25-02-2016

Ricevimento: martedì dopo le 16

La teoria degli insiemi è a fondamento della matematica: qualsiasi affermazione matematica può essere scritta nell'alfabeto

$\{\in, \to, =, \forall, \exists, \wedge, \vee, \neg, (), \text{variabili}\}$,

quindi anche senza numeri.

Un'altro aspetto della teoria degli insiemi è lo studio dell'infinito matematico: a partire da Cantor, l'infinito è diventato una cosa trattabile.

Def: un numero algebrico è radice di un polinomio a coeff. razionali.

Contrario di algebrico è trascendente.

Sorge una domanda che è ancora un problema aperto:

$X \subset \mathbb{R}$ infinito; è vero che $|X| = |\mathbb{N}|$ o $|X| = |\mathbb{R}|$?

Si è dimostrato che a ciò non si può rispondere con gli assiomi di Zermelo, che sono quelli su cui si basa la matem.

Cardinali: 0 1 2 ... $\aleph_0 = |\mathbb{N}|$ ... $\aleph_1$ diversi ... $\aleph_2$ diversi ...

Ordinali: $1^\circ, 2^\circ, 3^\circ$ ... ω ... $\omega+1$ $\omega+2$

$|\omega| = |\omega+1| = |\mathbb{N}|$

I cardinali rispondono alla domanda: "quanti sono?"

Gli ordinali a "quanti ce ne sono prima?"

Cos'è un insieme?

Frege (1800): ci sono le proprietà e le classi da esse def.

es: proprietà $P(x)$

classe (insieme) $\{x \mid P(x)\}$ assioma di astrazione

- Quindi dire $a \in \{x \mid P(x)\} \Leftrightarrow P(a)$ [è un assioma]
- Ogni proprietà sensata definisce una classe [altro assioma]
- Assioma di estensionalità: due classi sono uguali se hanno gli stessi elementi: $A = B \Leftrightarrow \forall x \ (x \in A \leftrightarrow x \in B)$

Però questo implica che non importa quante volte sia ripetuto un elemento, né in che ordine siano. Ad esempio,

$\{2, 2, 3, 5\} = \{3, 5, 2\}$

3 elementi.

La teoria degli insiem. di Frege entra in crisi a causa di Russell.

Paradosso di Russell:

$P(x) := (x \notin x)$

es: su $X = 3$ Vale $P(3)$ $(3 \notin 3)$ vera, 3 non è insieme

es: $\mathcal{P}$(l'insieme dei concetti) [l'insieme dei concetti è un concetto]

La classe di Russel è $R = \{x \mid x \notin x\}$.

Ma $R \in R$?

$R \in R \Leftrightarrow R \notin R$, Assurdo.

Poi arriva Cantor (1872):

Lui se ne frega del problema di Russel, perché dice che ai fini matematici R non è importante.

Domanda: quanti alberi (matematici) esistono?

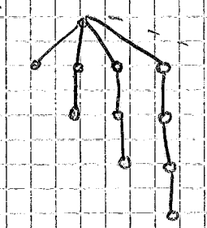
Dipende dalla definizione: ha senso identificarne 2 se sono isomorfi.

Def: albero ben fondato $\leftrightarrow$ non ci sono rami infiniti.

Un ramo è una successione $(x_n \mid n \in \mathbb{N})$ con x_{n+1} figlio di x_n

Es: non ben fondato: 

Es: ben fondato ma infinito:

- 2 livelli: 
- infiniti livelli:  Il figlio n-mo ha n discend.

Def: iper-albero: è ottenuto da una radice a cui si attaccano tutti gli infiniti alberi ben fondati.

oss: l'iper-albero è ben fondato. Chiamiamolo T.

Però, se T è ben fondato, esso stesso è uno dei suoi figli.  però così si crea un ramo infinito!

Quindi l'iper-albero non è né fondato né ben fondato.

oss: $\{x \mid P(x,y)\} \rightarrow$ y variabile libera, x variabile legata

Es: $\{x \in \mathbb{R} \mid x \geq y\} = [y, +\infty)$ dipende dal valore di y $\Rightarrow$ libera.

La domanda fondamentale, che Frege non considerava, è:

dove varia la x?

Zermelo lavora su questo.

Zermelo

Indebolisce l'assioma di Astrazione così:

(Data $P(x)$, dato un insieme A, posso formare l'insieme $B = \{x \in A \mid P(x)\}$.

Naturalmente, qui il problema è: da dove parto? Qual è la base? Ho bisogno di altri assiomi che "producano" gli A da cui partire.

- è l'Assioma di Comprensione: in realtà dovrei dire Schema di Assiomi di comprensione:

$\forall A, \exists B \left(B = \{x \in A \mid P(x)\}\right)$

$\forall c \left[c \in B \leftrightarrow (P(c) \wedge c \in A)\right]$

$\updownarrow$ def

$c \in \{x \in A \mid P(x)\}$

L'assioma di comprensione permette solo di creare sottoinsiemi, non insiemi più grandi di quelli già creati!

Zermelo propone:

- $\{x \in A \mid P(x)\}$ è un insieme $\forall P(x)$
- $\{x \mid P(x)\}$ è un insieme solo per certe P (tipo 9)
- Esiste $\{x \mid x \neq x\} = \emptyset$
- In realtà, $\{x \mid P(x)\}$ $\forall P(x)$ li chiamiamo classi; gli altri sono gli insiemi.

Per liberarci dai paradossi, facciamo una cosa tripartita:

$\begin{cases} \text{Proprietà} & P(x) \\ \text{Classi} & \{x \mid P(x)\} \\ \text{Insiemi} & \{x \in A \mid P(x)\} \end{cases}$

- $V = \{x \mid x = x\}$ classe universale (non è un insieme)
- $\emptyset = \{x \mid x \neq x\}$ classe vuota (è un insieme)

Le variabili x variano su insiemi, non su classi.

Si possono fare gli insiemi di insiemi: tutto si costruisce così, a partire dal vuoto; tutti gli insiemi saranno insiemi di insiemi.

$\emptyset$; $\{\emptyset\}$; $\{\emptyset, \{\emptyset\}\}$, ...

Ogni classe è una classe di insiemi;

Una classe è un insieme $\Leftrightarrow$ appartiene a un'altra classe.

Def: $A \subseteq B \Leftrightarrow \forall x \, (x \in A \rightarrow x \in B)$

Assiomi di Zermelo

Estensionalità: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A \Leftrightarrow \forall x\,(x \in A \leftrightarrow x \in B)$

$\Rightarrow$) logica

$\Leftarrow$) teoria degli insiemi

Coppia: $\forall a, b$, esiste $\{a,b\} = C$.

Più formalmente:

$\forall a,b\ \exists C\ [\forall u (u \in C \leftrightarrow u = a \vee u = b)]$

Per estensionalità, C è unico dati a e b.

Data l'unicità, possiamo definire le graffe: $C = \{a,b\}$

L'esistenza della coppia $\Rightarrow$ esistenza del singoletto:

$\{a\} := \{a,a\}$

Unione binaria: $\forall A, B$ esiste $A \cup B = \{x \mid x \in A \vee x \in B\}$

Di per sé è una classe, ma l'assioma dice che, se A e B sono insiemi, allora l'unione è un insieme. Formalmente:

$\forall A, B\ \exists C\ [\forall x (x \in C \Leftrightarrow x \in A \vee x \in B)] = A \cup B$

Insieme vuoto: $\exists a (\forall x (x \notin a))$; $a = \emptyset$.

Questi assiomi bastano a definire i numeri naturali.

29_02_2016

Continuiamo la lista di assiomi di Zermelo.

Unione: $\forall A$ [fam di insiemi] $\exists B (\forall x (x \in B \leftrightarrow \exists c \in A (x \in c)))$

In generale: $(\exists c \in A) P(c) \equiv \exists c (c \in A \wedge P(c))$ (abbreviaz.)

Analogamente, $(\forall c \in A) P(c) \equiv \forall c (c \in A \to P(c))$

Es] $A = \{a,b\}$; $\bigcup A = a \cup b$; $\bigcup \{a,b\} = a \cup b$ ($\{a,b\} = A$, B)

Quindi l'unione binaria è caso particolare di unione.

$B = \bigcup A$

Questi erano singoli assiomi; ora c'è uno schema di assiomi di comprensione:

data una proprietà $\varphi(x)$ (cioè una formula), c'è

(Assioma φ): $\forall A, \exists C (\forall u (u \in C \leftrightarrow u \in A \wedge \varphi(u)))$

$C = \{x \in A \mid \varphi(x)\}$

φ potrebbe contenere altre variabili oltre a x, che si comportano come parametri:

$\varphi(x, y)$, $y = (y_1, \dots, y_n)$

posso fare $\{x \in A \mid \varphi(x,y)\} = Q_y$

Es] $\{x \in \mathbb{R} \mid x \geq y\} = [y, +\infty)$

L'assioma di comprensione relativo a φ, scritto per bene, deve quantificare anche i parametri:

(Assioma φ): $\forall b, \forall A\ \exists C (\forall u (u \in C \leftrightarrow u \in A \wedge \varphi(u,b)))$.

Mancano, da essere elencati, i seguenti assiomi:

Infinito

Potenza

Scelta

Rimpiazzamento (schema)

Fondazione

Questi però li vediamo dopo: ora vediamo cosa si può fare con quelli già elencati.

Notazioni logiche: quali sono e come si usano.

$\underbrace{\vee \ \wedge \ \neg \ \to}_{\text{booleani}} \quad \underbrace{\forall \ \exists}_{\text{quantificatori}}$

Booleani: hanno le tavole di verità

φ	ψ	$(\varphi \wedge \psi)$	$(\varphi \vee \psi)$	$\neg\varphi$	$(\varphi \to \psi)$
0	0	0	0	1	1
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	1	0	1

Come dimostro $\varphi \to \varphi$?

Un modo è assumere φ (come ipotesi temporanea); dopo un po' di passaggi, arrivare a φ. Questo tipo di dimostrazione è detta secondaria; se però riesco ad arrivare a φ, $\varphi \to \varphi$ è non è più secondaria, cioè non dipende più dall'ipotesi aggiuntiva su φ; infatti, anche se φ fosse falsa, si avrebbe comunque $\varphi \to \varphi$

Quantificatori: non ha senso fare tavole di verità: ad esempio, per il $\forall$ bisognerebbe fare una tavola infinita.

Come si dimostra il $\forall$? Si prende un oggetto generico, si dividono i casi possibili, alla fine si mette $\forall$.

Generico vuol dire: un simbolo su cui non do informazioni, cioè su cui non ho fatto ipotesi. Allora le regole sono:

--- $P(a)$ per a generico $\to \forall a\, P(a)$

$P(a) \to \exists a\, P(a)$

Un procedimento corretto, passando per una dim secondaria, potrebbe essere: assumo $P(a)$ … ottengo $P(a)$ } dim secondaria

$\dfrac{P(a) \to P(a)}{\forall x (P(x) \to P(x))}$

Es| Dimostriamo che
$\exists x (V(x) \to \forall a (V(a)))$.
Ci sono due casi:

1) $\forall a V(a)$
$V(x) \to \forall a V(a)$ } tavole di verità
$\dfrac{}{\forall x (V(x) \to \forall a V(a))}$

2) $[\forall a V(a)]$ è falso $\Rightarrow$ $\exists a \neg V(a)$ è vera.
Allora posso scegliere a, cioè dire
Sia b t.c. $\neg V(b)$
$V(b) \to \forall x V(x)$ } tavole: qualsiasi cosa implica vero.
$\dfrac{}{\forall x (V(x) \to \forall a V(a))}$

■

Lo scopo è di ricostruire tutta la matematica in ZF, ad esempio $\mathbb{N}$, $\mathbb{R}$, funzioni...
Per costruire $\mathbb{N}$ si può fare così:

Von Neumann
$0 = \emptyset$;
$1 = \{0\}$;
$2 = \{0, 1\}$;
$3 = \{0, 1, 2\}$ - - -

Alternativa:
$0 = \emptyset$
$1 = \{0\}$
$2 = \{1\}$
$3 = \{2\}$ - - -

Es| secondo Von Neumann, $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$

■

Vorremmo ora definire la proprietà $P(n) \equiv$ (n è numero naturale).
Perché esiste il numero 3?

$3 = \{0, 1\} \cup \{2\} = \bigcup \{\{0, 1\}, \{2\}\}$
coppia di singl. — unione binaria — unione unaria

In generale, per fare il successore di x
$S(x) = x \cup \{x\}$
x^{+1}
In questo modo ho:
$0 = \emptyset$;
$1 = S(0)$;
$2 = SS(0)$... etc ma non ho ancora definito un numero naturale.
- bisogna dire cosa vuol dire "etc"
- precisazioni sulle proprietà.

"A parole" si possono definire numeri naturali giganti: ad es, si può def. il 'super-esponenziale' $2_n^x = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\}n$ volte,
cioè $\begin{cases} 2_0^x = x \\ 2_{n+1}^x = 2^{(2_n^x)} \end{cases}$

Oppure Ackermann (da definire).

Ora vediamo un paradosso semantico:
Sia n il minimo numero naturale non definibile con meno di 1000 lettere. (Quelli definibili con meno di 1000 sono un numero finito $\Rightarrow$ lo chiamo n_0: lui non è definibile con meno di 1000 lettere, ma l'ho appena definito! $n_0 = \min \{x \in \mathbb{N} \mid \underbrace{x \text{ non è def con} \leq 1000 \text{ lett}}_{P(x)}\}$

Ammessa l'esistenza di $\mathbb{N}$, sembrerebbe corretto, peccato che $P(x)$ non sia una "buona proprietà".
Quali sono le proprietà che vanno bene?

Proprietà = formula di ZF
Le formule sono:
$x \in x$, $x = x$, "oppure"
$x \in y$, $x = y$,
$F ::= (F \wedge F) \mid (F \vee F) \mid \neg F \mid (F \to F) \mid \forall x F \mid \exists x F$
Le formule quindi sono generate da queste regole, cioè sono il più piccolo insieme che gode delle regole sopra

Es| Per definire UA abbiamo usato una formula lecita:
$UA = \{x \mid \exists c (c \in A \wedge x \in C)\}$

Questa def induttiva si fa nella metateoria.
Come definiamo allora la proprietà $Nat(x)$?
Dobbiamo scrivere con una formula ammissibile
$Nat(x) \equiv$ (x si ottiene da $\emptyset$ usando S)
- $S(n) = n \cup \{n\}$ si riesce a scrivere in modo ammissibile.
- Un modo di riscrivere la proprietà è
$\equiv$ (x appartiene al più piccolo insieme che contiene $\emptyset$ ed è chiuso per S). Definendo $X \cap Y = \{a \mid a \in X \wedge a \in Y\}$,

si può definire l'intersezione di famiglie di insiemi

Def $\bigcap F = \bigcap_{Y \in F} Y = \{a \mid (\forall Y \in F)\, a \in Y\}$. Ma chi è $\bigcap \emptyset$?

$\bigcap \emptyset = \{a \mid \forall Y (\underbrace{Y \in \emptyset}_{\text{falsa}} \to a \in Y)\} = \{a \mid a = a\}$ non esiste.
(vera)

Allora prendo $F \neq \emptyset$. $\exists B (B \in F)$. Scelgo un tale B.

$\bigcap F = \bigcap_{Y \in F} Y = \{a \in B \mid (\forall Y \in F)(a \in Y)\}$.

Def: un insieme B è induttivo se $\emptyset \in B \wedge (\forall n \in B)(S(n) \in B)$

Allora definiamo
$Nat(x) \equiv x \in \bigcap_{B \text{ induttivo}} B$; sciogliendo,
$Nat(x) \equiv \forall B (B \text{ induttivo} \to x \in B)$
Con questa definizione, però, c'è un problema:
se non esistessero insiemi induttivi, ogni x sarebbe un Nat.
Si ovvia a questo problema con
Assioma dell'infinito: $\exists B (B \text{ induttivo})$.
Quindi la famiglia degli insiemi induttivi è non vuota.

MANCA LEZIONE DEL 1-3-2016

03-03-2016

OSS: $\omega = \{x \mid Nat(x)\}$ sembrerebbe una classe ma è un insieme:
infatti basta scegliere a caso un B induttivo e scrivere
$\omega = \{x \in B \mid Nat(x)\}$ ☒

Induzione:
$\varphi(x)$ formula;
1) $\varphi(0)$ Base
2) $\forall x (\varphi(x) \to \varphi(Sx))$ Passo induttivo
(1) $\wedge$ (2) $\to$ (3): $\forall x \in \omega \;\; \varphi(x)$

Dim: sia $C = \{x \in \omega \mid \varphi(x)\}$
Siccome per ipotesi vale (1) e (2), C è induttivo $\Rightarrow \omega \subseteq C$ [perché ω è il più piccolo insieme induttivo]; ma $C \subseteq \omega$
$\Rightarrow \omega = C$, cioè $(\forall x \in \omega)\varphi(x)$

Def: Coppia di Kuratowsk.
$\langle x, y \rangle = \{\{x\}, \{x, y\}\}$
$A \times B = \{\langle a, b \rangle \mid a \in A, b \in B\}$; sembra una classe, ma è un insieme perché $\langle a, b \rangle \in \mathcal{P}\mathcal{P}(A \cup B)$

Def $|X| = |Y|$ se $\exists f: X \to Y$ biunivoca.
Questa è la def di Frege, che però ha un difetto: in realtà non ho definito $|X|$ di per sé.
Per il momento, quindi, scrivere $|X| = |Y|$ è un abuso di notazione; si dovrebbe scrivere $|X| = \{Y \mid Y \sim X\}$ con $X \sim Y$ se $\exists f (f: X \to Y$ biunivoca). Peccato che Y non è limitato, quindi questo non è un insieme, tutt'al più una classe (in G-B). Persino
$|\{a\}| = \{\{b\} \mid b\}$ è una classe propria, cioè 1 è una classe propria!
(↑ Frege)
Sarebbe meglio definire, con VN, $|\{a\}| = 1 = \{0\} \in \omega$.
Questa va bene per gli insiemi finiti; bisogna estendere.
Per il momento, comunque, ci interessa solo confrontare cardinalità, quindi possiamo tenerci Frege.

Ci interessa, comunque, capire cosa vuol dire
$|X| \leq |Y| \leftrightarrow \exists f (f: X \to Y)$ iniettiva.

Def: $|X| < |Y| \leftrightarrow |X| \leq |Y| \wedge |X| \neq |Y|$

Teo $|\omega| < |\mathcal{P}(\omega)|$ è il teorema di Cantor
($|\mathcal{P}(\omega)| = 2^{|\omega|}$)

Dim
1) $|\omega| \leq |\mathcal{P}(\omega)|$, cioè c'è una funzione iniettiva:
certo, per esempio c'è $f: \omega \to \mathcal{P}(\omega)$
$n \mapsto \{n\}$

2) Sia $f: \omega \to \mathcal{P}(\omega)$. Mostro che non è surgettiva.
Dobbiamo trovare un insieme non nell'immagine, pur non conoscendo f. Un insieme del genere è

$D \subseteq \omega$, $D \notin \mathrm{Im}(f)$, $D \neq f(n)\ \forall n$, $D \in \mathcal{P}(\omega)$

$D = \{n \in \omega \mid n \notin f(n)\}$ → costruito da insiemi in $\mathcal{P}(\omega)$
→ gli n che vengono mandati da f in un insieme che non contiene n. Va bene anche se $= \emptyset$

Dico $D \notin \mathrm{Im}(f)$. Infatti, se fosse $D = f(n)$, potrei chiedermi: $n \in D$?

$n \in D \leftrightarrow n \notin f(n)$ ↯ ($f(n) = D$)

Quindi abbiamo dimostrato che esistono infiniti di cardinalità diverse. Vedremo che $|\mathcal{P}(\omega)| = \mathbb{R}$.

Ora vogliamo definire $\mathbb{Z}$.

Lo facciamo tramite una relazione di equivalenza sulle coppie di Kuratowski. Preso

$\mathbb{N} \times \mathbb{N}$, $E \subseteq (\mathbb{N} \times \mathbb{N})^2$ (Data una relazione $R \subseteq A \times B$, $aRb \leftrightarrow \langle a,b \rangle \in R$)

$\langle x,y \rangle E \langle a,b \rangle$

$x + b = y + a$

$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / E = \{[\langle x,y \rangle]_E \mid x,y \in \mathbb{N}\}$

a questo punto, si ha per esempio

$-3 = [\langle 2,5 \rangle] = [\langle 0,6 \rangle]$

Fino a qui, però, abbiamo diversi problemi: uno di essi è

- $\mathbb{N} \not\subseteq \mathbb{Z}$. Però c'è di sicuro una funzione iniettiva

$\mathbb{N} \to \mathbb{Z}$, $n \in \omega \mapsto n^{\mathbb{Z}} = [\langle n,0 \rangle]$

Quindi in effetti $\mathbb{Z}$ non contiene $\mathbb{N}$, ma contiene una sua copia isomorfa.

QUOZIENTI

Def $E \subseteq X \times X$ equivalenza se

$xEy \leftrightarrow \langle x,y \rangle \in E$

xEx

$xEy \leftrightarrow yEx$

$xEy \wedge xEz \to xEz$

Prop $xEy \leftrightarrow [x] = [y]$

$[x] = \{y \in X \mid yEx\}$

Dim Per esercizio.

Def $X/E = \{[x] \mid x \in X\}$. È un insieme perché $[x] \subseteq X \Rightarrow [x] \in \mathcal{P}(X)$ ⑪

⇒ lo posso limitare.

SOMME SU $\mathbb{N}$

Devo definire '+' su ω.

Ex Un modo sarebbe prendere $a,b \in \omega$;

1) Scegliere A, B disgiunti, $A \sim a$, $B \sim b$.
2) Scegliere $C \sim A \cup B \Rightarrow a+b = c$.

Va dimostrato che tutte queste scelte sono possibili.

(1) X, Y insiemi: $X \times \{0\}$, $X \times \{1\}$ sono disgiunti,
$\cong X$ $\cong Y$

(2) Dimostrare l'esistenza di C è quantomeno sbatti.

Def: elenchiamo intanto delle proprietà caratterizzanti del $+$

$$\circledast \begin{cases} x+0 = x \\ x + S(y) = S(x+y) \end{cases}$$

Sto definendo $x+n$ per induzione su n.

Però l'induzione, per il momento, era solo un modo per dimostrare qualcosa, non per definirla!

Oss Se esiste una funzione $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che verifica $\circledast$, allora è unica.

Questo si può dimostrare per induzione.

Notazione: $x+y = z$ è come dire $+(\langle x,y \rangle) = z$ che è come dire $\langle \langle x,y \rangle, z \rangle \in +$.

Voglio mostrare che $+, \tilde{+}$ verificano $\circledast \Rightarrow + = \tilde{+}$.

Fisso x. Per induzione su $n \in \omega$ mostro che $x+n = x \tilde{+} n$

- $P(0)$ vero: $x+0 = x$, $x \tilde{+} 0 = x$
- $P(n) \to P(Sn)$ ($P(n)$)

$x + Sn \overset{?}{=} x \tilde{+} Sn$

$S(x+n) \quad S(x \tilde{+} n)$

$x+n \overset{P(n)}{=} x \tilde{+} n$ ▨

Però dobbiamo prima dimostrare che esiste la funzione $+$!

Serve l'assioma dell'unione unaria.

Diciamo che f è "buona" se

$\exists A \subseteq \mathbb{N} \times \mathbb{N}$ t.c. $f : A \to \mathbb{N}$ e

f_1 dove è definita, verifica ⊛.
La funzione vista, definita sul vuoto, è buona.
In realtà mi serve qualcosa in più: prendiamo
$A = \mathbb{N}\times n$, $n = \{0,1,\dots,n-1\} \subseteq \mathbb{N}$.

[EX: $x \in \omega \to x \subseteq \omega$] (per induzione)

Con questo dominio ∃ una funzione buona a parte
$f_0 = \emptyset$?
f_1 : $f_1(x,0) = x$; $f_1 = \{\langle\langle x,0\rangle, x\rangle \mid x\in\omega\}$
f_2 : $f_2(x,0) = x$, $f_2(x,s0) = Sx$
f_3: $f_3(x,0) = x$, $f_3(x,s0) = Sx$, $f_3(x, ss0) = S(S(x,s0))$
ho $f_3 \supseteq f_2 \supseteq f_1 \supseteq f_0$
Quindi un po' di funzioni buone esistono.

Def: $x+n = b \leftrightarrow \exists f(f \text{ buona} \wedge f(x,n) = b)$
Cioè il + è l'unione di tutte le funzioni buone:
$+ = \bigcup_{f \text{ buone}} f = \bigcup\{f \mid f \text{ buona}\}$ $\begin{cases} \text{dom}(f) \in \omega\times n \subseteq \omega\times\omega \\ \text{Im}(f) \subseteq \omega \\ f \subseteq (\omega\times\omega)\times\omega \end{cases} \Leftarrow f \in \mathcal{P}((\omega\times\omega)\times\omega)$

Devo fare un tot di verifiche:
- $\forall n$ $\underbrace{\exists f \text{ buona t.c. } \langle x,n\rangle \in \text{dom}(f)}_{P(n)}$ (induz su n)
- $P(0)$ vera [f_1]
- $P(n) \to P(sn)$: data f buona per n, creiamo f' buona per $s(n)$ è $f'(x, s(z)) = S(f(x,z))$, $f'(x,0) = x$ ...

* RECUPERO LEZIONE 1-3-16 * (13)

EX] Dim che $10 \neq 12$; [si parte da $0 \neq 1$, dato che $0 \in 1$ ma $0 \notin 0$
⇒ per estensionalità sono insiemi diversi]

Oss] $Nat(n) \overset{\text{def}}{\leftrightarrow} \forall B[(0\in B \wedge \forall x(x\in B \to S(x)\in B)) \to n \in B]$ (ZF)
$Nat(n) = \bigcap\{B \mid B \text{ induttivo}\}$ (GB)

Ci chiediamo: $\exists \omega(\omega = \{n \mid Nat(n)\})$? O meglio, è un insieme?
cioè $\exists \omega(\forall x(x\in\omega \leftrightarrow Nat(x)))$?

Per l'assioma dell'infinito, $\exists B(B \text{ induttivo})$ ⇒ scelgo B_0 induttivo
Per definizione, $Nat(n) \to n \in B_0$ ⇒ $\omega = \{x\in B_0 \mid Nat(x)\}$
è un insieme per assioma di comprensione.

EX] $\exists x(\neg Nat(x))$?
Sì: per esempio $x = \{\emptyset, \{\{\emptyset\}\}\}$, o anche ω.

⊛ Dimostriamo che $\{\{\emptyset\}\}$ non lo è: $\neg Nat(\{\{\emptyset\}\})$
Cerco insieme induttivo a cui $\{\{\emptyset\}\}$ non appartiene, per esempio ω ⇒ Verifico $\{\{\emptyset\}\} \notin \omega$.

Def: $X \subseteq Y \leftrightarrow \forall n(n\in X \to n \in Y)$. Abbiamo l'induzione:

Teo] $(\forall A \subseteq \omega)(0\in A \wedge \forall x(x\in A \to S(x)\in A)) \to (A = \omega)$

Dim] Dato $A \subseteq \omega$, suppongo $0\in A \wedge \forall x(x\in A \to S(x)\in A)$, cioè A è induttivo. Per definizione di ω, $\forall B$ induttivo $(\omega \subseteq B)$.
Quindi $\omega \subseteq A \Rightarrow A = \omega$ ▨

Lemma: $\forall x\in\omega(x = 0 \vee \exists y(x = S(y)))$

Dim
- Dato $x\in\omega$, voglio $x = 0 \vee \exists y(x = S(y))$
- Per assurdo, $x \neq 0 \wedge \neg\exists y(x = S(y))$ - perché x non sarebbe il succ. di nessuno
- Osservo che $\omega - \{x\}$ rimane induttivo: si dovrebbe quindi avere $x \in \omega \subseteq \omega - \{x\}$ ↯ perché $x \notin \omega - \{x\}$

⊛ Tornando all'esercizio:
1) $0 \notin \{\{\emptyset\}\}$
2) $\{\{\emptyset\},\emptyset\} \overset{?}{=} S(x) = x \cup \{x\}$
   $\cup$ $\cup$
   x x
Controllo $\{\{0\},0\} \overset{?}{=} S(\{0\}) = \{0\} \cup \{\{0\},0\}$ ∋ 0
Ma $0 \notin \{\{0\},0\}$, perché $0 \neq \{0\}$
$\cup$ $\cup$
0 0

Es Dare una def migliore di $Nat(x)$ in modo che si possa mostrare che $Nat(0), Nat(Sa)), Nat(SS(0))$ -- ma $\neg Nat(\{\{0\}\})$ senza assioma dell'infinito.

Cerchiamo ora un modello di Est, Coppia, Unione, Comprensione (ver. anche per gli insiemi ereditariamente finiti).
Cerchiamo cioè un insieme con relazione $(\mathbb{D}, \overset{*}{\in})$.
Un possibile modello è $(\mathbb{N}, \in)$ con $\in$ descritta dagli esponenti in notazione binaria, cioè $n = \sum_{i=1}^{k} a_i 2^i = 2^{a_1} + 2^{a_2} + \dots + 2^{a_k}$
$\Rightarrow a_1, \dots, a_k \in n$, con $0 = \emptyset$

Es $17 = 2^0 + 2^4 \Rightarrow 17 = \{0, 4\}$
$22 = 2^1 + 2^2 + 2^4 \Rightarrow 22 = \{1, 2, 4\}$

$V_\omega = (\mathbb{N}, \overset{*}{\in})$ così definito verifica EST e gli altri 3 assiomi
$\Rightarrow$ ne è modello.
$22 = \{4, 2, 1\}$ ma $4 = 2^2 = \{2\} = \{2^1\} = \{\{1\}\} = \{\{\{0\}\}\}$
$\Rightarrow 22 = \{\{\{\{0\}\}\}, \{\{0\}\}, \{0\}\}$

Costruiamo ora $f: \mathbb{N} \longrightarrow V_\omega$
$0 \longmapsto \emptyset$
$2^{a_1} + \dots + 2^{a_n} \longmapsto \{f a_1, \dots, f a_n\}$
?
Vediamo ora come si comporta questa trasformazione rispetto al successore: $V_\omega \xrightarrow{g} \mathbb{N}$
?
$\emptyset \longmapsto 0$ — Nat(0)
$S\emptyset = \{\emptyset\} \longmapsto 2^{g(\emptyset)} = 2^0 = 1$ ⇝ Nat(1)
$SS\emptyset = \{\emptyset, \{\emptyset\}\} \longmapsto 2^{g(\emptyset)} + 2^{g(\{\emptyset\})} = 2^0 + 2^1 = 3$ ⇝ Nat(2)
$\Rightarrow (\mathbb{N}, \in^*) \overset{\sim}{=}_g (V_\omega, \in)$ — Nat(3) ?
$Sx = x \cup \dots$ ⇜

Invece $(\mathbb{N}, \in^*)$ non è modello per l'assioma dell'infinito.

Assioma potenza (o delle parti):
$\forall x \, \exists Y (Y = \mathcal{P}(x))$ con $Y = \mathcal{P}(x) = \{A \mid A \subseteq x\} =$
$= \forall A (A \in Y \longleftrightarrow A \subseteq x)$

Def: Una coppia ordinata, o di Kuratowski, è
$\langle x, y \rangle := \{\{x\}, \{x, y\}\}$

Es $\langle 3, 4 \rangle = \{\{3\}, \{3, 4\}\} \not\ni \{4\}$
$\langle 4, 3 \rangle = \{\{4\}, \{3, 4\}\} \ni \{4\}$

Ex Mostrare che $\langle x, y \rangle = \langle a, b \rangle \longleftrightarrow x = a \wedge y = b$

Def $A \times B = \{\langle a, b \rangle \mid a \in A \wedge b \in B\} = \{x \mid (\exists a \in A)(\exists b \in B)(x = \langle a, b \rangle)\} =$
$= \{x \in \mathcal{P}\mathcal{P}(A \cup B) \mid [(\exists a \in A)(\exists B \in B)](x = \langle a, b \rangle)\}$

Mostriamo $x \in \mathcal{P}\mathcal{P}(A \cup B)$:
$a \in A \Rightarrow \{a\} \subseteq A$ cioè $\{a\} \in \mathcal{P}(A)$ e dato che $A \subset A \cup B$, $\{a\} \in \mathcal{P}(A \cup B)$
$a \in A \cup B$?
$b \in A \cup B$ $\} \{a, b\} \subseteq A \cup B$ cioè $\{a, b\} \in \mathcal{P}(A \cup B)$
$\Rightarrow \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$ cioè $\langle a, b \rangle = \{\{a\}, \{a, b\}\} \in \mathcal{P}\mathcal{P}(A \cup B)$

Def: Una relazione binaria tra A e B è una $R \subseteq A \times B$.
Una funzione, $f: A \longrightarrow B$, è tale $\Leftrightarrow$
1) $f \subseteq A \times B$ ← Notazione: $\langle a, b \rangle \in f \longleftrightarrow f(a) = b$
2) $\langle a, b \rangle \in f \wedge \langle a, c \rangle \in f \Rightarrow b = c$
3) $\forall a \in A \; \exists b \in B : \langle a, b \rangle \in f$

Def: Due insiemi hanno la stessa cardinalità, $|X| = |Y| \longleftrightarrow$
$\exists f: X \longrightarrow Y$ biunivoca.

7.03.2016

Def $\varphi(x)$ formula $\Leftrightarrow \{x \mid \varphi(x)\}$ classe.
$\{x \mid \varphi(x)\} \subset \{x \mid \psi(x)\} \Leftrightarrow \forall x (\varphi(x) \longrightarrow \psi(x))$

$a \in \{x \mid \varphi(x)\} \Leftrightarrow \varphi(a)$
$\exists! y \; \varphi(x, y) \Leftrightarrow \exists y [\varphi(x, y) \wedge \forall z (\varphi(x, z) \longrightarrow z = y)]$

Def $\varphi(x, y)$ è una funzione classe se $\forall x \; \exists! y \; \varphi(x, y)$

Scrivo $\varphi(x) = y$ invece di $\varphi(x, y)$.
Osservo $\varphi(x) = y \wedge \varphi(x) = z \Rightarrow y = z$.

Def Se A è una classe e $(\forall x \in A) \exists! y \; \varphi(x, y)$ dico che φ è una funzione classe definita su A

Def $V = \{x \mid x = x\}$ è la classe universale.

La principale differenza tra insiemi e classi è che non si può quantificare sulle classi.

Def Dico che $\{x \mid \varphi(x)\}$ è un insieme $\Leftrightarrow$
$\exists a (\forall x \; x \in a \leftrightarrow \varphi(x))$
$\exists a (a = \{x \mid \varphi(x)\})$

ES:
- $\{x \mid x = a \vee x = b\}$ è un insieme per l'assioma della coppia;
- V non è un insieme. Infatti:
  se V è un insieme, allora lo è anche $R = \{x \in V \mid x \notin x\}$
  Allora otteniamo $R \in R \Leftrightarrow \underbrace{R \in V}_{\text{sempre vero}} \wedge R \notin R \Rightarrow$
  $R \in R \Leftrightarrow R \notin R$ ↯

ES:
- Una funzione classe è, ad esempio, $\varphi(x,y) \Leftrightarrow y = \{x\}$, cioè $\varphi(x) = \{x\}$
  Questa non è una funzione insieme, perché il suo dominio è V.
- $X \longmapsto \cup X$ è una funzione classe. $\varphi(x,y) \Leftrightarrow y = \cup x$
- $X \longmapsto \mathcal{P}(X)$: $\varphi(x,y) \Leftrightarrow y = \mathcal{P}(X)$

Schema di assioma di rimpiazzamento:
Se F è una funzione classe, allora $\{F(x) \mid x \in A\}$, con A insieme, è un insieme. ($= \mathrm{Im}(F|_A)$)

ES: $\{\{x\} \mid x \in A\}$ è un insieme.

La scrittura $B = \{F(x) \mid x \in A\}$ è, per definizione,
$\forall a (a \in B \Leftrightarrow \exists x \in A \; \underbrace{a = F(x)}_{F(x,a)})$

Rimpiazzamento alla ZF (senza usare le classi):
se $\forall x \; \exists! y \; F(x,y) \longrightarrow \forall A \; \exists B \; \forall a (a \in B \leftrightarrow \exists x \in A \; F(x,a))$

EX: Dimostriamo che esiste $A \times B$ senza usare l'assioma potenza.
$A \times B = \{\langle a,b \rangle \mid a \in A, b \in B\}$.
Fisso $b \in B$ e considero $A \times \{b\} = \{\langle a,b \rangle \mid a \in A\} = \{F_b(a) \mid a \in A\}$
definendo $F_b(a) = \langle a,b \rangle$ [$\varphi(b,x,y) \Leftrightarrow (y = \langle x,b \rangle)$]
$A \times B = \bigcup_{b \in B} A \times \{b\} = \bigcup \{\underbrace{A \times \{b\}}_{\text{insieme, per rimpiazzamento: } b \longmapsto A \times \{b\}} \mid b \in B\}$

Nota: funziona per qualunque definizione di $\langle x,y \rangle$
Abbiamo così definito le tre principali notazioni per gli insiemi che si usano:
- $\{a,b,c\} = \{a,b\} \cup \{c\} = \bigcup \{\{a,b\}, \{c\}\}$ [coppia + unione]
- $\{x \in A \mid \varphi(x)\}$ (comprensione)
- $\{F(x) \mid x \in B\}$ (rimpiazzamento)

OSS: F funzione classe, A insieme $\Rightarrow F|_A$ è una funzione. Infatti
$F|_A = \{\langle x,y \rangle \mid F(x,y) \wedge x \in A\}$ è un insieme = f.

DIM: $B = \mathrm{Im}(F|_A)$ è un insieme per rimpiazzamento:
$B = \{F(x) \mid x \in A\} = \{y \mid \exists x \in A \; F(x,y)\}$
$\langle x,y \rangle \in A \times B \Rightarrow f$ è un insieme. [Una funzione classe è un insieme $\Leftrightarrow$ il suo dominio è un insieme].

EX: Rimpiazzamento $\Rightarrow$ comprensione.

Ricorsione

Teo: Sia A una classe. Data una funzione classe,
$H: \omega \times A \to A$ [A, B classi: $A \times B = \{\langle x,y \rangle \mid x \in A \wedge y \in B\}$], $a \in A$
$\exists! f: \omega \to A$ definita per induzione, cioè $f(0) = a$, $f(n+1) = H(n, f(n))$

ES: $f(n) = n!$; $0! = 1$; $(n+1)! = \underbrace{(n+1)(n!)}_{H(n,n!)}$; $H(x,y) = (x+1)y$

OSS: Se le classi sono formule, come si può essere sicuri che non ci sono classi definite random, senza formule? In realtà, si può sempre scrivere $A = \{x \mid x \in A\}$. Infatti, le formule non servono a creare gli insiemi; gli insiemi esistono già, le formule servono solo a isolarne alcune proprietà.
Non tutte le sottoclassi appartengono a V: $A \subseteq V \begin{cases} A \in V \Rightarrow A \text{ ins.} \\ A \notin V \Rightarrow A \text{ non ins.} \end{cases}$

OSS: Il teorema di ricorsione funziona anche senza assioma dell'infinito: semplicemente, ω sarà una classe e non un insieme, e anche f sarà una funzione classe e non insieme.

OSS: Il teorema di ricorsione è un Meta-teorema: scrivo
$ZF \vdash \varphi$ per dire ZF dimostra φ:
$ZF \vdash$ i suoi assiomi: es. $\forall a \; \exists b \; b = \{a\}$
Nel caso della ricorsione il discorso è diverso: dice
per ogni H formula, esiste f t.c. $ZF \vdash (f(0) = a, f(n+1) = H(n, f(n)))$
è diverso da $ZF \vdash \forall H \exists f (f(0) = a, f(n+1) = H(n, f(n)))$

DIM del teo di ricorsione (⊛)
(Dobbiamo ancora definire $x \leq y$ per $x,y \in \omega$)
- L'unicità di f (se esiste) è facile: se $g: \omega \to A$ verifica ⊛ mostro $g = f$. Mostro $\forall n \in \omega$, $\underbrace{g(n) = f(n)}_{P(n)}$ per induzione.
  - $P(0)$ vera: $g(0) = f(0) = a$.

$P(n) \longrightarrow P(n+1)$ ovv $\quad g(n+1) = H(n, g(n)) = H(n, f(n)) = f(n+1)$

Per induzione su n, mostro che [esiste (unica)
$g: \{x \in \omega \mid x \le n\} \longrightarrow A$ t.c. $g(0) = a$, $g(i+1) = H(i, g(i))$
$\forall\, i \le n+1$] $= Q(n)$ (nome della proprietà)

- $Q(0)$ vera: $g = \{\langle 0, a\rangle\}$
- $Q(n) \longrightarrow Q(n+1)$: sia $p: \{x \in \omega \mid x \le n\} \longrightarrow A$ t.c. Ⓐ
  pongo $g(x) = p(x)$ per $x \le n$; $g(n+1) = H(n, p(n))$ $(= H(n, g(n)))$
  Ho così $Q(n+1)$.

Per ora abbiamo dimostrato che $\forall n\ \exists!\, g$ che verifica Ⓐ fino a n
Ora definisco $F: \omega \longrightarrow A$, $F(n) = g(n)$ dove g è l'unica funzione che verifica Ⓐ fino a n.
$F = \{\langle n, y\rangle \mid \underbrace{\exists\, g \text{ che verifica Ⓐ fino a } n,\ y = g(n)}_{\varphi(n,y)} \wedge n \in \omega\}$; $y = \varphi(n)$
$[\forall n \in \omega\ \exists!\, y\ \varphi(n, y)]$
F è una funzione classe, ma il dominio è un insieme $\Longrightarrow$ F insieme (per rimpiazzamento). Infatti applico il rimpiazzamento così:
la funzione classe a cui applicarlo è $n \longmapsto \langle n, \varphi(n)\rangle$ ∎

Ex: $f(0) = a$ $\quad f(n+1) = H_1(f(n), g(n))$
$g(0) = b$ $\quad g(n+1) = H_2(f(n), g(n))$
Dim che $\exists\, f, g$ del genere (inventando varianti di ricorsione)

Def di $+$: si può definire per ricorsione $\begin{cases} x + 0 = x \\ x + S(n) = S(x+n) \end{cases}$
Fisso x parametro; definisco $k \xmapsto{F} x + k$.

$F(0) = x$; $F(k+1) = S(F(k)) = H(k, F(k))$;
$H(x, y) = S(y)$
$F = F_x$; $x + n = F_x(n) = F(n)$
$F_x = \{\langle n, x+n\rangle \mid n \in \omega\}$; $n \longmapsto x+n$, $\forall x\ \exists!\, F_x$, $x \longmapsto F_x$
$x + n = y \iff F_x(n) = y$

Def di $\cdot$: $\begin{cases} x \cdot 0 = 0 \\ x \cdot S(y) = x \cdot y + x \end{cases}$

Def di exp: $\begin{cases} x^0 = 1 \\ x^{n+1} = x^n \cdot n \end{cases}$

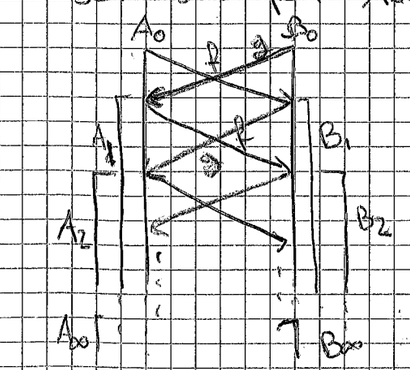
Ex: se A, B disgiunti, $A \sim n$, $B \sim k \Longrightarrow A \cup B \sim n+k$.
Si fa per induzione su k, fissato n.
Ex: stessi A e $B \Longrightarrow A \times B \sim n \cdot k$ [corrisp biunivoca]

8.3.2016

Teo di Cantor-Bernstein
$|A| \le |B| \ \wedge\ |B| \le |A| \Longrightarrow |A| = |B|$ (non è banale come sembra: il è il fatto dell'esistenza di funz. iniettive, che non è ovvio implichino l'esistenza di funz. biunivoche)

Es: $\mathbb{R} \supseteq [-1, 1]$;
$[-1, 1] \subseteq (-2, 2) \xrightarrow[\text{inv di H}]{x \mapsto \frac{x}{2}} (-1, 1) \subseteq [-1, 1]$
$\Longrightarrow$
$|[-1, 1]| \le |(-2, 2)| \le |[-1, 1]| \Longrightarrow |[-1, 1]| = |(-2, 2)|$ ma non è facile trovare una funzione biunivoca!
Proviamo a trovarne una tra $[-1, 1]$ e $[0, 1)$.
$[0, 1] \longrightarrow [0, 1)$: $1 \longmapsto \frac{1}{2}$, $\frac{1}{2} \longmapsto \frac{1}{3}$, $\dots$, $\frac{1}{n} \longmapsto \frac{1}{n+1}$, (gli altri vanno in se stessi)

Dim di Cantor
Per hp abbiamo $f: A \longrightarrow B$, $g: B \longrightarrow A$ iniettive.
Definiamo $A_0 = A$, $B_0 = B$; facciamo induzione su (A_n, B_n)
$A_{n+1} = g(B_n)$, $B_{n+1} = f(A_n)$
($\mathrm{Im}(g) \mid_{B_n}$) [ex: verificare che è una corretta appl di ricors. con H da coppie in coppie].
$A_n = \tilde{A}(n)$ sono funzioni; sto definendo per induz. $n \longmapsto (A_n, B_n)$.
Definisco poi $A_\infty = \bigcap_{n \in \omega} A_n$, $B_\infty = \bigcap_{n \in \omega} B_n$



Si ha che $B_0 \supset B_1 \xrightarrow{g}_{\sim} A_1 \supset A_2$;
$A_0 \supset A_1 \xrightarrow{f}_{\sim} B_1 \supset B_2$;
In generale si ha $A_{2n} \supset A_{2n+1} \xrightarrow{f}_{\sim} B_{2n+1} \supset B_{2n+2}$;
$A_{2n+1} \supset A_{2n+2} \xrightarrow{g}_{\sim} B_{2n} \supset B_{2n+1}$
Verificare, per dur, che queste sono corrisp biunivoche.

$\bigcup_{n\in\omega}(A_n \setminus A_{n+1}) \sim \bigcup_{n\in\omega}(B_n \setminus B_{n+1})$

$A = A_\infty \cup \bigcup_n (A_n \setminus A_{n+1}) = \left(\bigcap_{n\in\omega} A_n\right) \cup \bigcup_n (A_n \setminus A_{n+1})$

$A_0 \ni x \notin \bigcap_n A_n$; $\exists n.\ x \notin A_n$, prendo il minimo $x \notin A_n$

$x \in A_{n-1} \setminus A_n$

Dobbiamo sistemare $A_\infty \underset{g}{\overset{f}{\rightleftarrows}} B_\infty$. Infatti, voglio far vedere che $x \in A_\infty \Rightarrow f(x) \in B_\infty$.

Se no, $\exists n$ t.c. $f(x) \notin B_n \Rightarrow x \notin A_{n-1}$ ↯

Finire per ex (ma c'è tutto sulle dispense).

Teo (difficile): $\forall A, B$, $|A| \le |B| \ \vee\ |B| \le |A|$

Serve l'assioma della scelta.

Assioma della scelta (forma 1):

$R \subset X \times Y$;

$(\forall x \in X)(\exists y \in Y)(\langle x, y\rangle \in R)$

$\Downarrow$ $R(x,y)$

$\exists f (f: X \to Y \ \wedge\ (\forall x \in X) R(x, f(x)))$

Def: Una famiglia $(X_i \mid i \in I)$ è la funzione $I \longmapsto X_i$

$X : I \to V$, $X(i) = X_i$

Assioma della scelta (forma 2):

Data una famiglia $(X_i \mid i \in I)$ con $X_i \neq \emptyset$ $\forall i \in I$

$\Downarrow$

$\exists f: I \to \bigcup_{i\in I} X_i$ t.c. $f(i) \in X_i$ $\forall i$

Assioma della scelta (forma 3):

Dato F insieme di insiemi non vuoti $\Rightarrow$

$\exists g$ $(\forall X \in F)(g(F) \in X)$

$g : F \to \bigcup F$

Assioma della scelta (forma 4):

Data una famiglia $(X_i \mid i \in I)$, si può definire

$\prod_{i\in I} X_i = \{f : I \to V \mid \forall i \in I,\ f(i) \in X_i\}$

cioè la i-upla f è $(f(i) \mid i \in I) = (f_i \mid i \in I)$, $f_i \in X_i$

$X_i \neq \emptyset$ $\forall i \in I$ $\Rightarrow$ $\prod_{i\in I} X_i \neq \emptyset$

Oss f è una funzione $\Leftrightarrow$ $\forall a \in f$ $\exists x, y$, $a = \langle x, y\rangle$ e $\langle x, y\rangle\ A\ \langle x, z\rangle \in f \Rightarrow y = z$.

Allora $\mathrm{dom}(f) = \{x \in \bigcup\bigcup f \mid \exists y\ \langle x, y\rangle \in f\}$ è un insieme perché

$\mathrm{Im}(f) = \{y \in \bigcup\bigcup f \mid \exists x\ \langle x, y\rangle \in f\}$

Teniamo a mente che $x \in \{x\} \in \langle x, y\rangle \in f$ $\quad [a \in b \in c \Rightarrow a \in \bigcup c]$

$x \in \{x\} \in \bigcup f$

$x \in \bigcup\bigcup f$

Oss: $\emptyset \neq X_i \subseteq \omega$, $(X_i \mid i \in I)$

Voglio $f : f(i) \in X_i$; non serve l'assioma della scelta, basta definire $f(i) = \min(X_i)$.

Oss: Se $X_i \subseteq \mathbb{R}$? serve per forza l'assioma della scelta.

Ora, dati A, B e considerando sempre $|A|$ alla Frege, vorrei definire

1) $|A| + |B| = |C|$
2) $|A| \cdot |B| = |C|$
3) $|A|^{|B|} = |C|$

(1) $C \sim A \times \{0\} \cup B \times \{1\}$; $A \times \{0\} \sim A$, $B \times \{1\} \sim B$

Mostrare per ex. che è ben definita, cioè

$A \sim A'$, $B \sim B' \Rightarrow |A| + |B| \sim |A'| \sim |B'|$

(2) $C \sim A \times B$, $|A \times B| = |A|\,|B|$

(3) $|A|^{|B|} = |\{f \mid f : B \to A\}|$

Es Chiamiamo $1 = |\{a\}|$. Quant'è $|\omega| + 1$? È $|\omega|$.

$|\omega| = \aleph_0$.

$|\omega| + |\{a\}|$; trovo la corrisp biunivoca $\omega \cup \{a\} \to \omega$

$a \notin \omega$ $\qquad a \mapsto 0$; $n \mapsto n+1$

Es $\aleph_0 \cdot \aleph_0 = \aleph_0$

$|\omega \times \omega|$

0_2	1_2	2_2	3_2	…
0_1	1_1	2_1	3_1	…
0_0	1_0	2_0	3_0	…
ω				

Un modo per trovare la funz biunivoca $\omega \times \omega \to \omega$ è

$(n, k) \longmapsto 2^n(2k+1) - 1$

Ogni numero naturale si lascia esprimere in modo unico come potenza di 2 per un numero dispari; il -1 serve per scalare

n 0. Es, $(3,2): 2^3(2\cdot 2+1)-1 = 39$

Es $|\mathcal{P}(\omega)| = 2^{|\omega|} = |\{f \mid f: \omega \to 2\}|$, $2 = \{0,1\}$

Devo trovare corrisp biunivoca $\mathcal{P}(\omega) \sim \{f \mid f: \omega \to 2\}$

$A \mapsto f_A$, $A \subseteq \omega$;

$f_A(n) = \begin{cases} 0 & n \notin A \\ 1 & n \in A \end{cases}$; $g: \omega \to 2$, $A_g = \{n \mid g(n) = 1\}$

Lo stesso discorso non vale solo per ω, ma $\forall X$

$|\mathcal{P}(X)| = 2^{|X|}$

EX 1) $|A|(|B|+|C|) = |A|\cdot|B| + |A|\cdot|C|$

2) $|A|^{|B|+|C|} \overset{?}{=} |A|^{|B|}\cdot|A|^{|C|}$

3) $|A|^{(|B|\cdot|C|)} = (|A|^{|B|})^{|C|}$

4) $(|A|\cdot|B|)^{|C|} = |A|^{|C|}\cdot|B|^{|C|}$

sol(1): $A\times(B\times\{0\} \cup C\times\{1\}) \sim (A\times B)\times\{0\} \cup (A\times C)\times\{1\}$

$\langle a, \langle b, 0\rangle\rangle \longmapsto \langle\langle a,b\rangle, 0\rangle$

$\langle a, \langle c, 1\rangle\rangle \longmapsto \langle\langle a,c\rangle, 1\rangle$

Verificare che è biunivoca.

10.03.2016

sol(3)

$|\{f \mid f: C \to \{g \mid g: B \to A\}\}| \overset{?}{=}$

$= |\{h \mid h: B\times C \to A\}|$

L'idea è che una funz di due argom può essere vista come una di un solo arg. in questo modo:

$h(b,c) = f(c)(b)$, $f(c) = g$;

$B\times C \to A$
$\cong$
$B \to (C \to A)$

Analogia: $B \wedge C \to A$
$\equiv$
$B \to (C \to A)$

$h \mapsto f$

$f(c): B \to A$

$f(c)(b) = h(c,b)$

Le funz binarie possono essere viste come funz. unarie che vanno in funzioni unarie.

sol(2) $|\{f \mid f: B\times\{0\} \cup C\times\{1\} \to A\}| \overset{?}{=}$

$\overset{?}{=} |\{f_1 \mid f_1: B \to A\} \times \{f_2 \mid f_2: C \to A\}|$

devo trovare il modo di mandare biuniv. $f \longmapsto \langle f_1, f_2\rangle$

$f_1(b) = f(\langle b, 0\rangle)$; $f_2(c) = f(\langle c, 1\rangle)$ E viceversa.

EX Mostriamo che $\aleph_0 + \aleph_0 = \aleph_0$, quindi

$|\mathbb{N}| + |\mathbb{N}| = |\mathbb{N}|$; $\mathbb{N}\times\{0\} \cup \mathbb{N}\times\{1\} \sim \mathbb{N}$

$\langle n, 0\rangle \longmapsto 2n$

$\langle n, 1\rangle \longmapsto 2n+1$

Def X è numerabile se $|X| = |\mathbb{N}| = \aleph_0$

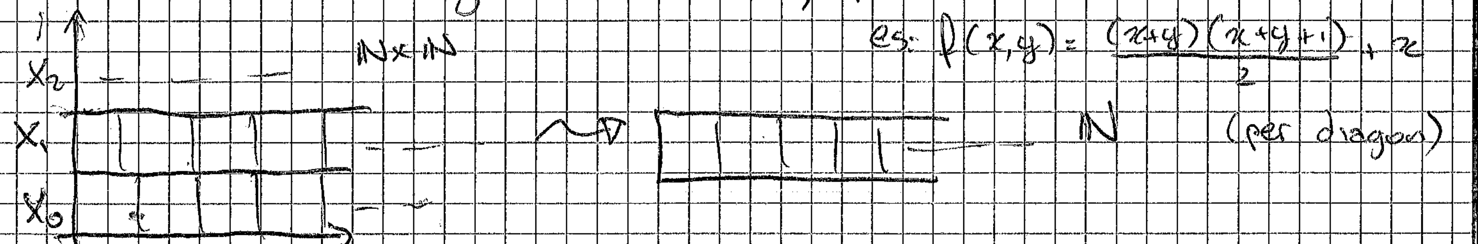
EX: Unione numerabile di insiemi numerabili è numerabile?

$X = \dot{\bigcup}_{n\in\mathbb{N}} X_n$ (disgiunta), $|X_n| = |\mathbb{N}|$; è numerabile, ma serve assioma della scelta.

$F: \omega \to V$, $X_n = F(n)$ [i sottoindici sono funzioni]

L'idea è: sistemo gli X_n in $\mathbb{N}\times\mathbb{N}$, poi vado in $\mathbb{N}$.

es: $f(x,y) = \frac{(x+y)(x+y+1)}{2} + x$



$\forall n \ \exists g_n (g_n: \mathbb{N} \to X_n$ biunivoca) ma non la conosco!

AC [assioma della scelta] $n \overset{G}{\longmapsto} g_n$

$\exists G: \omega \to V$, $G(n): \omega \to X_n \ \forall n$ ($G(n) = g_n$)

Ora che so che $\exists G$, posso dire (pura logica) Sia G t.c.

$\forall n$, $G(n): \omega \to X_n$, $H: \dot{\bigcup}_n X_n \to \mathbb{N}\times\mathbb{N}$

$x \in X_n \longmapsto \langle G^{-1}(x), n\rangle$

$x \in \dot{\bigcup}_n X_n \Rightarrow \exists! n \ x \in X_n$; Ho mostrato $|\dot{\bigcup}_n X_n| = |\mathbb{N}\times\mathbb{N}|$

e so che $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$.

Def $\mathbb{Q} = \mathbb{Z}\times(\mathbb{N}\setminus\{0\})/_E$; $q \in \mathbb{Q}$ $q = \langle a,b\rangle/_E$

$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb \Rightarrow \langle a,b\rangle E \langle c,d\rangle \Leftrightarrow a\cdot d = c\cdot b$

Def $(\mathbb{Z}, \cdot)$: $\langle a,b\rangle/_E \cdot \langle c,d\rangle/_E = \langle ac+bd, ad-bc\rangle/_E$ ($\langle a,b\rangle$ ≅ $a-b$)

$(a-b)\cdot(c-d) = ac - ad - bc + bd$

Devo verificare la buona definizione

Ex Definire $(\mathbb{Q}, +)$ e $(\mathbb{Q}, \cdot)$

Teo $|X| \geq |X/E|$

Dim $\exists f$ ($f: X \to X/E$ surgettiva) $a \mapsto a/E$
garantisce l'esistenza di una $g: X/E \to X$ iniettiva?
Sì, ma serve l'assioma della scelta:
Prop: $\exists f: X \to Y$ surg $\Rightarrow \exists g: Y \to X$ iniettiva
Dim: $\forall y \in Y \ \exists x \in X \quad fx = y$
$AC \Downarrow$
$\exists h: Y \to V \ \forall y \quad f(h(y)) = y$
$h(y_1) = h(y_2) \Rightarrow f(h(y_1)) = f(h(y_2)) \Rightarrow y_1 = y_2$

Coroll: $|\mathbb{Z}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| \leq |\mathbb{Z}|$
Dim $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}| \times |\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$
$|\mathbb{Q}| = |\mathbb{N}|$ (si può fare senza AC) ∎

Teo: $\forall n \ |X_n| \leq \aleph_0 \Rightarrow |\bigcup_{n \in \omega} X_n| \leq \aleph_0$
Dim: $\forall n \ \exists f_n: \mathbb{N} \to X_n$ surg. (ho bisogno di AC)
$F: \mathbb{N} \times \mathbb{N} \to \bigcup_{n \in \mathbb{N}} X_n$, $F(a,b) = f_a(b) \in X_a$ ∎

Ex $X \subseteq \mathbb{N} \Rightarrow |X| = |\mathbb{N}| \ \vee \ \exists n \in \omega \ (X \sim n)$

Oss: Se avessi già $\mathbb{R}$, potrei trovare una funzione $\mathbb{R} \to \mathcal{P}(\mathbb{Q})$
$r \longmapsto \{q \in \mathbb{Q} \mid q < r\} \subseteq \mathbb{Q} \quad [\in \mathcal{P}(\mathbb{Q})]$
Una funzione del genere è iniettiva perché tra due reali c'è un razionale: $r_1 < q < r_2$ (assioma Archimedeo)

Def: $X \in \mathcal{P}(\mathbb{Q})$ è un taglio di Dedekind se:
1) X non ha massimo
2) $a < b \in X \Rightarrow a \in X \quad a, b \in \mathbb{Q}$
3) $X \neq \emptyset, \ X \neq \mathbb{Q}$

Def Un $r \in \mathbb{R}$ è un taglio di Dedekind.

Def $x, y \in \mathbb{R}$; $x \leq y \leftrightarrow x \subseteq y$

Ex Definire $(\mathbb{R}, +)$ e $(\mathbb{R}, \cdot)$ sui tagli di Dedekind
- $(\mathbb{R}, +)$: $x +_{\mathbb{R}} y = \{a +_{\mathbb{Q}} b \mid a \in x \wedge b \in y\}$

Ex: Ogni insieme di reali limitato superiormente ha un sup. (F)
(assioma di continuità)
Idea: $F = \{x \mid x \in F\}$. $\sup(F) = \bigcup F$

Teo $|\mathbb{R}| = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})|$

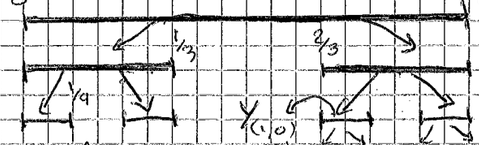
Oss $X \sim Y \Rightarrow \mathcal{P}(X) \sim \mathcal{P}(Y)$

Dim $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$ (assioma di Archimede)
Per l'altra dis si usa assioma di continuità.

14-03-2016

Mostriamo $|\mathbb{R}| \geq |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$.
$2^{\aleph_0} = \{f \mid f: \mathbb{N} \to \{0,1\}\}$ cioè le f sono successioni binarie; devo associare un $r \in \mathbb{R}$ ad ogni successione. Un modo per farlo è
$f \longmapsto \sum_{i=0}^{\infty} f(i) \frac{1}{10^i}$, cioè a $f = 0,1001110101\ldots \mapsto 0,01001110101\ldots$
e questa è chiaramente iniettiva? Definiamo (mostrarlo: serve principio del min).
$\sum_{i=0}^{\infty} f(i) \frac{1}{10^i} = \sup_{n \in \mathbb{N}} \sum_{i=0}^{n} f(i) \frac{1}{10^i}$ (serve la ricorsione).
$\exists$ il sup a patto di dim che tutti i termini siano limitati. ∎

Un'altra possibile dimostrazione dello stesso teorema si basa sull'insieme di Cantor:



$C = \bigcap_{n \in \mathbb{N}} X_n$
- è non vuoto: gli intervalli sono chiusi, gli estremi non si cancellano mai; l'insieme degli estremi è unione numerabile di roba finita, quindi è numerabile; ma C non contiene solo gli estremi.
L'insieme, visto come albero, ha $2^{\aleph_0}$ rami; a ogni ramo si associa una succ. binaria $f: \mathbb{N} \to 2$. Dato un qualsiasi $X_f \in C$, si ha $X_f \in \bigcap_n Y_{f|n}$ con $f|n = (f_0, f_1, \ldots, f_{n-1})$ e
$Y_{f|n+1}$ = il figlio sx o dx di $Y_{f|n}$ a seconda se $f(n) = 0$ o $f(n) = 1$.
Perché esiste X_f? Cioè, perché $\bigcap Y_{f|n} \neq \emptyset$? È una proprietà di $\mathbb{R}$: intersezione di una successione di intervalli chiusi e limitati (cioè ognuno contenuto in quelli precedenti) è non vuota (esercizio).
Detto questo, $f \longmapsto X_f$ è iniettiva $\Rightarrow |2^{\aleph_0}| \leq |C| \leq |\mathbb{R}|$
In questo modo non si usano somma e prodotto, ma un ordine totale completo (cioè ogni insieme limitato ha sup).

(∃ inf e sup)

Ex Sappiamo che $\mathbb{R}$ è completo e denso e non vuoto.
Deduciamo che non è numerabile, usando solo la completezza e l'ordine totale.

Dim L'idea è prendere un p.to a caso a_0 e un altro a caso b_0 t.c. $a_0 < b_0$; data la densità, prendo a_1, b_1 t.c. $a_0 < a_1 < b_1 < b_0$, poi a_2, b_2 ecc.
Allora posso fare $\bigcap_n [a_n, b_n] \neq \emptyset$ - Infatti, esiste $\sup_n a_n$, perché la succ degli a_n è limitata da b_0
$\inf_n b_n$. Scelgo x: $\sup a_n \leq x \leq \inf b_n$ e
$x \in \bigcap_n [a_n, b_n]$.

Per scegliere gli a_i si usa l'assioma della scelta. Formalizzare per ex.

Teo Se $|X| \geq \aleph_0 \Rightarrow |X| + \aleph_0 = |X|$.

Dim $f: \mathbb{N} \to X$ iniettiva. Sia $N = \mathrm{Im}(f) \subset X$, sia $A = X \setminus N$,
quindi $X = N \dot\cup A$, e $|X| = \underbrace{|N|}_{\aleph_0} + |A|$.

$|X| + \aleph_0 = |N| + |A| + \aleph_0 = \aleph_0 + |A| + \aleph_0 = \aleph_0 + \aleph_0 + A =$
$= \aleph_0 + A = |X|$.

Teo $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}| = \mathfrak{C}$ (continuo)

Dim Un modo per andare da $\mathbb{R} \to \mathbb{R} \times \mathbb{R}$ è mandare un allineam decimale in due, uno fatto con le cifre in posto pari, uno con quelle in posto dispari. Es
$0,2\,3\,4\,7\,9\,3\ldots \longmapsto (0,249\ldots, 0,373\ldots)$
Va aggiustato.

Un'altra possibile dim, che non va nemmeno aggiustata, è:
$|\mathbb{R}| = 2^{\aleph_0}$; $|\mathbb{R} \times \mathbb{R}| = 2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$

Ex Mostrare che $|\mathbb{N}^{\mathbb{N}}| \neq |\{0,1\}^{\mathbb{N}}|$

Dim Se p.a. ci fosse una corrispondenza biunivoca, l'idea è che si può modificare scambiando l'immagine della preimm del max di 101 con l'immagine del max di 100, in modo da mandare il max nel max; in questo modo, si guarda solo il resto dei due insiemi e si procede per induzione fino ad arrivare all'assurdo (formalizzare).

Ex: $\aleph_0$ è il più piccolo infinito (AC: teorema 20.14 delle disp).

Teo $|\{\text{irrazionali}\}| = \mathfrak{C}$
$\mathbb{R} \setminus \mathbb{Q}$, o meglio $\mathbb{R} \setminus \mathrm{Im}_f(\mathbb{Q})$, $f: \mathbb{Q} \hookrightarrow \mathbb{R}$ iniettiva

Dim $\mathbb{R} = \underbrace{(\mathbb{R} \setminus \mathbb{Q})}_{\text{infinito quanch} \geq \aleph_0} \dot\cup \underbrace{\mathbb{Q}}_{|\mathbb{Q}| = \aleph_0} \Rightarrow |(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}| + |\mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}|$

Teo $|\{\text{Algebrici}\}| < \mathfrak{C}$; A algebrico $\Leftrightarrow \exists\ p(x) \in \mathbb{Q}[x]$, $p(A) = 0$
$p(x) \neq 0$
$|\{\text{Algebrici}\}| = \aleph_0$

Dim I polinomi a coeff in $\mathbb{Q}$ sono una quantità numerabile. Infatti,
$\mathbb{Q}[x] = \bigcup_{n \in \mathbb{N}} \mathbb{Q}[x]^{\leq n}$ ← grado $\leq n$. Quanti sono $\mathbb{Q}[x]^{\leq n}$?
$|\mathbb{Q}^{\leq n}| = |\underbrace{\mathbb{Q} \times \mathbb{Q} \times \ldots \times \mathbb{Q}}_{n+1}|$, perché $a_0 + a_1 x + \ldots + a_n x^n \longmapsto$
$\longmapsto \langle a_0, a_1, \ldots, a_n \rangle$

Mostriamo $|\mathbb{Q}[x]^{\leq n}| = \aleph_0$. Per induzione:
- $n = 0 \Rightarrow |\mathbb{Q}[x]^{\leq 0}| = |\mathbb{Q}| = \aleph_0$
- $n \overset{\text{ind}}{\Longrightarrow} n+1$: $|\mathbb{Q}[x]^{\leq n+1}| = |\mathbb{Q}[x]^{\leq n} \times \mathbb{Q}| = |\mathbb{Q}[x]^{\leq n}| \cdot |\mathbb{Q}| =$ (coeff del grado n)
$\overset{\text{ind}}{=} \aleph_0 \cdot \aleph_0 = \aleph_0$.

$|\mathbb{Q}[x]| = |\bigcup_{n \in \mathbb{N}} \mathbb{Q}[x]^{\leq n}| = \aleph_0$

Ora, dato $p \in \mathbb{Q}[x]$, chiamiamo $A_p = \{\text{radici di } p\}$
$|A_p| \leq$ grado di $p < \aleph_0$.
$\{\text{Algebrici}\} = \bigcup_{p \in \mathbb{Q}[x]} A_p$ = Unione su $\aleph_0$ di insiemi con card $< \aleph_0$
$\Rightarrow |\{\text{Algebrici}\}| \leq \aleph_0 \Rightarrow = \aleph_0$

Teo $\{\text{Trascendenti}\} = \mathbb{R} \setminus \{\text{algebrici}\}$;
$|\{\text{Trascendenti}\}| = \mathfrak{C}$

Dim $|\mathbb{R}| = |(\mathbb{R} \setminus \mathrm{Alg}) \cup \mathrm{Alg}| = |\mathbb{R} \setminus \mathrm{Alg}| + |\mathrm{Alg}| = |\mathbb{R} \setminus \mathrm{Alg}| + \aleph_0 =$
$= \mathfrak{C}$, se no si avrebbe $\aleph_0 + \aleph_0 = \aleph_0$

Ex Giochino del biliardo senza attrito: esiste almeno una direzione per cui la pallina non torna mai al p.to di partenza.
Con le cardinalità: mettendo infiniti specchi ai lati del biliardo, la pallina torna al p.to iniziale solo se c'è una retta tra lei e un'immagine nel riflesso. I rifl. sono $\aleph_0 \times \aleph_0 \Rightarrow$ Idir in cui torna $= \aleph_0$

Buoni ordini

Def: Dato A insieme (o classe) un ordine totale $\leq$ su A è t.c.

per. $\begin{cases} x \leq x \\ x \leq y \wedge y \leq z \Rightarrow x \leq z \\ x \leq y \wedge y \leq x \Rightarrow x = y \end{cases}$

tot. $\{ \forall x, y \in A,\ x \leq y \vee y \leq x$

Def: un buon ordine è un ordine totale che, in più,

$\forall X \subseteq A \quad (X \neq \emptyset \Rightarrow X$ ha un minimo)

ES: insiemi finiti ordinati

ES: $(\mathbb{N}, \leq)$ (mostrare per es)

ES: $\mathbb{N} \times \mathbb{N}$ con ordine lessicografico: $(x,y) \leq (x',y') \Leftrightarrow$
$(y < y') \vee [(y = y') \wedge (x < x')]$

15.3.2016

Abbiamo visto "buoni ordini":

- $(A, \leq)$ con A finito
- $(\mathbb{N}, \leq)$
- $(\mathbb{N}+\mathbb{N}, \leq)$ dove $\mathbb{N}+\mathbb{N} = \mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}$
- $(\mathbb{N} \times \mathbb{N}, \leq_{Lex})$

Ex: Mostrare che unione e prodotto di buoni ordini è buon ordine.

Ci chiediamo ora se esistano buoni ordini più che numerabili.

Si può fare $(\mathcal{P}(\mathbb{N}), \leq)$ ordine totale in quanto $\mathcal{P}(\mathbb{N}) \cong \{f : \mathbb{N} \to 2\}$. Quindi, se $A \subseteq \mathbb{N}$, $B \subseteq \mathbb{N}$
$\Rightarrow A \leq B$ sse $f_A \leq f_B$ secondo le immagini.

Questo non è un buon ordine: $(1,1,\_) > (1,0,0\_) > (0,1,0\_) > \dots$
Ottengo una succ. decrescente infinita senza minimo.

Prop: Un ordine totale $(A, \leq)$ è un buon ordine $\Leftrightarrow$
$\nexists f (f : \mathbb{N} \to A \wedge \forall n\ f(n+1) < f(n))$

Dim: $\Rightarrow$) ovvia: se $\exists f$ così, la succ delle imm non ha minimo

$\Leftarrow$) Se A non è ben ordinato, $\exists B \subseteq A$ senza minimo,
sia S funzione di scelta. Sia $a_{n+1} := S(\{x \in B \mid x < a_n\})$, $a_0 := b$
Abbiamo che $S : \mathcal{P}(B) \setminus \{\emptyset\} \longrightarrow B$.
Una tale S $\exists$ per AC, infatti:

$\forall X \in \mathcal{P}(B) \setminus \{\emptyset\} \quad \exists x (x \in X) \xrightarrow{AC} \exists S : \mathcal{P}(B) \setminus \{\emptyset\} \to B \quad \forall x\ S(x) \in X$

Ora definiamo per induzione:

$\exists b (b \in B)$ (si può fare, perché $B \neq \emptyset$) - Per la ricursione,
$\exists a = \{a_n \mid n \in \omega\}$ t.c. $a_0 = b$, $a_{n+1} = S(\{x \in B \mid x < a_n\})$
osserviamo che l'insieme $\{x \in B \mid x < a_n\}$ è nel dominio di S, in
quanto $\neq \emptyset$, altrimenti a_n sarebbe il minimo.

Dettaglio tecnico

- Tuttavia, stiamo contemporaneamente definendo a_n e dim che
- S sia definita, sebbene il dominio di S dipenda da a_n.
- Risolviamo questo problema ponendo:

$a_{n+1} = \begin{cases} S(\{x \in B \mid x < a_n\}) & \text{se } \neq \emptyset \\ b & \text{se } = \emptyset \end{cases}$ così che S sia sempre ben def. Poi dimostro, per induzione su n, che il secondo caso non succede.

[concludere per es]

Def: Un insieme X è transitivo se $a \in b \in X \Rightarrow a \in X$ con $a, b \in V$. Equivalentemente: $\bigcup X \subseteq X$ o anche $a \in X \Rightarrow a \subseteq X$

ES:
- $a \in \{a\} \in \{\{a\}, \{a,b\}\}$, ma $a \not\subseteq \langle a,b \rangle$ (a meno che...)
  Quindi $\langle a,b \rangle$ non è transitivo.
- $2 = \emptyset$ è transitivo
- $1 = \{0\}$
  $2 = \{0,1\}$
  $3 = \{0,1,2\}$
  } transitivi

Ex: X transitivo $\Rightarrow S(x) = x \cup \{x\}$ è transitivo

Sol: $a \in b \in S(x) = X \cup \{x\} \Leftrightarrow b \in X \vee b \in \{x\} \Leftrightarrow b \in X \vee b = x$.
- Se $b \in X$, allora $a \in b \in X \to a \in X \to a \in X \cup \{x\}$
- Se $b = x$, allora $a \in X \to a \in S(x)$

Ex: ω è transitivo.

Oss: $\omega \cup \{\omega\}$ è transitivo. Lo indichiamo con $\omega+1$.
$S(S(\omega)) = S(\omega) \cup \{S(\omega)\} = \omega \cup \{\omega\} \cup \{S(\omega)\} := \omega+2$
è transitivo.

Def: $<$ è un ordine stretto totale se è transitivo, irriflessivo, totale.
$(A, <)$ è un buon ordine stretto sse $\forall X \in A\ \exists b (b \in X \wedge \forall u \in X (b < u \vee b = u))$
cioè esiste minimo. (b).

Def: X è un ordinale di Von Neumann [scriviamo $X \in ON$] se
X è transitivo e $(X, \in)$ è buon ordine stretto, cioè $a < b \Leftrightarrow a \in b$

Ex • $\emptyset$ è ordinale (ovvio)
• X ordinale $\to$ $S(X)$ ordinale.
Infatti: abbiamo già visto $S(X)$ transitivo. Sia $(a_n \mid n \in \mathbb{N})$ e $a_{n+1} \in a_n \in S(X)$.
$a_0 \in X \to \forall n\ a_n \in X \to a_{n+1} \in X$
$a_0 \in \{X\} \to a_0 \in X \to \forall n\ a_n \in X \to a_{n+1} \in X$
} Tutte succ in X, deve avere min.

Teo Se X è un insieme di ordinali $\Rightarrow \bigcup X$ è ordinale

Dim X transitivo $\to \bigcup X$ transitivo:
$a \in b \in \bigcup X \to \exists c (a \in b \in c \in X)$ e per transitività $a \in \bigcup X$

Lemma: vediamo che: $2 \in ON \to 2 \notin 2$: infatti se $2 \in 2$ ho la catena $a_n = 2$ ($\Rightarrow a_{n+1} \in a_n$) discendente in 2.

Lemma: vediamo che: $2 \in ON \wedge x \in 2 \to x \in ON$;
sia $z \in y \in X \in 2 \Rightarrow x, y, z \in 2$. Ma allora $z \in X$ perché $\in$ è un buon ordine su 2; quindi X transit.

Guardare sulle dispense la parte sugli ordinali.

Ex Definire $+, \cdot$ e coeff razionali usando gli assiomi.

17.03.2015

Ex (Da fare più avanti): Successioni di Goodstein
$n \longrightarrow$ lo scrivo in base 10; trasformo tutti i 10 in 11, sottraggo 1; itero: riscrivo tutto in base 11, trasformo gli 11 in 12, sottraggo 1, itero. Dimostrare che tende a 0.

Es
$$n = 5 \cdot 10^{9 \cdot 10^2 + 8} + 6 \cdot 10^{4 \cdot 10 + 1} + 8 \cdot 10 + 1$$
$\downarrow$ trasformo: 10 in 11
$$n' = 5 \cdot 11^{9 \cdot 11^2 + 8} + 6 \cdot 11^{4 \cdot 11 + 1} + 8 \cdot 11$$
$\downarrow$
$$n'' = 5 \cdot 12^{9 \cdot 12^2 + 8} + 6 \cdot 12^{4 \cdot 12 + 1} + \underbrace{8 \cdot 12 - 1}_{= 7 \cdot 12 + 11}$$
$\downarrow$
...

Sembra che cresca di brutto, ma prima o poi arrivo a 0.

Ex (più fattibile)
$[n_1, n_2, \dots, n_k]$ multinsieme: non conta l'ordine ma contano le molteplicità: $[3, 5, 3] = [3, 3, 5] \neq [3, 5]$
$[n_1, \dots, n_k] \xrightarrow[\text{con}]{\text{compresso}} [n_1, n_2, \dots, n_{k-1}, \underbrace{a_1, \dots, a_s}_{a_i < n_k}]$

Dim che iterando si arriva a $\emptyset$.

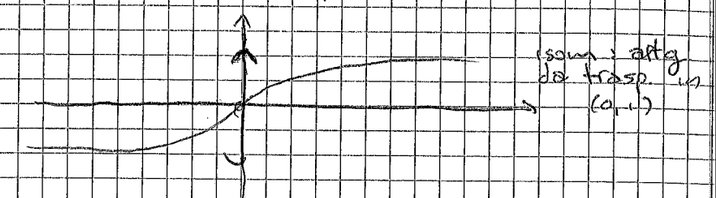
Es $[6, 5, 10] \longrightarrow [5, 5, 9, 9, 9, \dots, 9]$

Def $(A, \leq_A)$, $(B, \leq_B)$ tot ordinati;
$f: A \to B$ è crescente se $\forall x, y \in A (x < y \to f(x) < f(y))$

Def f è un isomorfismo d'ordine se è biunivoca e $x < y \Leftrightarrow f(x) < f(y)$

Def Il tipo di A $tp(A, \leq_A) = tp(B, \leq_B)$ se $\exists f: A \to B$ isomorfismo $(A, \leq_A) \cong (B, \leq_B)$

Es $(\mathbb{R}, \leq) \cong ((0,1), \leq)$



Ex $\mathbb{N}^{\mathbb{N}} = \{f \mid f: \mathbb{N} \to \mathbb{N}\}$ con ordine lessicografico
"successioni di num naturali"; es $f = (3, 5, 0, \boxed{7}, 8, \dots)$
$g = (3, 5, 0, \boxed{6}, 9, \dots)$
$f < g$ sse, detto k il min x dove $fx \neq gx$, si ha $f(k) < g(k)$.
$(\mathbb{N}, \leq) \cong \mathbb{R}^+$

L'idea è: $\mathbb{R}^+$ può essere diviso in interv semichiusi a sx:
$\mathbb{R}^+ = \bigcup_{n \in \mathbb{N}} [n, n+1)$
Una succ di $\mathbb{N}$ viene letta così: se la prima cifra è n, la succ corrisponde a un reale che sta nell'n-mo intervallino; se la seconda è k, sta nel k-mo sottointervallo dell'n-mo interv, eccetera.
Cioè: $f \longmapsto r_f$
$f(0) = k \to r_f \in [k, k+1) = \bigcup_{i \in \mathbb{N}} [a_i, a_{i+1})$
$f(1) = k' \to r_f \in [a_k, a_{k+1})$ e tc [formalizzare]

Def $(A, \leq_A)$ ordine totale;
$B \subseteq A$; Dico che B è iniziale se è una semiretta, cioè se $u < v \wedge v \in B \to u \in B$

Oss Un insieme ordinato può essere isomorfo a un suo sottoins. iniziale.
Es: $[0,1)^{\mathbb{R}} \cong [0, \frac{1}{2})^{\mathbb{R}}$, $x \longmapsto x/2$

Prop: Se $(A, \leq_A)$ è un buon ordine e $B \subseteq A$ iniziale, allora
• $B = A$ (impropria)
• $\exists a \in A$ $B = \{x \in A \mid x < a\} = [-\infty, a)$

Dim se $B \neq A$, $\exists c \in A \setminus B$; sia $a = \min(A \setminus B)$, esiste per la definizione di buon ordine.
$\Rightarrow B \overset{?}{=} \{x \in A \mid x < a\}$
$\subseteq$) $x < a \Rightarrow x \in B$ (a minimo)
$\supseteq$) $x \in B \rightarrow x < a$. In fatti, se così non fosse, sarebbe $x > a$.
Ma allora avrei $x \in B$, $x > a \Rightarrow a \in B$ ↯
B iniziale

Es $(\mathbb{N}, \leq)$; $\{x \in \mathbb{N} \mid x \leq 5\} = \{x \in \mathbb{N} \mid x < 6\}$

Lemma Se $f: (A, \leq_A) \longrightarrow (A, \leq_A)$ crescente, $(A, \leq_A)$ buon ordine,
$\Rightarrow \forall x \in A (f(x) \geq x)$. sembra la def di crescente, ma no.

Dim Per assurdo, sia z il minimo t.c. $f(z) < z$. Ma allora, siccome f crescente, $ff(z) < f(z)$, allora posso prendere $x' = f(z) < z$ ↯ perché contro minimalità di z.

Coroll. se $(A, \leq)$ buon ordine e $B \subseteq A$ limitato
(esiste $a \in A \mid \forall b \in B \; b < a$) $\Rightarrow (A, \leq_A) \not\cong (B, \leq_{A|B})$
cioè $\nexists f$ biunivoca t.c. $x < y \leftrightarrow fx < fy$.

OSS Può capitare che ci siano isom con sottoinsiemi illimitati
es $(\mathbb{N}, \leq) \cong (2\mathbb{N}, \leq)$, $x \mapsto 2x$

Dim Per assurdo, $f: A \to B$ isom→(crescente)
Ma allora $f(a) > a$; ma $a \notin B$, $f(a) \in B$ per def ↯
perché $b < a \; \forall b \in B$.

OSS In particolare, $(A, \leq_A)$ buon ordine; $B \subset A$ iniziale proprio
$\Rightarrow B$ limitato $\Rightarrow A \not\cong B$

Def $(A, \leq_A)$, $(B, \leq_B)$ buoni ordini; $tp(A, \leq_A) \leq tp(A, \leq_B)$
$\Leftrightarrow \exists f (f: A \to B \wedge f$ crescente $\wedge \underset{\text{iniziale}}{\text{Im}(f) \subseteq B})$

Ex $tp(A, \leq_A) \leq tp(B, \leq_B) \leq tp(C, \leq_C)$
$\rightarrow tp(A, \leq_A) \leq tp(C, \leq_C)$

Si fa con la composizione; devo però verificare che
Un segm iniziale di B va in un segm iniziale di C.

Teo $(A, \leq_A)$, $(B, \leq_B)$ buoni ordini. Allora
$tp(A, \leq_A) \leq tp(B, \leq_B) \vee tp(B, \leq_B) \leq tp(A, \leq_A)$

Def: $tp(A, \in_A)$ è un ordinale di Frege / Cantor / ?

Lemma $\alpha, \beta \in ON$; sono equivalenti
1) $\alpha \in \beta$
2) $\alpha \subseteq \beta$
3) $\alpha \subset \beta$ iniziale proprio

Dim
(1) $\Rightarrow$ (2): $\alpha \in \beta \rightarrow \alpha \subset \beta$ (β transitivo)
$\alpha \in \beta \rightarrow \alpha \neq \beta$, se no $\alpha \in \alpha$ ↯
$\Rightarrow \alpha \in \beta \rightarrow \alpha \subset \beta$

(2) $\Rightarrow$ (3): dati $x, y \in \beta$, $x \overset{\in}{<} y \in \alpha$, α transitivo $\rightarrow x \in \alpha$

(3) $\Rightarrow$ (1):
$\alpha \subset \beta$ iniziale proprio $\Rightarrow \alpha = \{x \in \beta \mid x \overset{?}{<} b\}$ per def; però
se $x < b \Rightarrow x \in \beta$, perché $x \overset{\in}{<} b \overset{\in}{\in} \beta$, β transitivo $\Rightarrow x \in b$
$\Rightarrow \alpha = \{x \mid x < b\} = \{x \mid x \in b\} \Rightarrow b = \alpha$ per estensionalità. ∎

Lemma $\alpha, \beta \in ON \Rightarrow \alpha \subseteq \beta \vee \beta \subseteq \alpha$ (due ordinali sono sempre confrontabili)

Dim: $\gamma = \alpha \cap \beta \Rightarrow \gamma \in ON \wedge \gamma \subseteq \alpha \wedge \gamma \subseteq \beta$
Basta mostrare $\gamma = \alpha \vee \gamma = \beta$.
Se così non fosse, pa, $\gamma \subset \alpha \wedge \gamma \subset \beta$
$\Rightarrow \gamma \in \alpha \wedge \gamma \in \beta \Rightarrow \gamma \in \alpha \cap \beta = \gamma \Rightarrow \gamma \in \gamma$ ↯

Lemma: $\alpha, \beta \in ON$; $(\alpha, \in) \cong (\beta, \in)$, cioè $\exists f: \alpha \to \beta$ biunivoca e t.c. preserva l'ordine, cioè $(\forall x, y \in \alpha)(x \in y \leftrightarrow fx \in fy)$
$\Rightarrow \alpha = \beta$; cioè, i buoni ordini sono rigidi.

Dim
Sappiamo già $\alpha \subseteq \beta \vee \beta \subseteq \beta$.
Se $\alpha \neq \beta$ avremmo $\alpha \underset{\text{iniz prop}}{\subset} \beta \vee \beta \underset{\text{iniz prop}}{\subset} \beta$ ↯ [un buon ordine non è mai isom a segm iniziale proprio]

Def $\alpha, \beta \in ON$; $\alpha \leq \beta$ se $\alpha \subseteq \beta$; $\alpha < \beta$ se $\alpha \in \beta$

OSS: $\alpha \leq \beta \leftrightarrow \alpha < \beta \vee \alpha = \beta$

Ex: Dimostrare che $|A| \leq |B| \rightarrow 2^{|A|} \leq 2^{|B|}$

22-3-16

Assioma di fondazione

$\forall x \; \exists a (a \in x \wedge a \text{ è } \in\text{-minimale})$, cioè

$\forall x \; \exists a (a \in x \wedge \forall v \in a (v \notin x))$

$\forall v \neg (v \in a \wedge v \in x)$

Es] Fondazione $\Rightarrow \nexists a$ t.c. $a = \{a\} \Rightarrow a \in \{a\} = a \Rightarrow a \in a$
$\Rightarrow a \in a \in a \dots$
Se $a = \{a\}$, a non ha elem $\in$-min. Infatti, l'unico elemento di $a = \{a\}$ è a che non è $\in$-min, perché $a \in a$.

Es] Fondazione $\Rightarrow \nexists a, b \quad a = \{b\}, \; b = \{a, b\}$
Infatti, $\in$ ciclo $b \in a \in b$

Es] Fond $\Rightarrow \nexists c, d \quad c = \{d\}, \; d = \{c\}$.
Se $\exists$, potrei prendere $A = c \cup d$ che non avrebbe minimale.

Es] $f: \mathbb{N} \to V$ funzione; Fond $\Rightarrow$ non è possibile che $\forall n \; f(n+1) \in f(n)$.
Infatti, $A = \{f(n) \mid n \in \mathbb{N}\}$ non ha elem minimale.

4-4-16

ON = ordinali di Von Neumann (classe propria).

Def: $x \in ON \iff$ è transitivo e ben ordinato $<$ da $\in$

Teo 1] Se $(X, \leq)$ buon ordine $\Rightarrow \exists! \; a \in ON \quad (X, <) \cong (a, \in)$
$a = \{x \mid x \in a\}$ $\quad ot(X, \in_X)$
cioè $\exists! f \quad f: X \to a \quad \forall a, b \in X \quad a < b \iff f(a) < f(b)$

Teo 2] Dati due buoni ordini $(A, \leq_A)$, $(B, \leq_B)$ vale una e una sola delle seguenti:
1) $(A, \leq_A)$ è isomorfo a $(B, \leq_B)$, scrivo $Tipo(A, \leq_A) = Tipo(B, \leq_B)$
2) $(A, \leq_A)$ è isomorfo a un segmento proprio di $(B, \leq_B)$
$Tipo(A, \leq_A) < Tipo(B, \leq_B) \iff ot(A, \leq_A) \in ot(B, \leq_B)$
3) $(B, \leq_B)$ è isom a un segm proprio di $(A, \leq_A)$

oss] Questo ci permette di osservare che se consideriamo la classe di tutti i buoni ordini e consideriamo le classi di equivalenza date dal buon ordinato ha isom $\Rightarrow$ ogni classe contiene 1 ordinale (rappresentante).

Ex] Trovare $X \subseteq \mathbb{R}$ t.c. $(\mathbb{N} \times \mathbb{N}, \leq_{lex}) \cong (X, \leq_{\mathbb{R}})$
$(a, b) \leq_{lex} (a', b') \iff b < b' \vee (b = b' \wedge a < a')$

$\mathbb{N} \times \mathbb{N} = (0,0), (1,0), (2,0), (3,0) \dots (0,1), (1,1), \dots (0,2), \dots$
Fare per esercizio

Ex] $(\mathbb{N} + \mathbb{N}, \leq)$, $\mathbb{N} + \mathbb{N} = (\mathbb{N} \times \{0\} \cup \mathbb{N} \times \{1\}, \leq_{lex}) \underset{segm}{\subset} (\mathbb{N} \times \mathbb{N}, \leq_{lex})$
Per mandarlo in un sottoins dei reali, posso ad esempio fare
$(n, 0) \longmapsto 1 - \frac{1}{n+1}$
$(n, 1) \longmapsto 2 - \frac{1}{n+1}$
} sottoinsieme di $\mathbb{R}$ isomorfo a $(\mathbb{N} \times \mathbb{N}, \leq_{lex})$
Quindi hanno associato lo stesso ordinale: lo si chiama $\omega + \omega \in ON$

Ex] Fare lo stesso con $(\mathbb{N} \times \mathbb{N} \times \mathbb{N}, \leq_{lex})$

Tutti i buoni ordini si possono rappresentare come sottoinsieme di $\mathbb{R}$?

Ex] $X \subseteq \mathbb{R}$, X ben ordinato da $\leq_{\mathbb{R}} \Rightarrow |X| \leq \aleph_0$

Infatti: si usa il fatto che $\mathbb{Q}$ sia numerabile e denso in $\mathbb{R}$.

Caso 1: X non ha max
Dato $a \in X$, l'insieme $\{b \in X \mid b > a\} \neq \emptyset \Rightarrow$ ha un minimo elemento a': $a < a'$ e non c'è nulla tra a e a' (in X).
Allora scelgo $q_a \in \mathbb{Q}$, $a < q_a < a'$
(Posso ben ordinare $\mathbb{Q}$, mettendolo in corrisp biunivoca con $\mathbb{N}$ e prendendo il buon ordine indotto da $\mathbb{N}$: in questo modo posso evitare di usare l'assioma della scelta).
$a \neq b \Rightarrow q_a \neq q_b$ (perché se $a < b \Rightarrow a < a' \leq b < b'$)
Quindi ho una funz inietiva $f: X \to \mathbb{Q}$, $a \mapsto q_a \Rightarrow |X| \leq |\mathbb{Q}| = \aleph_0$

Caso 2: X ha max: sia b. Faccio la stessa cosa, ma definisco $q_b \in \mathbb{Q}$: $b < q_b$. ∎

Ex] $X \subseteq \mathbb{R}$ t.c. $\forall a \in X$ ha un successore a' (cioè $a < a'$ e $\nexists b \in X \; a < b < a'$)
$\overset{?}{\Rightarrow}$ X buon ordine?
No: ad esempio, la succ. $\left(\frac{1}{n}\right)_{n \in \mathbb{N}}$ non lo è.

Oss Gli elementi di un buon ordine, a parte il min, sono di due tipi: quelli che hanno un predecessore e quelli che non lo hanno.

Def Se $(X, \leq_X)$ è buon ordine, $b \in X$ non ha predecessore $(\nexists\ a \mid b = a') \Rightarrow b$ si chiama punto limite.

Ex Trovare $(X, \leq_X)$ bene ordinato: $X \cong$ pti limite di X $\quad = D(X)$ (derivato di X)
(Tipico esercizio da esame)

Es
- $D(\mathbb{N}, \leq) \cong \{0\}$
- $D(\mathbb{N}+\mathbb{N}, \leq_{lex}) = \{(0,0), (0,1)\} \cong 2 = \{0,1\}$
- $D(\mathbb{N}\times\mathbb{N}, \leq_{lex}) = \{(0,n) \mid n \in \mathbb{N}\} \cong (\mathbb{N}, \leq)$

L'idea è trovare il sup, o l'unione, degli $\mathbb{N}\times\mathbb{N}\times\dots\times\mathbb{N}$

Ex Trovare $(X, \leq_X) \subseteq \mathbb{R}$ bene ordinato, $(X, \leq_X) \cong D(X)$

Oss $(A, \leq_A)$ e $(B, \leq_B)$ sono buoni ordini $\Rightarrow$ lo sono anche $A+B$ e $A\times B$ così ordinati:

$A+B = A\times\{0\} \cup B\times\{1\}$:
$(a,0) < (b,1)$; $(a,0) < (a',0) \iff a <_A a'$
$(b,1) < (b',1) \iff b <_B b'$

$(A\times B, \leq) \quad (a,b) < (a',b') \iff (b<b') \vee (b=b' \wedge a<a')$

Un'altra tecnica per produrre buoni ordini è fare il "sup" di buoni ordini.
Ad esempio, $(A_n, \leq_n)$ buon ordine, $n \in \mathbb{N}$.
Vorrei un buon ordine $(B, \leq_B)$ t.c.
$\forall n$ $(A_n, \leq_n) \cong$ segmento di $(B, \leq_B)$, cioè che li contenga tutti.

Teo Un tale buon ordine esiste, qualsiasi insieme di indici io scelga, anche non numerabile.

Caso semplice: $(A_n, \leq_n)$, $n \in \mathbb{N}$, $A_n \subseteq A_{n+1}$ e l'ordine di A_n è quello di A_{n+1} ristretto a A_n.
In questo caso, scelgo $B = \bigcup_n A_n$.
$x, y \in B \Rightarrow \exists n \in \mathbb{N}$ $x, y \in A_n$ e definisco
$x \leq_B y \iff x \leq_n y$ (non dipende dalla scelta di n)

è un buon ordine? Senza ulteriori ipotesi, no!

Es
$A_0 = \{0, 1\} \subseteq \mathbb{R}$
$A_1 = \{0, \frac{1}{2}, 1\} \subseteq \mathbb{R}$
$A_2 = \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$
$\vdots$
$A_n = \{0, \frac{1}{2^n}, \frac{2}{2^n}, \dots, \frac{2^n-1}{2^n}, 1\}$
$\vdots$
$\bigcup_n A_n = \left\{\frac{k}{2^n} \mid k, n \in \mathbb{N}\right\} \cong \mathbb{Q}$ (esercizio non facile)

Non è chiaramente un buon ordine, perché è denso.

Ex Mostrare che l'unione di ordini totali a due a due contenuti uno nell'altro con l'ordine indotto, è un ordine totale.
(In generale, non è un buon ordine anche se parto da buoni ordini)

L'ipotesi aggiuntiva che serve affinché venga un buon ordine, è che a due a due devono essere l'uno un segmento iniziale dell'altro.
Riassumendo, si ha il seguente teorema:

Teo Sia $(A_i, \leq_i)$ $i \in I$ buon ordine
Dati $i, j \in I$ $\left(\begin{array}{l} A_i \subseteq A_j \\ \leq_i = \leq_j|_{A_i} \\ A_i \text{ segm di } A_j \end{array}\right)$ o $\left(\begin{array}{l} A_j \subseteq A_i \\ \leq_j = \leq_i|_{A_j} \\ A_j \text{ segm di } A_i \end{array}\right)$

Allora $\bigcup A_i$ è un buon ordine con l'ordine $\leq = \left(\bigcup \leq_i\right)$
$\left(a \leq b \iff (a,b) \in (\leq) \iff \exists i\ (a,b) \in (\leq_i)\ a \leq_i b\right)$

Dim Si tratta di un ordine totale (per esercizio);
È un buon ordine: infatti, se $B = \bigcup A_i$ non fosse un buon ordine, esisterebbe $b_0 > b_1 > b_2 > \dots$ in B.
$b_0 \in A_i \Rightarrow b_n \in A_i$. Infatti:
sia j t.c. $b_n \in A_j$. Se $A_j \subseteq A_i \Rightarrow b_n \in A_i$. Se no, $A_i \subseteq A_j$ come segmento. Allora $b_0 \in A_i$, $b_n <_j b_0 \Rightarrow b_n \in A_i$ per definizione di segmento.
Avrei quindi una succ decrescente dentro A_i, ma A_i è buon ordine ⊥

Lemma: $A \subseteq [0, n] \Rightarrow A\times\mathbb{N} \cong X \subseteq [0, n+1]$ come segmento.