

# INSIEMI

Non si dà alcuna definizione formale agli insiem:

$x, y, z \in X \quad y \in Y$

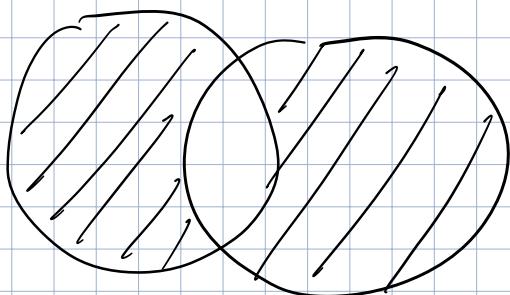
$$x \cap y = \{z : m \in X \wedge m \in Y\} \quad \text{INTERSEZIONE}$$

$$x \cup y = \{z : m \in X \vee m \in Y\} \quad \text{UNIONE}$$

$$x / y = \{z : m \in X \wedge m \notin Y\} \quad \text{COMPLEMENTARE}$$

$$\emptyset = \{m : m \neq m\} \quad \text{INSIEME VUOTO (assunto)}$$

## DIFERENZA SIMMETRICA



$$X \Delta Y =$$

$$\{m : m \in X, m \in Y \text{ e } m \notin (X \cap Y)\}$$

Il vuoto è elemento di ogni insieme

## RELATIVI

Sia  $X \neq \emptyset$ , per relazione uno-uno in  $X$

"intendiamo un sottoinsieme di  $X$ , anche chiamata  
"proprietà".

Considerando il prodotto cartesiano  $X^2 = X \times X = \{(x, y) : x, y \in X\}$ , il sottoinsieme  $R \subseteq X^2$  è detta Relazione in  $X$ .

$R \subseteq X \times X$  BINARIA

$R \subseteq X \times X \times X$  TERNARIA

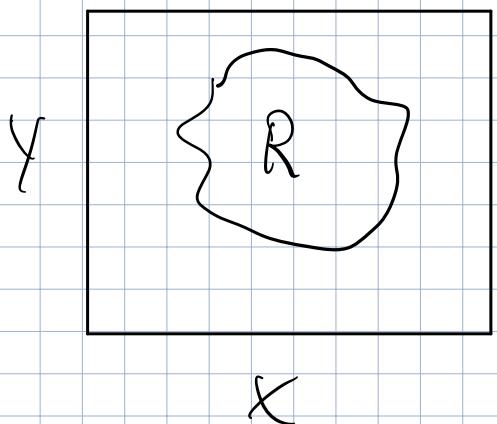
$R \subseteq X_1 \times X_2 \times \dots \times X_m$  m-ARIA

Il prodotto cartesiano

non è

COMMUTATIVO

Una proposizione O-aria non ha variabili da cui dipendere ed è detta "sentenza".

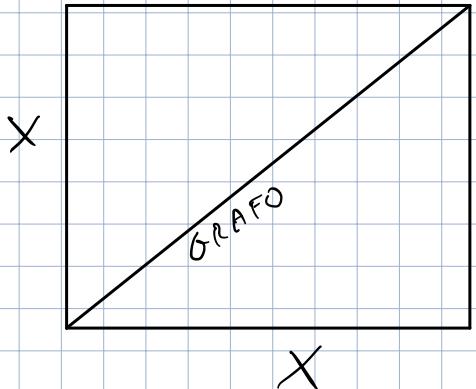


## UGUALANZA

$$\Delta_X := \{(x, x) : x \in X\}$$

Se la relazione è RIFLESSIVA allora comprende la diagonale

$$x R y \Rightarrow x y \Leftrightarrow (x, y) \in \Delta_X$$



## PROPRIETÀ DI R

RIFLESSIVA :  $\text{iff } \Delta_X \subseteq R$

ANTI RIFLESSIVA :  $\text{iff } \Delta_X \cap R = \emptyset$

SIMMETRICA : iff  $R^{-1} = R$

ANTISIMMETRICA : iff  $R \cap R^{-1} \subseteq \Delta(x)$

TRANSITIVA : iff  $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

## RELATIIONE DI EQUIVALENZA

Una relazione è detta d'equivalenza se è:

- RIFLESSIVA
- SIMMETRICA
- TRANSITIVA

Ad esempio il parallelismo  
fra rette è di equivalenza

## RELATIIONE DI ORDINE (POSET)

Una relazione è detta d'ordine se è:

- RIFLESSIVA
- ANTISIMMETRICA
- TRANSITIVA

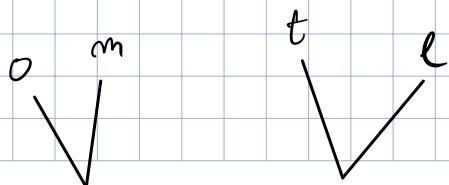
TOTALE SE:

$\forall t, t \in E, \forall t, t \in E : t \leq t \wedge t \leq t$

TRICOTOMIA

## DIAGRAMMA DI HASSE

Nel diagramma di Hasse si può mettere in relazione  
gli elementi in basso con quelli in alto, le relazioni  
sono legate da un segmento.



Quello di ordine TOTALE  
è rappresentato da una

$$y \not\propto z, m R z, m R l$$

"Coteno"

$$A - B - C - D - E - F$$

$y \not\propto z, m R z, m R l$

## INSIEMI LIMITATI

Sia  $X$  un poset  $Y \subseteq X$  è detto

LIMITATO SUPERIORMENTE: se esiste un elemento  
 $b \in X$ :  $y \leq b \quad \forall y \in Y$

L'elemento  $b$  è detto MAGGIORANTE in  $Y$ .

LIMITATO INFERIORMENTE: se esiste un elemento  
 $a \in X$ :  $a \leq y \quad \forall y \in Y$

L'elemento a cui detto MINDRANTE in  $Y$ .

Un elemento  $c' := \sup_x Y \subseteq X$  è detto

ESTREMO SUPERIORE in  $Y \subseteq X$  se:

- $c'$  è maggiore di tutti gli elementi di  $Y$

- $c'$  è il più piccolo dei maggioranti

Un elemento  $c'' := \inf_x Y \subseteq X$  è detto

ESTREMO INFERIORE in  $Y \subseteq X$  se:

- $c'$  è minore di tutti gli elementi di  $Y$

- $c'$  è il più grande dei minoranti

Se  $\inf_x Y$  esiste e appartiene ad  $Y$  è detto MINIMO

Se  $\sup_x Y$  esiste e appartiene ad  $Y$  è detto MASSIMO

Ne risulta che:

$$m := \min_x Y \Leftrightarrow \forall y \in Y \quad m \leq y \quad \forall y \in Y$$

$$M := \sup_x Y \Leftrightarrow y \leq M \quad \forall y \in Y \quad \forall y \in Y$$

## ORDINE LESSICO GRAMMATICO

Diciamo ordine lessico - grafico l'ordine delle parole dell'alfabeto  $p \leq q \Leftrightarrow p$  viene prima di  $q$  nel vocabolario.

# ALFABETO E LINGUAGGIO (il linguaggio contiene grammatica)

## FUNZIONI

Considerando due insiem:  $X \subset Y$ ,  $R \subseteq X \cdot Y$   
sono detti:

$$\text{DOMINIO } (R) := \{x : \exists y (y \in Y \wedge (x, y) \in R)\}$$

$$\text{CODOMINIO } (R) := \{y : \exists x (x \in X \wedge (x, y) \in R)\}$$

$$E := \{(x, y) : (x, y) \in X \cdot Y \wedge P(x, y)\}$$

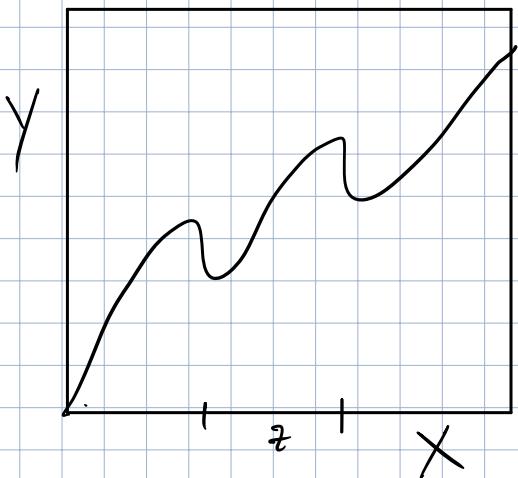
E' detto grafico di  $P$ . (Anche scritto  $gr(P)$ )

Una funzione da  $X$  a  $Y$  e' una relazione che  
chiaramente fa che rispetta le seguenti condizioni:

$$\textcircled{1} \quad \text{Dom}(RP) = X$$

$$gr(f) = RP$$

②  $\forall x \in X \exists ! y \in Y :$



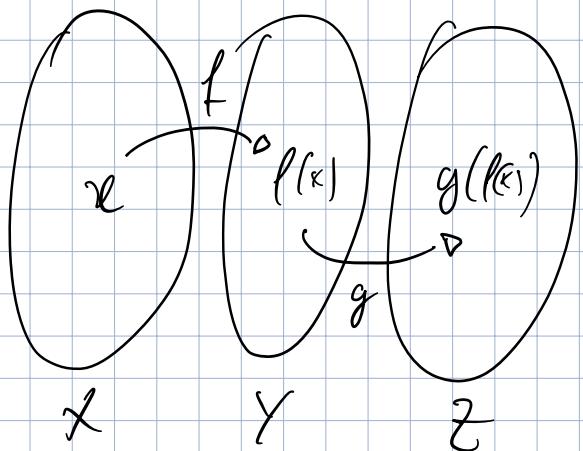
$f: X \rightarrow Y$  è detta **SURGETIVA**  
se  $p(x) = y$

$f: X \rightarrow Y$  è detta **INIETTIVA**  
 $\forall x, y \in X \quad x \neq y \Rightarrow p(x) \neq p(y)$

Una funzione iniettiva è quindi detta **BIETTIVA**.

### COMPOSIZIONE DI FUNZIONI

Siamo  $X, Y, Z$ , e due funzioni  $f: X \rightarrow Y$ ,  $g: Y \rightarrow Z$



$$X \rightarrow g(f(x))$$

$$X \rightarrow "z"$$

$$g \circ f \neq f \circ g$$

Se  $f(x) \subseteq \text{Dom}(g)$   $g \circ f = g \circ f(x) = g(f(x))$

Identità:  $i_d_x: X \rightarrow X$   $i_d_x(x) = x \quad \forall x \in X$

### INVERTIBILITÀ

$f: X \rightarrow Y$  è detta invertibile da sinistra se

$f^{-1}: Y \rightarrow X$  è una funzione

$g : Y \rightarrow X$  è detto invertibile destra se

$$\exists f : X \rightarrow Y : f \circ g = id_Y$$

Una funzione è detta **INVERTIBILE** se esiste un'immersione destra ed un simmetra.

Anendo fra insiem:  $X, Y, Z$  e due funzioni:  
 $f : X \rightarrow Y, g : Y \rightarrow Z$ , dimostrare che:

- (1) Se  $f \circ g$  sono iniettive  $\rightarrow g \circ f$  iniettive  
(2) Se  $f \circ g$  sono suriettive  $\rightarrow g \circ f$  suriettiva  
 $\Rightarrow$  Se  $f \circ g$  sono biettive  $\rightarrow g \circ f$  biettive

(1) Se  $f$  è iniettiva  $\Leftrightarrow \forall x_1, x_2 \in X, x_1 \neq x_2$   
 $\Rightarrow f(x_1) \neq f(x_2)$

Se  $g$  è iniettiva  $\Leftrightarrow \forall y_1, y_2 \in Y, y_1 \neq y_2$   
 $\Rightarrow g(y_1) \neq g(y_2)$

Vogliamo quindi provare che:  $\forall x_1, x_2 \in X, x_1 \neq x_2$   
 $\Rightarrow g \circ f(x_1) \neq g \circ f(x_2)$

Siamo  $x_1, x_2 \in X, x_1 \neq x_2$

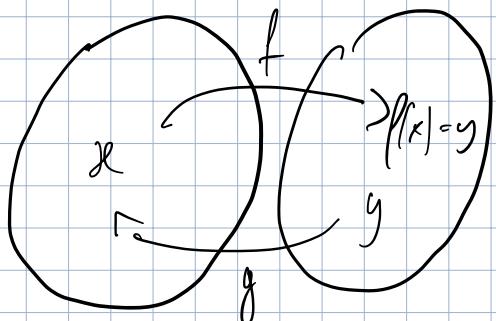
$$f(x_1) \neq f(x_2) \Rightarrow y_1 \in Y \neq y_2 \in Y$$

$$g(y_1) \neq g(y_2) \Leftrightarrow g(\rho(x_1)) \neq g(\rho(x_2))$$

$$\Downarrow \\ g \circ f(x_1) \neq g \circ f(x_2)$$

②  $g \circ f(x)$  è suriettivo se  $g \circ f(x) = z$   
 $g \circ f(x) = g(\rho(x)) = g(y) = z$

Se  $f: X \rightarrow Y$  è biettiva  $\Leftrightarrow f$  è invertibile  
 $f$  è invertibile se  $\exists! g: Y \rightarrow X : g \circ f = id_X \circ f \circ g = id_Y$



## INSIEME QUOTIENTE

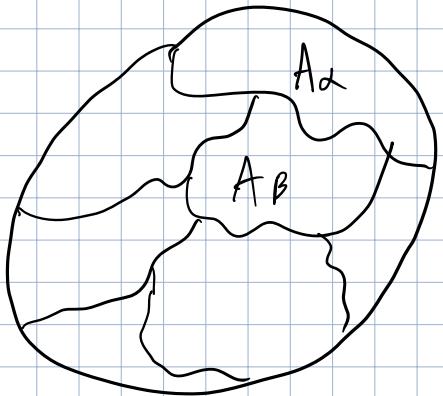
$X$  un insieme,  $R$  relazione di equivalenza su  $X$ .

$x \in X$

$$[x]_R = \{ y : y \in X \wedge y R x \}$$

$$x, y \in X \text{ se } R y \quad [x]_R \cap [y]_R = \emptyset$$

Possiamo dimostrare che presa una partizione possiamo ridurla ad una  $R$  che ci ridurrà la partizione iniziale.



$x, y \in X$

$x R y \Leftrightarrow \exists A_\alpha : x, y \in A_\alpha$

Dimostriamo che è di equivalenza  
dimostra che è una relazione.

Quando dato un insieme  $X$  ed una relazione  $R$   
di equivalenza in  $X$ , creare l'insieme  
**QUOTIENTE MOLTOLO R** ( $X/R$ )

$$X/R := \{[x]_R : x \in X\}$$

## STRUTTURA ALGEBRICA

$S \neq \emptyset$  si dice OPERAZIONE in  $S$  unaria  $f: S \rightarrow S$

si dice OPERAZIONE in  $S$  2-aria  $f: S \times S \rightarrow S$

si dice OPERAZIONE in  $S$   $n$ -aria  $f: S^n \rightarrow S$

Ex:  $N$   $(m, n) \in N^2 \rightarrow N$  è finita

la struttura algebrica è un insieme dotato di un numero finito di operazioni

**OPERAZIONI**

ESTERNE: ?

INTERNE: quelle che abbiamo definito.

$$(S, +) \quad +: S \times S \rightarrow S$$

$\forall x, y \in S \quad x+y = y+x$

COMMUTATIVA

$\forall x, y, z \in S \quad (x+y)+z = x+(y+z)$

ASSOCIAZIONE

$\forall x \in S \exists ! e \in S : x+e = x$

ELEMENTO NEUTRO

$\forall x \in S \exists ! y \in S : x+y = 0$

ELEMENTO OPPOSTO

Se l'operazione gode di queste proprietà è detta GRUPPO ABELIANO COMMUTATIVO,

Se manca la commutazione non è GRUPPO ABELIANO.

ANELLO: commutativo (o abeliano)

è una struttura algebrica  $(A, +_A, \cdot_A)$  in cui:

SOMMA è abeliana

PRODOTTO è un semigruppo (ASSOCIAZIONE, COMMUTATIVA, IDENTITÀ)

SEMIGRUPPO

è una struttura algebrica che possiede una sola operazione associativa.

MONOIDE

è una struttura algebrica che possiede una sola operazione associativa e l'identità.

$(S, *) \quad \forall x \in S \exists e \in S : x+e = e+x = x$

## CAMPOL

è una struttura dotata di 2 operazioni  $(\mathbb{K}, +, \cdot)$

$\mathbb{K} \neq \emptyset$ :

- $(\mathbb{K}, +)$  è un'omelie commutativa
- $(\mathbb{K} \setminus \{0\}, \cdot)$  è un gruppo abeliano

i.e.  $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \cdot_{\mathbb{K}})$  is a multiplicative commutative group. In other words, a field  $\mathbb{K}$  is a commutative ring with unity  $1_{\mathbb{K}}$  in which every element  $x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$  admits a multiplicative inverse  $x^{-1} \in \mathbb{K}$ .

Direct consequence of the field axioms are the next facts:

The additive identity  $0_{\mathbb{K}}$  of  $\mathbb{K}$  is unique.

Given  $x \in \mathbb{K}$ , the additive inverse  $-x \in \mathbb{K}$  is unique.

The multiplicative identity  $1_{\mathbb{K}}$  of  $\mathbb{K}$  is unique.

Given  $x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ , the inverse  $x^{-1} \in \mathbb{K}$  is unique<sup>12</sup>.

$0_{\mathbb{K}} \cdot_{\mathbb{K}} x = 0_{\mathbb{K}}$  for every  $x \in \mathbb{K}$ .

If  $x +_{\mathbb{K}} z = y +_{\mathbb{K}} z$ , then  $x = y$ .

If  $x \cdot_{\mathbb{K}} z = y \cdot_{\mathbb{K}} z$  and  $z \neq 0_{\mathbb{K}}$ , then  $x = y$ .

## CAMPOL ORDINATO

$$\mathbb{K} = (\mathbb{K}, +, \cdot, \leq)$$

$\leq$  è una relazione di ordine totale su  $\mathbb{K}$

Si devono verificare 2 condizioni di compatibilità:

$$(i) \quad \forall x, y, z \in \mathbb{K} \Rightarrow x \leq y \Rightarrow x + z \leq y + z \quad \forall z \in \mathbb{K}$$

$$(ii) \quad \forall x, y, z \in \mathbb{K} \Rightarrow x \leq y \Rightarrow x \cdot z \leq y \cdot z \quad \forall z \in \mathbb{K}$$

## Esempio d. campo finito

PSO

PRIMO

$\left\{ \begin{array}{l} \text{- naturale } > 1 \\ \text{- divisibile per le stesse o più 1} \end{array} \right.$

$1, 3, 5, \dots$  Euclide dimostra che sono infiniti.

Consider  $\mathbb{Z}$  l'insieme dei numeri interi.

$$\mathbb{Z} = \{ \mathbb{Z}, +, \cdot \}$$

Voglio introdurre in  $\mathbb{Z}$  una relazione di equivalenza, che chiamerò "congruenza,"

$$\text{Se } x, y \in \mathbb{Z} \quad x \equiv y \Leftrightarrow \exists t \in \mathbb{Z} : x - y = pt$$

Sarà ora quindi l'insieme quoziente:

$$\mathbb{Z}/\equiv := \{ [x]_{\equiv_p} : x \in \mathbb{Z} \} := \mathbb{Z}_p$$

Se  $p$  non fosse primo  $\mathbb{Z}$  si potrebbe strutturare  
solo come un campo.

$$p = 3 : \mathbb{Z}_3 := \{ [x]_{\equiv_3} : x \in \mathbb{Z} \}$$

$$y \equiv 1 \text{ in } \mathbb{Z} \quad [y]_{\equiv_3} = \{ y \in \mathbb{Z} : y \equiv 1 \pmod{3} \} =$$

$$\text{Numeri che dividono} \quad = y - 1 = 3t, \quad t \in \mathbb{Z}$$

$$\text{per 3 danno resto 1} \quad y \equiv 3t + 1$$

$$= \{ y = 3t + 1, \quad t \in \mathbb{Z} \} = \{ \pm 1, \pm 4, \pm 7, \dots \}$$

Ese.

$$[2]_{\equiv_3} = \{ y \in \mathbb{Z} : y \equiv 2 \pmod{3} \} = y = 3t + 2$$

Poss dimostrare che non ci sono altre classi oltre

$$[e]_3, [1]_3, [2]_3$$

In  $\mathbb{Z}_p$  ci hanno  $p-1$  classi.

Voglio introdurre in  $\mathbb{Z}_p$  una relazione

$$(\mathbb{Z}_p, +, \cdot)$$

Definisco somma e prodotto:

$$[x]_p + [y]_p = [x + \underbrace{y}]_p \quad \text{dove } \mathbb{Z}$$

$$[x]_p \cdot [y]_p = [x \cdot y]_p$$

$$[x]_p \in \underbrace{[y]_p}_{\text{Reciproco}} : [x]_p \cdot [y]_p = [1]_p$$

Ese.

$$[2]_3 \cdot [x]_3 = [1]_3$$

$$[2x]_3 \Leftrightarrow [2x]_3 = [1]_3$$

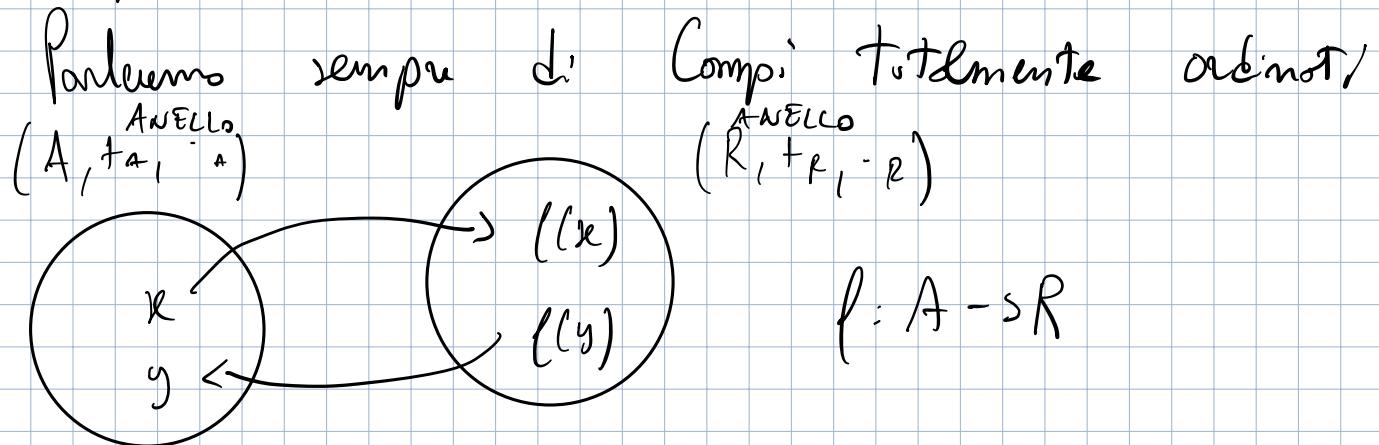
Due classi sono uguali quando gli elementi sono in

$$2x = 1 \text{ (resto 3)}$$

$$2x - 1 = 3t \quad t \in \mathbb{Z}$$

$$\boxed{2x = 3t + 1}$$

Il  $\mathbb{P}$  è un campo totalmente ordinato, ogni altro campo finito è ISOMORFO?



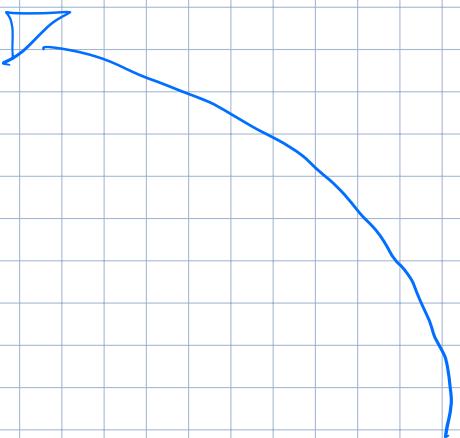
$$(i) x +_A y = f(x) +_R f(y)$$

IN GENERALE

$$(ii) x \cdot_A y = f(x) \cdot_R f(y)$$

NO

$$(iii) f(1_A) = f(1_R)$$



## MORFISMO

è OMOMORFISMO se

$f(A, +_A, \cdot_A) \rightarrow (R, +_R, \cdot_R)$  tale che quei siano

$x$  iniettivo è detto MONOMORFISMO

$x$  suriettivo è detto EPIMORFISMO

$x$  biettivo è detto ISOMORFISMO

## EPIMORFISMO CANONICO

Sia  $A$  un'omello e  $\sim$  una relazione bi eg.

Notate l'immagine quoziente  $A/\sim = \{[x]_\sim : x \in A\}$

$A/\sim$  è allo stesso un'omello con le operazioni.

Costituiamo una funzione  $\tilde{\pi} : A \rightarrow A/\sim$   
 $x \mapsto [x]_\sim$

$$\tilde{\pi}(x) = [x]_\sim$$

$$A \xrightarrow{f} B$$

VOGLIO DIRE CHE  $f$

E' SURIESTIMA

1)  $\tilde{\pi}(x+y) = \tilde{\pi}(x) + \tilde{\pi}(y)$

2)  $\tilde{\pi}(x \cdot y) = \tilde{\pi}(x) \cdot \tilde{\pi}(y)$

3)  $\tilde{\pi}(1_A) = 1_{A/\sim}$

4)  $\tilde{\pi}$  è suriettiva

↓

$$\forall y \in A/\sim \exists x \in A : \tilde{\pi}(x) = y$$

$$y \in A/\sim \Rightarrow y = [x]_\sim \quad x \in A$$

$$\text{dato che } \tilde{\pi}(x) = [x]_\sim = y$$

Dotto un' insieme  $X$  e un' ordine totale ( $\leq$ )

$$\emptyset \neq Y \subset X \quad \overline{X} \quad (Y)$$

$$\inf Y_x = e^{\prime}, \quad \sup Y_x = e^{\prime \prime}$$

Supponiamo che  $X$  sia un compo totalmente ordinato.

### TEOREMA DELLA CARATTERIZZAZIONE DELL'ESTREMO SUPERIORE $Y_x$

Sia  $e'' \in X$   $e'' = \sup Y_x$  se

(i)  $\forall x \in Y \quad x \leq e''$

(ii)  $\forall \varepsilon > 0 \exists x_\varepsilon \in Y : x_\varepsilon > e'' - \varepsilon$

### TEOREMA DELLA CARATTERIZZAZIONE DELL'ESTREMO INFERIORE $Y_x$

Sia  $e' \in X$   $e' = \inf Y_x$  se

(i)  $\forall x \in Y \quad x \geq e'$

(ii)  $\forall \varepsilon > 0 \exists x_\varepsilon \in Y : x_\varepsilon < e' + \varepsilon$

Se  $\mathbb{K}$  un compo totalmente ordinato  $(\mathbb{K}, +, \cdot, \leq)$

$$C_+ := \{x \in \mathbb{K} : x \geq 0\}$$

$$(i) \quad C_+ \cap C_- = \{0\}$$

$$(ii) C_+ \cap C_+ \subseteq C_+ \quad \forall x, y \in C_+ \quad x+y \in C_+$$

$$(iii) C_+ \cdot C_+ \subseteq C_+ \quad \forall x, y \in C_+ \quad x \cdot y \in C_+$$

$$(iii) C_+ \cup C_- = \mathbb{K}$$

Per rendere un campo, totalmente ordinato poss  
imporre una relazione di tale che:

$$\forall x, y \in \mathbb{K} \quad x \leq y \Rightarrow x - y \in C_+$$

## NUMERO NATURALE

Per poter definire in modo formalmente corretto  
dobbiamo lavorare con una teoria degli insiemii  
coerente. Quindi finché non li avremo definiti  
il termine "insieme" non è ancora chiaro.

Von Neumann creò questo modello → non ancora  
definito

Per aggiornare esiste un'insieme presto  $\emptyset$ , che chiamiamo  
0.

$$0 = \emptyset \quad 1 = \{0\} \quad 2 = 1 \cup \{1\} = \{0, 1\} \quad \dots$$

La teoria degli insiemii attuale non permette insiemii infiniti.

Un insieme è detto INDUITIVO se:

$$(i) \emptyset \in X$$

$$(ii) x \in X \Rightarrow X \cup \{x\} \in X$$

## ASSIOMI DI PEANO

Esiste un'insieme  $\mathbb{N}$  ed una funzione  $\sigma: \mathbb{N} \rightarrow \mathbb{N}$ :

$$(1) 0 \in \mathbb{N} \quad (\text{ci dice che } \mathbb{N} \neq \emptyset)$$

$$(2) \sigma: \mathbb{N} \rightarrow \mathbb{N} \quad \{\sigma\} \text{ è infinita}$$

$$\sigma(n) \neq 0 \quad \text{poiché } \sigma(n) \in \mathbb{N} \setminus \{0\}$$

$$\forall m, n \in \mathbb{N} \quad \sigma(m) \neq \sigma(n)$$

### (3) Principio di Induzione Matematica :

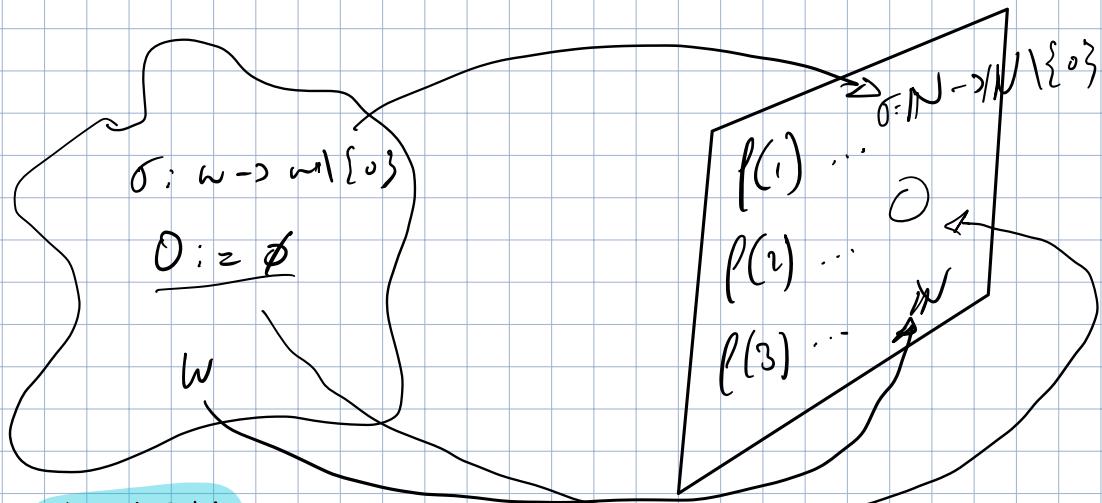
$X \subseteq \mathbb{N}$  :

(i)  $0 \in X$

(ii)  $\forall m \in X \rightarrow \sigma(m) \in X$  allora  $X = \mathbb{N}$

$$\omega = \{0, 1, 2, 3, \dots\}$$

l'insieme dei numeri  
costituito da Von Neumann.



MODELLO  
VON  
NEUMANN

P(1)

Quella di Peano è solo una teoria mentale  
Von Neumann ha l'insieme affinché la  
teoria funzioni.

$(\omega, \sigma)$  soddisfa gli assiomi di Peano :

(1)  $0 \in \omega$  ( $0 := \emptyset \in \omega$ )

(2)  $\sigma: \omega \rightarrow \omega \setminus \{0\}$  è iniettiva

(3)  $\forall X \subseteq \omega$  :

(i)  $0 \in X$

(ii)  $\forall m \in X \quad \sigma(m) \cup \{m\} \in X \Rightarrow X = \omega$

Pongo due che  $m \leq m$  in  $w \Leftrightarrow m \leq m$

Quindi  $(w, \leq)$  è totalmente ordinato, quindi:

(1)  $w \neq \emptyset$

(2)  $\leq \left\{ \begin{array}{l} \text{TRANSITIVA} \\ \text{ANTISIMMETRICA} \\ \text{RIFLESSIVA} \end{array} \right.$

(3) TRICOTOMIA

TEOREMA DI CATEGORIALITÀ DI AXE:

Tutti i modelli costuibili sono isomorfi.

Teorema di Ricorsione Debole:

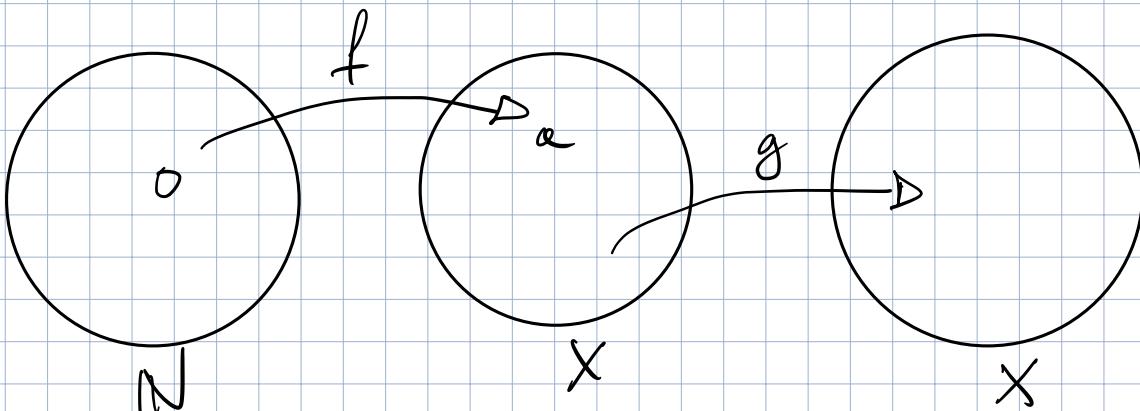
Se  $X$  un insieme,  $X \neq \emptyset$ .

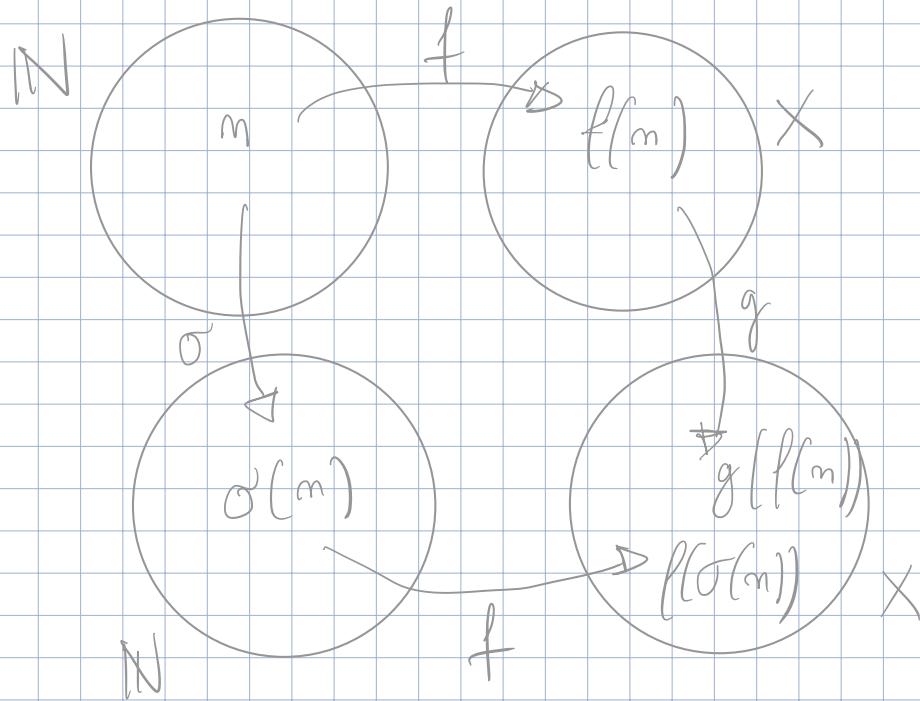
se  $g: X \rightarrow X$  e  $a \in X$

Allora  $\exists! f: \mathbb{N} \rightarrow X$ ,

$$(i) f(0) = a$$

$$(ii) \forall n \in \mathbb{N} \quad f(\sigma(n)) = g(f(n))$$





Questo teorema ci permette di definire  $+_n$  e  $\cdot_n$  in  $(\mathbb{N}, G)$

$$+/\chi := \mathbb{N} \neq \emptyset$$

$$\exists! f: \mathbb{N} \rightarrow \mathbb{N}$$

$$(g) \quad \sigma: \mathbb{N} \rightarrow \mathbb{N} \Rightarrow$$

$$(1) \quad f(0) = 0$$

$$0 = 0$$

$$(2) \quad \forall m \in \mathbb{N}$$

$$f(\sigma(m)) = g(f(m))$$

$$\text{Se } a = m$$

$$\begin{matrix} f: \mathbb{N} \rightarrow \mathbb{N} \\ / \quad m \mapsto f(m) = m+m \end{matrix}$$

$$(1) \quad f(0) = 0 + m = m$$

$$(2) \quad f(\sigma(m)) = \sigma(f(m))$$

$$\sigma(m) + m = \sigma(m+m)$$

$$0 + m = m$$

$$(m+1) + m = (m+m) + 1$$

E' possibile una sola  
funzione somma tale  
che valgono queste proprietà.

Allora definiamo somma in  $\mathbb{N}$ .

Allo stesso modo possiamo definire il prodotto:

$$\begin{cases} 0 \cdot_m m = 0 \\ 5(m) \cdot_m m = (m \cdot m) +_m m \end{cases}$$

In particolare  $(\mathbb{N}, +_n, \cdot_n)$  è un SEMIANELLO

$$(W, +, \cdot, \leq)$$

$$W = \{0, 1, 2, 3, \dots\}$$

$$m + m =$$

$$2 + 3 = 5$$

$$((2+1)+1)+1$$

$$2 = \{0, 1\}$$

$$3 = \{0, 1, 2\}$$

$$2+3=5=\{0, 1, 2, 3, 4\}$$

Forse il successivo in  $\mathbb{N}$  non ha senso  
il insieme che ha come unico elemento il successivo.

$(\mathbb{N}, \leq)$

- Principio di buon ordinamento (Zermelo)
- Ogni  $X \neq \emptyset$   $X \subseteq \mathbb{N}$  ammette minimo (supposto l'ordine  $\leq$ )

PRINCIPIO DI  
BUON ORDINAMENTO  $\hookrightarrow$  PRINCIPIO DI  
INDUZIONE

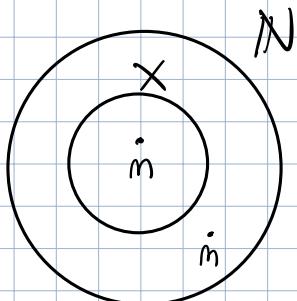
Forma (semantica) del principio di induzione:

$$X \subseteq \mathbb{N}$$

$$m \in \mathbb{N}$$

$$m \in X$$

$$m \notin X$$



Sia  $P(m)$  una proprietà  
o predicato in  $m \in \mathbb{N}$   
è una relazione 1-aria  
quindi un sottoinsieme di  $\mathbb{N}^2$ .

$$m \in X = P(X)$$

dov'è che  $P(X)$  è vero in  
 $m$ .

Principio di induzione (nella semantica)

Sia  $P(m)$  un predicato in  $\mathbb{N}$ . Supponiamo che:

(1)  $P(0)$  è vero,

(2)  $\forall m \geq 0 \quad P(m) \text{ vero} \Rightarrow P(m+1) \text{ vero}$

!!

$p(n)$  è vero  $\forall n \geq 0$

## GAUSS

$$1 + 2 + 3 + 4 \dots = \frac{m(m+1)}{2}$$

Se applico l'induzione:

(1)  $p(0)$  è vero  $0 = 0$

(2)  $\forall m \geq 0$   $p(m)$  vero  $\Rightarrow p(m+1)$  vero

$\Downarrow$

$$1 + 2 + 3 + 4 \dots m = \frac{m(m+1)}{2}$$

$$1 + 2 + 3 + 4 + (m+1) = 1 + 2 + 3 + 4 + m + (m+1)$$

$$\frac{m(m+1)}{2} + m + 1 =$$

$$(m+1)(m+2) = \frac{(m+1)(m+2)}{2}$$

$$(\mathbb{N} := \{0, 1, 2, 3, 4 \dots\}, +, \cdot, \leq)$$

$\leq$  è totale in  $\mathbb{N}$  [ $\forall m, n \in \mathbb{N}$   $m < n$ ,  $m = n$ ,  $m > n$ ]

1 2 3 4 5 (secondo la costituzionalità di Von Neumann)

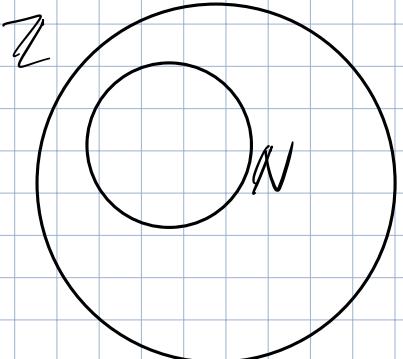
In  $\mathbb{N}$  valgono gli assunti di Peano.

Abbiamo intuito la ricorsione matematica  $\Rightarrow +, \cdot$ .

$m \leq m$  ( $m \in \mathbb{N}$ ) ricava vom Neumann  $m \subseteq m$   
 Insieme (Anello) der numeri interi  $(\mathbb{Z}, +, \cdot)$

$$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \pm \dots\}$$

Costruire  $\mathbb{Z}$



$$\mathbb{N} \times \mathbb{N} = \mathbb{N}^2 \{ (m, n) : m, n \in \mathbb{N} \}$$

introduco  $\Sigma$  la relazione definita da:

$$(m, n) \Sigma (s, t) \Leftrightarrow m + t = s + n$$

SOMMA IN  $\mathbb{N}$

Ex.  $(3, 2) \Sigma (2, 1) \Leftrightarrow \begin{matrix} 3+1 \\ 4 \end{matrix} = 2+2 \begin{matrix} 2 \\ 4 \end{matrix}$

La proposizione  $\Sigma$  è una relazione di equivalenza:

- RIFLESSIVA  $\forall (m, n) \in \mathbb{N}^2 (m, m) \Sigma (m, m) \Leftrightarrow m + m = m + m$

- SIMMETRICA  $\forall (\alpha, \beta) \in \mathbb{N}^2 (\alpha, \beta) \Sigma (\beta, \alpha) \Leftrightarrow (\alpha, \beta) \Sigma (\beta, \alpha)$

- TRANSITIVA  $\forall \begin{cases} (\alpha, \beta) \in \mathbb{N}^2 (\alpha, \beta) \Sigma (\beta, \gamma), (\beta, \gamma) \Sigma (\gamma, \delta) \end{cases} \Leftrightarrow (\alpha, \beta) \Sigma (\gamma, \delta)$

Essendo  $\Sigma$  di equivalenza ha un'insieme quoziente:

$$\mathbb{N}^2 / \Sigma := \left\{ [ (m, n) ]_{\Sigma} : (m, n) \in \mathbb{N}^2 \right\}$$

$$[ (m, n) ]_{\Sigma} := \left\{ (\alpha, \beta) : (\alpha, \beta) \in \mathbb{N}^2 \wedge (\alpha, \beta) \Sigma (m, n) \right\}$$

$\mathbb{N}/\Sigma^2$  introduces 2 operations:

$$[(m, n)]_{\Sigma} + [(s, t)]_{\Sigma} = [(m+s), (n+t)]_{\Sigma}$$

$$[(m, n)]_{\Sigma} \cdot [(s, t)]_{\Sigma} = [(ms+nt), (ns+mt)]_{\Sigma}$$

Ex.

$$[(3, 2)]_{\Sigma} + [(0, 1)]_{\Sigma} = [(3+0), (2+1)]_{\Sigma} = [(3, 3)]_{\Sigma}$$

$$[(3, 2)]_{\Sigma} \cdot [(0, 1)]_{\Sigma} = [(3 \cdot 0 + 2 \cdot 1), (2 \cdot 1 + 3 \cdot 0)]_{\Sigma} = [(2, 3)]_{\Sigma}$$

$(\mathbb{N}/\Sigma^2; +, \cdot)$  è un'anello commutativo.

$[(0, 0)]$  è l'elemento neutro della somma.

$$[(m, n)]_{\Sigma} + [(x, y)]_{\Sigma} = [(0, 0)]_{\Sigma}$$

"

$$[(m+x), (n+y)]_{\Sigma} = [(0, 0)]_{\Sigma}$$

||

$$x = m$$

$$m + x = n + y \quad y = m$$

Quindi  $-[(m, n)]_{\Sigma} = [(m, n)]_{\Sigma}$

$$[(m, n)]_{\Sigma} \cdot \underline{[(1, 0)]_{\Sigma}} = [(m \cdot 1 + n \cdot 0), (m \cdot 0 + n \cdot 1)]_{\Sigma} = [(m, n)]_{\Sigma}$$

ELEMENTO NEUTRO DEL PRODOTTO

$$\left\{ \left[ (0, m) \right]_{\Sigma} : m \in \mathbb{N} \right\} \cap \left\{ \left[ (m, 0) \right]_{\Sigma}, m \in \mathbb{N} \right\} = \emptyset$$

Definisco im  $(\mathbb{N}/\Sigma, +, \leq)$  introdus  $\subseteq$

$$\left[ (m, n) \right]_{\Sigma} \subseteq \left[ (s, t) \right]_{\Sigma} \Leftrightarrow m +_n t \leq m +_n s$$

Ex.  $\left[ (2, 3) \right]_{\Sigma} \subseteq \left[ (1, 2) \right]_{\Sigma} \Leftrightarrow 2 +_2 1 = 3 +_1 \quad (\text{VERA})$

$$[(0, 3)][(0, 2)][(0, 1)][(0, 0)][(1, 0)][(2, 0)][(3, 0)]$$

$$\begin{matrix} & & & & & & \\ & & & & & & \\ - & [(0, 1)] & & & & & \\ & & & & & & \end{matrix}$$

$$-3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3$$

$$\mathbb{N}/\Sigma = \mathbb{Z}$$

In  $(\mathbb{Z}, +, \cdot, \leq)$  è un anello commutativo ordinato

$$\mathbb{Z} \cdot \mathbb{N}^* := \left\{ (m, n) : m \in \mathbb{Z}, n \in \mathbb{N}^* \right\}$$

In  $\mathbb{Z} \cdot \mathbb{N}^*$  introduce la relazione  $\sim$  definita da:

$$\begin{pmatrix} m, n \\ s, t \end{pmatrix} \in \mathbb{Z} \cdot \mathbb{N}^* \quad (m, n) \sim (s, t) \Leftrightarrow m \cdot t = n \cdot s$$

Si dimostra che  $\sim$  è una relazione di eq. in  $\mathbb{Z} \cdot \mathbb{N}^*$ , ovvero essa fa insieme operante.

$\mathbb{Z} \cdot \mathbb{N}^*$  introduce due operazioni:

$$[(m,n)]_n + [(s,t)]_n = [(t \cdot m + s \cdot n), (m \cdot t)]_n$$

$$[(m,n)]_n \cdot [(s,t)]_n = [(m \cdot s), (m \cdot t)]_n$$

Note:  $(\mathbb{Z} \cdot \mathbb{N}^*, +, \cdot)$  è un campo  $\mathbb{Q}$  (Numeri razionali)

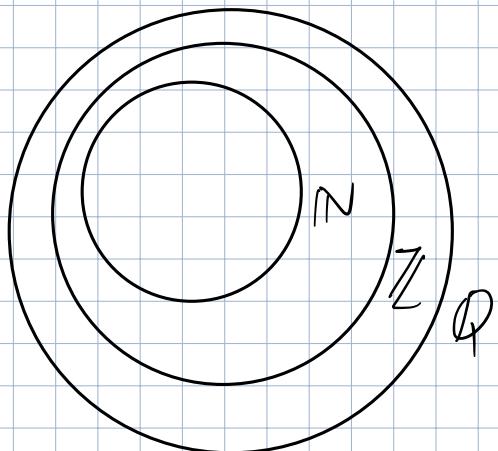
$$[(m,n)]_n = \frac{m}{n}$$

$$\frac{0}{1} = [(0,1)]_n \quad \text{elemento neutro della somma}$$

$$\frac{1}{1} = [(1,1)]_n \quad \text{unità del prodotto}$$

$(\mathbb{Z}; \leq)$  ordine totale  $\leq$

Osservazione:  $\mathbb{N} \subseteq \mathbb{Z} : \mathbb{Z} = \overline{\mathbb{N} \cup \mathbb{N}}$



$\mathbb{N}$  contiene "i numeri" ottenuti per ricorsione a partire dal punto.

$$\mathbb{N} \subset \mathbb{Z} \quad 1 \in \mathbb{Z} \Rightarrow 1 = [(1,0)]_{\Sigma} \rightarrow 1$$

$$1+1 = [(1,0)]_{\Sigma} + [(1,0)]_{\Sigma} = [(2,0)]_{\Sigma} \rightarrow 2$$

$$1+1+1 = [(3,0)]_{\Sigma}$$

$$1+1+1+1 = [(4,0)]_{\Sigma}$$

$$m \in \mathbb{N} \Rightarrow [(m,0)]_{\Sigma}$$

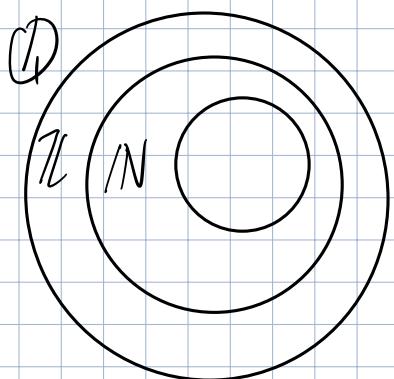
$F$  è biunivoca tra  $\mathbb{N}$  e  $\mathbb{Z} = \overline{\mathbb{N} \cup \mathbb{N}} \quad \{(m,0) : m \in \mathbb{N}\}$

$F: \mathbb{N} \rightarrow \mathbb{Z}$  morfismo di semianelli

In  $\mathbb{Z}$  si trova una "copia" di  $\mathbb{N}$ , semianello isomorfo

$$\text{In } (\mathbb{Q}, \leq) \quad [(m, n)]_v \leq [(s, t)]_v \Leftrightarrow m \cdot t \leq s \cdot n$$

$(\mathbb{Q}, \leq)$  è totale in  $\mathbb{Q}$



$\mathbb{Z} \subset \mathbb{Q}$  vuol dire che  
esiste un sottoanello di  $\mathbb{Q}$   
isomorfo a  $\mathbb{Z}$ .

$$B := \left\{ [(m, 1)]_v : m \in \mathbb{Z} \right\} \cong \mathbb{Z}$$

Ex.  $\mathbb{Z}_3 = \{0_3, 1_3, 2_3\} \quad 1_3 + 1_3 + 1_3 = 0_3$

Dato un Anello  $A$ :

$$\exists \text{ minimo intero } m : 1 + 1 + \dots = 0$$

$\underbrace{\phantom{1+1+\dots}}_{m-\text{volte}}$

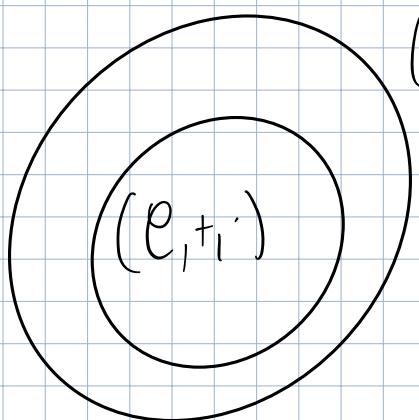
$\text{Ch}(A)$ : se non esiste si dice che  $A$  ha caratteristica 0.

Ex.  $\text{Ch}(\mathbb{Z}_3) = 3$

$\mathbb{K}$  campo totalmente ordinato  $\Rightarrow \text{Ch}(\mathbb{K}) = 0$

$(\mathbb{Q}, +, \cdot, \leq)$  campo tot. ordinato  $\Rightarrow \text{Ch}(\mathbb{Q}) = 0$

Dato um campo  $\mathbb{K}$  tot. ord. existe um subcampo.



$(\mathbb{K}, +, \cdot, \leq)$

P isomórfico a  $\mathbb{Q}$

Sia  $(\mathbb{K}, +, \cdot, \leq)$  totalmente ordenado

$$\text{Ch}(\mathbb{K}) = 0 \Rightarrow \mathbb{Q} \subseteq \mathbb{K}$$

$$\mathbb{N} \subset \mathbb{Q} \subseteq \mathbb{K}$$

Propriedade di Archimede:

$$(*) \forall x \in \mathbb{K} \exists m \in \mathbb{N} : m > x$$

S.ams intuisci solo sui campi Archimedici. \*)

Nei campi ordinati e Archimedici posso dare la definizione  
di "punte intuisci".

Proposizione :  $(\mathbb{K}, +, \cdot, \leq)$  totalmente ordinato + Archimede

$$\text{Allora } \forall x \in \mathbb{K} \exists \alpha_x \in \mathbb{Z} : \alpha_x \leq x < \alpha_x + 1$$

$$\forall x \in \mathbb{K} \exists \alpha_x \in \mathbb{Z} : x \in [\alpha_x, \alpha_x + 1]$$

$\lfloor x \rfloor := \lfloor x \rfloor$  parte intera

$\forall x \in \mathbb{K} \exists \lfloor x \rfloor \in \mathbb{Z} : \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

$x \in \mathbb{K} \quad x - \lfloor x \rfloor \in \mathbb{K}$

$x - \lfloor x \rfloor$  si dice parte frazionaria di  $x$ .  
mantissa di  $x$

(D) è Archimede perché:

$\forall x \in \mathbb{Q} \exists m \in \mathbb{N} : m > x$

## DENSITÀ DEI RAZIONALI

Sia  $\mathbb{K}$  un campo t.t. ord. e  $S \subset \mathbb{K}$  sia  
denso in  $\mathbb{K}$  se  $\forall x, y \in \mathbb{K} \exists c \in S : x < c < y$

Teorema:

$(\mathbb{K}, +, \cdot, \leq)$  totalmente ordinato:

Sono equivalenti i seguenti fatti:

(i)  $\forall x \in \mathbb{K} \exists m \in \mathbb{N} : m > x$  (\*) ;

(ii)  $\forall x, y \in \mathbb{K} : x > y \Rightarrow \exists m \in \mathbb{N} : mx > my$  ;

(iii)  $\mathbb{Q}$  è denso in  $\mathbb{K}$ .

Un campo t.t. ordinato è Archimede? In generale no.

Lo è  $\Leftrightarrow \mathbb{Q}$  è un'infima densa in  $\mathbb{K}$

$\mathbb{Q}$  è ordinatamente denso in  $\mathbb{K}$

## SPAZIO METRICO

Possiamo dire che due punti sono vicini o lontani solo introducendo il concetto di DISTANZA.

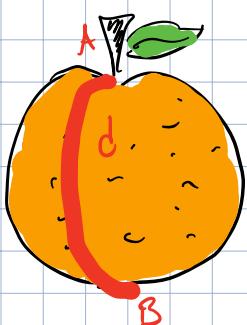
$X \neq \emptyset$  insiem + funzione distanza  $d$   
 $(X, d)$  è uno spazio metrico

Sia  $\mathbb{K}$  un campo  $(\mathbb{K}, +, \cdot, \leq)$  totalmente ordinato.

Ese.  $(\mathbb{Q}, +, \cdot, \leq)$  // induce

V

Struttura d: spazio metrico  $(\mathbb{K}, d)$



La curva d, minima comunica i detti geodesiche.

$$x, y \in \mathbb{K} \quad d(x, y) := |x - y|$$

$$d: \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$$

$$z \in \mathbb{K} \quad |z| := \max \{-z, z\}$$

$$\begin{cases} -z < z \\ -z = z \quad (z = 0) \\ z < z \end{cases}$$

Proprietà di  $d$ :

POSITIVITÀ

$$(1) \quad d(x, y) \geq 0 \quad \wedge \quad d(x, y) = 0 \quad \Leftrightarrow \quad x = y \quad \text{in } K$$

$$(2) \quad d(x, y) = d(y, x) \quad \forall x, y \in K \quad \text{SIMMETRIA}$$

$$(3) \quad d(x, z) = d(x, y) + d(y, z) \quad \forall x, y, z \in K \quad \text{DISUGUAGLIANZA TRIANGOLARE (MINKOWSKI)}$$

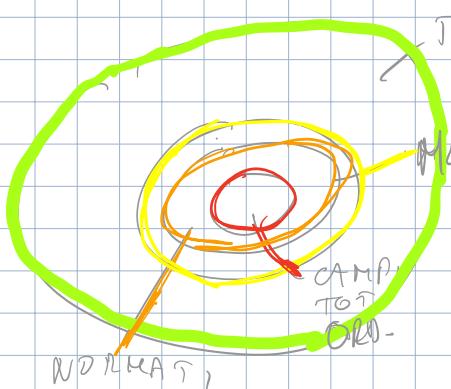
Una funzione  $d$  distanza si definisce queste tre proprietà, in  $K$  per esempio scriver:

$$(1) \quad |x - y| \geq 0 \quad \wedge \quad |x - y| = 0 \quad \Leftrightarrow \quad x = y$$

$$(2) \quad |x - y| = |y - x|$$

$$(3) \quad |x - y| = |x - z| + |z - y|$$

Poiché  $K$  è totalmente ordinato.



TOPLOGICO

METRICO

NORMATO

Un spazio Topologico

è un spazio (in cui ha

senza parlare di vicinanza fra

punti). Un spazio metris è

uno spazio topologico (in cui la vicinanza

di vicinanza è indicata dalla metrica).

Pertanto i spazi metrici sono sempre totalmente ordinati,

Def.

$$x \in K, x \neq 0. x_0 \in K$$

$x_0$  è interno a  $X \Leftrightarrow \exists \delta > 0 : B(x_0, \delta) \subseteq X$

$x_0$  è esterno a  $X \Leftrightarrow \exists \delta > 0 : B(x_0, \delta) \subseteq K \setminus X$

$x_0$  è di frontiera per  $X \Leftrightarrow \forall \delta > 0 : B(x_0, \delta) \cap X \neq \emptyset$

$$B(x_0, \delta) \cap (K \setminus X) \neq \emptyset$$

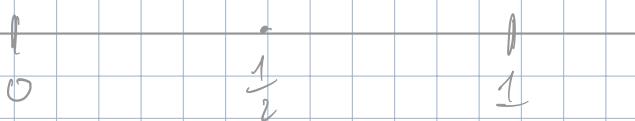
2e. è isolato per  $X \Leftrightarrow \exists \delta > 0 : B(x_0, \delta) \cap X = \{x_0\}$

2f. è di accumulazione per  $X \Leftrightarrow \forall \delta > 0 B(x_0, \delta) \cap (X \setminus \{x_0\}) \neq \emptyset$

Palla chiusa:  $\bar{B}(x_0, \delta) := \{x \in K : d(x, x_0) \leq \delta\}$

Palla aperta:  $B(x_0, \delta) := \{x \in K : d(x, x_0) < \delta\}$

Esempio (punto di accumulazione)  $x_0 \in [0, 1] \setminus \{\frac{1}{2}\}$



$\frac{1}{2}$  è di accumulazione

$$X^o := \{ x + K : x \text{ sia interno a } X \}$$

PARENTESE

$$\partial X := \{ x \in K : x \text{ sia di frontiera per } X \}$$

$$\overline{X} := \{ x \in K : x \text{ sia aderente ad } X \}$$

$$DX := \{ x \in K : x \text{ sia di accumulazione per } X \}$$

$$\Rightarrow \overline{X} := X \cup \partial X$$

$$\begin{array}{l} X^o \subseteq X \\ X \subseteq \overline{X} \end{array}$$

$$X \text{ è aperto in } K \Leftrightarrow X = X^o$$

$$X \text{ è chiuso in } K \Leftrightarrow X = \overline{X}$$

Sì dimostro che  $X \subseteq K$  è aperto in  $K \Leftrightarrow ]c, c[ \subseteq X$  è chiuso in  $K$ :

$$X = K \setminus ]c, c[$$

CLOSEN: insieme allo stesso tempo aperto e chiuso

Lo spazio è chiuso se gli omici chiusi sono il tutto e l'intero spazio.

$$IN^o = \emptyset \quad \partial IN = IN \quad \overline{IN} = IN \cup \partial IN = IN$$

Quindi  $IN$  è chiuso

**Proposition 5.2.** Let  $\mathbb{K} = (\mathbb{K}, +, \cdot, \leq)$  be a totally ordered field. The following facts hold:

- (i)  $\mathbb{K}$  and  $\emptyset$  are open sets;
- (ii) If  $(X_\alpha)_{\alpha \in J}$  is a family of open sets, then  $\bigcup_{\alpha \in J} X_\alpha$  is an open set;
- (iii) If  $X_1, \dots, X_k$  ( $k \in \mathbb{N}^*$ ) are open sets, then  $\bigcap_{i=1}^k X_i$  is an open set.

← FinTA  
↓ INFNTA

Atti Accad. Pelorit. Pericol. Cl. Sci. Fis. Mat. Nat., Vol. 99, No. S1, A17 (2021) [38 pages]

**Proposition 5.3.** Let  $\mathbb{K} = (\mathbb{K}, +, \cdot, \leq)$  be a totally ordered field. The following facts hold:

- (j)  $\mathbb{K}$  and  $\emptyset$  are closed sets;
- (jj) If  $(X_\alpha)_{\alpha \in J}$  is a family of closed sets, then  $\bigcap_{\alpha \in J} X_\alpha$  is a closed set;
- (jjj) If  $X_1, \dots, X_k$  ( $k \in \mathbb{N}^*$ ) are closed sets, then  $\bigcup_{i=1}^k X_i$  is a closed set.

## INSIEME

Teoria non ingenua def: insieme di Göd, Bernays,  
Von Neumann. (NGB)

- Skolem, Tarski e Fraenkel (ZF, ZFC)
- Morse e Kelley (MK)

Un **UNIVERSO** racchiude tutte le classi, ed è  
una **classe** universale e le classi che contiene  
sono dette **sotto classi**.

Se io sono  $x \in U$ ,  $x$  è **meazuramente**  
un **oggetto**, e  $y$  è **meazuramente** una **classe**

Tutti i simboli di filosofia non hanno significato

## **ASSIOMA DI ESTENSIONALITÀ**

I: assioma, prendi  $X$  e  $Y$  come classi, queste

Sono uguali se contengono gli stessi oggetti.

$$\forall z (z \in X \leftrightarrow z \in Y) = X = Y$$

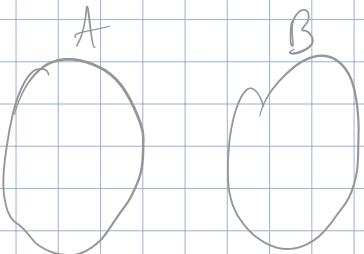
## ASSIOMA DI ASTRAZIONE

II: Fissa una proprietà che dipenda da un certo numero di classi.

$$Z := \{x : P(x, Y_1, \dots, Y_m)\}$$

Questo  $Z$  sono una classe.

$A, B$  insiem!



$$A \cap B = \{x : x \in A \wedge x \in B\}$$

$$\overbrace{P(x, A, B)}$$

$$A \cup B = \{x : x \in A \vee x \in B\}$$

$$\overbrace{P(x, A, B)}$$

$$\emptyset = \{x : x \neq x\}$$

INSEME  
VUOTO

Nella teoria ingenua degli insiemi ogni proprietà non dava luogo ad un insieme.

La provò è il paradosso di Russell:

$$\{x : x \neq x\} P(x) \text{ NON È UN INSEME}$$

Tonaperto al secondo giorno che genera una CLASSE.

## ASSIOMA DI COMPRENSIONE

III : Se prendo un insieme  $Y$ , col un suo insieme  $X \subseteq Y$ . Un insieme è una particolare classe.

## ASSIOMA DELL' INSIEME VUOTO

IV : La classe vuota è un insieme  
(Quindi anche l' insieme vuoto )

## ASSIOMA DELLA COPPIA

V : Se prende due oggetti,  $x, y$  e la classe  $\{x, y\}$   
 $\{z : z = x \vee z = y\}$

La classe  $\{x, y\}$  è un' insieme.

## ASSIOMA DELL' UNIONE

VI : Sia  $X$  un' insieme di insieme

$$\bigcup X := \{x : \exists y (y \in X \wedge x \in y)\}$$

è un insieme.

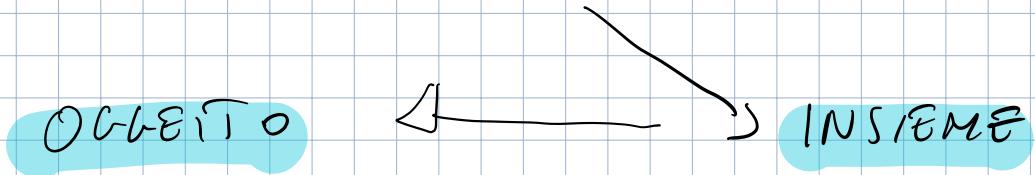
Accordi tra gli scrittori:

## ASSIOMA DEGLI OGGETTI

VII : Ogni oggetto è un insieme.

Gli insiemi sono classi che possono essere messe come oggetti.

Se la classe è un'insieme può avere 2 forme



Gli posso applicare  
l'appartenenza

$\in$

Gli posso applicare  
l'inclusione

$\subseteq$

La classe di Russel è una classe non un'insieme,

e queste classi vengono dette **CLASSE PROPIA**.

## ASSIOMA DELL'INFINITO

VIII : Esiste un insieme  $X$ :

$$(i) \quad \emptyset \in X$$

$$(ii) \quad \text{se } x \in X \rightarrow x \cup \{x\} \in X;$$

Questo assioma fa leop agli insiemi infiniti.

## ASSIOMA DELL'INSIEME POTENZA

X: Dato un insieme  $X$ , la classe

$$\wp(X) := \{Y : Y \subseteq X\}$$

chiamata  $Y$  è un insieme.

## ASSIOMA DEL REMPLAZZO

X: Sia  $f: X \rightarrow Y$  una funzione fra classi.

Se il dominio  $X$  ol'  $f$  è un insieme,  
l'immagine è un insieme.

$$f(X) := \{g : \exists x (x \in X \wedge f(x) = g)\}$$

## ASSIOMA DELLA SCELTA

XI: Se prendo una famiglia d. insiem. disgiointi  
e non vuoti.  $(X_\alpha)_{\alpha \in J}$

Se da ogni insieme prendo un elemento ho  
costituito un nuovo insieme.

$$\exists S : S \cap X_\alpha = \{x_\alpha\} \forall \alpha \in J$$

(dove  $J$  è un insieme)  
d: indic.

Ora questo mi permette di scegliere gli elementi di

prendere.

## ASSIOMA DI FONDAMENTALE

XII: Per ogni insieme  $X \neq \emptyset$  esiste un  $a \in X$ :

$$X \cap a = \emptyset$$

Dimostra che la dom di Russell non è un insieme:

$$\mathcal{R} \in \mathcal{U} \quad \text{iff} \quad x \notin x$$

Assumiamo per orrido che  $\mathcal{U}$  è un oggetto e quindi un insieme.

Quindi  $\mathcal{U} \in \mathcal{U}$  iff  $\mathcal{U} \notin \mathcal{U}$  che è una contraddizione.

La classe di tutti gli oggetti non è un insieme!

Ogni classe  $X$  è inclusa in  $C_{\text{obst}}$ , in particolare

$$\mathcal{U} \subseteq C_{\text{obst}}$$

Suppongo per orrido che  $C_{\text{obst}}$  sia un insieme (anche  $\mathcal{U}$  dovrebbe un insieme, ma è orrido perché abbiamo dimostrato che  $\mathcal{U}$  è una classe propria).

Se  $X \subset Y$  sono insiem allora  $X \times Y$  è un insieme.

$$\bigcup \{X \times \{y\} : y \in Y\} = \bigcup X \times Y = X \times Y$$

$y \in Y$

Per Kuratowski, possiamo definire:

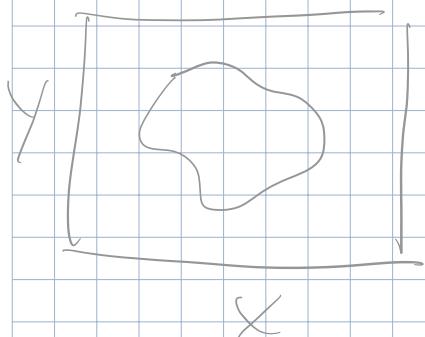
$$(x, y) := \underbrace{\{ \{x\} \}}_{\text{PER ASSIOMA DELLA UNIONE}}, \underbrace{\{x, y\}}_{\text{PER ASSIOMA DELLE COPPIE}}$$

$$(x, y) \neq (y, x) \quad \text{quando } x \neq y$$

Le Relazioni visto come sostanzialmente di cui invilire sono insiemi. Ad esempio il grb.

$X, Y$  classi

$X \times Y$  classi

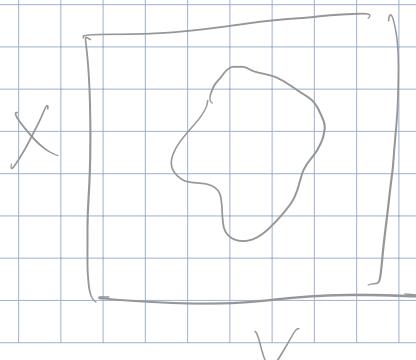


$$R \subseteq X \times Y$$

↓  
sottoinsieme

$X, Y$  (insiemi)

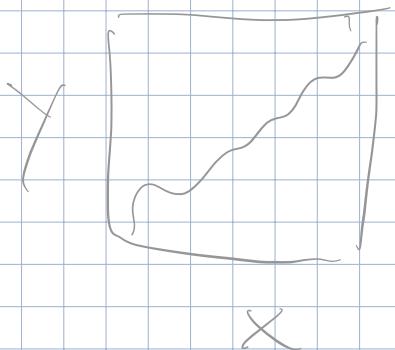
$X \times Y$  (insiemi)



$$R \subseteq X \times Y$$

↓  
sottoinsieme

$X, Y$  classi -  $f: X \rightarrow Y$  funzione fra classi



$\text{Gr}(f) = \{(x, f(x)) : x \in X \wedge f(x) \in Y\}$   
 $= X^+ f(X)$  è un insieme  
 per l'osservazione dell'impiego,

Dovendo ricordare tutte le classi per definire una  
 funzione da considerare come una relazione  
 sottoinsieme del prodotto cartesiano  $\text{Gr}(f)$ , ma essendo  
 che i membri omichi  $f$  sono un'insieme.

$X \times Y$  insieme,  $\wp(X \times Y)$  insieme

Sia  $f \in Y^X$ , per definizione  $\text{Gr}(f) \subseteq X \times Y$   
 $\text{Gr}(f) \in \wp(X \times Y)$ . Di conseguenza  $Y^X \subseteq \wp(X \times Y)$   
 è un insieme.

Famiglia: Prendo  $X, J$  due insiem: , allora dici una  
 famiglia di elementi di  $X$  parametrizzata da  $J$ ,  
 una funzione  $x: J \rightarrow X$ . L'immagine  $x(\alpha)$   
 è denotata da  $x_\alpha$ , dove  $\alpha$  è detto INDICE.  
 Una successione non è altro che una famiglia.

$$J \rightarrow X$$

$$\alpha \rightarrow \alpha(x) = x_\alpha$$

Il vantaggio è che possiamo unire in formule nonarie gli insiem.

$$(x)_{\alpha \in I}$$

$$(x)_{\alpha \in Q}$$

$$(x)_{\alpha \in N}$$

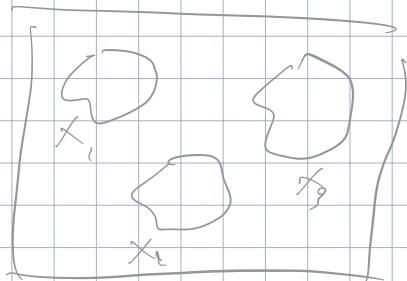
Ved. pag 17-33

## PRODOTTO DIETTO DELLA FATTORIA:

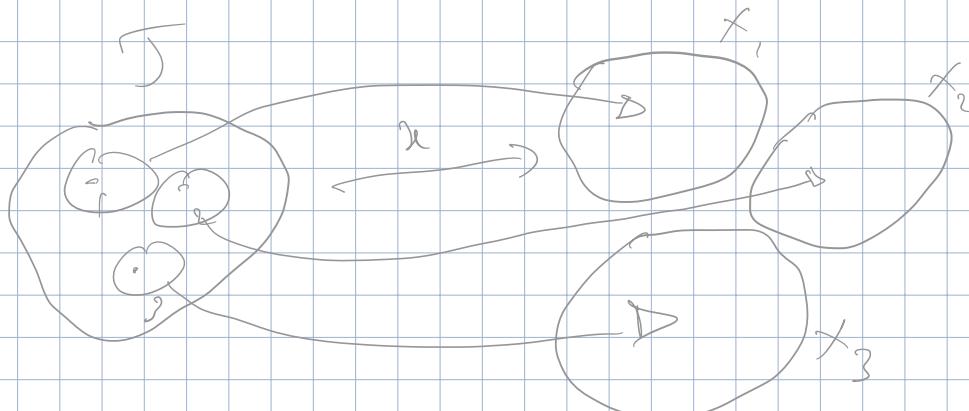
$$\prod_{\alpha \in J} X_\alpha := \left\{ x : x : J \rightarrow \bigcup_{\alpha \in J} X_\alpha : x_\alpha := x(\alpha) \in X_\alpha \text{ se } \alpha \in J \right\}$$

$$X_1, X_2, X_3$$

$$J := \{1, 2, 3\}$$



$$\prod_{i \in J} X_i := \left\{ x : J \rightarrow \bigcup_{i \in J} X_i ; x(i) \in X_i \right\}$$



## CARDINALITÀ (per Frege)

Un insieme è detto **finito** se c'è un  $n \in \mathbb{N}$  e una  $f$  biettiva  $f: J_n \rightarrow X$  ove  $J_n = \{1, \dots, n\}$ .

Se esiste una corrispondenza biunivoca fra numeri naturali e gli elementi dell'insieme.

**CARDINALITÀ**: il numero di elementi di un insieme finito.

Prendo 2 insiemi  $X, Y$ :

- dico che  $X \sim Y$ , quando esiste una  $f$  biettiva  $f: X \rightarrow Y$

Quindi  $X$  è finito se  $X \sim A \subseteq \mathbb{N}$ .

CARDINALITÀ  
 $|X| \leq |Y|$  se  $\exists f: X \rightarrow Y$  iniettiva

$|X| < |Y|$  se  $|X| \leq |Y|$  e  $X \neq Y$

## PRINCIPIO DEI CASSERII

Se  $f: J_m \rightarrow J_n$  è iniettiva allora sicuramente:

- $f$  è suriettiva
- $f$  è biettiva

## CONOLLAZIONE

(Teorema che è conseguenza del teorema  
che in esso stesso un Teorema)

- $m, m' \in \mathbb{N}$   $|J_m| \neq |J_{m'}|$ , se  $m < m'$   $|J_m| < |J_{m'}|$
- $B \subset A$   $|B| < |A|$  se  $A$  è finito.
- $X \neq \emptyset, Y \neq \emptyset$   $|X| \leq |Y|$   $f: X \rightarrow Y$  è suriettiva

$X, Y, Z$  insiem, vale:  $(\begin{array}{c} X \\ Y \\ Z \end{array} \in \text{Universo})$

- $X \sim X$  RIFLESSIVA
- $\exists X \sim Y$  allora  $Y \sim X$  SIMMETRIA
- $\exists X \sim Y, Y \sim Z$  allora  $X \sim Z$  TRANSITIVA

La relazione d. equipotenza è d. equivalente nella classe degli insiemi  $C_{\text{sets}}$ .

Definisco  $|X| := \{Y : Y \sim X\}$  è una classe

non esiste altra insieme qualsiasi né classe contenente più di non esiste classe ola classe.

Questa condizione è una classe d. equivalenze ovvero l'insieme degli insiem equipotenti ad  $X$ .

Alla d. questo è detto numero cardinale  $|X|$ .

$(\mathbb{N}; \in)$  è buon ordinamento  $\Rightarrow$  è ordinale  
 è anche transitivo

Nesse perché tutte le cardinalità sono insieme.

L'appartenenza non è necessariamente transitiva

$$x \in \{x\} \in \{\{x\}\}$$

## ARITMETICA TRANSFINITA

$$|X| + |Y| := |\overline{X \cup Y}| \text{ SOMMA DI CARDINALI}$$

Differenza simmetrica o unione disgiunta.

$$|X| \cdot |Y| := |\frac{X \times Y}{\text{INSIEME}}| \text{ PRODOTTO DI CARDINALI}$$

$$|Y|^{|X|} := |Y^X| \text{ POTENZA DI CARDINALI}$$

Ex.

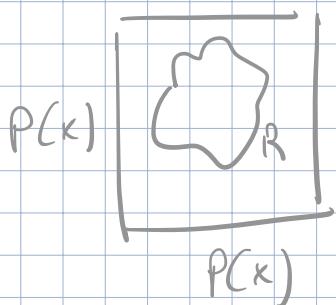
$$X := \{a, b, c\}$$

$$P(X) := \{\text{partizioni di } X\}$$

In  $P(X)$  considera la seguente relazione  $R$

$$A, B \in P(X)$$

$$A R B \text{ se } |A| = |B|$$



Una  $R$  di un' insieme è un'industria

Sarà l'insieme quoziente  $P(X)/R$

$$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{ab\}, \{ac\}, \{bc\}, \{a, b, c\}\}$$

$$[\{a\}]_R = \{\{a\}, \{b\}, \{c\}\}$$

$$[\emptyset]_R = \{\emptyset\}$$

$$[\{a, b\}]_R = \{\{a, b\}, \{ac\}, \{bc\}\}$$

$$[\{a, b, c\}]_R = \{\{a, b, c\}\}$$

$$\begin{aligned} P(X)/R &= \{[\{a\}], [\{b\}], [\{c\}], [\{ab\}], [\{ac\}], [\{bc\}], [\{a, b, c\}], [\emptyset]\} = \\ &= \{|\{a\}|, |\{b\}|, |\{c\}|, |\{ab\}|, |\{ac\}|, |\{bc\}|, |\{a, b, c\}|, |\emptyset|\} \end{aligned}$$

$$|\{a\}|^{|\{a,b\}|} := |\{\alpha\}^{\{ab\}}|$$

$\begin{matrix} a & b \\ \downarrow & \downarrow \\ \alpha & \end{matrix}$

$$\{a\}^{\{a,b\}} := \{f: \{a,b\} \rightarrow \{a\}\}$$

Esgiste umz sola funziona, quindi condimabta 1.

$$|\{a\}| + |\{b\}| := |\{a,b\}|$$

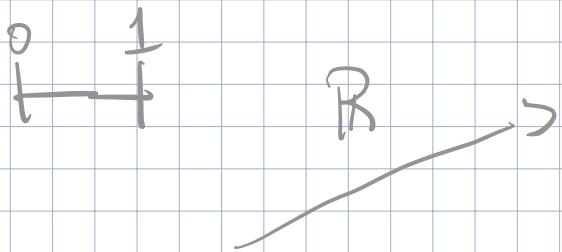
$$1 + 1 := 2$$

$$|\mathbb{N}| = \{x : x \sim \mathbb{N}\}$$

$$|\mathbb{N}|^{|\mathbb{N}|} := |\mathbb{N}^\mathbb{N}| \quad |\mathbb{R}|^{|\mathbb{N}|} := |\mathbb{R}^\mathbb{N}|$$

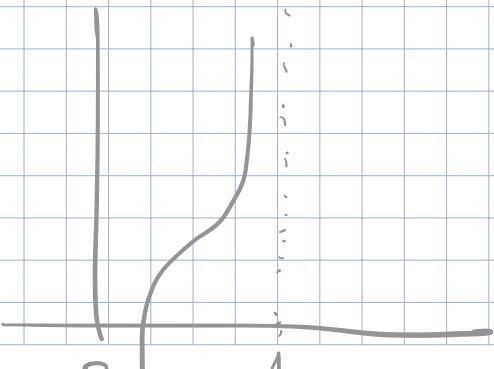
$$|\mathbb{R}| > |\mathbb{N}| \quad |\mathbb{N}| = |\mathbb{Q}| = |\mathbb{Z}|$$

Se prendo un segmento in  $\mathbb{R}$ , eol  $\mathbb{R}$



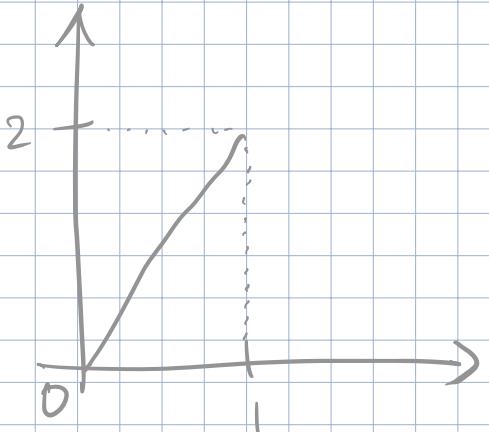
Chi ha condimabta massima?

$$|[0,1]| = |\mathbb{R}|$$



Esgiste umz funziona biuttu  $\mathbb{R}_2$   
 $\downarrow$   $[0,1] \rightarrow \mathbb{R}$  quali  
 hanno stessa condimabta.

$$| [0,1] | = | [0,1] |$$



Eiste una funzione biunivoca  
 $f: [0,1] \rightarrow [0,2]$  quindi  
 hanno stessa cardinalità.

Sia  $\mathcal{E}$  un insieme,  $X, Y, t \in \mathcal{P}(\mathcal{E})$   
 $\sim$  una relazione di equivalenza

$$\mathcal{P}(\mathcal{E})/\sim = \{[X] : X \in \mathcal{P}(\mathcal{E})\}$$

$X \leq Y$  se  $f: X \rightarrow Y$  è iniettiva.

Se in  $\mathcal{P}(\mathcal{E})$  ha una relazione d'ordine, la  
 avrà anche nel quozienti.

Diciamo  $\underline{|X| \leq |Y|}$  se  $\underline{|X| \leq |Y|}$  in  $\mathcal{P}(\mathcal{E})$

$$\begin{array}{c} \text{ORDINE TRA} \\ \text{CLASSI} \end{array} = \begin{array}{c} \text{PRECEDE} \\ \text{TRI INSIEMI} \end{array}$$

$(\wp(\mathcal{E})/\sim, \subseteq)$  è totalmente ordinato

(1)  $|X| \subseteq |X|$

(2) Se  $|X| \subseteq |Y|$  e  $|Y| \subseteq |X|$  allora  $|X| = |Y|$

(3) Se  $|X| \subseteq |Y|$  e

(4) TRICOTOMIA  $|X| < |Y|, |X| = |Y|, |Y| < |X|$

Se ho 2 insiem X, Y

$$|X| \subseteq |Y| \vee |Y| \subseteq |X|$$

Vediamo in che condizioni fare si assuma il  
Lemma di Zorn.

CANTO II:

FUNZIONI BOOLEANI:  $|\wp(X)| = |\{0,1\}^X| = 2^{|X|}$

Quanti sono le funzioni Booleane? Sono poi  
tutte le condizioni che i valori dell'insieme delle parti di X.

$$|X| = n \quad |\wp(X)| = 2^n$$

$$\{0,1\}^X := \{f_1, f_2, f_3, f_4\}$$

Possiamo dire che  $|\wp(X)| = |\{0,1\}^X|$  con una  
funzione caratteristica biettiva.

Esiste una sola funzione  
 (costante per cui  $m^0 = \text{sempre } 1$ )

$$f: \emptyset \rightarrow A$$

$$f: \emptyset \rightarrow \emptyset$$

Penso di un che  $|X| \subset 2^{1 \times 1}$

Un' insieme  $X$  è numerabile se  $X \sim \mathbb{N}$

$$\aleph_0 := |\mathbb{N}| - \text{potenza del numerabile}$$

$$\aleph_1 := |\wp(\mathbb{N})| = 2^{|\mathbb{N}|} - \text{potenza del continuo.}$$

$$\aleph_0 < \aleph_1$$

## CANTITÀ PITTATRONE DI INSIEME INFINTO

Se  $A$  è un' insieme,  $A$  è infinito se  $|\mathbb{N}| \leq |A|$

Un' altro modo per dire è,

$$\exists B \subset A : |B| = |A|$$

Ottavo modo  $|B| = |\mathbb{N}|$

## RELAZIONI TRA INSIEMI FINITI E NUMERABILI

|| Sia  $X$  un insieme e  $x_0 \in X$ , sia  $X$  numerabile  
allora  $X \setminus \{x_0\}$  è numerabile.

Corollario:

Sia  $X$  infinito numerabile, se gli sottogruppi di insieme finiti, la cardinalità rimane la stessa

Lemme:

$$|\mathbb{N} \times \{0,1\}| = |\mathbb{N}|$$

Corollario:

Siano  $X$  e  $Y$  insiemini  $|X| = |\mathbb{N}| \subset |Y| (= |\mathbb{N}|)$   
allora  $|X \cup Y| = |\mathbb{N}|$

PROVA: Sia  $f: X \rightarrow \mathbb{N}$  e  $g: Y \rightarrow \mathbb{N}$  biiettive  
la funzione  $h: \mathbb{N} \times \{0,1\} \rightarrow X \cup Y$

$$|A| \leq |B| \quad h(x) \begin{cases} g(m) & \text{se } x = (m, 0) \\ f(m) & \text{se } x = (m, 1) \end{cases}$$

$$\begin{matrix} A \\ B \end{matrix} \neq \emptyset$$

$$B \rightarrow A$$

$$|X \cup Y| \leq |\mathbb{N} \times \{0,1\}| = |\mathbb{N}|$$

$$|A| = |B| \iff |A| \leq |B| \wedge |B| \leq |A|$$

$$i : X \rightarrow X \cup Y$$

$$|N| = |X| \leq |X \cup Y| \leq |N \times \{0,1\}| = |N|$$

Corollario:

Sia  $(x_n)_{n \in J_m}$   $m \geq 1$  una famiglia di insiem numerabili

$$\left| \bigcup_{k \in J_m} X_k \right| = |N|$$

Ogn' insieme infinito può essere ripartito in insiem numerabili.

Corollario:

Sia  $X$  un' insieme infinito  $|X \setminus Z_m| = |X|$   
 allora  $|X \cup Z_m| = |X|$ , in più esiste  
 un  $|W| \subset |X|$  tale che  $|W| = |X|$ .

Corollario: Se  $X \subset Y$  sono insiem tali che  $|X| \leq |Y|$   
 allora  $|X \cup Y| = |Y|$

Corollario: Se  $X \subset Y$ :  $|X| < |Y| \Rightarrow |Y| = |Y \setminus X|$

# CARDINALITÀ DI PARTICOLARI INSIEMI

$$|\mathbb{Z}| = |\mathbb{N}| \quad |\mathbb{Q}| = |\mathbb{N}|$$

Cardinalità di  $\mathbb{R}$ :

$$I = ]0, 1[ = \{x \in \mathbb{R} : 0 < x < 1\}$$

$$|I| = |\mathbb{R}|$$

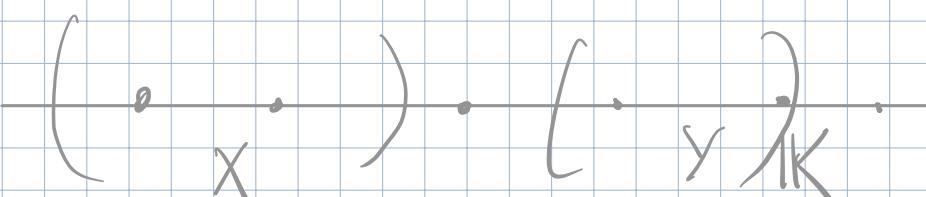
$$|\mathbb{R}| = |\mathfrak{c}\mathbb{N}|$$

## D-COMPLETITÀ

Se  $\mathbb{K}$  un campo tot. ord. (vale anche per insiem tot. ordinati)

Posi due insiem:  $X, Y \neq \emptyset$

$$X \subseteq Y \Leftrightarrow (\forall x \in X, \forall y \in Y, x \leq y)$$



11. insieme  $\mathbb{K}$  è detto D-completo se per ogni:

$$X, Y \neq \emptyset$$

$$X \subseteq Y \Rightarrow \exists z \in \mathbb{K} : \forall x \in X, \forall y \in Y, x \leq z \leq y$$

Teorema: Per un compo  $\mathbb{K}$  t.t. ordinato le seguenti osservazioni sono equivalenti:

(a)  $\mathbb{K}$  è D-completo

(b)  $\forall X \neq \emptyset, X \subseteq \mathbb{K}$  se  $U_X \neq \emptyset$  allora  $\sup_{\mathbb{K}} X$  esiste

(c)  $\forall X \neq \emptyset, X \subseteq \mathbb{K}$  se  $L_X \neq \emptyset$  allora  $\inf_{\mathbb{K}} X$  esiste

$U_X$  è l'insieme dei maggioranti di  $X$  in  $\mathbb{K}$   
 $L_X$  è l'insieme dei minoranti di  $X$  in  $\mathbb{K}$

$\mathbb{Q}$  NON È D-COMPLETO.

Perché non vengono (a), (b) del teorema

$$X := \{ q - q : \mathbb{Q} \cap q \geq 0, q^2 < 2 \}$$

PROVA:

Siccome 1 sarà comunque appartenente a  $X$ ,  $X \neq \emptyset$   
in più  $2 \in U_X$ , quindi se  $q \in X$ :

$$q^2 < 2 \Rightarrow q^2 < 4 \Rightarrow (q-2)(q+2) < 0 \Rightarrow q < 2$$

Supponiamo per assurdo che esiste  $P := \sup_{\mathbb{Q}} X$

che sia  $P = \min_{\mathbb{Q}} U_K$  e  $\rho \geq 1$ , per la tricotomia:

$$\begin{array}{c} P^2 < 2 \\ | \\ P^2 = 2 \\ | \\ P^2 > 2 \end{array}$$

Caso  $P^2 < 2$ :  $\mathbb{Q}$  è Archimedico



Teserma: I'omorfismo  $\varphi$ : Deckind complet. compo ordnat.

Siano  $|K_1| \subset |K_2|$  compi tot. ord. e una  
funzione biunivoca  $\varphi: |K_1| \rightarrow |K_2|$  è ditta un  
I'omorfismo corrente.

L'ordine di  $|K_1|$  si preserva in  $|K_2|$ .

$\forall x, y \in |K_1|, x <_1 y \text{ in } |K| \Rightarrow \varphi(x) <_2 \varphi(y) \text{ in } |K_2|$ .

Teserma: Esiste un'omib compo tot. ord. e  
D-completo e un' d' i'omorfismi uguali;

Dato un campo  $\mathbb{K}$  t.t. ord., o

$\emptyset$ -completo:

Axiome di Dedekind

$$(\mathbb{K}, +, \cdot, \leq) \stackrel{\text{def}}{\Leftrightarrow} \left\{ \begin{array}{l} \exists X, Y \neq \emptyset \\ X, Y \subseteq \mathbb{K} \\ X \subseteq Y \end{array} \right\} \text{SEPARATI}$$

Se hs 2 classi:

separate, esiste un  
elemento separatore.

$$\exists z \in \mathbb{K}: X \subseteq z \subseteq Y$$

Oppone:

$\mathbb{Q}$  non è  $\emptyset$ -completo.

$$(\mathbb{K}, +, \cdot, \leq) \text{ } \emptyset\text{-completo}$$



completo  $\neq$  Archimedeo

(1)  $\mathbb{K}$  è Archimedeo

(2)  $\mathbb{K}$  è completo alla Cauchy

$\mathbb{K}$  è archimedeo  $\Leftrightarrow \forall \frac{y}{x} \in \mathbb{K}^+ \exists n \in \mathbb{N}: ny > y$

Tradotto, se  $n$  non è limitato in  $\mathbb{K}$ .

mostra per ca. in  $\mathbb{R}$   $\lim_{n \rightarrow \infty} \frac{1}{n} = 0$



PROPRIETÀ  
DI ARCHIMEDE

Cauchy:

Sia  $(x_m)_m$  una successione di elementi in  $\mathbb{K}$

$f: \mathbb{N} \rightarrow \mathbb{K}$   
è detta d. Cauchy



$\forall \varepsilon > 0 \exists K \} \exists i \in \mathbb{N} : H_{m,m} \geq i \varepsilon \Rightarrow |x_m - x_{m'}| < \varepsilon$

Da un certo indice in poi  $x_m - x_{m'}$  è piccolo.

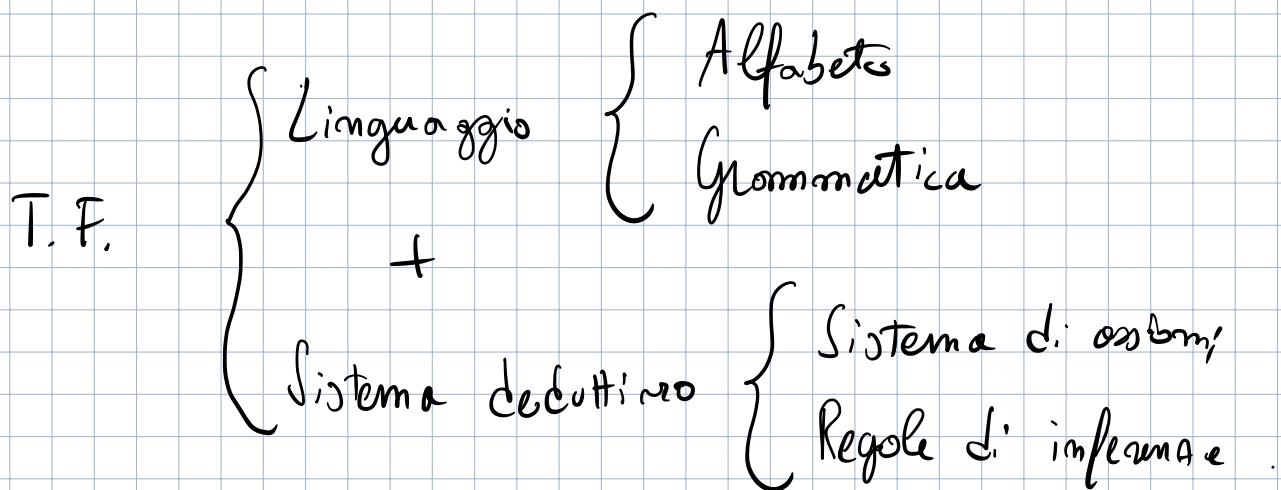
## LOGICA / LOGICHE

Secondo Russell esiste una sola logica, quella matematica, essendo l'unica formulabile.

"Teoria Formale" = Logica Matematica

Si possono costruire tante teorie formali.

Quando se ne crea una si dà:



Ogni teoria ha 2 livelli di lettura:

(1) Sintassi (grammaticalmente corretta o no)

(2) Semantica (controllo l'interpretazione)

Un' esempio d. teoria formale: LOGICA PROPOSITIONALE

Una estensione della logica proposizionale è la logica dei predicati, che esamina tutta la matematica costruita.

La sintassi è legata al simbolo  $\vdash$  (DIMOSTRAZIONE)

La semantica è legata al simbolo  $\models$  (SODDISFACIBILITÀ)

Teorema di completezza := (DIMOSTRABILE = SODDISFACIBILE)

Altro modo per descrivere teoria formale:

$$\mathcal{G} := (\Lambda, \Sigma, \Upsilon, \Pi)$$

- $\Lambda$  è contabile (numerabile) insieme di simboli detti alfabeto.
- $\Sigma$  è un sottoinsieme di espressioni, detto insieme delle formule ben formate o grammatica di  $\mathcal{G}$ .

Ese.  $\Lambda := \{\alpha, \beta, \heartsuit, \square, \$\}$  alfabeto

ESPRESSIONI  
EL LENGUAJE :  $\alpha\beta\heartsuit$      $\square\heartsuit\alpha$      $\heartsuit\heartsuit\heartsuit\alpha\beta$  (STRINGS)

La teoria del calcolo proposizionale  $L$

$$L := \{\Lambda_L, \Sigma_L, \Upsilon_L, \Pi_L\}$$

- Ponterei ( $\alpha$ )
- Variabile: affermazioni' non logiche sotto forma di simboli letterali
- Simboli logici:  $\neg$  (connessione unaria),  $\rightarrow$  (connessione binaria)

Ogni variabile proposizionale in una formula, detta formula atomica.

Se  $\rho$  e  $\psi$  sono formule atomiche, lo sono anche  $(\neg \rho)$ ,  $(\rho \rightarrow \psi)$

- $\Sigma$  assiomi: un'insieme finito o infinito di formule ben formate.

$$(A_L^1) (\rho \rightarrow (\psi \rightarrow \varphi))$$

$$(A_L^2) ((\varphi \rightarrow (\psi \rightarrow \zeta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \zeta)))$$

$$(A_L^3) (((\neg \varphi) \rightarrow (\neg \psi)) \rightarrow (((\neg \varphi) \rightarrow \varphi) \rightarrow \psi))$$

$$\forall \varphi, \psi, \zeta \in \Sigma_L$$

- $\overline{\Pi}$  la regola d' inferenza si riduce al modus ponens.

$$R_L := \{(\varphi, (\varphi \rightarrow \psi)) \mid \varphi, \psi \in \Sigma_L\} \subseteq (\Sigma_L \times \Sigma_L) \times \Sigma_L$$

Avevamo due simboli:

$$\boxed{\varphi} \quad \boxed{[\varphi \rightarrow \psi]}$$

grado e modo ponem do anche scrivere  $\psi$ .

$$(\varphi \wedge \psi) \text{ per } (\neg(\varphi (\varphi \rightarrow (\neg\psi))))$$

$$(\varphi \vee \psi) \text{ per } ((\neg\varphi) \rightarrow \psi)$$

$$(\varphi \leftrightarrow \psi) \text{ per } ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$$

Cosa vuol dire dimostrazione:

"La tua macchina da scrivere fa scrivere"

Una DIMOSTRAZIONE FORMALE è una successione finita di formule ben formate in cui l'ultima formula è  $\psi$  in cui ogni formula o è un'assunzione o è una formula ben formata che si ottiene dalle precedenti tramite modus ponens.

Esempio di formule ben formate:

$$\vdash_L (\beta \rightarrow \beta) \vee \beta \in \Sigma_L$$

$$\textcircled{1} (\beta \rightarrow ((\beta \rightarrow \beta) \rightarrow \beta)) \rightarrow (((\beta \rightarrow (\beta \rightarrow \beta)) \rightarrow (\beta \rightarrow \beta)))$$

$$\text{Assioma } (A_L^1) \quad \varrho = \beta, \psi = \beta, \zeta = \beta$$

$$\textcircled{2} (\beta \rightarrow ((\beta \rightarrow \beta) \rightarrow \beta)) \text{ Axioma } (A_L^1) \quad \varrho = \beta$$

$$\textcircled{3} (((\beta \rightarrow (\beta \rightarrow \beta)) \rightarrow (\beta \rightarrow \beta))) \quad (1+2+M^P)$$

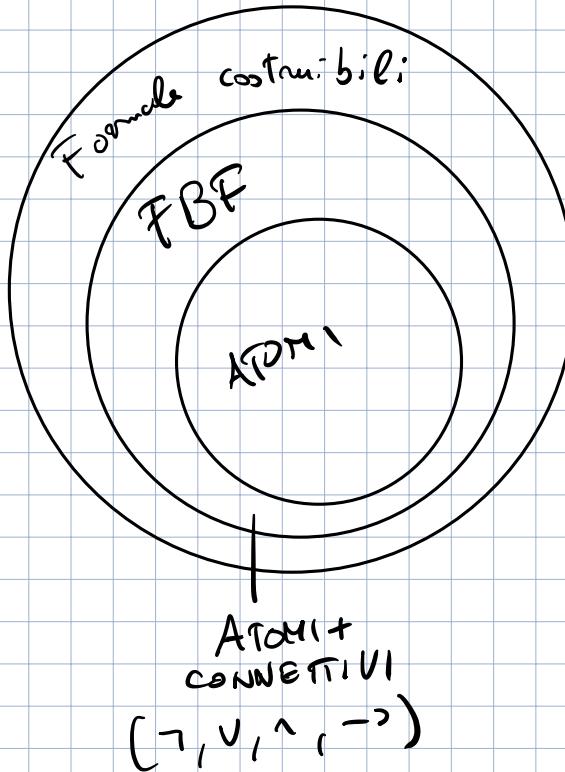
$$\textcircled{4} (\beta \rightarrow (\beta \rightarrow \beta)) \text{ Axioma } (A_L^1)$$

$$\textcircled{5} (\beta \rightarrow \beta)$$

Formule ben formate (FBF)

$$v : FBF \rightarrow \{0,1\}$$

VERO 1, FALSO 0



Dato che avere una funzione per ogni FBF  
sarebbe difficile lo costruire su tutte le formule  
atomiche e lo estendo alle FBF.

$$P \rightarrow Q = ((\neg P) \vee Q)$$

**Definizione:** Sia  $P$  una FBF e  $V$  una interpretazione:

Se  $v(P) = 1$ ,  $P$  è soddisfatta nell'interpretazione oppure chi  $V$  è un modello per  $P$ .

$$\boxed{\vdash v \models P}$$

Una formula ben formata è detta soddisfacibile se ha almeno un modello.  $\exists v : v(P) = 1 ?$

Quindi ci sono formule non dimostrabili e formule dimostrabili.

Esempio d.: formule non soddisfacibile =  $A \vee \neg A$

Le formule sempre false sono dette **contraddizioni**

Le formule sempre vere sono dette **tautologie**

$P$  è una tautologia se e solo se  $\neg P$  è una contraddizione.

Definizione:  $\Gamma$  è un'insieme di formule ben formate.  $\varphi$  è una formula ben formata.

Se tutte le formule di  $\Gamma$  sono soddisfacibili  $\Gamma$  è soddisfacibile.

$\Gamma \models \varphi$  se esiste un'interpretazione un'interpretazione che rende entrambi soddisfacibili.

$\vdash$  è conseguenze logica di  $\Gamma$ .

Proposizione:  $\Gamma \models \varphi$  solo se  $\Gamma \models (\neg \varphi)$  è insoddisfacibile

Proposizione: Se ha  $P \models Q$  solo se  $\models P \rightarrow Q$

Definizione: Due formule ben formate sono semanticamente equivalenti se e solo se hanno stesso valore.

L'EQUIVALENZA SEMANTICA è una relazione di equivalenza  
in  $\Gamma$ . ( $P \equiv Q$ )

La logica proposizionale è una teoria senza assiomi.  
(Non esiste il simbolo =)

$$\boxed{\phi \models P \Leftrightarrow F P}$$

Dire che  $\varphi \equiv \psi$  equivale a dire che  $(\varphi \models \psi) \vee (\psi \models \varphi)$

Teorema di deduzione semantica:

$$\{\varphi_1, \varphi_2\} \models \psi \Leftrightarrow \varphi \models (\varphi_1 \rightarrow \varphi_2)$$

Teorema di compattezza:  $\Gamma$  è soddisfacibile se e solo se  
è omogeneo ogni suo sottoinsieme finito.

Libro pag 128 (PER DIMOSTRAZIONE)

Il numero di connessioni costitutibili con  $n$  atomi  
è  $2^{(2^n)}$ .

## FORZE NORMALI

Un LETTERALE è una proposizione atomica. La sua negazione,

È detta FORMA NORMALE CONGIUNTIVA i' intersezioni finite  
 di unioni finite di letteral. (P<sup>c</sup>)  
 È detta FORMA NORMALE DISGIUNTIVA i' unione finite  
 di intersezioni finite di letteral. (P<sup>d</sup>)

$$\begin{aligned}
 P_i &= (A \vee B) \rightarrow C = \\
 &(\neg A \wedge \neg B) \vee C = \\
 &(\neg A \wedge \neg B) \vee C = \\
 &(\neg A \vee C) \wedge (\neg B \vee C) = \\
 &= P^c
 \end{aligned}$$

LOGICA  
PROPOSITIONALE

