7, 8\}$$

$$C \overset{def}{:=} \{9, 10, 11, 12\}$$

e siano $f: A \to B$ e $g: B \to C$ definite ponendo:

$f(a) = 3$, $f(b) = 7$, $f(c) = 2$, $f(d) = 4$

$f(e) = 6$, $f(i) = 8$, $f(h) = 5$

$g(1) = 9$, $g(2) = 9$, $g(3) = 11$, $g(4) = 10$

$g(5) = 12$, $g(6) = 11$, $g(7) = 11$, $g(8) = 12$

allora f è iniettiva e g è suriettiva ma

$(g \circ f)(a) = g(\underbrace{f(a)}_{3}) = g(3) = 11$

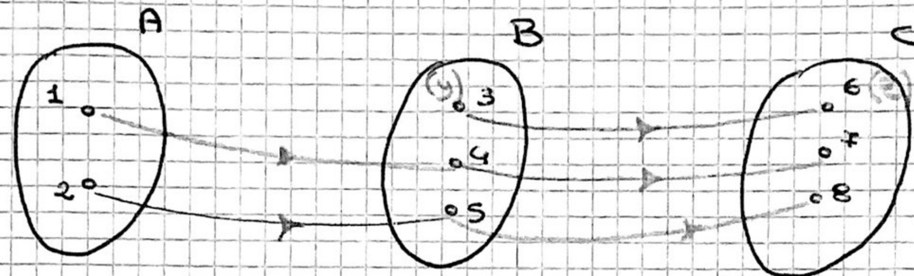
$(g \circ f)(e) = g(f(e)) = g(6) = 11$

$\Downarrow$

$g \circ f$ non è iniettiva

Proviamo a dimostrare che $g \circ f$ è suriettiva.

Sia $z \in C$. Poiché g è suriettiva $\Rightarrow \exists y \in B$ tale che $g(y) = z$



ma f non è necessariamente suriettiva = ?
ma allora, siano:

$A = \{1, 2\}$ $\quad B = \{3, 4, 5\}$ $\quad C = \{6, 7, 8\}$

Sia $f: A \to B$ definita da
$f(1) = 4, \quad f(2) = 5$

Sia $g: B \to C$ definita da
$g(3) = 6, \ g(4) = 7, \ g(5) = 8$

Allora f è iniettiva, g è suriettiva
ma

$g \circ f$ non è suriettiva perché:

$(g \circ f)(1) = g(f(1)) = g(4) = 7 \neq 6 \ (z)$

$(g \circ f)(2) = g(f(2)) = g(5) = 8 \neq 6 \ (z)$

esercizio: Sia $f: [5] \to [4]$ definita da

$f(1) = 4$, $f(2) = 3$, $f(3) = 1$
$f(4) = 4$, $f(5) = 1$

Siano
$x = \{1, 3, 5\}$ e $y = \{2, 4\}$

CALCOLARE $\underbrace{f(x)}_{\text{immagine}}$ e $\underbrace{f^{-1}(y)}_{\text{controimmagine}}$

Per definizione abbiamo che:

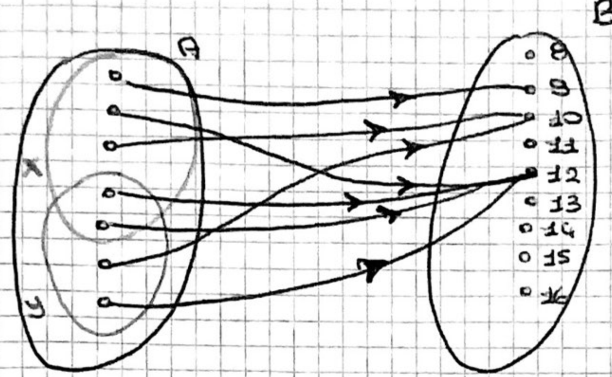
$$f(x) = f(\{1,3,5\}) = \{f(1), f(3), f(5)\} = \{4, 1\}$$

e che

$$f^{-1}(y) = \{a \in [5] : f(a) \in y\} =$$
$$= \{a \in [5] : f(a) \in \{2, 4\}\} =$$
$$= \{1, 4\}$$

controimmagine di 2 non esiste, ma di 4 sì
$f(1) = 4$ $f(4) = 4$

esercizio: Sia $f: A \to B$ e siano $x, y \subseteq A$.
È vero che
$f(x \cap y) = f(x) \cap f(y)$?



$f(x) = \{9, 10, 12\}$
$f(y) = \{10, 12\}$
$f(x \cap y) = \{12\}$

$\Rightarrow$ no, non è sempre vero

Sia $f: A \to B$, f biunivoca

DEF: L'inversa di f è la funzione:

$$f^{-1}: B \to A$$

definita da

$$f^{-1} \overset{def}{:=} \{(b,a) \in B \times A : (a,b) \in f\}.$$

OSS: quindi $\left[f(a) = b \iff f^{-1}(b) = a \right]$

PROP. 1.3.2: Siano $f, g, h: A \to A$. Allora:

1) $f \circ g: A \to A$;
2) $(f \circ g) \circ h = f \circ (g \circ h)$;
3) $f \circ Id_A = Id_A \circ f = f$;
4) f biunivoca $\Rightarrow f \circ f^{-1} = f^{-1} \circ f = Id_A$

DIMOSTRAZIONE:

1) È noto;

Siano $f, g: A \to B$.

DEF: f e g si dicono uguali scritto $f = g$ se $f(a) = g(a)$ per $\forall a \in A$

2) Sia $a \in A$. Allora

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g(h(a)))$$

e

$$(f \circ (g \circ h))(a) = f((g \circ h)(a)) = f(g(h(a)))$$

3) Sia $a \in A$. Allora:

$(f \circ Id_A)(a) = f(Id_A(a)) = f(a)$

e

$(Id_A \circ f)(a) = Id_A(f(a)) = f(a)$

4) Sia $a \in A$. Allora:

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

sia $b \overset{def}{:=} f^{-1}(a)$. Allora $f(b) = a$

$f(f^{-1}(a)) = \cancel{f(b) = a}\ f(b) = a = Id_A(a)$.

Inoltre

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

Sia $c \overset{def}{:=} f(a) \Rightarrow a = f^{-1}(c) = f^{-1}(f(a)) = (f^{-1} \circ f)(a)$

Sia $n \in \mathbb{P}$

DEF: Il gruppo simmetrico (di rango n) è:

$$S_n \overset{def}{:=} \{ f : [n] \to [n] : f \text{ Biunivoche} \}$$

Gli elementi di S_n si dicono PERMUTAZIONI

Se $f \in S_n$ Scriviamo: $f = a_1 a_2 \dots a_n$

dove $a_i \overset{def}{:=} f(i)$ per $\forall i \in [n]$

Esempio:

$$S_3 = \{123, 132, 213, 231, 312, 321\}$$

<u>OSS</u>: Se $f, g \in S_n$, $f = a_1 \dots a_n$, $g = b_1 \dots b_n$ allora

$$f \circ g = a_{b_1} a_{b_2} \dots a_{b_n}$$

esempio: $n = 7$, $f = 7152436$, $g = 2734165$

$$f \circ g = 1652739$$

$$g \circ f = 5217436$$

<u>OSS</u>: Sia $f \in S_n$, $f = a_1 \dots a_n$. Allora $f^{-1} = b_1 \dots b_n$ dove b_i è la posizione di i in ~~parola~~ $a_1 \dots a_n$ $(\forall i \in [n])$.

esempio: $n = 7$, $f = 7152436$. Allora

$$f^{-1} = 2465371$$

in effetti

$$f \circ f^{-1} = 1234567$$

$$f^{-1} \circ f = 1234567$$

Prop. 1.3.3 : Sia $f: A \to B$ e siano $x, y \subseteq B$.

Allora

1) $f^{-1}(x \cup y) = f^{-1}(x) \cup f^{-1}(y)$;

2) $f^{-1}(x \cap y) = f^{-1}(x) \cap f^{-1}(y)$.

DIMOSTRAZIONE

1) Sia $a \in f^{-1}(x \cup y) \Rightarrow f(a) \in x \cup y \Rightarrow$

$\Rightarrow$ o $f(a) \in x$ o $f(a) \in y$.

se $f(a) \in x \Rightarrow a \in f^{-1}(x) \Rightarrow a \in f^{-1}(x) \cup f^{-1}(y)$

se $f(a) \in y \Rightarrow a \in f^{-1}(y) \Rightarrow a \in f^{-1}(x) \cup f^{-1}(y)$

VICEVERSA

Sia $a \in f^{-1}(x) \cup f^{-1}(y) \Rightarrow$

$\Rightarrow$ o $a \in f^{-1}(x)$ o $a \in f^{-1}(y)$

se $a \in f^{-1}(x) \Rightarrow f(a) \in x \Rightarrow f(a) \in x \cup y$
$\Rightarrow a \in f^{-1}(x \cup y)$

se $a \in f^{-1}(y) \Rightarrow f(a) \in y \Rightarrow f(a) \in x \cup y$
$\Rightarrow a \in f^{-1}(x \cup y)$

2) analogo

es. [17] Sia $f: A \to B$ dimostrare che

$$f(f^{-1}(B)) = B \iff f \text{ è suriettiva}$$

<u>OSS</u> Sia $f: A \to B$, f biunivoca. ~~Allora~~ e $Y \subseteq B$.
Allora

$f^{-1}(Y)$ ha 2 significati
(controimmagine di Y tramite
f, e immagine di Y tramite
f^{-1})
ma il risultato non cambia

Dimostriamolo.

Sia $(x,y) \in A \times (B \setminus C) \Rightarrow x \in A$ e $y \in B \setminus C \Rightarrow$

$\Rightarrow x \in A$ e $y \in B$ e $y \notin C \Rightarrow$

$\Rightarrow (x,y) \in A \times B$ e $(x,y) \notin A \times C \Rightarrow$

$\Rightarrow (x,y) \in (A \times B) \setminus (A \times C) \Rightarrow$ ok

Viceversa

Sia $(x,y) \in (A \times B) \setminus (A \times C) \Rightarrow$

$\Rightarrow (x,y) \in (A \times B)$ e $(x,y) \notin (A \times C) \Rightarrow$

$\Rightarrow x \in A$ e $y \in B$ e $y \notin C \Rightarrow$
(se $y \in C \Rightarrow (x,y) \in A \times C$, assurdo!)

$\Rightarrow x \in A$ e $y \in B \setminus C \Rightarrow (x,y) \in A \times (B \setminus C)$

Tavola di verità? Si può fare ma con attenzione.

$\overset{x}{A}$	$\overset{y}{B}$	$\overset{y}{C}$	$B \setminus C$	$A \times (B \setminus C)$	$A \times B$
1	1	1	0	0	1
1	1	0	1	1	1
0	0	1	0	0	0
0	0	0	0	0	0
1	0	1	0	0	0
1	0	0	0	0	0
0	1	1	0	0	0
0	1	0	$\cancel{0}$ 1	0	0

$A\times C$	$(A\times B)\setminus(A\times C)$
1	0
0	1
0	0
0	0
1	0
0	0
0	0
0	0

Le colonne corrispondono. A $A\times(B\setminus C)$ e $(A\times B)\setminus(A\times C)$ sono uguali $\Rightarrow$ è sempre vero.

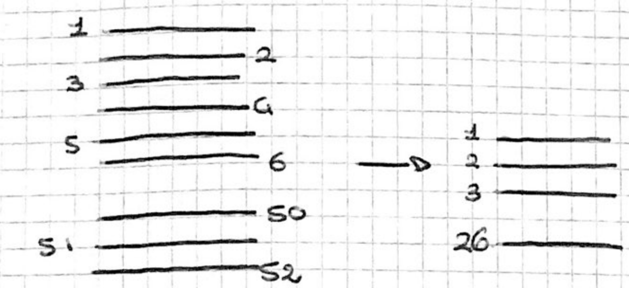
es. [2-] : Sia $p \in S_{52}$ definita da

$p = 1\ 27\ 2\ 28\ 3\ 29\ \dots\ 25\ 51\ 26\ 52$

calcolare il più piccolo $K \in \mathbb{N}$ tale che

$$\underbrace{p \circ p \circ \dots \circ p}_{K} = Id_{[52]}$$

OSS : p è la "smazzata perfetta"



PROP. 1.4.2 Sia un insieme e R una relazione di equivalenza su A. Allora le classi di equivalenza rispetto ad R sono una partizione di A.

DIM. Le classi di equivalenza di R sono sottoinsiemi di A, mai sono vuoti, sono disgiunti (per 1.4.1) e la loro unione è tutto A (se $x \in A \Rightarrow xRx \Rightarrow$ $\Rightarrow x \in [x]_R$)

esempio: Definiamo una relazione su $\mathbb{Z}$ ponendo

$$mRn \iff \underset{\text{(divide)}}{3 \mid} (m-n) \quad \left(\begin{array}{l}\text{cioè} \\ \exists k \in \mathbb{Z} \\ \text{tale che} \\ m-n = 3\cdot k\end{array}\right)$$

Allora R è di equivalenza.

- Sia $m \in \mathbb{Z} \Rightarrow m-m = 3\cdot 0 \Rightarrow mRm \Rightarrow$ R è RIFLESSIVA
- Siano $m,n \in \mathbb{Z}$ tali che $mRn \Rightarrow \exists k \in \mathbb{Z}$ tale che $m-n = 3\cdot k \Rightarrow n-m = 3\cdot(-k)$ e $-k \in \mathbb{Z} \Rightarrow$ $\Rightarrow 3 \mid (n-m) \Rightarrow nRm \Rightarrow$ R è SIMMETRICA
- Siano $m,n,p \in \mathbb{Z}$ tali che mRn e $nRp \Rightarrow$ $\Rightarrow \exists k, l \in \mathbb{Z}$ tali che $m-n = 3\cdot k$ e $n-p = 3l \Rightarrow$ $\Rightarrow m-p = 3k+3l = 3(k+l)$ e $k+l \in \mathbb{Z} \Rightarrow$ $\Rightarrow pRm \Rightarrow$ R è TRANSITIVA

CHI SONO LE CLASSI DI EQUIVALENZA?

Abbiamo che

$$[0]_R = \{m \in \mathbb{Z} : 0Rm\} = \{m \in \mathbb{Z} : 3 \mid (m-0)\} =$$
$$= \{m \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tale che } m = 3k\} =$$
$$= \{0, 3, -3, 6, -8, 9, -9, \dots\}$$

$[1]_R = \{m \in \mathbb{Z} : 1 R m\} =$

$= \{m \in \mathbb{Z} : \exists k \in \mathbb{Z}$ tale che $m-1 = 3k\} =$

$= \{3k+1 : k \in \mathbb{Z}\} = \{1, 4, -2, 7, -5, 10, -8, \dots\}$

$[2]_R = \{m \in \mathbb{Z} : 2 R m\} =$

$= \{m \in \mathbb{Z} : \exists k \in \mathbb{Z}$ tale che $m-2 = 3k\} =$

$= \{3k+2 : k \in \mathbb{Z}\} = \{2, 5, -1, 8, -4, \dots\}$

In generale otteniamo

$[i]_R = \{3k+i : k \in \mathbb{Z}\}$

Quindi

$[0]_R = [3]_R = [-3]_R = [6]_R = [-6] = \dots$

$[1]_R = [4]_R = [-2]_R = [7]_R = [-5]_R = \dots$

$[2]_R = [5]_R = [-1]_R = [8]_R = [-4]_R = \dots$

Pertanto ci sono 3 classi di equivalenza es. Consideriamo le seguenti relazioni su $\mathbb{Z}$

$$m \leq n$$

$$m = n \quad \text{o} \quad m-n \text{ è dispari}$$

$$|m-n| \leq 9$$

$$m \mid n$$

$\forall\, m,n \in \mathbb{Z}$

Quali riflessive? Simmetriche? Transitive?

	RIFL.	SIMM.	TRANS.
$m \leq n$	✓ $(m \leq m)$	✗ $(1 \leq 5$ ma $5 \not\leq 1)$	✓ $(m \leq n$ e $n \leq p \Rightarrow m \leq p)$
$m = n$ o $m-n$ disp.	✓	✓ ($m-n$ disp $\Rightarrow n-m$ disp)	✗ (5-6 è disp, 6-3 è disp ma 5-3 non è disp)
$\|m-n\| \leq 9$	✓ $(m-m \leq 9)$	✓ $\|m-n\| = \|n-m\|$	✗ $\|8-2\| \leq 9$, $\|16-8\| \leq 9$, $\|16-2\| \not\leq 9$
$m \mid n$	~~✗~~ ✓	✗	

1.4 RELAZIONI

Siano A, B insiemi.

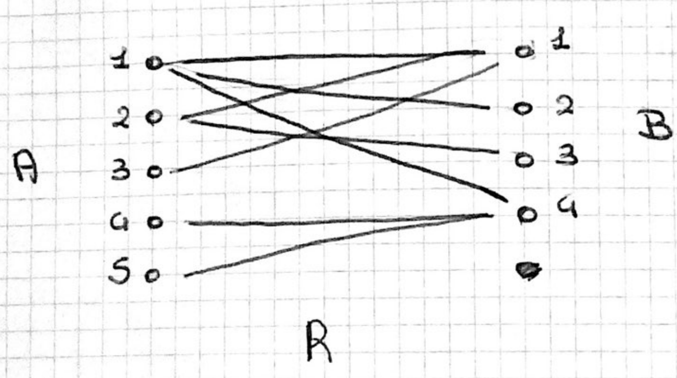
<u>DEF</u> Una relazione tra A e B è un sottoinsieme ~~R~~ $R \subseteq A \times B$.
Se $(a, b) \in R$ scriviamo aRb (letto "a è in relazione R con b").
Se $A = B$ si dice che R è una relazione su A

<u>OSS</u> Una funzione $f : A \to B$ è una relazione tra A e B

<u>eg.</u> $A = [5]$, $B = [4]$

$R = \{(1,1), (1,2), (2,1), (2,3), (4,4), (5,4), (3,1), (1,4)\}$

posso rappresentare R graficamente in questo modo



Sia R una relazione su A.

DEF: 1) R è riflessiva se $(a,a) \in R$ per $\forall\, a \in A$;

2) R è simmetrica se per ~~ogni coppia~~ $\forall\, a, b \in A$ vale che $(a,b) \in R \Rightarrow (b,a) \in R$

3) R è transitiva se $\forall\, a, b, c \in A$ vale che $(a,b) \in R$ e $(b,c) \in R \Rightarrow (a,c) \in R$

DEF: R si dice una relazione di equivalenza se R è riflessiva, simmetrica e transitiva

Sia R di equivalenza. Sia $a \in A$.

DEF La classe di equivalenza di a rispetto ad R è

$$[a]_R \overset{def}{:=} \{ b \in A : aRb \}.$$

PROP. 1.G.1 Sia R di equivalenza su A e siano $a, b \in A$. Allora

o $[a]_R = [b]_R$

o $[a]_R \cap [b]_R = \emptyset$

DIM. Sia $c \in [a]_R \cap [b]_R \Rightarrow c \in [a]_R$ e $c \in [b]_R \Rightarrow$

$\Rightarrow aRc$ e $bRc \Rightarrow aRc$ e $cRb \Rightarrow$

$\Rightarrow aRb.$ $(\Rightarrow bRa)$

Sia $x \in [a]_R \Rightarrow xRa \xRightarrow{(aRb)} xRb \Rightarrow x \in [b]_R$

Viceversa

Se $y \in [b]_R \Rightarrow yRb \xRightarrow{(bRa)} yRa \Rightarrow y \in [a]_R$

es [2] : Quante relazioni di equivalenza ci sono su $[3]$? (Risposta : 5)

DEF : Una partizione (o partizione insiemistica) di A è un insieme

$\pi \overset{def}{:=} \{B_1, \dots, B_k\}$ $(k \in \mathbb{N})$

tale che:

1) $B_i \subseteq A$ e $B_i \neq \emptyset$ per $\forall i = 1, \dots, k$;

2) $B_1 \cup \dots \cup B_k = A$;

3) $B_i \cap B_j = \emptyset$ per $\forall 1 \leq i, j \leq k$, $i \neq j$

$B_1, \dots, B_k$ si dicono i blocchi di π e si dice che π ha k blocchi esempio : $A = [9]$. Allora

$$\pi = \{\{1,4\}, \{5\}, \{2,6,9\}, \{3,7,8\}\}$$

è una partizione di $[9]$ in 4 blocchi.

OSS Sia π una partizione di A.
Definiamo una relazione R su A ponendo

$aRb \iff$ a e b $\in$ allo stesso blocco di π

allora R è di equiv.

(dalla lez. precedente)

In effetti, sia $A = [7]$, $B = [16] \setminus [7]$, e siano $x = \{1,2,3,4,5\}$, $y = \{4,5,6,7\}$, e sia $f : A \to B$ definita ponendo

$f(1) = 9$, $f(2) = 12$, $f(3) = 10$, $f(4) = 12$
$f(5) = 12$, $f(6) = 10$, $f(7) = 12$

Allora

$$f(x) = \{9, 12, 10\}, \quad f(y) = \{12, 10\}$$

e

$$f(x \cap y) = f(\{4,5\}) = \{12\}$$

ma

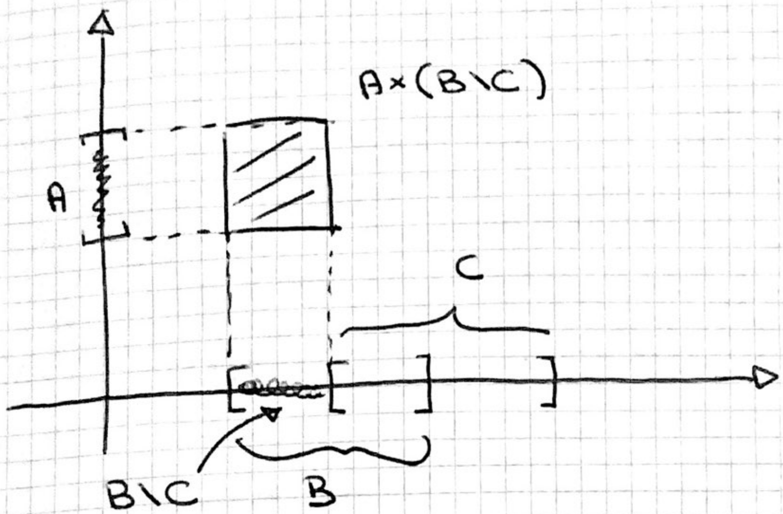
$$f(x) \cap f(y) = \{10, 12\}.$$

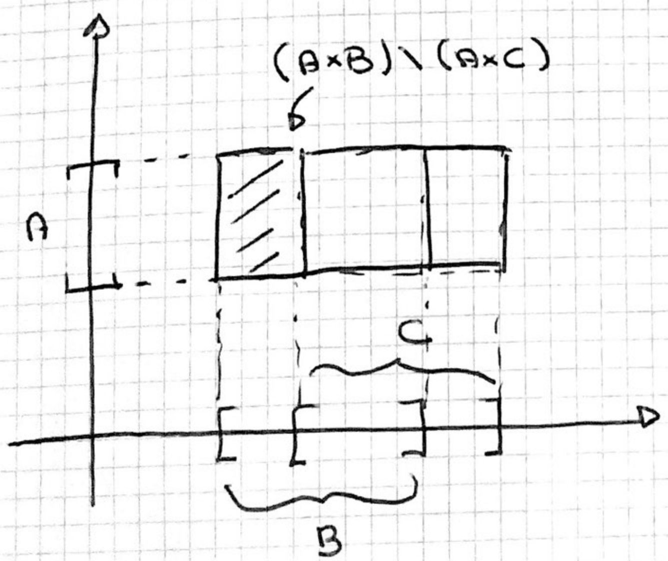
Quindi, non è sempre vero

es A, B, C insiemi. E' vero che

$$A \times (B \setminus C) \overset{?}{=} (A \times B) \setminus (A \times C) \quad ?$$

Posso usare i diagrammi di Venn?
Avrei bisogno di 4 dimensioni, ma a volte si può fare...





Sembra di sì

Quindi K è il minimo numero di smazzate perfette dopo le quali il mazzo torna nell'ordine iniziale

es: Sia $f: A \to B$ e siano $x, y \subseteq B$.
Dimostrare che

$$f^{-1}(x \setminus y) = f^{-1}(x) \setminus f^{-1}(y)$$

Sia $a \in f^{-1}(x \setminus y) \Rightarrow f(a) \in x \setminus y \Rightarrow$
$\Rightarrow f(a) \in x$ e $f(a) \notin y \Rightarrow a \in f^{-1}(x)$ e
$a \notin f^{-1}(y) \Rightarrow a \in f^{-1}(x) \setminus f^{-1}(y) \Rightarrow$ OK

Viceversa

Sia $a \in f^{-1}(x) \setminus f^{-1}(y) \Rightarrow a \in f^{-1}(x)$ e
$a \notin f^{-1}(y) \Rightarrow f(a) \in x$ e $f(a) \notin y \Rightarrow$
$\Rightarrow f(a) \in x \setminus y \Rightarrow a \in f^{-1}(x \setminus y)$

es: Sia R la relazione $\mathbb{Z}$ definita ponendo

$m R n \Leftrightarrow m = n$ o $m + n = 5$

$\forall n, m \in \mathbb{Z}$. Equivalenza?

1) RIFLESSIVA?
Sia $n \in \mathbb{Z} \Rightarrow m = m \Rightarrow m R m \Rightarrow$ OK

2) SIMMETRICA?
Siano $m, n \in \mathbb{Z}$ tali che $m R n \Rightarrow$
$\Rightarrow$ o $m = n$ o $m + n = 5$.
Se $m = n \Rightarrow n = m \Rightarrow n R m \Rightarrow$ OK
Se $m + n = 5 \Rightarrow n + m = 5 \Rightarrow n R m \Rightarrow$ OK

3) TRANSITIVA?
Siano $m, n, k \in \mathbb{Z}$ tali che $m R n$ e $n R k$.
Quindi (o $m = n$ o $m + n = 5$) $(m R n)$
e (o $n = k$ o $n + k = 5$) $(n R k)$

3) TRANSITIVA ?

Siano (a,b), (c,d), $(e,f) \in \mathbb{Z} \times \mathbb{Z}^*$ tali che

$(a,b) R (c,d)$ e $(c,d) R (e,f) \Rightarrow$

$\Rightarrow ad = bc$ e $cf = de \Rightarrow$

$\Rightarrow afd = fbc$ e $bcf = bde \Rightarrow$

$\Rightarrow afd = bde$. ma $d \neq 0 \Rightarrow$

$\Rightarrow af = be \Rightarrow (a,b) R (e,f)$

Quindi R è di equivalenza.

CLASSI DI EQUIVALENZA

Sia $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Allora

$$[(a,b)]_R = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* : ad = bc\} \Rightarrow$$

$$\Rightarrow \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* : \frac{a}{b} = \frac{c}{d}\}$$

- se $m = n$ e $n = k \Rightarrow m = k \Rightarrow mRk \Rightarrow$ OK
- se $m = n$ e $n + k = 5 \Rightarrow m + k = 5 \Rightarrow$
  $\Rightarrow mRk \Rightarrow$ OK
- se $m + n = 5$ e $n = k \Rightarrow m + k = 5 \Rightarrow mRk =$ OK
- se $m + n = 5$ e $n + k = 5 \Rightarrow n = 5 - m$ e
  $n = 5 - k \Rightarrow 5 - k = 5 - m \Rightarrow k = m \Rightarrow mRk \Rightarrow$ ok

Quindi, R è di equivalenza

CHI SONO LE CLASSI DI EQUIV.?

Sia $n \in \mathbb{Z}$, allora

$$[n]_R = \{m \in \mathbb{Z} : mRn\} =$$
$$= \{m \in \mathbb{Z} : \text{o } m = n \text{ o } m + n = 5\} =$$
$$= \{n, 5-n\}$$

<u>es</u>: Sia R la relazione su $\mathbb{Z} \times \mathbb{Z}^*$
($\text{dove } \mathbb{Z}^* :\overset{def}{=} \mathbb{Z} \setminus \{0\}$)
definita da
$(a,b) \, R \, (c,d) \iff ad = bc$
$\forall (a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$.
Equivalenza?

1) RIFLESSIVA = ?
Siano $(a,b) \in \mathbb{Z} \times \mathbb{Z}^* \Rightarrow ab = ba \Rightarrow (a,b) R (a,b) \Rightarrow$
$\Rightarrow$ OK

2) SIMMETRICA?
Siano $(a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$ tali che
$(a,b) \, R \, (c,d) \Rightarrow ad = bc$. Ma $(c,d) \, R \, (a,b)$
$\iff cb = da$.
Pertanto $(c,d) \, R \, (a,b) \Rightarrow$ OK

<u>es</u> [2-] : Sia R la relazione su $\mathbb{Z}$ definita ponendo

$$mRn \iff m-n \text{ è pari } \left(\text{cioè } 2 \mid (m-n)\right)$$

$\forall m,n \in \mathbb{Z}$.

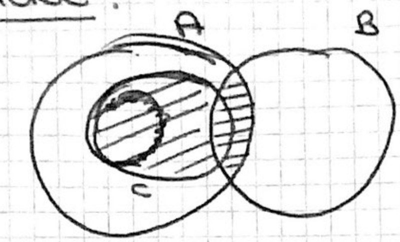
Equivalenza?

es: Siano A, B, C insiemi tali che $C \subseteq A$.

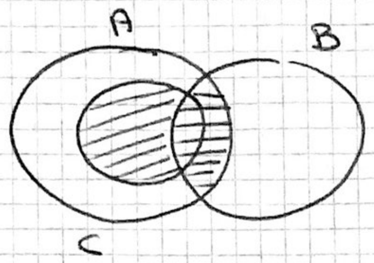
È vero che allora

$$A \cap (B \cup C) \overset{?}{=} (A \cap B) \cup C$$

INTUIZIONE:



$A \cap (B \cup C)$



$(A \cap B) \cup C$

conclusione: sembra di sì

DIMOSTRAZIONE:

Sia $x \in A \cap (B \cup C) \Rightarrow x \in A$ e $x \in (B \cup C) \Rightarrow$

$\Rightarrow x \in A$ e $x \in B$ o $x \in C$

Se $x \in B \Rightarrow x \in (A \cap B) \Rightarrow x \in (A \cap B) \cup C$

Se $x \in C \Rightarrow x \in C \cup (A \cap B)$

VICEVERSA

Sia $x \in (A \cap B) \cup C \Rightarrow x \in (A \cap B)$ o $x \in C$

se $x \in C \Rightarrow x \in A \Rightarrow x \in C \cup B \Rightarrow x \in A \cap (B \cup C)$

se $x \in (A \cap B) \Rightarrow x \in A$ e $x \in B \Rightarrow x \in A$ e $x \in B \cup C \Rightarrow$

$\Rightarrow x \in A \cap (B \cup C)$

TAVOLA DI VERITÀ

A	B	C	$B \cup C$	$A \cap B$	$A \cap (B \cup C)$	$(A \cap B) \cup C$
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	0	1	1
1	0	0	0	0	0	0
~~0~~	~~1~~	~~1~~	~~1~~			
0	1	0	0	0	0	0
~~0~~	~~0~~	~~1~~	~~1~~			
0	0	0	0	0	0	0

impossibile perché $C \subseteq A$

es.

Consideriamo le seguenti relazioni su $\mathbb{Z}$

$$m \le n$$

$$m = n \quad o \quad m-n \text{ è dispari}$$

$$|m-n| \le 9$$

$$m \mid n$$

$\forall\, m, n \in \mathbb{Z}$

Quali riflessive? Simmetriche? Transitive?

	RIFL	SIMM.	TRANS.
$m \le n$	✓ ($m \le m$)	✗ ($1 \le 5$ ma $5 \not\le 1$)	✓ ($m \le n$ e $n \le p$ $\Rightarrow$ $m \le p$)
$m = n$ o $m-n$ disp.	✓	✓ ($m-n$ disp $\Rightarrow$ $n-m$ disp)	✗ ($5-6$ e' disp ma $5-3$ non e' disp; $6-3$ e' disp)
$\|m-n\| \le 9$	✓ ($m-m \le 9$)	✓ $\|m-n\| = \|n-m\|$	✗ $\|8-2\| \le 9$, $\|16-8\| \le 9$, $\|16-2\| \not\le 9$
$m \mid n$	✓	✗	✓

(se $m \mid n$ e $n \mid p$ $\Rightarrow$

$\Rightarrow \exists\, k, l \in \mathbb{Z}$ tali che

$n = m \cdot k$ e $p = n \cdot l$ $\Rightarrow$

$\Rightarrow p = (m \cdot k) \cdot l = m (k\, l)$

e $k\, l \in \mathbb{Z}$ $\Rightarrow m \mid p$)