Elementi di Teoria degli Insiemi

A.A. 2022-2023

SIMONE SACCANI

NASCITA DELLA TEORIA DEGLI INSIEMI

<u>PROBLEMA</u>: $\frac{a_0}{2} + \sum_{n=1}^{+\infty} a_n \cos(nx) + b_n \sin(nx) = \frac{a_0'}{2} + \sum_{n=1}^{+\infty} a_n' \cos(nx) + b_n' \sin(nx) \quad \forall x \in \mathbb{R}$

Ipotizziamo siano due serie convergenti

segue che $\forall n \ a_n = a_n' \wedge b_n = b_n'$?

<u>Georg Cantor</u>: la risposta è sì

DEF. $X \subseteq \mathbb{R}$ è un insieme di unicità se

$\forall x \notin X, \ S(x) = \frac{a_0}{2} + \sum_{n=1}^{+\infty} a_n \cos(nx) + b_n \sin(nx) = 0 \Rightarrow \forall n \ a_n = 0 \wedge b_n = 0$

Lemma di Cantor Se X soddisfa la proprietà (*) seguente, allora X è di unicità.

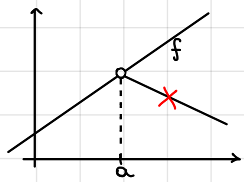
(*) Per ogni $f: \mathbb{R} \longrightarrow \mathbb{R}$ continua, vale la seguente implicazione.

(i) $\forall [a,b]$, con $[a,b] \cap X = \emptyset$, $f|_{[a,b]}$ è lineare

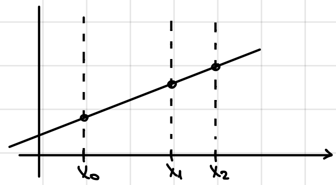
(ii) $\forall x \in \mathbb{R}$, se f ha derivata dx e sx in x, allora coincidono

allora f è lineare $(f = ax + b)$

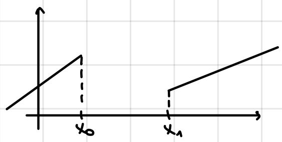
<u>esempio</u> $X = \{a\}$ ha la proprietà (*)



<u>esempio</u> un qualunque insieme finito di punti soddisfa (*)



<u>non-esempio</u> $X = [x_0, x_1]$ non gode di (*)



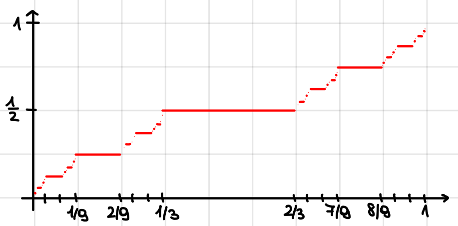
<u>OSS</u> (*) $\Rightarrow$ X non contiene intervalli (X ha parte interna vuota)

<u>non-esempio</u> $\mathbb{Q}$ non gode di (*) perché (i) è una condizione vuota

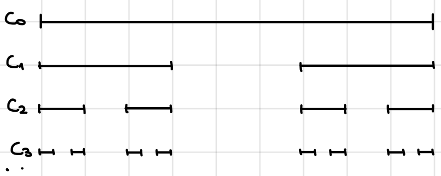
Un chiuso a parte interna vuota soddisfa (*)?

<u>esempio</u> "Scala di Cantor" o "scala del diavolo"

$f: [0,1] \longrightarrow [0,1]$



Costruita a partire dall'insieme di Cantor:

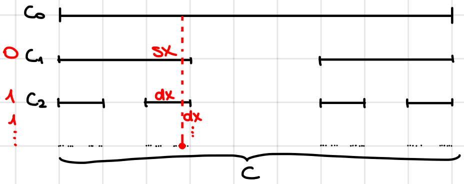


$C = C_0 \cap C_1 \cap C_2 \cap C_3 \cap \ldots$

OSS C non soddisfa (*)
tuttavia C è chiuso a parte interna vuota

Teorema di Cantor-Lebesgue Se X è chiuso e numerabile (ossia $X=\{x_i \mid i\in\mathbb{N}\}$) allora soddisfa (*)

Domanda: perché C non è numerabile?
OSS Esiste una corrispondenza biunivoca
$\alpha : C \longrightarrow \{\text{sequenza binaria}\} = (a_i)_{i\in\mathbb{N}} = a_0, a_1, a_2, \dots$ con $a_i \in \{0,1\}$



OSS Se potessi numerare i punti di C, potrei numerare le sequenze binarie

Proposizione Non è possibile numerare le sequenze binarie

DIMOSTRAZIONE
Per assurdo

$0 \longrightarrow a_1\ a_2\ a_3 \dots$
$1 \longrightarrow a_1'\ a_2'\ a_3' \dots$
$2 \longrightarrow a_1''\ a_2''\ a_3'' \dots$
$\vdots$

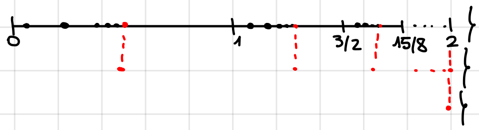
Considero la diagonale e la inverto: $\bar{a}_1\ \bar{a}_2'\ \bar{a}_3'' \dots$
Non può corrispondere a n, perché la $n+1$-esima cifra è diversa $\lightning$ $\square$

Domanda: come dimostriamo il teorema?

DEF Dato $X \subseteq \mathbb{R}$, il derivato di Cantor-Bendixson di X è
$X' := X \setminus \{\text{punti isolati di } X\}$
$X^{(0)} = X$, $X^{(n+1)} = (X^{(n)})'$

OSS se X' soddisfa (*), allora X soddisfa (*)
DIMOSTRAZIONE
f è lineare nei punti isolati di X, quindi applicando (*) su X', f è lineare

esempio successione con limite $S =$
$S = \{1-\frac{1}{n} \mid n>1\} \cup \{1\}$
$S' = \{1\} \implies S'$ soddisfa (*) $\implies S$ ha (*)

esempio $S = \{$  $\}$

$S' = \{ \}$
$S'' = \{ \}$
S'' ha (*) $\implies S'$ ha (*) $\implies S$ ha (*)

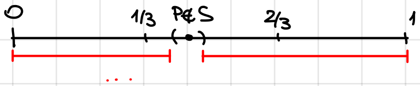
Domanda: esiste n t.c. $S^{(n)} = \emptyset$ se S è chiuso è numerabile?

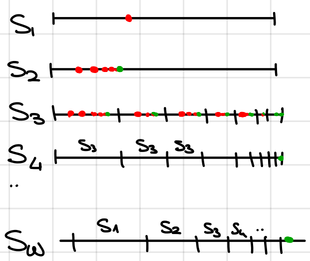
Fatto Sia $S \subseteq \mathbb{R}$ un insieme chiuso t.c. $S' = S$
Allora S non è numerabile

DEF. $X \subseteq \mathbb{R}$ è **perfetto** se X è un chiuso a parte interna vuota e $S' = S$

> **Proposizione** Un insieme perfetto è in corrispondenza biunivoca con le successioni binarie

DIMOSTRAZIONE (idea)
Supponiamo $0 = \inf S$ e $1 = \sup S$
$\exists\, I$ int. di P t.c. $I \cap S = \emptyset$





$S_1^{(1)} = \emptyset$

$S_2^{(2)} = \emptyset \quad S_2^{(1)} \neq \emptyset$

$S_3^{(3)} = \emptyset \quad S_3^{(2)} \neq \emptyset$

$S_4^{(4)} = \emptyset \quad S_4^{(3)} \neq \emptyset$

$S_\omega^{(n)} \neq \emptyset$

> **Lemma** Sia $S^{(\omega)} = S^{(0)} \cap S^{(1)} \cap S^{(2)} \cap \dots$
> Se $S^{(\omega)}$ soddisfa (*), allora S soddisfa (*)

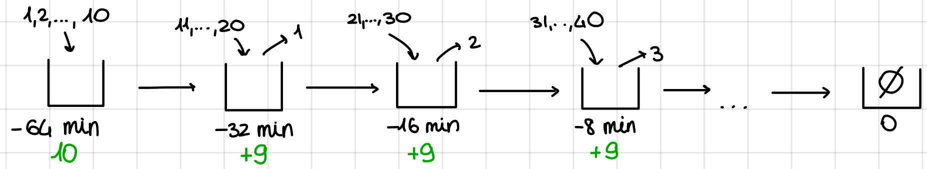
DIMOSTRAZIONE
Sia f una funzione che soddisfa l'ipotesi di (*)
Ci basta vedere che se $[a,b]$ non contiene punti di $S^{(\omega)}$ allora f è lineare su $[a,b]$
$[a,b] \cap S^{(\omega)} = \emptyset \implies [a,b] \cap S^{(0)} \cap S^{(1)} \cap S^{(2)} \cap \dots = \emptyset$
$\implies \exists n$ t.c. $[a,b] \cap S^{(0)} \cap S^{(1)} \cap \dots \cap S^{(n)} = \emptyset \implies \exists n$ t.c. $[a,b] \cap S^{(n)} = \emptyset$ $\square$

OSS S_ω soddisfa (*), infatti $\underbrace{(S_\omega^{(\omega)})'}_{= S_\omega^{(\omega+1)}} = \emptyset$

$S^{(\omega+n)} = (S^{(\omega+n-1)})'$
$\vdots$
$S^{(2\omega)} \quad \dots \quad S^{(\omega^2)} \quad \dots \quad S^{(\omega^\omega)} \quad \dots \quad S^{(\omega^{\omega^\omega})}$
$S^{(\varepsilon_0)}$

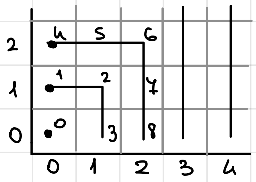
$S^{(n)} = \emptyset \implies S$ ha (*) per induzione

OSS Se A è numerabile e $B \subseteq A$, allora B è numerabile esempio



$(9\aleph_0 = \aleph_0)$

esempio Esiste una bigezione tra $\mathbb{N}^2$ e $\mathbb{N}$ $(|\mathbb{N}^2| = |\mathbb{N}|)$



Altro modo $(a,b) \longmapsto 2^a(2b+1) - 1$

esempio $|\mathbb{R}^2| = |\mathbb{R}|$

① $|\mathbb{R}| = |(0,1)|$

$x \longmapsto \frac{1}{2} + \frac{1}{\pi} \arctan x$

② idea per $|\mathbb{R}^2| = |(0,1)^2| \overset{!}{=} |(0,1)| = |\mathbb{R}|$

$(0.a_1a_2a_3\ldots, 0.b_1b_2b_3\ldots) \longmapsto 0.a_1b_1a_2b_2a_3b_3\ldots$

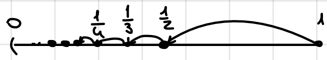
a_i, b_i cifre decimali

guaio: $0.1000\ldots = 0.0999\ldots$

③ $|(0,1)| = |(0,1]|$ $\qquad |\{1\ 2\ 3\ 4\ 5\ \ldots\}| = |\{2\ 3\ 4\ 5\ \ldots\}|$

costruisco $f: (0,1] \to (0,1)$

$x \longmapsto \begin{cases} \frac{1}{n+1} & \text{se } x = \frac{1}{n}, n \in \mathbb{N} \\ x & \text{altrimenti} \end{cases}$



④ Ci basta dimostrare $|(0,1]^2| = |(0,1]|$

Scrivo lo sviluppo decimale infinito dei numeri in $[0,1]$

$(0.04700109\ldots, 0.2007014\ldots) \longmapsto 0.04|2|7|007|001|01|09|4|\ldots$

un gruppo è $0\ldots0$[non 0]

⑤ $\mathbb{R}^2 \to (0,1)^2 \to (0,1]^2 \to (0,1] \to (0,1) \to \mathbb{R}$ tutte bigezioni

Domanda: In generale, se S è infinito, $|S^2| = |S|$? Boh

(se si assume AC, sì)

PARADOSSO di Russell

Sia $N = \{x \mid x \notin x\}$ $\qquad N \overset{?}{\in} N$

$N \in N \Leftrightarrow N \notin N$ ↯

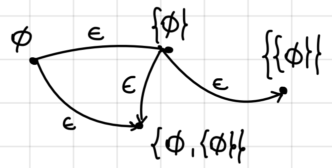
$\Rightarrow$ $\{x \mid \text{proprietà di } x\}$ in generale non si può dire

PARADOSSO di Berry

- Il vocabolario italiano annovera una quantità finita di parole
- $\forall n \in \mathbb{N}$, esiste una quantità finita di possibili frasi di al più n parole
- per il principio del minimo esiste n = "il minimo numero naturale che non si può definire con meno di 20 parole" ↯

LINGUAGGIO DELLA TEORIA DEGLI INSIEMI

Variabili: $x, y, z, X, Y, Z, \alpha, \beta, \dots$ rappresentano sempre insiemi
Relazioni: $=, \in$
Formule atomiche: var = var, var $\in$ var



Intuizione: l'universo insiemistico è un gigantesco grafo diretto aciclico

Formule: (1) formule atomiche
(2) form $\wedge$ form
form $\vee$ form
$\neg$ form
(3) $\forall$var. form
$\exists$var. form

Significato dei connettivi logici:
$A \wedge B$ è vera se A è vera e B è vera
$A \vee B$ è falsa se A è falsa e B è falsa
$A \to B$ è falsa se A è vera e B è falsa $\qquad A \to B \equiv \neg A \vee B$
$\neg A$ è vera se A è falsa

abbreviazione
$\exists x \; \varphi(x) \equiv$ c'è un insieme con la proprietà φ
$\forall x \; \varphi(x) \equiv$ tutti gli x godono della proprietà φ

esempio
- sia S un insieme qualunque e P una proprietà qualunque
  $\exists x \in S \; P(x) \to (\forall y \in S \; P(y))$
- $\varphi \Leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$
  Verificare che $\varphi \Leftrightarrow \psi$ è vera se e solo se φ e ψ hanno lo stesso valore di verità
- $\neg\neg\varphi \equiv \varphi$
  $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$
  $\varphi \wedge (\psi \vee \tau) \equiv (\varphi \wedge \psi) \vee (\varphi \vee \tau)$
  $\neg(\varphi \wedge \psi) \equiv (\neg\varphi) \vee (\neg\psi)$
- $\neg \exists x \; \varphi(x) \equiv \forall x \; \neg\varphi(x) \qquad \neg \forall x \; \varphi(x) \equiv \exists x \; \neg\varphi(x)$
- $\exists x \in A \; \varphi(x)$ è sgrammaticata: $\exists x \in A \; \varphi(x) \equiv \exists x \; (x \in A \wedge \varphi(x))$
  $\forall x \in A \; \varphi(x) \equiv \forall x \; (x \in A \to \varphi(x))$
- $A \subseteq B \equiv \forall x \in A \;\; x \in B$
  $A = B \cup C \equiv \forall x \; (x \in A \Leftrightarrow x \in B \vee x \in C)$
  $A = B \cap C \equiv \forall x \; (x \in A \Leftrightarrow x \in B \wedge x \in C)$

NOTA: non abbiamo mai detto che $A \cup B$ e $A \cap B$ esistono

DEF. Una classe è una proprietà di alcuni insiemi: $\quad x \in \mathcal{C} \equiv \varphi(x)$
la classe di tutti gli insiemi V. $\quad x \in V \equiv x = x$
le classi che non sono insiemi si chiamano classi proprie
NOTA: in ZFC, le classi non sono oggetti; in GB sì

I PRIMI ASSIOMI

(Zermelo - Fraenkel con assioma della scelta (AC))

① **Assioma dell'insieme vuoto**

$\exists x \ \forall y \quad y \notin x$

② **Assioma di estensionalità**

$\forall a \ \forall b \quad a = b \longleftrightarrow \forall x \ (x \in a \longleftrightarrow x \in b)$

Proposizione Esiste un solo insieme vuoto

$\exists! x \ \forall y \ y \notin x$

DIMOSTRAZIONE

Siano x_1 e x_2 due insiemi vuoti.

Per estensionalità: $(\forall y \ (y \notin x_1) \wedge \forall y \ (y \notin x_2)) \longrightarrow x_1 = x_2$ □

<u>NOTAZIONE</u> Denotiamo con $\emptyset$ l'insieme vuoto

$x = \emptyset \ \equiv \ \forall y \ (y \notin x)$

③ **Assioma di separazione**

$\forall A \ \exists B \ \forall x \ x \in B \longleftrightarrow (x \in A \wedge \varphi(x))$

è uno SCHEMA di assiomi

Proposizione $\forall A \ \exists! B \ \forall x \ x \in B \longleftrightarrow (x \in A \wedge \varphi(x))$

DIMOSTRAZIONE

Fissato A, siano B_1 e B_2 due insiemi che verificano la richiesta.

Allora $x_1 \in B_1 \longleftrightarrow x \in A \wedge \varphi(x) \longleftrightarrow x \in B_2$

Concludo per estensionalità: $B_1 = B_2$ □

<u>NOTAZIONE</u> Denotiamo B come

$B = \{x \in A \mid \varphi(x)\} \ \equiv \ \forall x \ x \in B \longleftrightarrow (x \in A \wedge \varphi(x))$

Potrebbe capitare che φ ha altre variabili libere: $\varphi(x, a_1, \dots, a_n)$

L'assioma diventa: $\forall A \ \exists B \ \forall x \ x \in B \longleftrightarrow (x \in A \wedge \varphi(x, a_1, \dots, a_n))$

$\forall a_1, \dots, a_n$ implicita

Proposizione Non esiste l'insieme di tutti gli insiemi

DIMOSTRAZIONE

Per assurdo supponiamo esista l'insieme V t.c. $\forall x \ x \in V$

Per separazione $\exists B \ \forall x \ x \in B \longleftrightarrow (x \in V \wedge x \notin x)$

che equivale a $\exists B \ \forall x \ x \in B \longleftrightarrow x \notin x$

Assegno $x = B$: $B \in B \longleftrightarrow B \notin B$ ↯ □

④ **Assioma del paio**

$$\forall a \forall b \exists B \forall x \; x \in B \longleftrightarrow (x=a \lor x=b)$$

Proposizione $\forall a \forall b \exists! B \forall x \; x \in B \longleftrightarrow (x=a \lor x=b)$

DIMOSTRAZIONE

Per assurdo, siano B_1, B_2 due insiemi che soddisfano la proprietà.
Allora $x \in B_1 \longleftrightarrow x=a \lor x=b \longleftrightarrow x \in B_2$
Per estensionalità $B_1 = B_2$ □

Corollario $\forall a \exists! B \forall x \; x \in B \longleftrightarrow x=a$

DIMOSTRAZIONE

Basta prendere $b=a$ nell'assioma □

<u>OSS</u> per estensionalità $\{a,b\} = \{b,a\}$

Def. La **coppia di Kuratowski** è
$$(a,b) \equiv \{\{a\},\{a,b\}\}$$

Proposizione $(a,b) = (a',b') \longleftrightarrow (a=a' \land b=b')$

DIMOSTRAZIONE

Fissiamo $C = (a,b) = (a',b')$

$x=a \longleftrightarrow \forall y \in C \;\; x \in y \longleftrightarrow \forall y \; (y=\{a\} \lor y=\{a,b\}) \longrightarrow x \in y$

Noto che $(A \lor B) \to C \equiv (A \to C) \land (B \to C)$, quindi diventa

$x=a \longleftrightarrow \forall y \; (y=\{a\} \longrightarrow x \in y) \land (y=\{a,b\} \longrightarrow x \in y) \overset{\text{paio}}{\longleftrightarrow} \forall y \; (x=a) \land (x=a \lor x=b)$

$\longleftrightarrow x=a$

Alla stessa maniera $x=a' \longleftrightarrow \forall y \in C \; x \in y \longleftrightarrow x=a$ ossia $a=a'$

Passiamo a b e b'. Supponiamo $b \neq a$ e $b' \neq a$

$x=b \longleftrightarrow x \neq a \land \exists y \in C \; x \in y \longleftrightarrow x \neq a \land (x \in \{a\} \lor x \in \{a,b\})$

$\longleftrightarrow x \neq a \land (x=a \lor (x=a \lor x=b)) \longleftrightarrow x=b$

Analogamente $x=b' \longleftrightarrow x \neq a \land \exists y \in C \; x \in y \longleftrightarrow x=b$ ossia $b=b'$

Mancano i casi $b=a, b' \neq a$; $b \neq a, b'=a$; $b=a, b'=a$

Basta considerare il primo caso : $b=a \;\; b' \neq a$

L'ipotesi è $(a,b) = (a',b')$, cioè $(a,a) = (a,b')$:

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

Ma $\{a,b'\} \in$

Infatti, se $\{a,b'\} \in \{\{a\}\} \xrightarrow{\text{paio}} \{a,b'\} = \{a\}$

$\ni b' \notin$

Altrimenti avrei $b' \in \{a\} \xrightarrow{\text{paio}} b' = a$ ↯ □

<u>NOTAZIONE</u> $(a,b,c) = ((a,b),c)$

$(a_1, a_2, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$

<u>OSS</u> $(a_1, \dots, a_n) = (a_1', \dots, a_n') \longleftrightarrow (a_1 = a_1' \land \dots \land a_n = a_n')$

⑤ **Assioma dell'unione**
$\forall A\ \exists B\ \forall x\quad x\in B \longleftrightarrow \exists y\in A\ \ x\in y$

Proposizione $\forall A\ \exists! B\ \forall x\quad x\in B \longleftrightarrow \exists y\in A\ \ x\in y$

DIMOSTRAZIONE
Per assurdo, siano B_1, B_2 due insiemi che soddisfano la proprietà.
Allora $x\in B_1 \longleftrightarrow \exists y\in A\ \ x\in y \longleftrightarrow x\in B_2$
Per estensionalità $B_1 = B_2$ □

NOTAZIONE $B=\bigcup A$ $\equiv \forall x\ \ x\in B \longleftrightarrow \exists y\in A\ \ x\in y$

esempio $A=\{\{1,2,3\},\emptyset,\{2,3,4\}\}$
$\Rightarrow \bigcup A=\{1,2,3,4\}$

operazioni elementari sugli insiemi

Def. $a\cup b := \bigcup\{a,b\}$ usando l'assioma del paio e dell'unione
Verifica $\forall x\ \ x\in a\cup b \longleftrightarrow x\in a \lor x\in b$
$\forall x\ \ x\in \bigcup\{a,b\} \xleftrightarrow{\text{unione}} \exists y\in\{a,b\}\ \ x\in y \xleftrightarrow{\text{paio}} \exists y\ (y=a \lor y=b)\land x\in y \longleftrightarrow x\in a \lor x\in b$

Def. Dato un insieme $A\neq\emptyset$, $x\in \bigcap A \longleftrightarrow \forall y\in A\ \ x\in y$
$A\neq\emptyset$ perché avremmo $\bigcap\emptyset = V$

Proposizione Data una classe non vuota $\mathcal{C}$, esiste un unico insieme B tale che
$\forall x\ \ x\in B \longleftrightarrow \forall y\in\mathcal{C}\ \ x\in y$

DIMOSTRAZIONE
Per ipotesi $\exists y\ \ y\in\mathcal{C}$. Fisso y_0 tale che $y_0\in\mathcal{C}$ e considero
$B=\{x\in y_0 \mid \forall y\in\mathcal{C}\ \ x\in y\}$ (esiste per estensionalità) □

Def. $a\cap b = \bigcap\{a,b\}$
Verifica $x\in a\cap b \longleftrightarrow (x\in a \land x\in b)$

Def. $a\setminus b = \{x\in a \mid x\notin b\}$ per separazione
$a\Delta b = (a\setminus b)\cup(b\setminus a)$

Proprietà:
- associatività: $(a\cup b)\cup c = a\cup(b\cup c) = a\cup b\cup c$ $\quad (a\cap b)\cap c = a\cap(b\cap c) = a\cap b\cap c$
  $(a\Delta b)\Delta c = a\Delta(b\Delta c) = a\Delta b\Delta c$
- distributività: $a\cup(b\cap c) = (a\cup b)\cap(a\cup c)$ $\quad a\cap(b\cup c) = (a\cap b)\cup(a\cap c)$
- leggi di De Morgan: $a\setminus(b\cup c) = (a\setminus b)\cap(a\setminus c)$ $\quad a\setminus(b\cap c) = (a\setminus b)\cup(a\setminus c)$
- $a_1\Delta\dots\Delta a_n = \{x \mid x$ appartiene a un numero dispari di $a_1,\dots,a_n\}$

Def. $\{a,b,c\} = \{a\}\cup\{b\}\cup\{c\}$
In generale $\{a_1,\dots,a_n\} = \{a_1\}\cup\dots\cup\{a_n\}$
Verifica $x\in\{a,b,c\} \longleftrightarrow (x=a \lor x=b \lor x=c)$

⑥ **Assioma dell'insieme potenza**
$\forall A\ \exists B\ \forall x\ x\in B \longleftrightarrow (\forall C\ C\in x \longrightarrow C\in A)$

<u>OSS</u> per estensionalità, B è unico
<u>NOTAZIONE</u> $B=\mathcal{P}(A)$ $\equiv$ $\forall x\ x\in B \longleftrightarrow (\forall y\ y\in x \longrightarrow y\in A)$

<u>OSS</u> $a\in A \wedge b\in B \longrightarrow (a,b)\in \mathcal{P}(\mathcal{P}(A\cup B))$
<u>Verifica</u> $a\in A\cup B,\ b\in A\cup B \longrightarrow \{a\}\subseteq A\cup B,\ \{a,b\}\subseteq A\cup B$
$\xrightarrow{\text{parti}} \{a\}\in\mathcal{P}(A\cup B),\ \{a,b\}\in\mathcal{P}(A\cup B) \longrightarrow \{\{a\},\{a,b\}\}\subseteq \mathcal{P}(A\cup B)$
$\xrightarrow{\text{parti}} \{\{a\},\{a,b\}\}\in\mathcal{P}(\mathcal{P}(A\cup B))$

DEF. $A\times B=\{x\in\mathcal{P}(\mathcal{P}(A\cup B)) \mid \exists a\in A\ \exists b\in B\ x=(a,b)\}$
<u>Verifica</u> $x\in A\times B \longleftrightarrow \exists a\in A\ \exists b\in B\ x=(a,b)$

DEF. Una **relazione binaria** tra A e B è un sottoinsieme di $A\times B$.
Data $R\subseteq A\times B$, possiamo scrivere xRy per $(x,y)\in A\times B$

DEF. $R\subseteq A\times A$ è una **relazione di equivalenza** se
(i) è **riflessiva**: $\forall x\in A\ \ xRx$
(ii) è **simmetrica**: $\forall x\in A\ \forall y\in A\ \ xRy \longrightarrow yRx$
(iii) è **transitiva**: $\forall x\in A\ \forall y\in A\ \forall z\in A\ \ (xRy \wedge yRz) \longrightarrow xRz$

DEF. $\leq\ \subseteq A\times A$ è una **relazione d'ordine** se
(i) è **riflessiva**: $\forall x\in A\ \ x\leq x$
(ii) è **antisimmetrica**: $\forall x\in A\ \forall y\in A\ \ (x\leq y \wedge y\leq x) \longrightarrow x=y$
(iii) è **transitiva**: $\forall x\in A\ \forall y\in A\ \forall z\in A\ \ (x\leq y \wedge y\leq z) \longrightarrow x\leq z$

DEF. $<\ \subseteq A\times A$ è una **relazione d'ordine stretto** se
(i) è **antiriflessiva**: $\forall x\in A\ \ \neg\, x<x$
(ii) è **asimmetrica**: $\forall x\in A\ \forall y\in A\ \ x<y \longrightarrow \neg\, y<x$
(iii) è **transitiva**: $\forall x\in A\ \forall y\in A\ \forall z\in A\ \ (x<y \wedge y<z) \longrightarrow x<z$

<u>NOTA</u> Non serve chiedere la proprietà asimmetrica
DIMOSTRAZIONE
Supponiamo $x<y$ e $y<x$
Per la transitività $x<x$ ↯ □

DEF. Una relazione d'ordine $R\subseteq A\times A$ si dice **totale** se
$\forall x,y\in A\ \ xRy \vee yRx$
Nel caso di R di ordine stretto, la totalità equivale alla tricotomia: $a<b \vee a=b \vee b<a$

<u>OSS</u> Sia $\leq$ di ordine largo.
Allora la relazione $< \ \equiv\ \leq \setminus \{x\in A\times A \mid \exists a\ x=(a,a)\} = \leq \setminus \Delta(A)$
$a<b \longleftrightarrow a\leq b \wedge a\neq b$ è di ordine stretto.
Sia $<$ di ordine stretto
Allora la relazione $\leq\ \equiv\ < \cup \{x\in A\times A \mid \exists a\ x=(a,a)\} = < \cup\ \Delta(A)$
$a\leq b \longleftrightarrow a<b \vee a=b$ è di ordine largo.
La corrispondenza è biunivoca.

Def. Data una relazione binaria $R \subseteq A \times B$, definiamo:

$\mathrm{Dom}(R) = \{x \in A \mid \exists y \in B \ (x,y) \in R\}$

$\mathrm{Im}(R) = \{y \in B \mid \exists x \in A \ (x,y) \in R\}$

Def. Una **funzione** $f: A \to B$ e' un sottoinsieme di $A \times B$ tale che

$\forall x \in A \ \exists! y \in B \ (x,y) \in f$

NOTAZIONE $\quad y = f(x) \equiv (x,y) \in f$

Def. Una funzione $f: A \longrightarrow B$ è:

(i) **iniettiva** se $\forall y \in \mathrm{Im}(f) \ \exists! x \ \ y = f(x)$

(ii) **suriettiva** se $\forall y \in B \ \exists x \in A \ \ y = f(x)$

(iii) **biunivoca** se è iniettiva e suriettiva

Def. Se $f: A \longrightarrow B$ è biunivoca

$f^{-1} = \{(y,x) \in B \times A \mid y = f(x)\}$

Def. Data $g: A \longrightarrow B$ e $f: B \longrightarrow C$, definiamo

$f \circ g = \{(x,y) \in A \times C \mid y = f(g(x))\}$

Numeri naturali

Vorremmo codificare n con un insieme di n elementi

$0 = \emptyset \quad 1 = \{\emptyset\} \quad 2 = \{0,1\} \quad 3 = \{0,1,2\} \quad \dots \quad n = \{0,1,\dots,n-1\}$

Def. $s(x) = x+1 \equiv x \cup \{x\}$

Def. S è un **insieme induttivo** se soddisfa

(i) $\emptyset \in S$

(ii) $\forall x \in S \quad s(x) \in S$

Assioma dell'infinito

$\exists X \quad \emptyset \in X \wedge \forall y \in X \quad y \cup \{y\} \in X$

Def. $\mathbb{N} = \omega$ è l'intersezione di tutti gli insiemi induttivi

$x \in \omega \longleftrightarrow \forall S \quad \emptyset \in S \wedge (y \in S \longrightarrow s(y) \in S) \longrightarrow x \in S$

Proposizione La definizione è ben posta

DIMOSTRAZIONE

Sia X induttivo (esiste per l'assioma dell'infinito)

$\omega := \{x \in X \mid \forall S \ \ S \text{ induttivo} \longrightarrow x \in S\}$ $\square$

Assiomi di Peano (al 2° ordine)

Dato un insieme $\mathbb{N}$, un elemento $0 \in \mathbb{N}$, e una funzione $succ : \mathbb{N} \longrightarrow \mathbb{N}$, diciamo che $(\mathbb{N}, 0, succ)$ soddisfa gli assiomi di Peano se:

P1 $\forall m,n \in \mathbb{N} \quad succ(m) = succ(n) \longrightarrow m = n$

P2 $\neg \exists x \in \mathbb{N} \quad 0 = succ(x)$

P3 Schema di induzione

Data una proprietà (formula) $\varphi(x)$

$$(\varphi(0) \wedge \forall n \ \varphi(n) \longrightarrow \varphi(succ(n))) \longrightarrow \forall n \ \varphi(n)$$

Teorema $(\omega, \emptyset, s)$ soddisfa gli assiomi di Peano

DIMOSTRAZIONE

P3: fissiamo φ e consideriamo

$X = \{n \in \omega \mid \varphi(n)\}$ (esiste per separazione)

Osserviamo che X è induttivo:

- $\emptyset \in X \longleftarrow \varphi(0)$
- $n \in X \rightarrow n+1 \in X \longleftarrow (\varphi(n) \longrightarrow \varphi(n+1))$

Di conseguenza, $\omega \subseteq X$ $(\omega = X)$, ossia $\forall n \in \omega$, $n \in X$, $\forall n \in \omega \ \varphi(n)$

P2: $\forall n \ n+1 \neq 0$ (equivale a $\nexists n \ n+1 = 0$)

$n+1 = n \cup \{n\} \ni n \longrightarrow n \cup \{n\} \neq \emptyset$

P1: $\forall m,n \in \mathbb{N} \quad m = n \longleftrightarrow m+1 = n+1$

$\longrightarrow$: immediata

$\longleftarrow$: $m+1 = n+1 \longrightarrow \bigcup m+1 = \bigcup n+1 \xrightarrow{\text{Lemma}} m = n$ $\square$

Lemma $\forall m \ \bigcup s(m) = m$

DIMOSTRAZIONE

Per induzione:

- $m = 0 \quad \bigcup m+1 = \bigcup \emptyset \cup \{\emptyset\} = \bigcup \{\emptyset\} = \emptyset = 0$
- $\bigcup m+1 = m \longrightarrow \bigcup (m+1)+1 = m+1$

$\bigcup (m+1)+1 = \bigcup m+1 \cup \{m+1\} = \bigcup m \cup \{m\} \cup \{m+1\} = \bigcup m \cup \{m\} \cup \{m \cup \{m\}\} =$
$= (\bigcup m \cup \{m\}) \cup (\bigcup \{m \cup \{m\}\}) = m \cup m \cup \{m\} = m \cup \{m\} = m+1$ $\square$

Proposizione $\forall n \in \mathbb{N} \quad n = 0 \longleftrightarrow \nexists m \quad n = s(m)$

DIMOSTRAZIONE

Equivalente, per P2, dobbiamo dimostrare: $n \neq 0 \longrightarrow \exists m \in \mathbb{N} \quad n = m+1$

Per induzione

- $n = 0$ vero perché $n \neq 0 \longrightarrow \dots \equiv F \longrightarrow \dots$ (ex falso quodlibet)
- $n+1 \quad (n \neq 0 \longrightarrow \exists m \in \mathbb{N} \ n = m+1) \longrightarrow (n+1 \neq 0 \longrightarrow \underbrace{\exists m \in \mathbb{N} \ n+1 = m+1}_{V}) \equiv \dots \longrightarrow V \equiv V$

$\square$

Corollario $succ : n \longmapsto n+1$ è una bigezione tra $\mathbb{N}$ e $\mathbb{N} \setminus \{0\}$

Def. $\forall m,n \in \mathbb{N} \quad m<n \longleftrightarrow m \in n$

<u>OSS</u> $m<n \longrightarrow m<s(n)$

$m<n \longrightarrow s(m)=n \ \vee \ s(m)<n$

<u>OSS</u> $m<n+1 \longleftrightarrow m<n \ \vee \ m=n$

DIMOSTRAZIONE

$m \in n+1 \longleftrightarrow m \in n \cup \{n\} \longleftrightarrow m \in n \vee m \in \{n\} \longleftrightarrow m<n \ \vee \ m=n \ \square$

Teorema $<$ è una relazione d'ordine totale

DIMOSTRAZIONE

(iii) transitività: $\forall a,b,c \in \mathbb{N} \quad a<b \wedge b<c \longrightarrow a<c$

Per induzione su c:

- $c=0 \quad a<b \wedge b<0 \longrightarrow a<0$

  $b \in \emptyset \qquad a \in \emptyset \equiv F \longrightarrow F \equiv V$

- $((a<b \wedge b<c) \longrightarrow a<c) \longrightarrow ((a<b \wedge b<c+1) \longrightarrow a<c+1) \equiv \qquad A\rightarrow(B\rightarrow C)\equiv(A\wedge B)\rightarrow C$

  $\equiv (((\underline{a<b \wedge \underset{*}{b<c}}) \longrightarrow a<c) \wedge (\underset{\circ}{\underline{a<b}} \wedge b<c+1)) \longrightarrow a<c+1$

  $b<c+1 \longrightarrow b<c \ \vee \ b=c$

  Se $b<c$, per l'ip. induttiva $\xrightarrow{*} a<c \longrightarrow a \in c \subseteq c\cup\{c\} \longrightarrow a<c+1$

  Se $b=c \xrightarrow{\circ} a<c \longrightarrow a \in c \subseteq c\cup\{c\} \longrightarrow a \in c+1 \longrightarrow a<c+1$

(i) antiriflessività: $\forall a \in \mathbb{N} \quad \neg a<a$

Induzione su a

- $a=0 \qquad \neg 0<0 \longleftarrow \neg \emptyset \in \emptyset$
- $(\neg a<a) \longrightarrow (\neg a+1<a+1)$

  Assumiamo per assurdo che $a+1<a+1$

  Per l'oss. si hanno 2 casi: $a+1<a \longrightarrow a \in a+1 \in a \longrightarrow a<a$ ↯

  $a+1=a \longrightarrow a \in a+1=a \longrightarrow a<a$ ↯

Resta da dimostrare che $\forall a,b \in \mathbb{N} \quad a<b \vee a=b \vee b<a$

Per induzione su b (è simmetrica)

- $b=0 \quad \forall a \quad a<0 \vee a=0 \vee 0<a \longleftrightarrow \forall a \quad a=0 \vee 0<a$

  Per induzione su a

  - $a=0 \quad$ ovvio
  - $(a=0 \vee 0<a) \longrightarrow (\overset{F}{a+1=0} \vee 0<a+1)$

    Se $a=0 \longrightarrow a+1 = 0\cup\{0\} = \{\emptyset\} \ni 0$

    Se $0 \in a \longrightarrow 0 \in a \subseteq a\cup\{a\} \longrightarrow 0 \in a+1 \longrightarrow 0<a+1$

- $(\underset{①}{a<b} \vee \underset{②}{a=b} \vee \underset{③}{b<a}) \longrightarrow (a<b+1 \vee a=b+1 \vee b+1<a)$

  ① $a<b \longrightarrow a<b<b+1 \longrightarrow a<b+1$

  ② $a=b \longrightarrow a=b<b+1 \longrightarrow a<b+1$

  ③ Dobbiamo dimostrare. $b<a \longrightarrow a=b+1 \vee b+1<a$

  Induzione su a:

  - $a=0 \qquad b<0 \longrightarrow \dots \equiv F \longrightarrow \dots \equiv V$
  - $(b<a \longrightarrow a=b+1 \vee b+1<a) \longrightarrow (b<a+1 \longrightarrow a+1=b+1 \vee b+1<a+1)$

    $\equiv ((b<a \longrightarrow a=b+1 \vee b+1<a) \wedge \underline{b<a+1}) \longrightarrow a+1=b+1 \vee b+1<a+1$

    Si hanno quindi 2 casi: se $b<a \longrightarrow b+1=a<a+1 \longrightarrow b+1<a+1$

    $\searrow b+1<a<a+1 \longrightarrow b+1<a+1$

    se $b=a \longrightarrow b+1=a+1$ $\square$

corollario $\forall n \in \mathbb{N}$, $n = \{a \in \mathbb{N} \mid a < n\}$

DIMOSTRAZIONE

Sappiamo che $a \in \mathbb{N} \to (a < n \leftrightarrow a \in n)$

Manca da dimostrare che $a \in n \to a \in \mathbb{N}$

Per induzione su a:

- $a = 0 \in n \to 0 \in \mathbb{N}$
- $(a \in n \to a \in \mathbb{N}) \to (a+1 \in n \to a+1 \in \mathbb{N}) \equiv ((a \in n \to a \in \mathbb{N}) \wedge a+1 \in n) \to a+1 \in \mathbb{N}$

  $a+1 \in n \leftrightarrow a \cup \{a\} \in n \to a \in n \to$ per ipotesi $a \in \mathbb{N}$

  $\to$ per P2 $a+1 \in \mathbb{N}$ $\square$

corollario $\forall a, b \in \mathbb{N}$ $a \leq b \leftrightarrow a \subseteq b$

Principio di induzione (forma forte)

Sia $\varphi(x)$ una proprietà, allora

$(\forall n \in \mathbb{N}\ (\forall m < n\ \varphi(m)) \to \varphi(n)) \to \forall n\ \varphi(n)$

DIMOSTRAZIONE

Consideriamo $\psi(n) \equiv \forall m < n\ \varphi(m)$

Dimostriamo $\forall n\ \psi(n)$ per induzione

- $n = 0$: $\forall m < 0\ \varphi(m)$ vera a vuoto
- $\underbrace{\forall m < n\ \varphi(m)}_{\downarrow \text{hp.}\ \varphi(n)} \to \forall m < n+1\ \varphi(m) \equiv \forall m\ (m < n \vee m = n)\ \varphi(m)$

  se $m < n$, $\varphi(n)$ immediato

  se $m = n$, ho $\varphi(n)$ per l'ipotesi

In conclusione $\forall n\ \psi(n)$, ossia $\forall n\ \forall m < n\ \varphi(m)$

Osserviamo che $\psi(n+1) \to \varphi(n) \to \forall n\ \varphi(n)$ $\square$

Principio del minimo

Sia $A \subseteq \omega$. Se $A \neq \emptyset$, allora $\exists n \in A\ \forall x \in A\ n \leq x$

DIMOSTRAZIONE

Consideriamo la contronominale: A non ha minimo $\to A = \emptyset$

Assumiamo quindi $\forall n \in A\ \exists x \in A\ x < n$. Dobbiamo mostrare che $\forall n \in \omega, n \notin A$

Per induzione forte $(\forall x < n\ x \notin A) \to n \notin A$

$\equiv (\neg \exists x < n\ x \in A) \to n \notin A \equiv (\neg \exists x \in A\ x < n) \to n \notin A \equiv n \in A \to \exists x \in A\ x < n$ $\square$

DEF. Un insieme totalmente ordinato $(A, \leq)$ si dice **bene ordinato** se
$\forall B \subseteq A, B \neq \emptyset \longrightarrow \exists x \in B \ \forall y \in B \ x \leq y$

Proposizione $(\omega, \leq)$ è bene ordinato

DIMOSTRAZIONE
Dobbiamo mostrare che: $B \subseteq \omega$ non ha un minimo $\longrightarrow B = \emptyset$
Consideriamo $C = \omega \setminus B$. Vogliamo mostrare $C = \omega$
Per il principio di induzione forte, ci basta $(\forall x < n \ x \in C) \longrightarrow n \in C$
ossia $(\forall x < n \ x \notin B) \longrightarrow n \in C$
Quindi se $n \in B$, n è il minimo di B, ma B non ha minimo
$\longrightarrow n \notin B \longrightarrow B = \emptyset$ □

esempio
- ω
- se A è bene ordinato da $<$ e $B \subseteq A$, allora B è bene ordinato da $<$
- tutti gli $n \in \omega$ sono bene ordinati da $\in$
- $\omega \cup \{\omega\} = \omega + 1$ è bene ordinato da $\in$ $\quad 0 < 1 < 2 \ \dots < \omega$
- $\omega \cup \{\omega\} \cup \{\omega \cup \{\omega\}\} = (\omega+1)+1$ è bene ordinato da $\in$
- se α è bene ordinato da $\in$, allora $\alpha \cup \{\alpha\} = \alpha + 1$ è bene ordinato da $\in$

operazioni aritmetiche

OSS ESTENSIONALITA' per le FUNZIONI
Date $f, g : A \longrightarrow B$,
$$f = g \longleftrightarrow \forall x \in A \ \ f(x) = g(x)$$
DIMOSTRAZIONE
$$(x,y) \in f \longleftrightarrow y = f(x) \longleftrightarrow y = g(x) \longleftrightarrow (x,y) \in g \quad \square$$

NOTAZIONE Indichiamo con B^A o ${}^A B$ l'insieme delle funzioni da A a B, che esiste per separazione in $\mathcal{P}(A \times B)$

Teorema di ricorsione numerabile (1° forma)
Dato un insieme S, un elemento $c \in S$ e una funzione $h : \omega \times S \longrightarrow S$, esiste un'unica funzione $f : \omega \longrightarrow S$ tale che
$f(0) = c$ e $f(n+1) = h(n, f(n)) \ \forall n \in \omega$

DIMOSTRAZIONE
Vogliamo trovare una formula $\varphi(n,y)$ che dice "$y = f(n)$" poi costruiamo $f = \{(n,y) \in \omega \times S \mid \varphi(n,y)\}$
DEF. Sia $g : n+1 \longrightarrow S$. Diciamo che g è una **n-approssimazione** se
$g(0) = c$ e $\forall x < n \ \ g(x+1) = h(x, g(x))$
$y = f(n) \longleftrightarrow \varphi(n,y) \equiv$ "esiste una n-approssimazione g t.c. $y = g(n)$"
Dimostriamo che: ① $\forall n \ \exists$ una n-appross. ② $\forall n \ \exists!$ una n-appross. $\Big\}$ $\forall n \ \exists! y \ \ \varphi(n,y)$ quindi f è ben definita
③ la funzione f soddisfa la richiesta ed è unica

① Per induzione:
- $n = 0$: $\{(0,c)\}$ è una 0-approssimazione
- sia g una n-appr., allora $g \cup \{(n+1, h(n, g(n)))\}$ è una n+1 appr.

② Siano g_1 e g_2 due n-approssimazioni, allora $g_1 = g_2$
Per induzione su n:
- $n=0$ $\{(0,c)\}$ è l'unica 0-appr.
- se g_1, g_2 sono due n-appr., allora $g_1 = g_2$
  Le n+1-appr. sono $g_1 \cup \{(n+1, h(n, g_1(n)))\}$ e $\overset{g_1}{\overset{\parallel}{g_2}} \cup \{(n+1, h(n, \overset{g_1(n)}{\overset{\parallel}{g_2(n)}}))\}$
  Per estensionalità, sono uguali.

③ Per induzione su n:
- $n=0$: $f = \{(0,c)\} \longleftrightarrow f(0)=c$
- la n+1-appr è $f \cup \{(n+1, h(n, f(n)))\}$
  f soddisfa per ipotesi induttiva
  $(n+1, h(n, f(n))) \longleftrightarrow f(n+1) = h(n, f(n))$

L'unicità di f segue facilmente per induzione
Date f' e f" che soddisfano la ricorsione, allora:
$f'(\emptyset) = c = f''(\emptyset)$ e $f'(s(n)) = h(n, f'(n)) \overset{\text{ip. ind.}}{=} h(n, f''(n)) = f''(s(n))$ □

esempio $\begin{cases} a+0 = a \\ a+s(b) = s(a+b) \end{cases}$ $\begin{cases} a\cdot 0 = 0 \\ a\cdot s(b) = a\cdot b + a \end{cases}$ $\begin{cases} a^0 = 1 \\ a^{s(b)} = a^b \cdot a \end{cases}$

esempio Definizione di $+ . \omega \times \omega \longrightarrow \omega$
$+ := \{((x,y),z) \in (\omega\times\omega)\times\omega \mid \underset{\text{“}x+y=z\text{”}}{\varphi(x,y,z)}\}$

$\varphi(x,y,z) \equiv \exists f \in {}^{\omega}\omega : (f(0)=x) \wedge (\forall b \in \omega \; f(s(b)) = s(f(b))) \wedge (f(y) = z)$

Teorema Supponiamo che $(A, 0_A, succ_A)$ soddisfi gli assiomi di Peano.
Allora $(A, 0_A, succ_A) \cong (\omega, 0, s)$, ossia che $\exists f : \omega \longrightarrow A$ biunivoca t.c. $(f(0) = 0_A) \wedge (\forall n \in \omega : f(s(n)) = succ_A(f(n)))$.

DIMOSTRAZIONE
Per il th. di ricorsione numerabile $\exists! f$ che soddisfi le condizioni.
Bisogna dimostrare che f è biunivoca.
(1) f è surgettiva, ossia che $\forall y \in A \; \exists x \in \omega \; f(x) = y$
Per induzione in A su y:
- $y = 0_A$ $\quad 0_A = f(0)$
- $y = succ_A(y')$, $\quad f(x') = y'$ (hp. induttiva)
  $f(s(x')) = succ_A\, f(x') = succ_A\, y' = y$

(2) f è iniettiva
Considero x minimo t.c. $\exists y.\, y \neq x \wedge f(x) = f(y)$ (da cui $y > x$)
- se $x=0$ $\quad f(y) = 0_A = f(x)$
  ma $f(y) = 0_A$ se $y=0$ $\vee$ $f(y) = succ_A(f(y'))$ se $y = s(y')$
  Se $y \neq x$, non siamo in nessuno dei due casi (0 non è un successore e $y \neq x = 0$) ↯
- se $x = s(x')$: $succ_A\, f(x') = f(s(x')) = f(x) = f(y) = f(s(y')) = succ_A\, f(y')$
  Da questo segue $f(x') = f(y')$ ($succ_A$ è iniettiva),
  ma d'altra parte $s(x') \neq s(y') \Rightarrow x' \neq y'$ ASSURDO per la minimalità ↯ □

OSS Dato $x \in \omega$, o $x = 0$ o $\exists y \in \omega$ t.c. $x = S(y)$

DIMOSTRAZIONE

Per induzione su x:

- $x = 0$ ✓
- $x = S(n)$ ✓ □

OSS $\forall n \in \omega$ $\quad \underset{\text{Peano}}{n+1} = \underset{\text{funzione }+}{n+1}$

DIMOSTRAZIONE $n+1 = (n+0) +_p 1 = n +_p 1$

NOTAZIONE Indichiamo con $1 = 0+1$, $2 = 1+1$, $3 = 2+1$, ...

Teorema di ricorsione numerabile (2° forma)

Data $h : \bigcup_{n \in \omega} {}^n A \longrightarrow A$, esiste un'unica $f : \omega \longrightarrow A$ t.c. $\forall n \in \omega$ $f(n) = h(f|_n)$

DIMOSTRAZIONE

Definisco f' per ricorsione numerabile (1° forma):

$$f' : \omega \longrightarrow \bigcup_{n \in \omega} {}^n A \quad \text{t.c.} \quad f'(\emptyset) = \emptyset$$

$$f'(S(n)) = f'(n) \cup \{(n, h(f'(n)))\}$$

Ora poniamo $f(n) = f'(S(n))(n)$

Verifichiamo ora per induzione che $\forall n \in \omega$ $f|_n = f'(n)$

- $n = 0$ immediato
- $n = S(m)$. $f|_{S(m)} = f|_m \cup \{(m, f(m))\} \overset{\text{hp. ind}}{=} f'(m) \cup \{(m, f'(S(m))(m))\} =$
$= f'(m) \cup \{(m, h(f'(m)))\} = f'(S(m))$ □

OSS La notazione $\bigcup_{n \in \omega} {}^n \omega$ è impropria, ma l'insieme può essere ottenuto per separazione in $\mathcal{P}(\omega \times A)$

CARDINALITÀ

DEF. Due insiemi A e B hanno la stessa **cardinalità**, o sono **equipotenti**, $|A| = |B|$
se esiste una corrispondenza biunivoca $f: A \longrightarrow B$

DEF. $|A| \leq |B|$ se $\exists\, B' \subset B$ tale che $|A| = |B'|$
Equivalentemente : $\exists\, g: A \longrightarrow B$ iniettiva

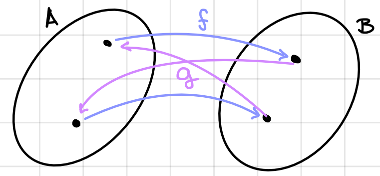
OSS la $|\ | = |\ |$ soddisfa le condizioni di una relazione di equivalenza :
- riflessività : $|A| = |A|$
- simmetria : $|A| = |B| \longrightarrow |B| = |A|$
- transitività : $|A| = |B| \wedge |B| = |C| \longrightarrow |A| = |C|$

OSS la $|\ | \leq |\ |$ è :
- riflessiva : $|A| \leq |A|$
- compatibile con $|\ | = |\ |$: $|A| \leq |B| \wedge |B| = |C| \longrightarrow |A| \leq |C|$
  $|A| = |B| \wedge |B| \leq |C| \longrightarrow |A| \leq |C|$
- transitiva : $|A| \leq |B| \wedge |B| \leq |C| \longrightarrow |A| \leq |C|$

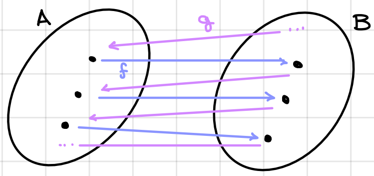
NOTAZIONE Data $f: A \longrightarrow B$ e $C \subseteq A$
$$f[C] = \{ y \in B \mid \exists x \in C \ \ y = f(x) \} = \{ f(x) \mid x \in C \}$$

Teorema di Cantor-Bernstein-Schröder
$|A| \leq |B| \wedge |B| \leq |A| \longrightarrow |A| = |B|$
ossia $\exists f: A \rightarrow B$ iniettiva $\wedge\ \exists g: B \rightarrow A$ iniettiva $\longrightarrow \exists h: A \rightarrow B$ biunivoca

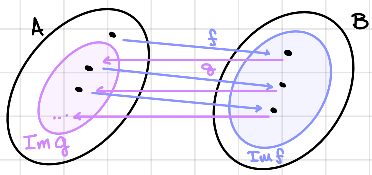
DIMOSTRAZIONE (idea)

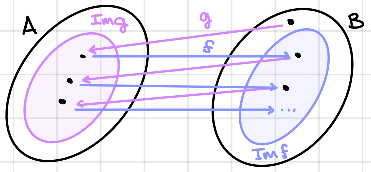


percorso circolare



percorso illimitato in avanti e indietro





percorsi illimitati in avanti ma non indietro

DIMOSTRAZIONE

Siano $f: A \longrightarrow B$ iniettiva , $g: B \longrightarrow A$ iniettiva
Sia $B_0 = B \setminus f[A]$
Sia $A_i = g[B_i]$, $B_{s(i)} = f[A_i]$
$$\begin{bmatrix} \omega \longrightarrow \mathcal{P}(A) \times \mathcal{P}(B) \\ i \longmapsto (A_i, B_i) \end{bmatrix}$$
Definiamo $A_* = \bigcup_{i \in \omega} A_i \qquad B_* = \bigcup_{i \in \omega} B_i$

Siano: $h: A \longrightarrow B$
$$a \longmapsto \begin{cases} f(a) & \text{se } a \notin A_* \\ g^{-1}(a) & \text{se } a \in A_* \end{cases}$$

$k: B \longrightarrow A$ "$k = h^{-1}$"
$$b \longmapsto \begin{cases} f^{-1}(b) & \text{se } b \notin B_* \\ g(b) & \text{se } b \in B_* \end{cases}$$

$h(k(b)) \overset{?}{=} b$

- supponiamo $b \notin B_*$: allora $h(k(b)) = h(f^{-1}(b))$
  se per assurdo $f^{-1}(b) \in A_* \Rightarrow f^{-1}(b) \in A_i \Rightarrow f(f^{-1}(b)) \in B_{s(i)}$ per definizione,
  quindi $b \in B_{s(i)}$, ossia $b \in B_*$, assurdo $\lightning$
  Dunque $f^{-1}(b) \notin A_* \Rightarrow h(f^{-1}(b)) = f(f^{-1}(b)) = b$
- se invece $b \in B_*$, $h(k(b)) = h(g(b)) \underset{\substack{\uparrow \\ g(b) \in A_*}}{=} g^{-1}(g(b)) = b$

Analogamente $k(h(a)) = a$ $\square$

corollario $|\ \ | \leq |\ \ |$ è un ordine (non necessariamente totale)

$|A| \Uparrow |B|$
$\underbrace{< \ = \ > \ \perp}$ → si esclude solo con l'assioma di scelta

Def. $|A| < |B| \equiv |A| \leq |B| \wedge |A| \neq |B|$

Teorema di Cantor
$|A| < |\mathcal{P}(A)|$

DIMOSTRAZIONE
Dobbiamo dimostrare che non esiste una $f: A \longrightarrow \mathcal{P}(A)$ biunivoca
Notiamo $A \hookrightarrow \mathcal{P}(A)$: $a \longmapsto \{a\}$ iniettiva
quindi $|A| \leq |\mathcal{P}(A)|$
Suppongo, per assurdo, che $\exists f$ biunivoca.
Considero $\{x \in A \mid x \notin f(x)\} = N \in \mathcal{P}(A)$
Supponiamo che $N = f(n)$. Avrei che
$n \in N \longleftrightarrow n \in f(n) \longleftrightarrow n \notin N$ per definizione. $\lightning$ $\square$

Def. $|A| + |B| = |A \times \{0\} \cup B \times \{1\}| \equiv |A \sqcup B|$
$|A| + |B| = |C| \equiv \exists f: A \sqcup B \longrightarrow C$ biunivoca
$|A| \cdot |B| = |A \times B|$
$|A|^{|B|} = |{}^{B}A|$

<u>oss</u> la definizione è ben data
Dati $|A| = |A'|$ $|B| = |B'|$:
$|A \sqcup B| = |A' \sqcup B'|$, $|A \times B| = |A' \times B'|$, $|{}^{A}B| = |{}^{A'}B'|$

DIMOSTRAZIONE
Fissate $f: A \to A'$, $g: B \longrightarrow B'$ bigezioni, abbiamo

$A \sqcup B \longrightarrow A' \sqcup B'$
$(a,0) \longmapsto (f(a),0)$
$(b,1) \longmapsto (g(b),1)$

$A \times B \longrightarrow A' \times B'$
$(a,b) \longmapsto (f(a),g(b))$

${}^{B}A \longrightarrow {}^{B'}A'$
$h \longmapsto f \circ h \circ g^{-1}$

$\square$

NOTAZIONE (abuso) Se non ci si confonde, per $n \in \omega$, scriviamo n al posto di $|n|$

Ad es. $2+4=6$ $\quad (|2|+|4|=|6|)$

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

DIMOSTRAZIONE

$$2^{|A|} = |{}^{A}2| = |{}^{A}\{0,1\}|$$

$$\mathcal{P}(A) \longrightarrow {}^{A}\{0,1\}$$

$$S \longmapsto \chi_S(x) = \begin{cases} 1 & \text{se } x\in S \\ 0 & \text{se } x\notin S \end{cases}$$

$\square$

corollario $|A| < 2^{|A|}$

proposizione Dati A, B, C con $|B| \leq |C|$:

$|A|+|B| \leq |A|+|C| \qquad |A|^{|B|} \leq |A|^{|C|}$

$|A|\ |B| \leq |A| \cdot |C| \qquad |B|^{|A|} \leq |C|^{|A|}$

DIMOSTRAZIONE

Sia $f: B \to C$ iniettiva, con $|B| = |B'|$ dove $B' = f[B]$

Ora $B' \subseteq C \longrightarrow A \times \{0\} \cup B' \times \{1\} \subseteq A \times \{0\} \cup C \times \{1\}$

$\longrightarrow |A \times \{0\} \cup B' \times \{1\}| \leq |A \times \{0\} \cup C \times \{1\}|$

$\longrightarrow |A| + |B'| \leq |A| + |C|$

Le altre sono analoghe.

$\square$

proposizione Scrivendo α, β, γ per $|A|, |B|, |C|$

$\alpha + 0 = \alpha$	$\alpha + \beta = \beta + \alpha$	$(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$
$\alpha \cdot 0 = 0$	$\alpha \cdot \beta = \beta \cdot \alpha$	$(\alpha\cdot\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$
$\alpha \cdot 1 = \alpha$	$\alpha + (\beta+\gamma) = (\alpha+\beta)+\gamma$	$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
$\alpha^0 = 1$	$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$	
$\alpha^1 = \alpha$	$\alpha(\beta+\gamma) = \alpha\cdot\beta + \alpha\cdot\gamma$	
$1^\alpha = 1$	$(\alpha+\beta)\cdot\gamma = \alpha\cdot\gamma + \beta\cdot\gamma$	

DIMOSTRAZIONE

$$|A|^{|B|+|C|} = |A|^{|B|} \cdot |A|^{|C|}$$

$${}^{B\cup C}A \longrightarrow {}^{B}A \times {}^{C}A$$

$$f \longmapsto (g,h) \quad \text{con} \quad g(b) = f((b,0)),\ h(c) = f((c,1))$$

Per l'inversa: $f((\alpha,\beta)) = \begin{cases} g(\alpha) & \text{se } \beta=0 \\ h(\alpha) & \text{se } \beta=1 \end{cases}$

$\square$

cardinalità finite

Def. A è **finito** se $\exists n \in \omega \quad |A| = |n|$

Def. A è **Dedekind-finito** se
$\neg \exists B \subsetneq A \quad |A| = |B|$

Proposizione (principio dei cassetti) FINITO $\longrightarrow$ DEDEKIND-FINITO
Un insieme finito non è in corrispondenza biunivoca con un suo sottoinsieme proprio

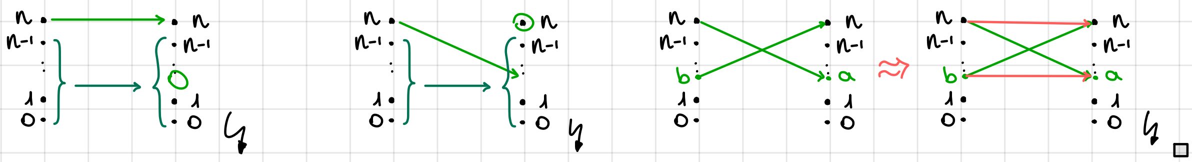
DIMOSTRAZIONE

Ci basta dimostrare che dato $n \in \omega$ qualunque, n è Dedekind-finito

Perché dato un insieme finito A, $|A| = |n|$
$\exists f : A \longrightarrow n$ biunivoca

Supponiamo che esista $B \subsetneq A$ con $|B| = |A|$
allora esiste $g : A \longrightarrow B$ biunivoca
$f \circ g \circ f^{-1} : n \longrightarrow f[B] \subsetneq n$ biunivoca

Procediamo per induzione su n:
- 0 è Dedekind-finito
- Supponiamo che n sia D-finito
Dobbiamo dimostrare che $s(n)$ è D-finito.
Per assurdo, supponiamo $f : s(n) \longrightarrow B \subsetneq s(n)$ biunivoca



corollario Se A è finito, allora $\exists! n \quad |A| = |n|$

DIMOSTRAZIONE

Per assurdo, $|n| = |A| = |m|$
Senza perdita di generalità $n < m \Rightarrow n \subsetneq m$ ↯ □

<u>OSS</u> Se esiste $f : \omega \longrightarrow A$ iniettiva,
allora A non è D-finito (e in particolare non è finito)

DIMOSTRAZIONE

$$g : A \longrightarrow A \setminus \{f(0)\}$$
$$a \longmapsto \begin{cases} f(s(f^{-1}(a))) & \text{se } a \in f[\omega] \\ a & \text{altrimenti} \end{cases}$$

è biunivoca □

Proposizione Sia A infinito, allora $\forall n \in \omega \quad |n| < |A|$

DIMOSTRAZIONE

L'uguaglianza non può valere

Devo dimostrare che $\forall n \in \omega \quad \exists f \in {}^nA$ iniettiva

Per induzione su n:

- $n = 0 \quad f = \emptyset$
- Data $f : n \longrightarrow A$ iniettiva, cerco $f' : s(n) \longrightarrow A$ iniettiva

  Siccome A è infinito, f non è sorgettiva, quindi

  $\exists x \in A \setminus \operatorname{Im} f$

  Definisco $f' = f \cup \{(n,x)\}$ $\square$

Lemma $|n| + |1| = |s(n)|$

DIMOSTRAZIONE

$$n \times \{0\} \cup \{(0,1)\} \longrightarrow n \cup \{n\}$$

$$(\alpha, \beta) \longmapsto \begin{cases} \alpha & \text{se } \beta = 0 \\ n & \text{se } \beta = 1 \end{cases} \quad \square$$

Proposizione Dati $m, n \in \omega$

$|m| + |n| = |m+n| \qquad |m| \cdot |n| = |m \cdot n|$

$|m|^{|n|} = |m^n|$

DIMOSTRAZIONE

$|m+n| = |m| + |n|$ Per induzione su n

- $n = 0$: $\underbrace{|m| + |0|}_{|m|} = |\underbrace{m+0}_{m}|$
- $s(n)$: $|m| + |s(n)| \overset{\text{lemma}}{=} |m| + (|n| + |1|) = (|m| + |n|) + |1| \overset{\text{hp. ind.}}{=}$

  $= |m+n| + |1| \overset{\text{lemma}}{=} |s(m+n)| = |m + s(n)|$

$|m \cdot n| = |m| \cdot |n|$ Per induzione su n:

- $n = 0$. $|m \cdot 0| = 0 = |m| \cdot 0$
- $s(n)$: $|m| \cdot |s(n)| \overset{\text{lemma}}{=} |m| \cdot (|n| + |1|) = |m| \cdot |n| + |m| \overset{\text{hp.ind}}{=} |m \cdot n| + |m| \overset{+}{=} |m \cdot n + m| = |m \cdot s(n)|$

$|m|^{|n|} = |m^n|$ Per induzione su n:

- $n = 0$: $|m|^0 = 1 = |m^0|$
- $s(n)$: $|m|^{|s(n)|} \overset{\text{lemma}}{=} |m|^{|n|+|1|} = |m|^{|n|} \cdot |m| \overset{\text{hp.ind}}{=} |m^n| \cdot |m| \overset{\cdot}{=} |m^n \cdot m| = |m^{s(n)}|$ $\square$

esercizio Dimostrare che si può fare la sottrazione $(m > n)$

cardinalità del numerabile $\aleph_0$

Def. Diciamo che A è al più numerabile se $|A| \leq |\omega|$
e A è numerabile se $|A| = |\omega|$
Si pone $|\omega| = \aleph_0$

Def. $(A, <_A) \sim (B, <_B)$ sono isomorfi se e solo se
$\exists f: A \to B$ biunivoca t.c. $\forall x, y \quad x <_A y \longleftrightarrow f(x) <_B f(y)$

OSS Due ordini totali $(A, <_A)$ $(B, <_B)$ sono isomorfi
se e solo se $\exists f: A \to B$ biunivoca t.c. $\forall x, y \quad x <_A y \longrightarrow f(x) <_B f(y)$ (f è crescente)

DIMOSTRAZIONE

Suppongo $f(x) <_B f(y)$ e considero x, y.
Per la totalità dell'ordine su A:

$$x < y \longrightarrow f(x) <_B f(y)$$
$$x = y \longrightarrow f(x) = f(y) \quad \text{↯}$$
$$x > y \longrightarrow f(x) >_B f(y) \quad \text{↯} \quad \square$$

OSS Sia $|A| = n$ con $n \in \omega$ e sia $<_A$ un ordine totale su A.
Allora $(A, <_A) \sim (n, \in)$

DIMOSTRAZIONE

Per induzione su n
- $n = 0 \quad A = \emptyset \longrightarrow (\emptyset, <_A) \sim (\emptyset, \in)$
- $n = s(m)$, $|A| = s(m)$

  Consideriamo un elemento $a \in A$. Allora $|A \setminus \{a\}| = m$
  Quindi per ipotesi induttiva $(A \setminus \{a\}, <_A) \sim (n, \in)$ e ha un massimo.
  Considero il più grande fra questo e a: ho così il massimo di A, μ
  Ora $(A \setminus \{\mu\}, <_A) \sim (n, \in)$. Fisso l'isomorfismo f:
  Costruisco

$$A \longrightarrow s(m)$$
$$x \longmapsto \begin{cases} f(x) & \text{se } x \neq \mu \\ m & \text{se } x = \mu \end{cases}$$

$\square$

OSS L'ordine $(\omega, <)$ soddisfa le seguenti proprietà:
(1) è un buon ordine
(2) è illimitato (superiormente): $\forall x \in \omega \; \exists y \in \omega \quad x < y$
(3) ogni $A \subseteq \omega$ superiormente limitato e non vuoto ha un massimo

DIMOSTRAZIONE

(1) è conseguenza del principio del minimo ; per (2) basta considerare $s(n)$
(3) $A \subseteq \omega$ sup lim $\longrightarrow \exists n \; \forall a \in A \quad a \overset{\in}{<} n \longrightarrow \exists n \; A \subseteq n \longrightarrow A$ ha massimo $\square$

Lemma Sia $f: \omega \longrightarrow A$, insieme ordinato, t.c. $\forall n \in \omega \; f(n) < f(s(n))$ allora f è crescente $\forall m < n \in \omega \; f(m) < f(n)$

DIMOSTRAZIONE

Per induzione su n

- $n = 0$ vero a vuoto
- $s(n)$: $\forall m < s(n) \; f(m) < f(s(n))$ assumendo $\forall m < n \; f(m) < f(n)$

$m < s(n) \longrightarrow m = n \vee m < n$: se $m < n$ $f(m) \overset{\text{hp.ind}}{<} f(n) \overset{\text{hp}}{<} f(s(n))$

se $m = n$ $f(m) = f(n) \overset{\text{hp}}{<} f(s(n))$ $\square$

Proposizione Se un ordine totale $(A, <)$ soddisfa (1), (2), (3), $(A, <_A) \sim (\omega, <)$

DIMOSTRAZIONE

Costruisco $f: \omega \longrightarrow A$

$0 \longmapsto \min_{<_A} A$

$s(n) \longmapsto \min_{<_A} \{x \in A \mid f(n) < x\}$ (teorema di ricorsione – 1° f)

- f è ben definita perché $\{x \in A \mid f(n) < x\} \neq \emptyset$ per (2) e quindi ha un minimo per (1)
- f è crescente
  Per il lemma, ci basta $f(n) < f(s(n))$, vero per costruzione
  $\Longrightarrow f$ è iniettiva
- f è surgettiva
  Per assurdo, se non è così, sia $x \in A \setminus \operatorname{Im} f$ minimo
  Se $\forall n \in \omega \; f(n) < x \Longrightarrow \operatorname{Im} f$ è sup lim. e non ha massimo ↯
  Se $\exists n \in \omega \; x < f(n)$
  Considero $m \in \omega$ massimo t.c. $f(m) < x$
  Considero $f(s(m)) = x$ ↯ $\square$

Teorema Se A è al più numerabile, allora o A è finito o A è numerabile
$|A| \leq \aleph_0 \longrightarrow |A| = \aleph_0 \vee \exists n \in \omega \; |A| = n$

DIMOSTRAZIONE

$\exists \; f: A \longrightarrow \omega$ iniettiva

Sia $B = f[A]$. Chiaramente $|A| = |B|$

Ci basta dimostrare che se $B \subseteq \omega$ allora B è finito o numerabile.

Supponiamo che B non sia finito e constatiamo che soddisfa (1), (2), (3) con l'ordine indotto da ω $\square$

Lemma $|A \cup B| \leq |A| + |B|$

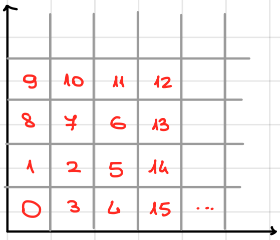
DIMOSTRAZIONE

$$f: A \cup B \longrightarrow A \sqcup B$$
$$x \longmapsto \begin{cases} (x, 0) & \text{se } x \in A \\ (x, 1) & \text{se } x \in B \setminus A \end{cases}$$

f è iniettiva $\square$

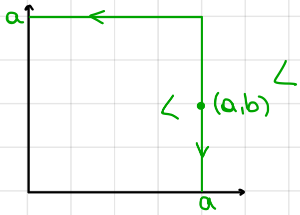
Lemma $\aleph_0 \cdot \aleph_0 = \aleph_0$

DIMOSTRAZIONI ALTERNATIVE



$$f : \omega \times \omega \longrightarrow \omega$$
$$(a,b) \longmapsto 2^a(2b+1)-1$$

DIMOSTRAZIONE



$$(a,b) < (a',b') \equiv \begin{cases} \max(a,b) < \max(a',b') \\ \max(a,b) = \max(a',b') \wedge a < a' \\ \max(a,b) = \max(a',b') \wedge a = a' \wedge b < b' \end{cases}$$

<u>Piano</u>: $(a,b)<(a',b')$ è totale e soddisfa (1), (2), (3)

quindi $(\omega\times\omega, <) \sim (\omega, \in)$

① irriflessività: $(a,b) \not< (a,b)$

② transitività: $(a,b) < (a',b') \wedge (a',b') < (a'',b'')$

$\max(a,b) \leq \max(a',b') = \max(a',b') \leq \max(a'',b'')$

③ totalità

se $(a,b) \nleq (a',b') \longrightarrow (a,b) = (a',b')$

④ (1) buon ordinamento

$A \subseteq \omega\times\omega,\ A \neq \emptyset$

Considero $m = \min\{n \in \omega \mid \exists (a,b) \in A \ \max(a,b) = n\}$

Considero $A' = \{(a,b) \in A \mid \max(a,b) = m\}$

$m_a = \min\{a \in \omega \mid \exists b \ (a,b) \in A'\}$

$A'' = \{(a,b) \in A' \mid a = m_a\}$

$m_{ab} = \min\{b \in \omega \mid (a,b) \in A''\}$

$\longrightarrow (a,b)$ è il minimo di A

(2) $(\omega\times\omega, <)$ illimitato

$(a,b) < (S(a), S(b))$

(3) $A \subseteq \omega\times\omega,\ A \neq \emptyset$ sup. lim. ha massimo

$\exists (a,b) \in \omega\times\omega \ \ \forall (a',b') \in A \ \ (a',b') < (a,b)$

Fissato (a,b), sia $m = \max(a,b)$

$\forall (a',b') \in A \ \ \max(a',b') \leq m \implies A \subseteq S(m) \times S(m)$, che è finito

$\square$

Proposizione $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \aleph_0$

DIMOSTRAZIONE

$\aleph_0 \leq \aleph_0 + 0 \leq \aleph_0 + \aleph_0 = 2 \cdot \aleph_0 \leq \aleph_0 \cdot \aleph_0$

$\aleph_0^n = \aleph_0$ per induzione su n:

- $\aleph_0^2 = \aleph_0$
- $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 \overset{\text{hp ind}}{=} \aleph_0 \cdot \aleph_0 = \aleph_0$ $\square$

Def. $\mathbb{Z} \equiv \omega \times \omega / \sim$

dove $(a,b) \sim (c,d) \Leftrightarrow a+c = b+d$

Def. $\mathbb{Q} \equiv \mathbb{Z} \times \omega / \sim$

dove $(a,b) \sim (c,d) \Leftrightarrow a(d+1) = c(b+1)$

Lemma $|A| \leq \aleph_0$ e $f: A \longrightarrow B$ surgettiva allora $|B| \leq \aleph_0$

DIMOSTRAZIONE

Esiste $g: A \longrightarrow \omega$ iniettiva.

Costruisco $h: B \longrightarrow \omega$

$y \longmapsto \min(g[\{x \in A \mid f(x) = y\}])$

- h è ben definita: infatti $\{x \in A \mid f(x) = y\} \neq \emptyset$ perché f è surgettiva.
- h è iniettiva: se $h(y) = h(y')$ allora $h(y) = g(a) = g(a') = h(y')$ dove $f(a) = y$ e $f(a') = y'$. Per l'iniettività di g: $a = a' \Rightarrow y = f(a) = f(a') = y'$ □

Def. $a \in \mathbb{R}$ si dice algebrico se $\exists p \in \mathbb{Z}[x], p \neq 0$, t.c. $p(a) = 0$

Sia $\mathbb{A} = \{$numeri reali algebrici$\}$

esercizio Dimostrare che $\mathbb{A}$ è numerabile: $|\mathbb{A}| = \aleph_0$

Considero $\mathbb{A}^{\leq d} = \{$algebrici di grado $\leq d\}$

- $\mathbb{A}^{\leq 1} = \mathbb{Q}$, $|\mathbb{A}| = \aleph_0$
- $|\mathbb{A}^{=2}| = \aleph_0$

$\phi: (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z} \times \mathbb{Z} \times \{0,1\} \longrightarrow \mathbb{A}^2$

$(a,b,c,d) \longmapsto$ la d-esima soluzione di $ax^2 + bx + c = 0$

ϕ è surgettiva

- $|\mathbb{A}^{=n}| = \aleph_0$ allo stesso modo

Possiamo allora costruire

$\Phi: (\omega \setminus \{0\}) \times \omega \longrightarrow \mathbb{A}$

$(d,n) \longmapsto$ n-esimo algebrico di ordine d

↳ non è ben definita perché manca un'enumerazione esplicita (servirebbe AC)

Proposizione (AC) Se $|A| \leq \aleph_0$ e $\forall x \in A$ $|x| \leq \aleph_0$ allora $|\bigcup A| \leq \aleph_0$

Lemma Siano $f: \omega \longrightarrow A$ surgettiva, $g: \omega \longrightarrow {}^{\omega}(\bigcup A)$ t.c. $g(x)[\omega] = f(x)$ allora $|\bigcup A| \leq \aleph_0$

DIMOSTRAZIONE

Basta trovare h: numerabile $\longrightarrow \bigcup A$ surgettiva

$h: \omega \times \omega \longrightarrow \bigcup A$

$(x,y) \longmapsto g(x)(y)$ □

Def. $\mathcal{P}^{=\alpha}(X) = \{Y \in \mathcal{P}(X) \mid |Y| = \alpha\}$

$\mathcal{P}^{fin}(X) = \{Y \in \mathcal{P}(X) \mid |Y| < \aleph_0\}$

Proposizione Se $|X| \leq \aleph_0$, allora $|\mathcal{P}^{fin}(X)| \leq \aleph_0$

DIMOSTRAZIONE

Se $|X| < \aleph_0$, $\mathcal{P}^{fin}(X) = \mathcal{P}(X)$ e $|\mathcal{P}(X)| = 2^{|X|} < \aleph_0$.

Siccome $\mathcal{P}^{fin}(X) = \bigcup_{n \in \omega} \mathcal{P}^{\leq n}(X)$, basta esibire una successione di enumerazioni α_n di $\mathcal{P}^{\leq n}(X)$

Fissiamo $f : \omega \longrightarrow \omega \times A$, $f : x \longmapsto (f_1(x), f_2(x))$ surgettiva (perché X è al più numerabile)

Per ricorsione:

- $n=0$: $\mathcal{P}^{\leq 0}(X) = \{\emptyset\}$ e $\alpha_0 = \emptyset$
- $n = s(m)$: $\alpha_{s(m)}(x) = \begin{cases} \emptyset & \text{se } x=0 \\ \alpha_m(f_1(x-1)) \cup \{f_2(x-1)\} & \text{se } x>0 \end{cases}$

Dimostriamo per induzione che $\forall n \in \omega$ $\alpha_n : \omega \longrightarrow \mathcal{P}^{\leq n}(X)$ è surgettiva:

- $n=0$: immediato
- $n = s(m)$: per hp. ind, $\alpha_m : \omega \longrightarrow \mathcal{P}^{\leq m}(X)$ è surgettiva

  Dato $Y \in \mathcal{P}^{\leq s(m)}(X)$, abbiamo due casi: o $Y = \emptyset$, allora $Y = \alpha_{s(m)}(0)$, oppure $y \in Y$, quindi $|Y \setminus \{y\}| \leq m$ e allora $Y \setminus \{y\} = \alpha_m(t)$ per un certo $t \in \omega$.

  Per la surgettività di f, $(t, y) = f(x)$ per qualche $x \in \omega$. Quindi

  $\alpha_{s(m)}(x+1) = \alpha_m(f_1(x)) \cup \{f_2(x)\} = (Y \setminus \{y\}) \cup (\{y\}) = Y$ $\square$

esercizio (soluz)

$a_d x^d + \ldots + a_1 x + a_0 \longleftrightarrow \{(d, a_d), (d-1, a_{d-1}), \ldots, (1, a_1), (0, a_0)\}$

$\Longrightarrow \mathbb{Z}[x] \subseteq \mathcal{P}^{fin}(\omega \times \mathbb{Z})$

$|\mathcal{P}^{fin}(\omega \times \mathbb{Z})| \leq \aleph_0 \Longrightarrow |\mathbb{Z}[x]| = \aleph_0$

$\mathbb{Z}[x] \times \omega \longrightarrow \mathbb{A}$

$(p, n) \longmapsto$ n-esima radice di p se esiste e $p \neq 0$, altrimenti 0 (nell'ordine di $\mathbb{R}$)

Def. Sia $(A, <)$ totalmente ordinato e $B \subseteq A$.

B è **denso in $(A,<)$** se $\forall x, y \in A$ $x<y$ $\exists z \in B$ $x<z<y$

$(A,<)$ è **denso** se è denso in se stesso, cioè $\forall x, y \in A$ $x<y$ $\exists z \in A$ $x<z<y$

esempio $\mathbb{Q}$ è denso:

$\forall x, y \in \mathbb{Q}, x<y \longrightarrow x < \frac{x+y}{2} < y$

ω non è denso

$\nexists z \in \omega$ t.c. $0<z<1$

esempio $(\mathbb{Q}, <) \sim (\mathbb{Z}_{(2)} = \{\frac{a}{2^b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}, <)$

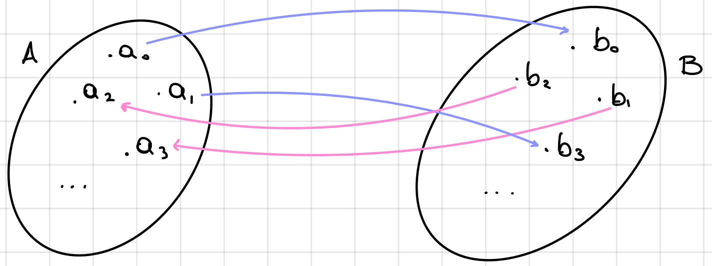
Teorema di isomorfismo di Cantor

Sia $(A,<)$ un insieme totalmente ordinato tale che.
$|A| = \aleph_0$
- $(A,<)$ è denso
- $(A,<)$ non ha estremi (ossia non ha massimo o minimo elemento)

Allora $(A,<) \cong (\mathbb{Q},<)$

<u>OSS</u> Sia $F \subseteq \mathcal{P}(A \times B)$ un insieme di funzioni.
Se $\forall f_1, f_2 \in F \quad f_1|_{Dom(f_1)\cap Dom(f_2)} = f_2|_{Dom(f_1)\cap Dom(f_2)}$ (ossia $\forall x \in Dom(f_1)\cap Dom(f_2) \quad f_1(x) = f_2(x)$)
allora $\bigcup F$ è una funzione : $\bigcup\{Dom(f) \mid f \in F\} \longrightarrow B$

DIMOSTRAZIONE

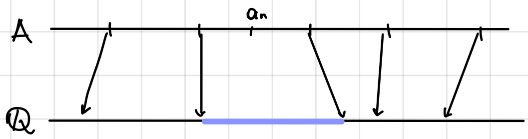


"back and forth"

Fissiamo. $A = \{a_i \mid i \in \omega\}$ e $\mathbb{Q} = \{q_i \mid i \in \omega\}$
<u>Scopo</u>: costruire $\{f_i\}_{i\in\omega}$ con $A_i \subseteq A$ e $Q_i \subseteq \mathbb{Q}$ finiti t.c
1. $f_i : A_i \longrightarrow Q_i$
2. f_i sia un isomorfismo fra $(A_i,<)$ e $(Q_i,<)$
3. $f_i \subseteq f_{S(i)}$
4. $\{q_0,\dots,q_i\} \subseteq Im f_{i+1}$
   $\{a_0,\dots,a_i\} \subseteq Dom f_{i+1}$

Considero $f = \bigcup\{f_i \mid i \in \omega\}$
Dati $a,b \in A$, $a<b$
$f(a) = f_i(a) = f_{max(i,j)}(a) < f_{max(i,j)}(b) = f_j(b) = f(b)$
Costruiamo le f_i per ricorsione:
- $f_0 = \emptyset$
- $f_{S(n)}$: $\quad f_n \quad \underline{f_{n+0.5}} \quad f_{n+1}$
  - se $a_n \in Dom f_n$: $f_{n+0.5} = f_n$
  - se $a_n \notin Dom f_n$. $f_{n+0.5} = f_n \cup \{(a_n, y)\}$
    sia k è minimo t.c. $f_n \cup \{(a_n, q_k)\}$ è iso : allora $y = q_k$
    (k esiste perché A_i è finito e $\mathbb{Q}$ è denso e senza estremi)

  $\underline{f_{S(n)}}$
  - se $q_n \in Im f_{n+0.5}$: $f_{S(n)} = f_{n+0.5}$
  - se $q_n \notin Im f_{n+0.5}$: $f_{S(n)} = f_{n+0.5} \cup \{(x, q_n)\}$
    sia h è minimo t.c. $f_{n+0.5} \cup \{(a_h, q_n)\}$ è iso : allora $x = a_h$



$\square$

Def. Dati $(A,<_A)$, $(B,<_B)$ ordini totali, definiamo il prodotto lessicografico di ordini $(A,<_A)\times(B,<_B)=(A\times B,<_{A\times B})$ tale che

$$(a,b)<_{A\times B}(a',b') \equiv b<_B b' \lor (b=b' \land a<_A a')$$

("$(A,<)\times(B,<)$ è A ripetuto B volte")

Corollario Sia $(A,<)$ un ordine totale numerabile. Allora esiste $B\subseteq\mathbb{Q}$ t.c. $(A,<)\sim(B,<)$

DIMOSTRAZIONE

Considero $(\mathbb{Q},<)\times(A,<)$

osservo che $|\mathbb{Q}\times A|=\aleph_0$

e $\mathbb{Q}\times A$ è denso senza estremi

$\Rightarrow (\mathbb{Q},<)\times(A,<)\sim(\mathbb{Q},<)$ per Cantor

Ma $A \hookrightarrow \mathbb{Q}\times A$

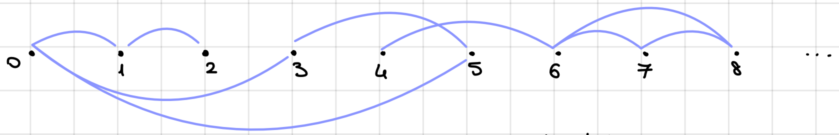
$a \longmapsto (0,a)$ $\square$

esercizio Dimostra che se $(A,<)$ è denso e $2\le|A|\le\aleph_0$, allora

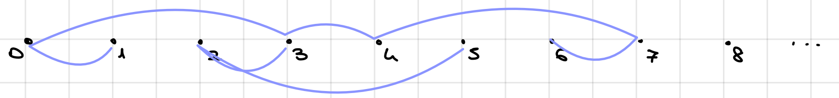
$$(A,<)\sim\begin{cases}]0,1[_{\mathbb{Q}} \\ [0,1[_{\mathbb{Q}} \\ ]0,1]_{\mathbb{Q}} \\ [0,1]_{\mathbb{Q}} \end{cases}$$

Def. Un grafo su V è una relazione simmetrica e irriflessiva in $V\times V$

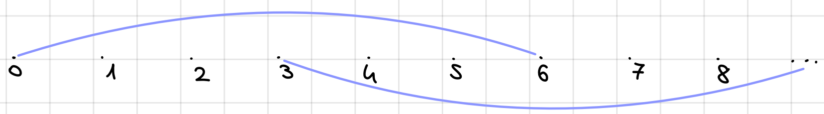
Per ogni coppia, tiro una moneta: se esce testa metto un arco



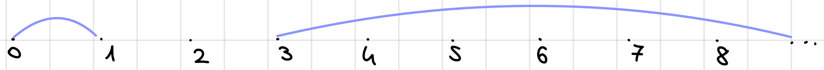
$\cong$ con probabilità 1



Lo rifaccio con una moneta truccata: esce testa all' 1% $\cong$ con probabilità 1



$\cong$ con probabilità 1



Def. Un grafo su $V=\omega$ si dice grafo random se

$\forall A,B\subseteq V\ (|A|<\aleph_0 \land |B|<\aleph_0 \land A\cap B=\emptyset) \Rightarrow \exists v\in V$

$\forall a\in A\ (v,a)\in G \quad \forall b\in B\ (v,b)\notin G$

Proposizione I grafi random sono tutti isomorfi

cardinalità del continuo $\mathcal{C}$

Def. Sia $(A,<)$ un insieme totalmente ordinato, $B \subseteq A$
- $M \in A$ è un **maggiorante** di B se $\forall b \in B \; M \geq b$
- $m \in A$ è un **minorante** di B se $\forall b \in B \; m \leq b$
- $x \in A$ è l'**estremo superiore** di B se x è il minimo dei maggioranti : $\sup B$
- $y \in A$ è l'**estremo inferiore** di B se y è il massimo dei minoranti $\inf B$

NOTA : sup e inf in generale non esistono, ma se esistono sono unici

Def. $(A,<)$ è **completo** se
$\forall B \subseteq A$ superiormente limitato $\exists \sup B$

esercizio Dimostrare che in $\mathbb{Q}$
$\{x \in \mathbb{Q} \mid x^2 < 2\}$ non ha un sup (senza usare $\mathbb{R}$)

Def. Sia $(A,<)$ un ordine totale
B è un **segmento iniziale** di A se
$\forall b \in B \; \forall c \in A \; c < b \longrightarrow c \in B$
$A_a = \{x \in A \mid x < a\}$ si dice **segmento iniziale principale** determinato da $a \in A$

Def. Sia $(A,<)$ un ordine totale
B è una **sezione di Dedekind** di A se
B è un segmento iniziale proprio $(B \neq A)$, non vuoto e senza massimo

Def. $\mathbb{R} \overset{\text{def.}}{=} \{A \in \mathcal{P}(\mathbb{Q}) \mid A \text{ è una sezione}\}$

Def. Dati $a,b \in \mathbb{R}$
$a < b \equiv a \subset b$

Lemma Un'unione di segmenti iniziali è un segmento iniziale

DIMOSTRAZIONE
Sia $A = \bigcup\{A_i \mid i \in \omega\}$ dove gli A_i sono segmenti iniziali
Sia $a \in A$, $b < a$. Poiché $a \in A$, $a \in A_i$ per un certo $i \Rightarrow b < a \equiv b \subset a \in A_i$
$\Rightarrow b \in A_i \Rightarrow b \in A \Rightarrow A$ è un segmento iniziale. □

Proposizione $\mathbb{R}$ è un ordine completo

DIMOSTRAZIONE
$A \subseteq \mathbb{R}$, $A \neq \emptyset$, $\forall a \in A \; a \leq m$. $\sup A = \bigcup A$
- $\bigcup A \in \mathbb{R}$
  - Poiché $a \leq m \equiv a \subseteq m$, $\bigcup A \subseteq m \Rightarrow \bigcup A \neq \mathbb{Q}$
  - $\bigcup A \neq \emptyset$ poiché $\exists a \in A \Rightarrow a \in \bigcup A$
  - Sia $a \in \bigcup A$, $b <_{\mathbb{Q}} a \Rightarrow a \in X \in A \Rightarrow b \in X \Rightarrow b \in \bigcup A$ ($\bigcup A$ è un segmento iniziale)
  - Sia m max di $\bigcup A$ per assurdo
    $\exists X \in A$ t.c. $m \in X \Rightarrow m$ è il max di X $\lightning$
- $\bigcup A$ è il minimo maggiorante (perché l'ordine è il contenimento) □

<u>Oss</u> $f : \mathbb{Q} \longrightarrow \mathbb{R}$
$a \longmapsto \mathbb{Q}_a = \{x \in \mathbb{Q} \mid x < a\}$
f è strettamente crescente

Corollario $\aleph_0 < |\mathbb{R}|$

DIMOSTRAZIONE
$\mathbb{R}$ è senza estremi, è denso
Se fosse numerabile, avremmo $(\mathbb{R}, <) \sim (\mathbb{Q}, <)$
ma $\mathbb{R}$ è completo e $\mathbb{Q}$ non lo è $\lightning$ $\square$

Teorema Sia $(A, <)$ un ordine totale, completo e senza estremi e sia $B \subseteq A$ denso in A e numerabile
Allora $(A, <) \sim (\mathbb{R}, <)$

DIMOSTRAZIONE
B è numerabile, denso, senza estremi $\Longrightarrow \exists f : B \longrightarrow \mathbb{Q}$ iso
Definiamo: segue dalla densità di B

$g : A \longrightarrow \mathbb{R}$
$a \longmapsto f[B_a] = f[\{b \in B \mid b < a\}]$

$a_1 < a_2 \longrightarrow a_1 < b < a_2$
$f(b) \in f[B_{a_2}]$ e $f(b) \notin f[B_{a_1}]$ g iniettiva

- $x \in f[B_{a_1}]$ $x = f(b)$ con $b < a_1 < a_2 \longrightarrow x \in f[B_{a_2}]$ rispetta l'ordine
- $r \in \mathbb{R}$ vogliamo trovare a t.c. $r = f[B_a]$
  $a = \sup_A (f^{-1}[r])$ g surgettiva $\square$

Aritmetica delle cardinalità

"finito" $< \aleph_0 < 2^{\aleph_0}$

- $2^{2^{\aleph_0}} > 2^{\aleph_0}$
- $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \aleph_0} = 2^{\aleph_0}$
- Siano A, B o "finito" o $\aleph_0$ o $2^{\aleph_0}$
  $A + B = A \cdot B = \max\{A, B\}$
  eccetto il caso $A \cdot 0 = 0 \cdot B = 0$

<u>Dim</u> Sia $A \leq B$: $B \leq \begin{matrix} A+B \\ A \cdot B \end{matrix} \leq B^2 = B$

Ipotesi del continuo
Non esiste un insieme A t.c.
$\aleph_0 < |A| < c = 2^{\aleph_0}$

L'ipotesi del continuo è indecidibile con la teoria ZFC

proposizione Sia $|A| = \aleph_0$ e $B \subseteq A$, $|B| < \aleph_0$
Allora $|A \setminus B| = \aleph_0$

DIMOSTRAZIONE

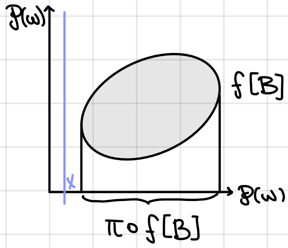
$A \setminus B \subseteq A$, quindi $|A \setminus B| \le \aleph_0$

se fosse $|A \setminus B| < \aleph_0$, si avrebbe $|A| = |(A \setminus B) \cup B| \le |A \setminus B| + |B| < \aleph_0 + \aleph_0 = \aleph_0$ ↯ $\square$

proposizione $|A| = 2^{\aleph_0}$, $B \subseteq A$, $|B| \le \aleph_0$
Allora $|A \setminus B| = 2^{\aleph_0}$

DIMOSTRAZIONE

Fisso $f : A \longrightarrow \mathcal{P}(\omega) \times \mathcal{P}(\omega)$ bigettiva



$\pi \circ f : B \longrightarrow \pi \circ f[B]$ surgettiva
$\Longrightarrow \quad |\pi \circ f[B]| \le \aleph_0$
$\Longrightarrow \exists\, x \in \mathcal{P}(\omega) \quad x \notin \pi \circ f[B]$

Considero l'insieme $\{x\} \times \mathcal{P}(\omega)$:

$\{x\} \times \mathcal{P}(\omega) \cap f[B] = \emptyset$

$\Longrightarrow \{x\} \times \mathcal{P}(\omega) \subset \mathcal{P}(\omega) \times \mathcal{P}(\omega) \setminus f[B]$

$f^{-1}(\{x\} \times \mathcal{P}(\omega)) \subseteq A \setminus B$

ma $|\{x\} \times \mathcal{P}(\omega)| = |\mathcal{P}(\omega)| = 2^{\aleph_0}$

$\Longrightarrow |A \setminus B| \geqslant 2^{\aleph_0}$ $\square$

IDEA per $|\mathbb{R}| = 2^{\aleph_0}$

$2^{\aleph_0} = |{}^{\omega}\{0,1\}|$

$\{\{a_i\}_{i\in\omega} \mid \forall i \ a_i \in \{0,1\}\}$

$\{a_i\}_{i\in\omega} \longmapsto \sum_{i=0}^{+\infty} a_i 2^{-i}$ ma non è proprio iniettiva. $\sum_{i=0}^{+\infty} a_i 3^{-i}$

$|\mathcal{P}(\omega)| \le |\mathbb{R}|$ e $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$ con $|\mathcal{P}(\mathbb{Q})| = 2^{\aleph_0}$

$\Longrightarrow |\mathbb{R}| = 2^{\aleph_0}$

DEF. Dati $a, b \in \mathbb{R}$

$a+b = \{s+t \mid s \in a, t \in b\}$

Dati $a, b > 0$

$ab = \{r \in \mathbb{Q} \mid r \leq 0\} \cup \{st \mid s \in a, s > 0, t \in b, t > 0\}$

PROPOSIZIONE A meno di isomorfismi, $\mathbb{R}$ è l'unico campo ordinato completo

PROPOSIZIONE $|\mathbb{R}| = 2^{\aleph_0}$

DIMOSTRAZIONE

$A = \{X \in \mathcal{P}(\omega) \mid X \neq \emptyset \wedge \underbrace{|\omega \setminus X| = \aleph_0}_{X \text{ è coinfinito}}\}$

Dati $a, b \in A$

$a < b \equiv \exists i \in \omega \quad a \cap i = b \cap i \wedge i \in b \wedge i \notin a$

$B = \mathcal{P}^{fin}(\omega) \setminus \{\emptyset\} \subseteq A$

Si verifica che $(A, <)$ è un ordine totale, (completezza)

e $B \subseteq A$ è denso in A, $|B| = \aleph_0$

→ si costruisce il c t.c. $a < c < b$ con le cifre binarie

Fissiamo $f : B \to \mathbb{Q}$ iso

$\mathbb{Q} \sim B \subseteq A \hookrightarrow \mathbb{R}$

$a \longmapsto f(\{b \in B \mid b < a\}) = f[B_a]$

ed è crescente $\longrightarrow$ iniettiva

$\Rightarrow |A| \leq |\mathbb{R}|$

Ma $A = \mathcal{P}(\omega) \setminus (\{\emptyset\} \cup \underbrace{\{X \subseteq \omega \mid |\omega \setminus X| < \aleph_0\}}_{\updownarrow \, \mathcal{P}^{fin}(\omega)}$ $\longrightarrow$ funzione complementare

Quindi $|\mathbb{R}| \geq |A| = 2^{\aleph_0}$

Inoltre $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$ quindi $|\mathbb{R}| \leq 2^{\aleph_0}$

$\Rightarrow |\mathbb{R}| = 2^{\aleph_0}$ $\square$

I BUONI ORDINAMENTI

Def. $(A,<)$ è un buon ordinamento se ogni sottoinsieme non vuoto ha un minimo:
$$\forall B \subseteq A \quad B \neq \emptyset \longrightarrow \exists x \in B \ \forall y \in B \ x \leq y$$

Def. Sia $(A,<)$ un ordine totale
$B \subseteq A$ è un segmento iniziale di A se
$$\forall x \in B \ \forall y \in A \quad y < x \longrightarrow x \in B$$
Un segmento iniziale B è proprio se $B \neq A$
Un segmento iniziale B è principale se
$$\exists a \in A \quad B = A_a = \{x \in A \mid x < a\}$$

Def. Siano $(A,<_A)$ e $(B,<_B)$ buoni ordini
$$(A,<_A) \prec (B,<_B)$$
se $\exists C \subset B$ t.c. C è segmento iniziale di B $\wedge (A,<_A) \sim (C,<_B)$

Def. Siano $(A,<_A)$ e $(B,<_B)$ buoni ordini
$$(A,<_A) \preceq (B,<_B) \quad \equiv \quad (A,<_A) \prec (B,<_B) \ \vee \ (A,<_A) \sim (B,<_B)$$

> **Proposizione** Ogni segmento iniziale proprio di un buon ordine è principale

DIMOSTRAZIONE
Fissiamo $(A,<)$ b.o.
Sia $B \subseteq A$ s.i. proprio
Sia $a = \min(A \setminus B)$: dico che $B = A_a$
- $A_a \subseteq B$
  Per assurdo, $a' \in A_a$, $a' \notin B \longrightarrow a' < a$ ↯ per la minimalità di a
- $B \subseteq A_a$
  Per assurdo, $b \in B$, $b \notin A_a \longrightarrow a \leq b \longrightarrow a \in B$ ↯ □

<u>esercizio</u> la proposizione caratterizza i buoni ordini

> **Lemma** Sia $(A,<)$ un buon ordine e sia $f: A \to A$ crescente
> Allora $\forall x \in A \quad x \leq f(x)$

DIMOSTRAZIONE
Per assurdo, sia y minimo t.c. $y > f(y)$
$\longrightarrow y > f(y) > f(f(y))$
Quindi, se $y' = f(y)$, $y' > f(y')$ ↯ per la minimalità di y □

corollario (1) Un buon ordine non è isomorfo a un suo segmento iniziale proprio.
(2) L'identità è il solo isomorfismo tra un buon ordine e se stesso
(3) Se $(A,<)$ e $(B,<)$ sono buoni ordini isomorfi, allora esiste un unico isomorfismo tra di loro.

DIMOSTRAZIONE

(1) Sia $f : A \longrightarrow A_a$ isomorfismo
$f(a) \in A_a \longrightarrow f(a) < a$ $\lightning$

(2) Per assurdo, sia $f(x) \neq x$
Se $f(x) < x$ $\lightning$ per il lemma
Se $f(x) > x$ $\lightning$ considerando f^{-1}

(3) Se $f : A \longrightarrow B$, $g : A \longrightarrow B$ iso con $f \neq g$, allora
$g^{-1} \circ f : A \longrightarrow A$ è diverso dall'identità $\square$

<u>OSS</u> $(A,<_A) \preccurlyeq (B,<_B) \wedge (B,<_B) \preccurlyeq (C,<_C) \longrightarrow (A,<_A) \preccurlyeq (C,<_C)$

DIMOSTRAZIONE

Fissiamo $f : A \longrightarrow B$ crescente t.c. $f[A]$ è s.i. di B
e $g : B \longrightarrow C$ crescente t.c. $g[B]$ è s.i. di C
Quindi $g \circ f[A]$ è un s.i di C
Infatti sia $g(f(a)) \in g \circ f[A]$ e sia $x < g(f(a))$
Ora $g(f(a)) \in g[B]$ che è s.i. di $C \Rightarrow x \in g[B] \Rightarrow x = g(y)$ con $y \in B$
Poi g è un iso tra B e $g[B]$, quindi $g(y) < g(f(a)) \Rightarrow y < f(a) \in f[A]$
Ma anche $f[A]$ è un s.i $\Rightarrow y \in f[A] \Rightarrow y = f(z)$ con $z \in A$
Quindi $x = g(f(z)) \Rightarrow x \in g \circ f[A]$ $\square$

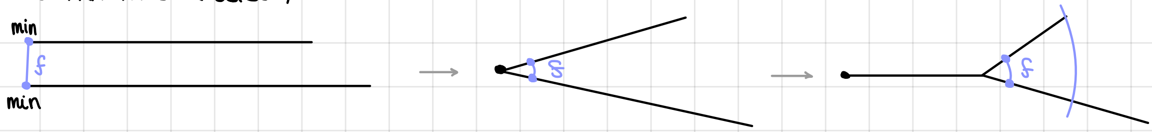
<u>OSS</u> Se $(A,<_A) \preccurlyeq (B,<_B) \wedge (B,<_B) \preccurlyeq (A,<_A) \longrightarrow (A,<_A) \sim (B,<_B)$

DIMOSTRAZIONE

Fissiamo $f : A \longrightarrow B$ crescente t.c. $f[A]$ è s.i. di B
e $g : B \longrightarrow A$ crescente t.c. $g[B]$ è s.i. di A
$g \circ f$ è un iso tra A e un s.i di A
Non può essere un s.i. proprio, quindi coincide con A
$\Rightarrow g \circ f = id_A$
Analogamente $f \circ g = id_B$, quindi
f è un iso tra A e B con inversa g. $\square$

Teorema Dati $(A,<_A),(B,<_B)$ buoni ordini, vale una e una sola delle seguenti:
(i) $(A,<_A) \prec (B,<_B)$
(ii) $(A,<_A) \sim (B,<_B)$
(iii) $(B,<_B) \prec (A,<_A)$

DIMOSTRAZIONE (idea)



DIMOSTRAZIONE

$f := \{(a,b) \in A \times B \mid A_a \sim B_b\}$

Devo verificare che f è crescente, $\mathrm{Dom} f$ è s.i di A, $\mathrm{Im} f$ è s.i di B, $\mathrm{Dom} f = A$ o $\mathrm{Im} f = B$

(1) f è una funzione
Per assurdo $(a,b) \in f$, $(a,b') \in f \longrightarrow B_b \sim A_a \sim B_{b'}$
Se $b<b'$: B_b è s.i proprio di $B_{b'}$ $\lightning$

(2) f è crescente
Per assurdo, siano $a,a' \in A$ con $a<a'$ t.c. $f(a) \geq f(a')$.
Allora $A_{a'} \sim B_{f(a')} \precsim B_{f(a)} \sim A_a$
$\hookrightarrow$ segue da $B_{f(a')} \subseteq B_{f(a)}$ poiché $f(a) \geq f(a')$
$\longrightarrow A_{a'} \precsim A_a$ $\lightning$ poiché A_a è s.i. proprio di $A_{a'}$ in quanto $a<a'$.

(3) $\mathrm{Dom} f$ è un s.i. di A
Sia $a \in \mathrm{Dom} f$ e $a'<a$
$\longrightarrow \exists b : (a,b) \in f \longleftrightarrow A_a \sim B_b$ e sia g l'isomorfismo
$(A_a)_{a'} \sim (B_b)_{g(a')}$ perché g iso
$\;\; \| \qquad\qquad \|$
$A_{a'} \qquad B_{g(a')} \longrightarrow (a', g(a')) \in f \longrightarrow a' \in \mathrm{Dom} f$

(4) $\mathrm{Im} f$ è s.i di B
simmetrica alla precedente

(5) $\mathrm{Dom} f = A$ o $\mathrm{Im} f = B$
Sappiamo già che f è un isomorfismo di ordini tra $\mathrm{Dom} f$ (s.i di A) e $\mathrm{Im} f$ (s.i di B)
Per assurdo $\mathrm{Dom} f = A_a$ e $\mathrm{Im} f = B_b$. Quindi $f(a) = b$ $\lightning$ $\square$

esercizio $(A,\leq_A)$ b.o., $B \subsetneq A$
$(B,<_A) \precsim (A,<_A)$

operazioni aritmetiche tra buoni ordinamenti

<u>NOTAZIONE</u> $\mathcal{A}=(A,<_A)$ $\quad \mathcal{B}=(B,<_B)$ $\quad \mathcal{C}=(C,<_C)$

DEF. $\mathcal{A}+\mathcal{B}=\mathcal{C}$ se $\mathcal{C}\sim(A\sqcup B,<_+)$ $\qquad$ A $<$ B

dove $(m,x)<_+(n,y) \equiv \begin{cases} x=y=0 \wedge m<_A n \\ x=y=1 \wedge m<_B n \\ x=0 \wedge y=1 \end{cases}$

DEF. $\mathcal{A}\times\mathcal{B}=\mathcal{C}$ se $\mathcal{C}\sim(A\times B,<_\times)$

dove $(a,b)<_\times(a',b') \equiv \begin{cases} b<_B b' \\ b=b' \wedge a<_A a' \end{cases}$

DEF. Data $f:B\longrightarrow A$, definisco il supporto di f:
$\operatorname{supp} f := \{x\in B \mid f(x)\neq \min A\}$

DEF. $\mathcal{A}^{\mathcal{B}}=\mathcal{C}$ se $\mathcal{C}\sim(\{f\in {}^B A \mid |\operatorname{supp} f|<\aleph_0\}, <_{exp})$
dove $f<_{exp} g \equiv \exists m\in B \;\; f(m)<_A g(m) \wedge \forall n\in B \;\; m<_B n \;\; f(n)=g(n)$

<u>esercizio</u> Sia $(\mathbb{N}[x],<)$ l'insieme dei polinomi a coefficienti in $\mathbb{N}$ con l'ordine seguente
$p<q \equiv \exists N\in\mathbb{N} \;\; \forall m>N \;\; p(m)<q(m)$
Dimostrare che $(\mathbb{N}[x],<)\sim(\omega,<)^{(\omega,<)}$

> **Proposizione** le relazioni appena definite sono buoni ordini

DIMOSTRAZIONE

Dimostriamo che dato $X\subseteq {}^B A$ insieme di funzioni a supporto finito, $X\neq\emptyset$
X, ha un minimo rispetto a $<_{exp}$
Per assurdo: $\exists f \; \exists X \;\; f\in X \wedge \forall g\in X \; |\operatorname{supp} g|<\aleph_0 \wedge$ " X non ha minimo.
Fisso f t.c. $\max(\operatorname{supp} f)=\mu$ sia minimo tra tutti i controesempi e, a parità,
$f(\max(\operatorname{supp} f))$ sia minimo
Fisso X corrispondente
$X_1=\{g\in X \mid \max(\operatorname{supp} g)<\mu\}$
$X_2=\{g\in X \mid \max(\operatorname{supp} g)=\mu \wedge g(\mu)<f(\mu)\}$
$X_3=\{g\in X \mid \max(\operatorname{supp} g)=\mu \wedge g(\mu)=f(\mu)\}$
$X_4=X\setminus(X_1\cup X_2\cup X_3)$
Uno fra X_1,X_2,X_3 non ha minimo.
Se X_1 non ha minimo, deve essere $X_1=\emptyset$
Allo stesso modo dovrebbe essere $X_2=\emptyset$ (avremmo un controesempio più piccolo)
$\Rightarrow X_3\neq\emptyset$ e non ha minimo
Costruisco $X_3'=\left\{h \mid \exists g\in X_3 \;\; h(x)=\begin{cases} g(x) & x\neq\mu \\ \min A & x=\mu \end{cases}\right\}$ (perché il valore in μ è irrilevante per l'ordinamento)
Siccome $X_3'\sim X_3$, X_3' non ha minimo $\lightning$ (per la minimalità di μ) $\square$

proposizione Gli ordini appena definiti passano al quoziente per isomorfismi, ossia se $\mathcal{A} \sim \mathcal{A}'$, $\mathcal{B} \sim \mathcal{B}'$ allora $\mathcal{A} + \mathcal{B} \sim \mathcal{A}' + \mathcal{B}'$, $\mathcal{A} \times \mathcal{B} \sim \mathcal{A}' \times \mathcal{B}'$, $\mathcal{A}^{\mathcal{B}} \sim \mathcal{A}'^{\mathcal{B}'}$

DIMOSTRAZIONE

Fissati isomorfismi $f: A \to A'$ e $g: B \to B'$, è facile scrivere esplicitamente gli isomorfismi richiesti.
Per esempio, nel caso $\mathcal{A}^{\mathcal{B}}$, si considera la restrizione alle funzioni a supporto finito di

$$\begin{aligned} {}^{B}A &\longrightarrow {}^{B'}A' \\ h &\longmapsto f \circ h \circ g^{-1} \end{aligned}$$

□

proposizione Siano $\mathcal{A} = (A, <_A)$, $\mathcal{B} = (B, <_B)$, $\mathcal{C} = (C, <_C)$ buoni ordini. Allora valgono:

$$(\mathcal{A}+\mathcal{B})+\mathcal{C} \sim \mathcal{A} + (\mathcal{B}+\mathcal{C})$$
$$(\mathcal{A}\times\mathcal{B})\times\mathcal{C} \sim \mathcal{A} \times (\mathcal{B}\times\mathcal{C})$$
$$\mathcal{A}\times(\mathcal{B}+\mathcal{C}) \sim \mathcal{A}\times\mathcal{B} + \mathcal{A}\times\mathcal{C}$$
$$\mathcal{A}^{\mathcal{B}+\mathcal{C}} \sim \mathcal{A}^{\mathcal{B}} \times \mathcal{A}^{\mathcal{C}}$$
$$\mathcal{A}^{\mathcal{B}\times\mathcal{C}} \sim (\mathcal{A}^{\mathcal{B}})^{\mathcal{C}}$$

DIMOSTRAZIONE

Facili verifiche □

NON VALGONO: $\mathcal{A}+\mathcal{B} \sim \mathcal{B}+\mathcal{A}$, $(\mathcal{A}+\mathcal{B})\times\mathcal{C} \sim \mathcal{A}\times\mathcal{C} + \mathcal{B}\times\mathcal{C}$
$(\mathcal{A}\times\mathcal{B})^{\mathcal{C}} \sim \mathcal{A}^{\mathcal{C}} \times \mathcal{B}^{\mathcal{C}}$

<u>esempio</u> • • • · · · · · • $\omega+1 \not\sim \omega$ (ha un max)
• • • • · · · · · · $1+\omega \sim \omega$

<u>esercizio</u> Dimostra che $|(\omega,<)^{(\omega,<)}| = \aleph_0$

Ordinali di von Neumann

Def. X è **transitivo** se $\forall y \in X \quad y \subseteq X$
Equivalentemente $\forall y \in X \ \forall z \in y \quad z \in X$

Def. α è un **ordinale di Von Neumann** se
α è transitivo e $(\alpha, \in)$ è un buon ordine

esempio
- ω è un ordinale
- $n \in \omega$ è un ordinale
  $S(\omega) = \omega \cup \{\omega\}$
- $S(S(\omega))$
- $S(\text{ordinale})$

NOTAZIONE Indichiamo $\alpha \in \mathrm{Ord} \equiv$ "α è un ordinale"

OSS Se $\alpha \in \mathrm{Ord}$ e $\beta \in \alpha$, allora $\beta \in \mathrm{Ord}$ e $\beta = \alpha_\beta$

DIMOSTRAZIONE
Scopo: $\delta \in \gamma \in \beta \longrightarrow \delta \in \beta$
$\gamma \in \beta \in \alpha$, per la transitività di α $\gamma \in \alpha$
$\delta \in \gamma \in \alpha$, per la transitività di α $\delta \in \alpha$
$\Rightarrow \delta <_\alpha \gamma <_\alpha \beta \xrightarrow{\text{tr. di } <_\alpha} \delta <_\alpha \beta \longleftrightarrow \delta \in \beta \Rightarrow \beta$ è transitivo
Per la transitività di α, $\beta \subseteq \alpha \Longrightarrow \beta$ è un buon ordine da $\in$
$\Longrightarrow \beta \in \mathrm{Ord}$
$\gamma \in \alpha_\beta \Longleftrightarrow \gamma \in \alpha \wedge \gamma <_\alpha \beta \Leftrightarrow \gamma \in \alpha \wedge \gamma \in \beta \Leftrightarrow \gamma \in \beta$ $\square$

OSS Se $f: A \to B$ e' un isomorfismo tra $(A, <_A)$ e $(B, <_B)$,
allora preso qualunque $a \in A$ si ha $f[A_a] = B_{f(a)}$

DIMOSTRAZIONE
$x \in B_{f(a)} \Leftrightarrow x <_B f(a) \Leftrightarrow f^{-1}(x) <_A a \Leftrightarrow f^{-1}(x) \in A_a \Leftrightarrow x \in f[A_a]$ $\square$

Proposizione Siano $\alpha, \beta \in \mathrm{Ord}$.
$(\alpha, \in) \sim (\beta, \in) \longrightarrow \alpha = \beta$

DIMOSTRAZIONE
Fissiamo $f: \alpha \to \beta$ isomorfismo di ordini.
Claim $\forall x \in \alpha \quad f(x) = x$
Per assurdo, sia $\mu \in \alpha$ minimo t.c. $f(\mu) \neq \mu$
Allora $\mu = \alpha_\mu$ e
$\mu = f[\mu] = f[\alpha_\mu] = B_{f(\mu)} = f(\mu)$ $\lightning$ $\square$

Teorema Dati $\alpha, \beta \in Ord$, vale una e una sola delle seguenti:
(i) $(\alpha, \in) \prec (\beta, \in)$ se e solo se $\alpha \in \beta$
(ii) $(\alpha, \in) \sim (\beta, \in)$ se e solo se $\alpha = \beta$
(iii) $(\beta, \in) \prec (\alpha, \in)$ se e solo se $\beta \in \alpha$

DIMOSTRAZIONE
Se $(\alpha, \in) \sim (\beta, \in)$, la proposizione ci dà $\alpha = \beta$; il viceversa è immediato.
Se $(\alpha, \in) \prec (\beta, \in) \longrightarrow (\alpha, \in) \sim (\beta, \in)_\gamma \longrightarrow (\alpha, \in) \sim (\gamma, \in) \longrightarrow \alpha = \gamma \longrightarrow \alpha \in \beta$
Viceversa, $\alpha \in \beta \longrightarrow (\alpha, \in) \sim (\beta, \in)_\alpha \longrightarrow (\alpha, \in) \prec (\beta, \in)$.
Il caso $(\beta, \in) \prec (\alpha, \in)$ è simmetrico. □

NOTAZIONE Dati $\alpha, \beta \in Ord$ $\alpha < \beta \equiv \alpha \in \beta$

Proposizione Siano $\alpha, \beta \in Ord$
$\alpha \leq \beta \longleftrightarrow \alpha \subseteq \beta$

DIMOSTRAZIONE
$\Rightarrow$ $\alpha < \beta \Rightarrow \alpha \in \beta \overset{\beta\ tr.}{\Rightarrow} \alpha \subseteq \beta$
$\vee$
$\alpha = \beta \Rightarrow \alpha \subseteq \beta$
$\Leftarrow$: $\alpha \subseteq \beta$ e per assurdo $\beta < \alpha$
$\longrightarrow \beta \in \alpha \subseteq \beta \longrightarrow \beta \in \beta$ $\lightning$ □

Proposizione Dato $\alpha \in Ord$
$s(\alpha)$ è il minimo ordinale maggiore di α

DIMOSTRAZIONE
$s(\alpha)$ è un ordinale, infatti:
- transitività: se $\beta \in s(\alpha)$, o $\beta \in \alpha$ o $\beta = \alpha$.
  In entrambi i casi $\beta \subseteq \alpha \subseteq s(\alpha)$
- buon ordine: $s(\alpha)$ è un insieme di ordinali, quindi $\in$ è un ordine totale su $s(\alpha)$
  Sia $X \subseteq s(\alpha)$, $X \neq \emptyset$. o $X = \{\alpha\}$ o $X \cap \alpha \neq \emptyset$
  Nel primo caso X ha minimo, nel secondo, $\min(X \cap \alpha)$ è il minimo di X.

$\alpha < s(\alpha)$ perché $\alpha \in \alpha \cup \{\alpha\}$
Supponiamo ora $\alpha < \beta$, vogliamo mostrare $s(\alpha) \leq \beta$
$\alpha < \beta \longrightarrow \alpha \in \beta \longrightarrow \alpha \subseteq \beta$
$\{\alpha\} \subseteq \beta \longrightarrow \alpha \cup \{\alpha\} \subseteq \beta \longrightarrow s(\alpha) \leq \beta$ □

Corollario $\forall \alpha, \beta \in Ord$ $\beta \leq \alpha \longleftrightarrow \beta < s(\alpha)$

proposizione Sia X un insieme di ordinali.
(1) Se $X \neq \emptyset$, allora esiste il minimo di X e $\min X = \bigcap X$
(2) Esiste $\sup X =$ il minimo dei maggioranti di X e $\sup X = \bigcup X$
(3) Esiste un $\alpha \in \mathrm{Ord}$ $\alpha \notin X$

DIMOSTRAZIONE

(1) Fisso $\alpha \in X$ (perché $X \neq \emptyset$)
Considero $s(\alpha) \cap X \subseteq s(\alpha)$
Sia $\mu = \min(s(\alpha) \cap X)$
Sostengo che $\mu = \min X$
Infatti $\gamma \in X$: o $\gamma \in s(\alpha) \Rightarrow \mu \leq \gamma$ perché μ è min
o $\gamma \notin s(\alpha) \Rightarrow s(\alpha) \subseteq \gamma \Rightarrow \mu \leq \alpha < \gamma$
$\bigcap X$ è un insieme di ordinali, quindi è bene ordinato da $\in$, ed è transitivo:
$\alpha \in \beta \in \bigcap X \Leftrightarrow \forall \gamma \in X \ \alpha \in \beta \in \gamma \Rightarrow \forall \gamma \in X \ \alpha \in \gamma \Leftrightarrow \alpha \in \bigcap X$
$\forall \gamma \in X \ \bigcap X \subseteq \gamma \Rightarrow \bigcap X \leq \gamma$
Considero $\mu = \min X$: $\forall \gamma \in X \ \mu \leq \gamma \Rightarrow \mu \subseteq \gamma \Rightarrow \mu \subseteq \bigcap X$
$\Rightarrow \bigcap X = \mu$

(2) $\bigcup X$ è un ordinale, infatti:
- transitività: dato $\alpha \in \bigcup X$, esiste $\beta \in X$ t.c. $\alpha \in \beta$
  Per la transitività di β, $\alpha \subseteq \beta$, da cui $\alpha \subseteq \bigcup X$
- buon ordine: ogni $\alpha \in \bigcup X$ appartiene a un $\beta \in X$, e quindi è un ordinale
  $\Rightarrow$ un sottoinsieme non vuoto di $\bigcup X$ è un insieme di ordinali e quindi ha minimo per (1).

$\sigma \in \mathrm{Ord}$ è un maggiorante di $X \Leftrightarrow \bigcup X \leq \sigma$, infatti
$\forall \alpha \in X \ \alpha \leq \sigma \Leftrightarrow \forall \alpha \in X \ \alpha \subseteq \sigma \Leftrightarrow \bigcup X \subseteq \sigma \Leftrightarrow \bigcup X \leq \sigma$

(3) Basta prendere $s(\sup X)$. $\square$

corollario Un insieme di ordinali è un ordinale se e solo se è transitivo

DIMOSTRAZIONE

Il buon ordinamento vale per il punto (1) della prop. $\square$

paradosso di Burali-Forti La classe Ord è una classe propria.

Assioma di rimpiazzamento

Def. Date classi A e B, una **funzione classe** da A a B e' una formula $\varphi(x,y)$ t.c.
$$\forall x\in A\ \exists! y\in B\ \ \varphi(x,y)$$

NOTAZIONE $F(x)=y \equiv \varphi(x,y)$

esercizio Dimostrare che esiste $F(n)=\underbrace{\{\dots\{}_{n\text{ volte}}\emptyset\}\dots\}$

Cerchiamo una funzione classe $F:\omega\longrightarrow V$ t.c.
$F(\emptyset)=\emptyset \qquad F(S(n))=\{F(n)\}$

⑧ Assioma di rimpiazzamento (schema di)

Data una funzione classe $F:V\longrightarrow V$
$$\forall A\ \exists B\ \forall y\ \ y\in B\longleftrightarrow \exists x\in A\ \ F(x)=y$$

OSS per estensionalità B è unico

NOTAZIONE $B=F[A]$

OSS Dato un insieme A e una funzione classe $G:A\longrightarrow V$ esiste ed è unico $G[A]$

DIMOSTRAZIONE

Basta applicare l'assioma alla funzione classe $F:V\rightarrow V$
$F(x)=y \equiv (x\in A\wedge G(x)=y)\vee(x\notin A\wedge y=\emptyset)$ □

Teorema Dato $(A,<)$ buon ordine, $\exists!\ \alpha\in \mathrm{Ord}\quad (\alpha,\in)\sim(A,<)$

DIMOSTRAZIONE

L'unicità è immediata (segue da $\alpha\sim\alpha'\longrightarrow\alpha=\alpha'$)
$A'=\{a\in A\mid \exists\beta\in\mathrm{Ord}\ \ \beta\sim A_a\}$
Se $a\in A'$, $\exists!\beta\in\mathrm{Ord}\ \ \beta\sim A_a$
$F(a)\equiv$ l'unico $\gamma\in\mathrm{Ord}$ t.c. $\gamma\sim A_a$

Dimostriamo che $\alpha=F[A']$

1. α è un ordinale $\Leftarrow \alpha$ è transitivo
   Dati $\gamma\in\beta\in\alpha \overset{?}{\Longrightarrow} \gamma\in\alpha$
   $\beta\in\alpha\Rightarrow\beta\sim A_a$ per un certo a e $f:\beta\rightarrow A_a$ isomorfismo
   $\gamma\in\beta\Rightarrow\gamma=\beta_\gamma \quad \underbrace{\gamma\sim f[\gamma]=(A_a)_{f(\gamma)}}_{F(f(\gamma))=\gamma}=A_{f(\gamma)} \quad\Rightarrow\gamma\in\alpha$

2. A' è segmento iniziale di A (simmetrico di 1)
3. α e A' sono isomorfi
   Dati $a_1<a_2 \Rightarrow A_{a_1}\prec A_{a_2}$
   $F(a_1)\prec F(a_2) \quad\Leftrightarrow\quad F(a_1)<F(a_2)$
4. $A'=A$
   Supponiamo per assurdo $A'=A_a\sim\alpha\ \Rightarrow a\in A'$ ↯ □

soluzione es.

$F(n)=x \equiv \exists f \ \underbrace{\text{'}f \text{ è una funzione'}}_{\exists A,B \ f\in {}^A B \ \text{oppure} \ \exists B \ f \in {}^{S(n)}B} \wedge \mathrm{Dom} f = S(n) \wedge f(0)=\emptyset \wedge \forall m<n \ f(S(m)) = \{f(m)\}$

Def. (V1) Dati $\alpha,\beta \in \mathrm{Ord}$, definiamo $\alpha+\beta$, $\alpha\cdot\beta$, α^β come, rispettivamente, l'unico ordinale tale che

$$\alpha+\beta \sim (\alpha,<_\alpha)+(\beta,<_\beta) \qquad \alpha\cdot\beta \sim (\alpha,<_\alpha)\cdot(\beta,<_\beta)$$
$$\alpha^\beta \sim (\alpha,<_\alpha)^{(\beta,<_\beta)}$$

Teorema: induzione transfinita (V1) Data una formula insiemistica $\varphi(x)$
se $\forall \alpha \in \mathrm{Ord} \ (\forall \beta \in \alpha \ \varphi(\beta)) \longrightarrow \varphi(\alpha)$
allora $\forall \alpha \in \mathrm{Ord} \ \varphi(\alpha)$

DIMOSTRAZIONE

Per assurdo $\neg\varphi(\alpha)$

Considero $X=\{\beta \in S(\alpha) \mid \neg\varphi(\beta)\} \subseteq S(\alpha)$
e $X \neq \emptyset$ perché $\alpha \in X$

Sia $\alpha' = \min_\in X$

$\forall \gamma \in \alpha' \ \varphi(\gamma) \Longrightarrow \varphi(\alpha')$ ↯ $\square$

Def. Un ordinale α è un ordinale successore se e solo se $\exists \beta \in \mathrm{Ord} \quad \alpha = S(\beta)$
Un ordinale α è un ordinale limite se α non è successore e $\alpha \neq 0$

<u>OSS</u> Un ordinale α è successore se e solo se ha un massimo elemento

DIMOSTRAZIONE

β è il massimo di α se e solo se α è il minimo ordinale $>\beta$
se e solo se $\alpha = S(\beta)$ $\square$

Teorema: induzione transfinita (V2) Data una formula $\varphi(x)$, se
- $\varphi(\emptyset)$
- $\forall \alpha \in \mathrm{Ord} \quad \varphi(\alpha) \longrightarrow \varphi(S(\alpha))$
- $\forall \lambda$ ordinale limite $(\forall \beta<\lambda \ \varphi(\beta)) \longrightarrow \varphi(\lambda)$

allora $\forall \alpha \in \mathrm{Ord} \ \varphi(\alpha)$

DIMOSTRAZIONE

- $\alpha = 0$ o α limite: immediato
- $\alpha = S(\gamma) \longrightarrow \gamma < \alpha$

$$\begin{array}{ccc} (\forall \beta<\alpha \ \varphi(\beta)) & \longrightarrow & \varphi(\alpha) \\ \downarrow & & \Updownarrow \\ \varphi(\gamma) & \longrightarrow & \varphi(S(\gamma)) \end{array}$$

$\square$

Teorema di ricorsione transfinita (V1)

Data una funzione classe $G: V \longrightarrow V$, esiste una unica funzione classe $F: \mathrm{Ord} \longrightarrow V$ t.c.

$$\forall \alpha \in \mathrm{Ord} \quad F(\alpha) = G(F|_\alpha)$$

$\{(\beta, F(\beta)) \mid \beta \in \alpha\}$

<u>NOTA</u> per unicità si intende:

data $F'(\alpha) = G(F'|_\alpha)$

allora $\forall \alpha \in \mathrm{Ord} \quad F(\alpha) = F'(\alpha)$

DIMOSTRAZIONE

Definiamo $H: \mathrm{Ord} \longrightarrow V$ con

$f = H(\alpha) \equiv f$ è una funzione $\wedge \mathrm{Dom}(f) = \alpha \wedge \forall \beta < \alpha \quad f(\beta) = G(f|_\beta)$

Verifichiamo per induzione transfinita su α che H è una funzione classe:

- $\alpha = 0$: $f = H(0) \Leftrightarrow f = \emptyset$
- $\alpha = S(\gamma)$: per hp. ind $\exists! f = H(\gamma)$. Sia $f' = f \cup \{(\gamma, G(f))\}$

  f' è una funzione con $\mathrm{Dom}(f') = \mathrm{Dom}(f) \cup \{\gamma\} = \gamma \cup \{\gamma\} = S(\gamma)$

  Dato $\beta < \alpha$: se $\beta < \gamma$ allora $f'(\beta) = f(\beta) = G(f|_\beta) = G(f'|_\beta)$

  se $\beta = \gamma$ allora $f'(\gamma) = G(f) = G(f'|_\gamma)$

  Per l'unicità, sia $g = H(\alpha)$. Siccome $\mathrm{Dom}(g) = \mathrm{Dom}(f') = \alpha$, basta verificare $\forall \delta \in \alpha \; g(\delta) = f'(\delta)$.

  Dalla def., $g|_\gamma = H(\gamma)$, e per l'unicità di $H(\gamma)$, $g|_\gamma = f$.

  Quindi, se $\delta < \gamma$, $g(\delta) = g|_\gamma(\delta) = f(\delta) = f'(\delta)$. Altrimenti $\delta = \gamma$ e $g(\gamma) = G(g|_\gamma) = G(f) = f'(\gamma)$
- $\alpha = \lambda$ limite. Per hp. ind. $\forall \beta < \lambda \; \exists! f = H(\beta)$, dobbiamo mostrare $\exists! g = H(\lambda)$

  Per rimpiazzamento esiste $F[\lambda]$, sia $h = \bigcup F[\lambda]$. Vogliamo mostrare $g = H(\lambda) \Leftrightarrow g = h$

  (1) h è una funzione

  Siano $f_1, f_2 \in H[\lambda]$, con $f_1 = H(\beta_1)$, $f_2 = H(\beta_2)$ e $\beta_1 < \beta_2$.

  Allora per definizione $f_2|_{\beta_1} = H(\beta_1) \xrightarrow{\text{hp.ind}} f_2|_{\beta_1} = f_1$

  (2) $\mathrm{Dom}(h) = \lambda$

  $\mathrm{Dom}(h) = \bigcup \{\mathrm{Dom}\, H(\beta) \mid \beta < \lambda\} = \bigcup \{\beta \mid \beta < \lambda\} = \lambda$

  (3) $\forall \beta < \lambda \quad h(\beta) = G(h|_\beta)$

  Dato $\beta < \lambda \longrightarrow S(\beta) < \lambda$, quindi, detta $f = H(S(\beta))$, abbiamo $h(\beta) = f(\beta) = G(f|_\beta) = G(h|_\beta)$

  Supponiamo ora $g = H(\lambda)$, dobbiamo mostrare $g = h$. Dato $\beta < \lambda$, abbiamo $g|_\beta = h|_\beta = H(\beta)$ per l'unicità di $H(\beta)$ (hp. ind.). Quindi $g(\beta) = G(g|_\beta) = G(h|_\beta) = h(\beta)$

Quindi H è una funzione classe. Definiamo

$$y = F(\alpha) \equiv \exists f \quad f = H(S(\alpha)) \wedge f(\alpha) = y$$

Dobbiamo verificare che $F(\alpha) = G(F|_\alpha)$. Detta $f = H(S(\alpha))$, $F|_\alpha = f|_\alpha$,
infatti preso $\beta < \alpha$ e $f' = H(S(\beta))$, $F(\beta) = f'(\beta) = f(\beta)$ perché le H coincidono sull'intersezione dei domini. Quindi $F(\alpha) = f(\alpha) = G(f|_\alpha) = G(F|_\alpha)$

Per l'unicità, siano F_1 e F_2 che soddisfano la definizione.
Per induzione transfinita, assumiamo $\forall \beta < \alpha \quad F_1(\beta) = F_2(\beta)$.
Ma allora $F_1|_\alpha = F_2|_\alpha$, quindi $F_1(\alpha) = G(F_1|_\alpha) = G(F_2|_\alpha) = F_2(\alpha)$ $\square$

Def. Date classi A, B, $x \in A \times B \equiv \exists a \in A \; \exists b \in B \quad x = (a,b)$

Teorema di ricorsione transfinita (V2) Dato $\gamma \in Ord$, due funzioni classe $G_1 : Ord \times V \longrightarrow V$ e $G_2 : V \longrightarrow V$, esiste un'unica funzione classe F t.c.

$$F(0) = \gamma$$
$$F(S(\alpha)) = G_1(\alpha, F(\alpha))$$
$$F(\lambda) = G_2(F|_\lambda)$$

DIMOSTRAZIONE

Applichiamo la ricorsione transfinita (V1) con

$$G(f) = \begin{cases} \emptyset & \text{se } f \text{ non è una funzione con } Dom(f) \in Ord \\ \gamma & \text{se } f = \emptyset \\ G_1(\alpha, f(\alpha)) & \text{se } Dom(f) = S(\alpha) \text{ per qualche } \alpha \in Ord \\ G_2(f) & \text{se } Dom(f) = \lambda \text{ limite} \end{cases}$$

$\square$

Corollario Esistono le funzioni classe di somma, prodotto e potenza di ordinali così definite:

$$\begin{cases} \alpha + 0 = \alpha \\ \alpha + S(\beta) = S(\alpha + \beta) \\ \alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\} \end{cases} \qquad \begin{cases} \alpha \cdot 0 = 0 \\ \alpha \cdot S(\beta) = \alpha \cdot \beta + \alpha \\ \alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\} \end{cases}$$

$$\begin{cases} \alpha^0 = 1 \\ \alpha^{S(\beta)} = \alpha^\beta \cdot \alpha \\ \alpha^\lambda = \sup\{\alpha^\beta \mid \beta < \lambda\} \end{cases}$$

Def. Una funzione classe $F : Ord \longrightarrow Ord$ mai decrescente si dice continua se per ogni ordinale limite λ vale $F(\lambda) = \sup F[\lambda]$

Proposizione $\forall \alpha, \beta \in Ord$ $\quad \alpha + \beta \sim (\alpha, \in) + (\beta, \in)$
$\alpha \cdot \beta \sim (\alpha, \in) \cdot (\beta, \in) \qquad \alpha^\beta \sim (\alpha, \in)^{(\beta, \in)}$

DIMOSTRAZIONE

Per induzione transfinita (V2) su β

I casi 0 e successore sono conseguenze immediate delle definizioni

Ad esempio:
- $\alpha \sim (\alpha + 0, \in) \sim (\alpha, \in) + (0, \in) \sim \alpha$
- $(\alpha + \beta, \in) \sim (\alpha, \in) + (\beta, \in)$

  $(S(\alpha + \beta), \in) \sim ((\alpha, \in) + (\beta, \in)) + (1, \in) \sim (\alpha, \in) + ((\beta, \in) + (1, \in)) \sim (\alpha, \in) + (S(\beta), \in)$

- $\alpha + \lambda = \bigcup\{\alpha + \beta \mid \beta < \lambda\}$

  $(\alpha + \beta, \in) \longrightarrow (\alpha, \in) + (\beta, \in)$ al variare di β

  $\underbrace{(\bigcup_{\beta<\lambda} \alpha + \beta, \in)}_{(\alpha + \lambda, \in)} \longrightarrow \bigcup_{\beta<\lambda} (\alpha, \in) + (\beta, \in) = \underbrace{(\alpha, \in) + \bigcup_{\beta<\lambda} (\beta, \in)}_{(\alpha, \in) + (\lambda, \in)}$

- Analogo per $\alpha \cdot \lambda$
- Analogo per α^λ con un aggiustamento tecnico

$\square$

Aritmetica ordinale

Lemma Dati A, B insiemi di ordinali
$\forall a \in A\ \exists b \in B\ a \leq b \longrightarrow \sup A \leq \sup B$

DIMOSTRAZIONE
Segue dalla def. di sup $\square$

Proposizione Le funzioni $(\alpha,\beta) \mapsto \alpha+\beta$, $(\alpha,\beta)\mapsto \alpha\cdot\beta$, $(\alpha,\beta)\mapsto\alpha^\beta$ sono strettamente crescenti nel secondo argomento e crescenti in senso largo nel primo argomento, cioè:

$$\beta_1 < \beta_2 \longrightarrow \alpha+\beta_1 < \alpha+\beta_2$$
$$\alpha\cdot\beta_1 < \alpha\cdot\beta_2 \qquad \alpha>0$$
$$\alpha^{\beta_1} < \alpha^{\beta_2} \qquad \alpha>1$$
$$\alpha_1<\alpha_2 \longrightarrow \alpha_1+\beta \leq \alpha_2+\beta$$
$$\alpha_1\cdot\beta \leq \alpha_2\cdot\beta \qquad \beta>0$$
$$\alpha_1^\beta \leq \alpha_2^\beta$$

DIMOSTRAZIONE
Dimostriamo per la somma, per prodotto e esponenziale è analogo.

(1) $\beta_1<\beta_2 \longrightarrow \alpha+\beta_1<\alpha+\beta_2$
Per induzione transfinita (V2) su β_2
- $\beta_2=0$ ok
- $\beta_2=S(\gamma)$: $\beta_1<S(\gamma) \longrightarrow \beta_1\leq\gamma \longrightarrow \beta_1=\gamma \vee \beta_1<\gamma$
  se $\beta_1<\gamma$ per hp. ind $\alpha+\beta_1<\alpha+\gamma<\alpha+S(\gamma)=S(\alpha+\gamma)=\alpha+\beta_2$
  se $\beta_1=\gamma$ $\alpha+\beta_1<S(\alpha+\beta_1)=\alpha+S(\gamma)=\alpha+\beta_2$
- $\beta_2=\lambda$ limite: $\beta_1<\lambda \longrightarrow S(\beta_1)<\lambda$
  $\alpha+\beta_1 \overset{\text{hp ind}}{<} \alpha+S(\beta_1)\leq\alpha+\lambda=\sup\{\alpha+\gamma \mid \gamma<\lambda\}$

(2) $\alpha_1<\alpha_2 \longrightarrow \alpha_1+\beta\leq\alpha_2+\beta$
Per induzione transfinita (V2) su β
- $\beta=0$: ovvio
- $\beta=S(\gamma)$: $\alpha_1<\alpha_2 \xrightarrow{\text{hp ind}} \alpha_1+\gamma\leq\alpha_2+\gamma \longrightarrow S(\alpha_1+\gamma)\leq S(\alpha_2+\gamma)$
  $\longrightarrow \alpha_1+S(\gamma)=\alpha_1+\beta\leq\alpha_2+\beta=\alpha_2+S(\gamma)$
- $\beta=\lambda$ limite: $\alpha_1<\alpha_2 \longrightarrow \underset{\sup_{\beta<\lambda}\{\alpha_1+\beta\}}{\alpha_1+\lambda} \leq \underset{\sup_{\beta<\lambda}\{\alpha_2+\beta\}}{\alpha_2+\lambda}$
  e per hp. ind. $\alpha_1+\beta\leq\alpha_2+\beta$
  quindi la disuguaglianza vale per il lemma $\square$

<u>OSS</u> Sia $A\subseteq \mathrm{Ord}$
$\sup A\notin A \Rightarrow \sup(A)$ è limite

DIMOSTRAZIONE
Per assurdo, assumo $\sup A = S(\alpha)\notin A$
$\exists\beta\in A \quad \alpha<\beta\leq S(\alpha) \Longrightarrow \beta=S(\alpha)$ $\lightning$ $\square$

OSS Dati $A \subseteq Ord$ e $\alpha \in Ord$

$\alpha + \sup A = \sup(\{\alpha+\gamma \mid \gamma \in A\})$

$\alpha \sup A = \sup\{\alpha \cdot \gamma \mid \gamma \in A\}$

$\alpha^{\sup A} = \sup\{\alpha^{\gamma} \mid \gamma \in A\}$

DIMOSTRAZIONE

Se $\beta = \sup A \in A$: $\alpha+\beta \leq \sup\{\alpha+\gamma \mid \gamma \in A\} \leq \alpha+\beta$

Se $\beta = \sup A \notin A \implies \beta = \lambda$

$\alpha+\lambda = \sup\{\alpha+\gamma_1 \mid \gamma_1 < \lambda\} = \sup\{\alpha+\gamma_2 \mid \gamma_2 \in A\}$

Dato $\gamma_1 < \lambda$, non è maggiorante di A, quindi esiste $\beta_1 \in A$ con $\gamma_1 < \beta_1 \longrightarrow \alpha+\gamma_1 < \alpha+\beta_1$

Viceversa, dato $\beta_2 \in A$, siccome $\sup A = \lambda$ è limite, $\beta_2 < S(\beta_2) < \lambda$, quindi ponendo $\gamma_2 = S(\beta_2)$ vale $\alpha+\beta_2 < \alpha+\gamma_2$

Analogo per $\cdot$ e $\wedge$ $\square$

> **Proposizione** Dati $\alpha, \beta, \gamma \in Ord$
>
> $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$ $\qquad$ $\alpha\cdot(\beta\cdot\gamma) = (\alpha\cdot\beta)\cdot\gamma$
>
> $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$ $\qquad$ $\alpha^{\beta+\gamma} = \alpha^{\beta}\cdot\alpha^{\gamma}$ $\qquad$ $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\cdot\gamma}$

DIMOSTRAZIONE

1) Per induzione transfinita su γ

- $\gamma = 0$: $\alpha+(\beta+0) = \alpha+\beta = (\alpha+\beta)+0$
- $\gamma = S(\delta)$: $\alpha+(\beta+\delta) = (\alpha+\beta)+\delta$

  $\alpha+(\beta+S(\delta)) = \alpha+S(\beta+\delta) = S(\alpha+(\beta+\delta)) \overset{\text{hp.ind}}{=} S((\alpha+\beta)+\delta) = (\alpha+\beta)+S(\delta)$
- $\gamma = \lambda$ $\quad$ $\alpha+(\beta+\lambda) = (\alpha+\beta)+\lambda$

  $\alpha+(\beta+\lambda) = \alpha+\sup\{\beta+\delta \mid \delta<\lambda\} = \sup\{\alpha+(\beta+\delta) \mid \delta<\lambda\} \overset{\text{hp ind}}{=}$

  $= \sup\{(\alpha+\beta)+\delta \mid \delta<\lambda\} = (\alpha+\beta)+\lambda$

Gli altri casi sono analoghi. $\square$

> **Lemma (sottrazione di ordinali)** Dati $\alpha, \beta \in Ord$ con $\alpha \leq \beta$, esiste un unico γ t.c.
>
> $\alpha+\gamma = \beta$

DIMOSTRAZIONE

L'unicità di γ è ovvia

$\gamma_1 < \gamma_2 \implies \beta = \alpha+\gamma_1 < \alpha+\gamma_2 = \beta$ ↯

Considero il minimo δ t.c. $\alpha+\delta > \beta$ (che esiste perché $\beta < S(\beta) \leq \alpha+S(\beta)$)

Dico che δ è successore

per assurdo $\alpha+\delta = \sup\{\alpha+\varepsilon \mid \varepsilon<\delta\} > \beta$

$\implies \exists\, \varepsilon<\delta$ t.c. $\alpha+\varepsilon > \beta$ ↯

Sia $\delta = S(\gamma)$

$\alpha+S(\gamma) = S(\alpha+\gamma) > \beta$

$\alpha+\gamma \leq \beta < S(\alpha+\gamma)$

$\implies \alpha+\gamma = \beta$ $\square$

Lemma (divisione euclidea di ordinali) Dati $\alpha \in Ord$, $\beta \in Ord, \beta > 0$ esistono unici $\gamma \in Ord$, $\rho \in Ord$, $\rho < \beta$ t.c.
$$\alpha = \beta \cdot \gamma + \rho$$

DIMOSTRAZIONE

L'unicità di ρ segue da quella di γ

Per assurdo $\gamma_1 < \gamma_2$ $\quad \alpha = \beta \cdot \gamma_1 + \rho_1 < \beta \cdot \gamma_1 + \beta = \beta \cdot S(\gamma_1) \leq \beta \cdot \gamma_2 \leq \beta \cdot \gamma_2 + \rho_2 = \alpha$ ↯

Per l'esistenza, prendo il minimo ε t.c. $\alpha < \beta \cdot \varepsilon$

Dico che ε è successore $\varepsilon = S(\gamma)$: se non lo fosse

$\alpha < \beta \cdot \varepsilon = \sup\{\beta \cdot \delta \mid \delta < \varepsilon\}$ ma allora esiste $\delta < \varepsilon$ t.c. $\alpha < \beta \cdot \delta$ ↯

Allora $\beta \cdot \gamma \leq \alpha \longrightarrow \beta \cdot \gamma + \delta = \alpha$

Per assurdo sia $\delta \geq \beta$: $\alpha = \beta \cdot \gamma + \delta \geq \beta \cdot \gamma + \beta = \beta \cdot S(\gamma) = \beta \cdot \varepsilon > \alpha$ ↯ □

Teorema: forma normale di Cantor Ogni $\alpha \in Ord$ si scrive in maniera unica come
$$\alpha = \omega^{\alpha_1} k_1 + \omega^{\alpha_2} k_2 + \ldots + \omega^{\alpha_n} k_n$$
con $\alpha_1 > \ldots > \alpha_n$ ordinali e $k_1, \ldots, k_n \in \omega \setminus \{0\}$

DIMOSTRAZIONE

<u>Unicità</u> Per assurdo, sia α il minimo t.c.

$\omega^{\alpha_1} k_1 + \ldots + \omega^{\alpha_n} k_n = \omega^{\alpha_1'} k_1' + \ldots + \omega^{\alpha_m'} k_m' = \alpha$

Ci basta dire che $\alpha_1 = \alpha_1'$ e $k_1 = k_1'$; infatti allora

$\omega^{\alpha_2} \cdot k_2 + \ldots + \omega^{\alpha_n} \cdot k_n = \omega^{\alpha_2'} \cdot k_2' + \ldots + \omega^{\alpha_m'} \cdot k_m' < \omega^{\alpha_1}$ ↯ per la minimalità di α

Se $\alpha_1 = \alpha_1'$ allora $\omega^{\alpha_1} \cdot k_1 + \ldots = \omega^{\alpha_1} \cdot k_1' + \ldots$, quindi

$k_1 = k_1'$ per la divisione euclidea

Se infine $\alpha_1 < \alpha_1'$ abbiamo

$\omega^{\alpha_1} \cdot k_1 + \ldots + \omega^{\alpha_n} \cdot k_n < \omega^{S(\alpha_1)} \leq \omega^{\alpha_1'} \cdot k_1' + \ldots + \omega^{\alpha_m'} \cdot k_m'$ ↯

<u>Esistenza</u> Sia α minimo t.c. α non ha una forma normale di Cantor

Sia ε minimo t.c. $\omega^{\varepsilon} > \alpha$ (che esiste perché $\alpha < \omega^{S(\alpha)}$)

Come al solito, $\varepsilon = S(\alpha_1)$

$\omega^{\alpha_1} \leq \alpha$ per la minimalità di ε

$\Rightarrow \alpha = \omega^{\alpha_1} k_1 + \rho_1$ con $\rho_1 < \omega^{\alpha_1}$

- Se per assurdo $k_1 \geq \omega$

$\alpha < \omega^{S(\alpha_1)} = \omega^{\alpha_1} \cdot \omega \leq \omega^{\alpha_1} \cdot k_1 + \rho_1 = \alpha$ ↯

- Se fosse $k_1 = 0$

$\alpha = \rho_1 < \omega^{\alpha_1}$ ↯

Ora ρ_1 ha una forma normale di Cantor:

$\alpha = \omega^{\alpha_1} \cdot k_1 + \rho_1 = \omega^{\alpha_1} \cdot k_1 + (\omega^{\alpha_2} \cdot k_2 + \ldots)$

Inoltre $\rho_1 < \omega^{\alpha_1} \Rightarrow \omega^{\alpha_2} < \omega^{\alpha_1} \Rightarrow \alpha_2 < \alpha_1$

quindi α è in forma normale □

<u>esempio</u> $\varepsilon_0 = \omega^{\omega^{\omega^{\omega^{\cdots}}}}$ cioè $\varepsilon_0 = \omega^{\varepsilon_0}$

proposizione Sia $F: Ord \longrightarrow Ord$ una funzione classe debolmente crescente e continua
Allora F ha una classe propria di punti fissi : $F(\alpha) = \alpha$

DIMOSTRAZIONE

Se $F(\alpha)=\alpha$, α è un punto fisso.

Se $\alpha < F(\alpha)$, allora definiamo $\alpha_n = F^n(\alpha)$

(oppure $H: n \longmapsto \alpha_n$ con $H(0)=\alpha$, $H(s(\beta)) = F(H(\beta))$, $H(\lambda) =$ fate voi)

Sia $\beta = \sup\{\alpha_n \mid n \in \omega\}$

$F(\beta) = \sup\{F(\alpha_n) \mid n \in \omega\} = \sup\{\alpha_{s(n)} \mid n \in \omega\} = \beta$

ed è una classe propria perché è superiormente illimitata □

esercizio Esiste una funzione classe $G: Ord \longrightarrow Ord$
che è una bigezione tra Ord e $Fix(F)$

DEF. $\varepsilon_\alpha \equiv \alpha$-esimo punto fisso di $x \longmapsto \omega^x$

esercizio ε_0 è numerabile
$\varepsilon_{\varepsilon_0}$ è numerabile
Sia ζ_0 il minimo t.c. $\zeta_0 = \varepsilon_{\zeta_0}$. Dimostrare che $|\zeta_0| = \aleph_0$

operazioni in forma normale di cantor

Lemma Dati $\alpha, \beta, \gamma \in Ord$
$\alpha < \omega^\beta \leq \gamma \longrightarrow \alpha + \gamma = \gamma$

DIMOSTRAZIONE

Abbiamo che $\alpha + \gamma \geq \gamma$

Bisogna mostrare $\alpha + \gamma \leq \gamma$

Scrivendo α in forma normale otteniamo

$\alpha = \omega^{\beta_1} \cdot k_1 + \ldots + \omega^{\beta_n} \cdot k_n$ con $\beta_1 > \ldots > \beta_n$

Quindi $\alpha = \omega^{\beta_1} \cdot k_1 + \ldots + \omega^{\beta_n} \cdot k_n \leq \omega^{\beta_1} \cdot k_1 + \ldots + \omega^{\beta_1} \cdot k_n = \omega^{\beta_1}(k_1 + \ldots + k_n) = \omega^{\beta_1} \cdot k$

Ora da $\alpha < \omega^\beta$ segue $\beta_1 < \beta$, quindi $s(\beta_1) \leq \beta$ e perciò possiamo scrivere

$\gamma = \omega^{s(\beta_1)} + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma'$

da cui $\alpha + \gamma \leq \omega^{\beta_1} \cdot k + \omega^{\beta_1} \cdot \omega + \gamma' = \omega^{\beta_1}(k + \omega) + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma' = \gamma$

dove questa uguaglianza segue da

$k + \omega = \sup\{k + n \mid n \in \omega\} = \omega$ □

proposizione Per le somme ($m,n\neq 0$)

$$\omega^\alpha\cdot m+\omega^\beta\cdot n=\begin{cases}\omega^\alpha m+\omega^\beta n & \alpha>\beta\\ \omega^\alpha(m+n) & \alpha=\beta\\ \omega^\beta\cdot n & \alpha<\beta\end{cases}$$

Per i prodotti si applica la proprietà distributiva, poi

$$\beta>0 \longrightarrow (\omega^{\alpha_1}\cdot k_1+\dots)\cdot\omega^\beta=\omega^{\alpha_1+\beta}$$

$$n\in\omega\setminus\{0\} \longrightarrow (\omega^{\alpha_1}\cdot k_1+\dots)\cdot n=\omega^{\alpha_1}\cdot k_1\cdot n+\omega^{\alpha_2}k_2+\dots$$

Per le potenze si usano $\alpha^{\beta+\gamma}=\alpha^\beta\cdot\alpha^\gamma$ e $\alpha^{\beta\cdot n}=(\alpha^\beta)^n$, poi

$$k^{\omega^{1+\alpha}}=\omega^{\omega^\alpha}$$

$$\beta>0\wedge\alpha_1>0\longrightarrow(\omega^{\alpha_1}\cdot k_1+\omega^{\alpha_2}\cdot k_2+\dots)^{\omega^\beta}=\omega^{\alpha_1\cdot\omega^\beta}$$

DIMOSTRAZIONE

La regola per le somme è immediata.

Per il prodotto, osserviamo che $n\,\omega=\omega$ per $n\in\omega\setminus\{0\}$, infatti:

$$\omega\leq n\cdot\omega=\sup\{n\cdot i\mid i\in\omega\}=\sup\{m\mid m\in\omega\}=\omega$$

Ora scrivendo $\beta=1+\gamma$

$$\omega^{\alpha_1+\beta}=\omega^{\alpha_1}\cdot\omega^\beta\leq(\omega^{\alpha_1}\cdot k_1+\omega^{\alpha_2}\cdot k_2+\dots)\cdot\omega^\beta\leq(\omega^{\alpha_1}\cdot k_1+\dots+\omega^{\alpha_1})\cdot\omega^\beta=$$
$$=\omega^{\alpha_1}(k_1+1)\,\omega^\beta=\omega^{\alpha_1}(k_1+1)\,\omega\,\omega^\gamma=\omega^{\alpha_1}\,\omega\,\omega^\gamma=\omega^{\alpha_1+\beta}$$

L'altra regola del prodotto si ottiene facilmente per induzione su n.

Questa è immediata:

$$k^{\omega^{1+\alpha}}=k^{\omega\cdot\omega^\alpha}=(\sup\{k^n\mid n\in\omega\})^{\omega^\alpha}=\omega^{\omega^\alpha}$$

Per dimostrare l'ultima, consideriamo il caso particolare $(\omega^\alpha\cdot k)^\omega=\omega^{\alpha\omega}$:

$$\omega^{\alpha\omega}\leq(\omega^\alpha\cdot k)^\omega=\sup\{(\omega^\alpha\cdot k)^n\mid n\in\omega\}=\sup\{\omega^{\alpha\cdot n}\cdot k\mid n\in\omega\}\leq$$
$$\leq\sup\{\omega^{\alpha(n+1)}\mid n\in\omega\}\leq(\omega^\alpha)^\omega=\omega^{\alpha\cdot\omega}$$

Siccome $\beta>0$, scriviamo $\beta=1+\gamma$, quindi abbiamo $\omega^\beta=\omega\cdot\omega^\gamma$

$$\omega^{\alpha_1\cdot\omega^\beta}\leq(\omega^{\alpha_1}\cdot k_1+\omega^{\alpha_2}\cdot k_2+\dots)^{\omega^\beta}\leq(\omega^{\alpha_1}(k_1+1))^{\omega\cdot\omega^\gamma}=\omega^{\alpha_1\cdot\omega\cdot\omega^\gamma}=\omega^{\alpha_1\cdot\omega^\beta}$$

$\square$

Gli aleph

OSS Se $\alpha, \beta \in Ord$, allora o $|\alpha| < |\beta|$ o $|\alpha| = |\beta|$ o $|\beta| < |\alpha|$

DIMOSTRAZIONE

Necessariamente o $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$

$\longrightarrow |\alpha| \leq |\beta| \vee |\beta| \leq |\alpha|$ $\square$

DEF. $\alpha \in Ord$ è iniziale se $\forall \beta < \alpha \quad |\beta| < |\alpha|$

esercizio iniziale $\wedge$ infinito $\longrightarrow$ limite

Teorema di Hartogs Dato un insieme X esiste $\alpha \in Ord$ t.c.

$$|\alpha| \nleq |X|$$

cioè non esiste una funzione iniettiva da α a X

DIMOSTRAZIONE

Considero $Y = \{ R \in P(X \times X) \mid \exists A \subseteq X \text{ "} R \text{ è un buon ordine su } A \text{"} \}$

Considero la funzione classe

$$F : Y \longrightarrow Ord$$
$$R \longmapsto \alpha \sim R$$

Quindi per rimpiazzamento, esiste $F[Y]$

Sia $\alpha = S(\sup(F[Y]))$ allora $|\alpha| \nleq |X|$ $\square$

DEF. Dato X, il numero di Hartogs di X $H(X)$ è il minimo ordinale α t.c. $|\alpha| \nleq |X|$

OSS Dato X, $H(X)$ è un ordinale iniziale

DIMOSTRAZIONE

Per assurdo, $\alpha < H(X)$ $|\alpha| = |H(X)|$

ma allora $|H(X)| = |\alpha| \leq |X|$ $\lightning$ $\square$

corollario gli ordinali iniziali sono una classe propria

DIMOSTRAZIONE

Se non lo fossero, sarebbero un insieme X.

Considero $H(\sup X)$ $\square$

proposizione Sia C una classe propria di ordinali.
Esiste un'unica funzione classe $F : Ord \longrightarrow C$ crescente e surgettiva

DIMOSTRAZIONE

Per ricorsione (1° forma)

$$F(\alpha) = \min (C \setminus F[\alpha])$$ $\square$

Def. $\omega_\alpha \overset{\text{def.}}{=} \min\left(Ord_{\text{inInf}} \setminus \{\omega_\beta \mid \beta < \alpha\}\right)$

ossia $\omega_0 = \omega$

$\omega_{s(\alpha)} = H(\omega_\alpha)$

$\omega_\lambda = \sup\{\omega_\alpha \mid \alpha \in \lambda\}$ per λ limite

<u>NOTAZIONE</u> $|X| = \aleph_\alpha \quad \equiv \quad |X| = |\omega_\alpha|$

<u>OSS</u> Se $\aleph_0 \leq |X| \leq \aleph_\alpha \longrightarrow \exists \beta \in Ord \quad |X| = \aleph_\beta$

DIMOSTRAZIONE

$|X| \leq \aleph_\alpha \longrightarrow \exists f : X \longrightarrow \omega_\alpha$ iniettiva

$a \prec b \Leftrightarrow f(a) < f(b)$ definisce un b.o. su X

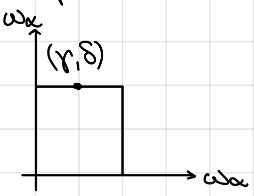
$\longrightarrow \exists \beta \in Ord \quad |X| = |\beta|$

Considero β minimo: è iniziale $\square$

Lemma $\aleph_\beta \cdot \aleph_\beta = \aleph_\beta$

DIMOSTRAZIONE

Scopo: ordinare $\omega_\alpha \times \omega_\alpha$ in modo isomorfo a ω_α



$$(\gamma,\delta) \prec (\gamma',\delta') \equiv \begin{cases} \max(\gamma,\delta) < \max(\gamma',\delta') \\ \max(\gamma,\delta) = \max(\gamma',\delta') \wedge \gamma < \gamma' \\ \max(\gamma,\delta) = \max(\gamma',\delta') \wedge \gamma = \gamma' \wedge \delta < \delta' \end{cases}$$

Osserviamo che $\prec$ è un buon ordine su $\omega_\alpha \times \omega_\alpha$

Dimostriamo che $(\omega_\alpha \times \omega_\alpha, \prec) \sim \omega_\alpha$ per induzione transfinita

Assumo $\forall \beta < \alpha \quad (\omega_\beta \times \omega_\beta, \prec) \sim \omega_\beta$

Sia $\gamma \sim (\omega_\alpha \times \omega_\alpha, \prec)$: devo dimostrare $\gamma = \omega_\alpha$

1. γ è iniziale

Altrimenti, esiste $\delta < \gamma$ t.c. $|\delta| = |\gamma| \longrightarrow \delta \sim (\omega_\alpha \times \omega_\alpha, \prec)_{(\varepsilon,\pi)} \subseteq \mu \times \mu$ dove $\mu = s(\max(\varepsilon,\pi))$

$|\mu| < |\omega_\alpha| \longrightarrow |\mu \times \mu| = |\mu| < |\omega_\alpha|$ perché μ è un aleph

$\Rightarrow |\omega_\alpha \times \omega_\alpha| = |\gamma| = |\delta| \leq |\mu \times \mu| = |\mu| < |\omega_\alpha| \quad \lightning$

2. $\gamma = \omega_\alpha$

Chiaramente $\gamma \not< \omega_\alpha$

Supponiamo per assurdo che $\omega_\alpha < \gamma$

Come prima, otteniamo $|\gamma| \leq |\mu \times \mu| = |\mu| < |\omega_\alpha| \quad \lightning \quad \square$

Proposizione $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\max\{\alpha,\beta\}}$

DIMOSTRAZIONE

Assumo $\alpha \leq \beta$: $\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta \cdot 2 \leq \aleph_\beta \cdot \aleph_\alpha \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta \quad \square$

<u>OSS</u> Dato X, se esiste $\prec$ b.o. su X, allora $\exists \alpha \in Ord \quad |X| = \aleph_\alpha$

ASSIOMA DI SCELTA

⑨ **Assioma della scelta (AC)**

Dato X insieme di insiemi non vuoti,
allora esiste una funzione di scelta per X,
cioè $f: X \longrightarrow \bigcup X$, con $\forall A \in X \; f(A) \in A$

Proposizione AC $\longleftrightarrow$ ogni f surgettiva ha un'inversa destra
cioè se $f: A \to B$ surgettiva $\exists g: B \to A \quad f \circ g = id_A$

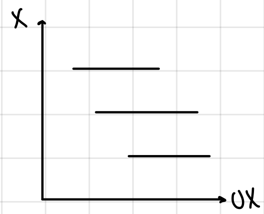
DIMOSTRAZIONE

$\Rightarrow$ Fisso $f: A \to B$ surgettiva

Sia $h: P(A) \setminus \{\emptyset\} \longrightarrow A$ una funzione di scelta

$$g: B \longrightarrow A$$
$$b \longmapsto h[\{x \in A \mid f(x) = b\}]$$ dove l'insieme è non vuoto.

Si verifica $f \circ g = id_A$



$\Leftarrow$ X insieme di insiemi non vuoti

Sia $Y = \bigcup \{ A \times \{A\} \mid A \in X \}$

oppure $Y = \{(a, A) \mid a \in A \in X\}$

Considero $f: Y \longrightarrow X$

$$(a, A) \longmapsto A \quad \text{surgettiva}$$

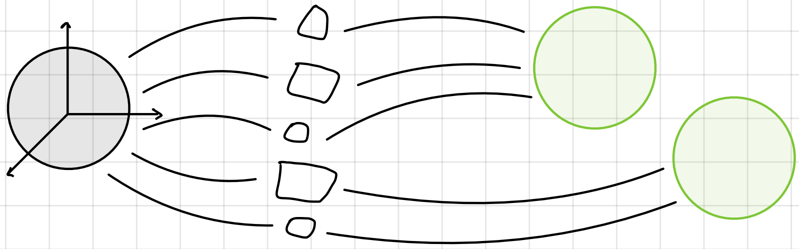
La sua inversa destra $g: X \longrightarrow Y$

$$A \longmapsto (a, A)$$

Componendo con la proiezione sulla prima componente:

$\pi \circ g: A \longmapsto a \in A$ è una funzione di scelta. □

PARADOSSO DI BANACH-TARSKI



ESERCIZIO cappelli dei Puffi

Teorema di Zermelo (Teorema del buon ordinamento) Ogni insieme è bene ordinabile
$\forall S \ \exists < \in S \times S \quad (S,<)$ è un buon ordinamento

Def. Dato $(S,<)$ ordine parziale
- una **sottocatena** è un $A \subseteq S$ t.c. la restrizione di $<$ ad A è un ordine totale
- un **maggiorante** di $A \subseteq S$ è un $x \in S$ t.c. $\forall y \in A \ \ y \leq x$
- $x \in S$ è un **elemento massimale** se $\neg \exists y \in S \ \ x < y$

Lemma di Zorn Ogni insieme parzialmente ordinato in cui ogni sottocatena ammette maggioranti ha elementi massimali.

Teorema AC $\longleftrightarrow$ Teorema di Zermelo $\longleftrightarrow$ Lemma di Zorn

DIMOSTRAZIONE

<u>Piano</u>:
$$\begin{tikzcd} \text{Zermelo} \arrow[r, "1"'] & AC \arrow[r, "2"'] \arrow[rr, bend left, "2'"] & \text{Zorn} \arrow[r, "3"'] & \text{Zermelo} \end{tikzcd}$$

(1) Sia X insieme di insiemi non vuoti
Considero $<$ b.o. su $\bigcup X$
Costruisco $f: X \longrightarrow \bigcup X$
$f(A) = \min_< A$ è una funzione di scelta di X

(2'-Idea) $X \rightsquigarrow$ b.o. su X alternativamente $F: \alpha \to X$ biunivoca, $\alpha \in Ord$
Fisso $h: \mathcal{P}^{\neq\emptyset}(X) \longrightarrow X$ funzione di scelta
$F(\alpha) = h(X \setminus F[\alpha])$ non funziona
$$F(\alpha) = \begin{cases} h(X \setminus F[\alpha]) & \text{se } F[\alpha] \subsetneq X \\ \spadesuit & \text{altrimenti} \end{cases}$$

(2) $(X,<)$ ordine parziale
$\forall A \subseteq X \quad A$ sottocatena $\longrightarrow \exists x \in X \ \forall a \in A \ \ a \leq x$
Per assurdo, X non abbia elementi massimali $\forall x \in X \ \exists y \in X \ \ x < y$
$\forall A \subseteq X \quad A$ sottocatena $\longrightarrow \exists x \in X \ \forall a \in A \ \ a < x$
Fisso $h: \mathcal{P}^{\neq\emptyset}(X) \longrightarrow X$ funzione di scelta
$F(\alpha) = h(\{x \in X \mid \forall p \in F[\alpha] \ p < x\})$
Devo dimostrare che F è crescente
Sia per assurdo $\alpha \in Ord$ minimo t.c. $\exists \beta < \alpha \quad F(\beta) \nless F(\alpha)$
$F(\alpha)$ è un maggiorante della sottocatena $F[\alpha]$ $\quad \lightning$
quindi $F(\alpha) > F(\beta) \in F[\alpha]$ $\lightning$

(3) Dato X, voglio trovare un buon ordine su X, alternativamente $f: \alpha \to X$ biunivoca, $\alpha \in Ord$
Sia $Y =$ "funzioni $\alpha \longrightarrow X$ iniettiva con $\alpha \in Ord$" $\quad (\Leftrightarrow \alpha \in \mathcal{H}(X))$
$(Y, \subseteq)$ soddisfa le ipotesi di Zorn: l'elemento massimale f è anche surgettivo
Se non lo fosse, esisterebbe $y \in Y \setminus Im(f)$ per cui $f' = f \cup \{(Dom(f), y)\} > f$ $\lightning$
<u>Verifica</u>: Sia C catena di Y: $\bigcup C$ è una funzione iniettiva
Date $f, g \in C \longrightarrow \underbrace{f|_{Dom f \cap Dom g}}_{f} = \underbrace{g|_{Dom f \cap Dom g}}_{g|_{Dom f}} = f$
$f \subseteq g \longrightarrow$

$\square$

conseguenze immediate di AC

proposizione Ogni insieme è equipotente a un ordinale iniziale. In particolare, ogni cardinalità infinita è un aleph.

DIMOSTRAZIONE
Per il teorema di buon ordinamento ogni insieme è bene ordinabile, quindi, per le proprietà degli ordinali iniziali, equipotente ad un unico ordinale iniziale.
La seconda segue dal fatto che gli ω_α sono tutti e soli gli ordinali iniziali infiniti $\square$

proposizione Assumere che ogni insieme è equipotente ad un ordinale implica AC

DIMOSTRAZIONE
Se $|X| = |\alpha|$ con $\alpha \in Ord$, c'è una bigezione fra X e α, e quindi un buon ordinamento di X. $\square$

proposizione Tutte le cardinalità sono confrontabili:
$\forall X, Y \quad |X| < |Y| \ \vee \ |X| = |Y| \ \vee \ |Y| < |X|$

DIMOSTRAZIONE
Segue dal fatto che le cardinalità degli ordinali sono confrontabili $\square$

proposizione La confrontabilità delle cardinalità implica AC

DIMOSTRAZIONE
Dimostriamo il teorema del buon ordinamento.
Per definizione $|H(X)| \nleq |X|$, quindi $|X| < |H(X)|$
Ossia esiste $f : X \longrightarrow H(X) \in Ord$ iniettiva $\square$

corollario $\forall X$ infinito $|X \times X| = |X|$

DIMOSTRAZIONE
Se $|X| = \aleph_\alpha$ abbiamo $|X \times X| = |\omega_\alpha \times \omega_\alpha| = |\omega_\alpha| = |X|$ $\square$

corollario $\forall X \quad X$ infinito $\longleftrightarrow \aleph_0 \leq |X|$

DIMOSTRAZIONE
$\longleftarrow$: già vista
$\longrightarrow$: $\aleph_0$ è il minimo aleph infinito $\square$

proposizione X è finito $\longleftrightarrow$ X è Dedekind-finito

DIMOSTRAZIONE
$\longrightarrow$: già visto
$\longleftarrow$: Supponiamo X non sia finito, allora $|X| = \aleph_\alpha$ per qualche α, allora esiste $f : \omega_\alpha \longrightarrow X$ biunivoca

$$g : X \longrightarrow X \setminus \{f(0)\}$$
$$x \longmapsto f \circ s \circ f^{-1}(x)$$

è una bigezione fra X e $X \setminus \{f(0)\} \subsetneq X$ ↯ $\square$

Proposizione $0 < |X| \leq |Y| \longleftrightarrow \exists f: Y \to X$ surgettiva

DIMOSTRAZIONE

$\rightarrow$: Data $g: X \to Y$ iniettiva e $a \in X$, la funzione

$$f: Y \longrightarrow X$$
$$y \longmapsto \begin{cases} f^{-1}(y) & \text{se } y \in f[X] \\ a & \text{altrimenti} \end{cases} \quad \text{è surgettiva}$$

$\leftarrow$: Data $f: Y \to X$ surgettiva, un'inversa destra è iniettiva □

Proposizione Se $|S| \leq \aleph_\alpha$ e $\forall A \in S$ $|A| \leq \aleph_\alpha$, allora $|\bigcup S| \leq \aleph_\alpha$

DIMOSTRAZIONE

Possiamo assumere $\emptyset \notin S \neq \emptyset$. Basta esibire una funzione surgettiva $f: \omega_\alpha \times \omega_\alpha \to \bigcup S$. Sia $g: \omega_\alpha \to S$ surgettiva. Per ipotesi, $H_A := \{h: \omega_\alpha \to A \mid h \text{ è surgettiva}\}$ è non vuoto.

Sia ℓ una funzione di scelta per $\{H_A \mid A \in S\}$

Allora
$$f: \omega_\alpha \times \omega_\alpha \longrightarrow \bigcup S$$
$$(x, y) \longmapsto \ell(H_{g(x)})(y) \quad \text{è surgettiva.}$$

Infatti preso $z \in \bigcup S$, esiste $A \in S$ tale che $z \in A$, quindi esiste $x \in \omega_\alpha$ tale che $z \in g(x) = A$. Siccome $h = \ell(H_A)$ è surgettiva $\omega_\alpha \to A$, esiste $y \in \omega_\alpha$ tale che $z = h(y) = \ell(H_{g(x)})(y)$ □

Corollario Un'unione numerabile (risp. al più numerabile) di insiemi numerabili (risp. al più numerabili) è numerabile (risp. al più numerabile).

<u>OSS</u> Sia $\mathcal{P}^{\leq n}(X) = \{A \in \mathcal{P}(X) \mid |A| \leq n\}$

Se X è infinito e $0 < n < \omega$ allora $|\mathcal{P}^{\leq n}(X)| = |X|$

DIMOSTRAZIONE

La disuguaglianza $|X| \leq |\mathcal{P}^{\leq n}(X)|$ segue dal fatto che

$X \to \mathcal{P}^{\leq n}(X)$: $x \mapsto \{x\}$ è iniettiva.

Per l'altra disuguaglianza, sia $|X| = \aleph_\alpha$, allora $|{}^n X| = \aleph_\alpha^n = \aleph_\alpha$, quindi basta osservare che la funzione seguente è surgettiva.

$${}^n X \longrightarrow \{A \in \mathcal{P}(X) \mid 0 < |A| \leq n\} \subseteq \mathcal{P}^{\leq n}(X)$$
$$f \longmapsto \mathrm{Im}(f)$$

□

Proposizione Se X è infinito, $|\mathcal{P}^{fin}(X)| = |X|$

DIMOSTRAZIONE

$\mathcal{P}^{fin}(X) = \bigcup \{\mathcal{P}^{\leq n}(X) \mid n \in \omega\}$ è unione di $\aleph_0 < |X|$ insiemi di cardinalità $|X|$ □

Proposizione Un ordine totale $(A,<)$ è un buon ordine se e solo se non esiste una successione decrescente $\{a_n\}_{n\in\omega}$ di elementi di A.

DIMOSTRAZIONE

Se $\{a_n\}_{n\in\omega}$ è una successione decrescente, allora $\{a_n \mid n\in\omega\}$ non ha minimo, quindi $(A,<)$ non è un buon ordine.

Se $(A,<)$ non è un buon ordine, sia $S\subseteq A$ con $S\neq\emptyset$ che non ha minimo.

Consideriamo una funzione di scelta $f: \mathcal{P}^{\neq\emptyset}(S)\longrightarrow S$ e, fissato $a_0\in S$ qualunque, definiamo per ricorsione $a_{n+1}=f(\{x\in S \mid x<a_n\})$

Siccome S non ha minimo, l'insieme a cui è applicata f non è mai vuoto, per cui la sequenza a_n è ben definita. □

Teorema di Tarski Se per ogni X infinito $|X\times X|=|X|$, allora vale AC

DIMOSTRAZIONE

Dato X infinito, cerchiamo un buon ordinamento di X.

Basta costruire una funzione g che immerge X negli ordinali.

Per ipotesi su $X\sqcup H(X)$:

$$|X\times H(X)|\leq|(X\sqcup H(X))\times(X\sqcup H(X))|=|X\sqcup H(X)|$$

Quindi esiste una funzione iniettiva $f: X\times H(X)\longrightarrow X\sqcup H(X)$

Dato $a\in X$, consideriamo

$$\begin{aligned} f_a : H(X) &\longrightarrow X\sqcup H(X) \\ b &\longmapsto f(a,b) \end{aligned}$$

Se l'immagine $f_a[H(X)]$ di f_a fosse contenuta in X, avremmo una funzione iniettiva $H(X)\longrightarrow X$ ↯, quindi $f_a[H(X)]\cap H(X)\neq\emptyset$. Definiamo

$$\begin{aligned} g: X &\longrightarrow H(X) \\ a &\longmapsto \min(f_a[H(X)]\cap H(X)) \end{aligned}$$

g è ben definita perché $f_a[H(X)]\cap H(X)\subseteq H(X)$ è un insieme di ordinali, quindi ha minimo. Inoltre g è iniettiva perché, dati $a\neq b$,

$$g(a)=f(a,*)\neq f(b,*)=g(b)$$ □

Proposizione: Forme equivalenti di AC Assumendo gli assiomi di estensionalità, insieme vuoto, separazione, paio, unione, parti, infinito e rimpiazzamento, le seguenti proposizioni sono equivalenti:

assioma di scelta

- ogni funzione surgettiva ha un'inversa destra
- teorema del buon ordinamento
- lemma di Zorn
- ogni cardinalità infinita è un alef
- $\forall X,Y \quad |X|\leq|Y| \vee |Y|\leq|X|$
- $\forall X \quad |X|\geq\aleph_0 \longrightarrow |X\times X|=|X|$

Applicazioni di AC

Proposizione Sia $A \subseteq \mathbb{R}$, allora
$$x \in \bar{A} \longleftrightarrow \exists \{x_i\}_{i\in\omega} \, (\forall i \in \omega \; x_i \in A) \wedge (\lim_{i\to+\infty} x_i = x)$$

NOTA: $x \in \bar{A} \equiv \forall \varepsilon > 0 \quad]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$

DIMOSTRAZIONE

$\leftarrow$: $\forall \varepsilon > 0 \; \exists i \; x_i \in \,]x-\varepsilon, x+\varepsilon[\cap A$

quindi $\forall \varepsilon > 0 \;]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$ ossia $x \in \bar{A}$

$\rightarrow$: Sia f una funzione di scelta per $P(A) \setminus \{\emptyset\}$

Definiamo $x_i = f\left(A \cap \left]x - \frac{1}{i+1}, x + \frac{1}{i+1}\right[\right)$ $\square$

OSS $\mathcal{B}$ è una base se e solo se è un sottoinsieme linearmente indipendente di V massimale per inclusione.

Proposizione Dato uno spazio vettoriale V e $X \subseteq V$ linearmente indipendente, esiste una base $\mathcal{B}$ di V tale che $X \subseteq \mathcal{B}$

DIMOSTRAZIONE

Applichiamo il lemma di Zorn all'insieme dei sottoinsiemi A di V linearmente indipendenti tali che $X \subseteq A$, ordinati per inclusione.
Occorre dimostrare che l'unione di una catena di insiemi linearmente indipendenti C è linearmente indipendente.
Siano $a_1, \dots, a_n \in \bigcup C$. Siano $A_1, \dots, A_n \in C$ tali che per ogni $i = 1, \dots, n$ $a_i \in A_i$.
Siccome C è una catena per inclusione, c'è un $j \in \{1, \dots, n\}$ tale che A_j include tutti gli altri A_i. Quindi $a_1, \dots, a_n \in A_j$, e, siccome A_j è indipendente,
$$x_1 a_1 + \dots + x_n a_n = 0 \longleftrightarrow x_1 = \dots = x_n = 0$$
$\square$

esempio Esiste una funzione $f: \mathbb{R} \longrightarrow \mathbb{R}$ tale che
$$\forall x, y \in \mathbb{R} \quad f(x+y) = f(x) + f(y)$$
tuttavia f non è della forma $f(x) = k \cdot x$

DIMOSTRAZIONE

Sia $\mathcal{B}$ una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale
Fissiamo $b_1 \in \mathcal{B}$. Consideriamo la funzione
$$f: \mathbb{R} \longrightarrow \mathbb{Q}$$
$$x \longmapsto y_1 \text{ tale che } \exists y_2, \dots, y_n \;\; x = b_1 y_1 + \dots + b_n y_n$$
$\square$

Teorema di Dehn Un cubo ed un tetraedro regolare non si possono scomporre in un numero finito di poliedri equivalenti.

DIMOSTRAZIONE

Costruiamo $f:\mathbb{R}\to\mathbb{R}$ additiva tale che $f(x)=0$ se e solo se $x=k\pi$, $k\in\mathbb{Q}$.

Sia $\mathcal{B}$ base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale tale che $\pi\in\mathcal{B}$. Definiamo

$$f(\pi q_0+b_1q_1+\dots+b_nq_n)=b_1q_1+\dots+b_nq_n \quad \text{per ogni } q_0,\dots,q_n\in\mathbb{Q},\ b_1,\dots,b_n\in\mathcal{B}\setminus\{\pi\}$$

(f è la proiezione sul complementare del sottospazio $\pi\mathbb{Q}$)

L'additività è una conseguenza della $\mathbb{Q}$-linearità.

Inoltre $f(x)=0$ se e solo se $x=\pi q_0$ con $q_0\in\mathbb{Q}$.

Definiamo il valore di un poliedro come la somma dei valori degli spigoli: il valore di uno spigolo di lunghezza l che forma un angolo diedro α è $l\cdot f(\alpha)$

Quando tagliamo un poliedro A con un piano, ottenendo due poliedri B e C, la somma dei valori di B e C equivale al valore di A.

Infatti, il taglio forma nuovi spigoli con angoli diedri α_1 e α_2 tali che $\alpha_1+\alpha_2=\pi$, quindi $l\cdot f(\alpha_1)+l\cdot f(\alpha_2)=l\cdot f(\alpha_1+\alpha_2)=0$

Può dividere uno spigolo l in due l_1 e l_2 senza alterare l'angolo diedro, quindi $l_1\cdot f(\alpha)+l_2\cdot f(\alpha)=l\cdot f(\alpha)$

Infine può spezzare l'angolo diedro lasciando inalterata la lunghezza, e si conclude analogamente.

Ora il valore di un cubo è nullo, perché tutti i diedri hanno ampiezza $\frac{1}{2}\pi$

Occorre mostrare che il valore di un tetraedro non è mai nullo.

Si vede che i diedri del tetraedro sono $\alpha=\arccos\frac{1}{3}$: basta dire che α non è multiplo razionale di π. In altri termini, se $n\in\mathbb{N}$, $n\alpha$ non è multiplo intero di π.

Questo equivale a dire $z^n\notin\mathbb{R}$ dove $z=\cos\alpha+i\sin\alpha$.

Ora $z=\frac{1}{3}(1+2i\sqrt{2})$: per induzione si mostra che $(1+2i\sqrt{2})^n=x_n+y_n i\sqrt{2}$ con $x_n,y_n\in\mathbb{Z}$

Sempre per induzione, otteniamo: per n dispari $x_n\equiv 1\ (3)$ $y_n\equiv 2\ (3)$

per n pari $\neq 0$ $x_n\equiv 2\ (3)$ $y_n\equiv 1\ (3)$

In particolare, in nessun caso $y_n=0$. $\square$

Promemoria Una misura σ-additiva su $P(\mathbb{R})$ è una funzione $\mu : P(\mathbb{R}) \longrightarrow \mathbb{R}^{\geq 0} \cup \{+\infty\}$ tale che $\mu(\emptyset) = 0$ e, se $\{A_i\}_{i \in \omega}$ è una successione di elementi disgiunti di $P(\mathbb{R})$, allora
$$\mu(\bigcup \{A_i \mid i \in \omega\}) = \sum_{i=0}^{+\infty} \mu(A_i)$$
μ si dice invariante per traslazioni se $\forall x \in \mathbb{R}, A \in P(\mathbb{R})$
$$\mu(A) = \mu(\underbrace{\{y \in \mathbb{R} \mid y - x \in A\}}_{= A+x})$$

OSS Se $A \subseteq B \subseteq \mathbb{R}$, allora $\mu(A) \leq \mu(B)$

DIMOSTRAZIONE

$\mu(B) = \mu(A \cup (B \setminus A)) = \mu(A) + \mu(B \setminus A) \geq \mu(A)$ □

Proposizione (Vitali) Non esiste una misura σ-additiva ed invariante per traslazioni μ su $P(\mathbb{R})$ tale che $\mu([0,1[) = 1$

DIMOSTRAZIONE

Per assurdo, esista μ

Cerchiamo degli insiemi disgiunti $A_i \subseteq [0,1[$ con $i \in \omega$ tali che per ogni $i, j \in \omega$ $\mu(A_i) = \mu(A_j)$ e $[0,1[= \bigcup \{A_i \mid i \in \omega\}$.

Questo è assurdo perché, se $\mu(A_i) = \mu(A_j) = 0$, allora $\mu([0,1[) = \sum_{i=0}^{+\infty} 0 = 0 \neq 1$; se invece $\mu(A_i) = \mu(A_j) = k > 0$, allora $\mu([0,1[) = \sum_{i=0}^{+\infty} k = +\infty \neq 1$

Sia $i \longmapsto q_i$ un'enumerazione di $\mathbb{Q}$.

Sia $\mathcal{B}$ una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale tale che $b_0 = 1 \in \mathcal{B}$.

Definiamo $R_i := \{x \in \mathbb{R} \mid x = r_0 \cdot 1 + q_i \cdot b_1 + r_2 \cdot b_2 + \dots + r_n \cdot b_n \text{ con } r_0, r_2, \dots, r_n \in \mathbb{Q}\}$

$A_i := R_i \cap [0,1[$ (ossia $x \in R_i$ se e solo se la componente b_1 è q_i)

Siccome $\{q_i\}_{i \in \omega}$ enumera i razionali, $\{R_i\}_{i \in \omega}$ è una partizione di $\mathbb{R}$, e quindi $\{A_i\}_{i \in \omega}$ è una partizione di $[0,1[$

Dimostriamo che $\mu(A_i) = \mu(A_j)$. Siano $\delta = (q_j - q_i) b_1$, $k = \lceil \delta \rceil$

Consideriamo l'insieme $A_i + \delta$

$x \in R_i \Leftrightarrow x \in \mathrm{Span}(\mathcal{B} \setminus \{b_1\}) + q_i b_1 \Leftrightarrow x + \delta \in \mathrm{Span}(\mathcal{B} \setminus \{b_1\}) + q_j b_1 \Leftrightarrow x + \delta \in R_j$

Quindi $A_i + \delta = (R_i + \delta) \cap [\delta, \delta+1[= R_j \cap [\delta, \delta+1[= \underbrace{(R_j \cap [\delta, k[)}_{= X_1} \cup \underbrace{(R_j \cap [k, \delta+1[)}_{= X_2}$

Similmente, per $n \in \mathbb{N}$:

$x \in R_j \Leftrightarrow x \in \mathrm{Span}(\mathcal{B} \setminus \{b_1, 1\}) + \mathbb{Q} + q_j b_1 \Leftrightarrow x + n \in \mathrm{Span}(\mathcal{B} \setminus \{b_1, 1\}) + \mathbb{Q} + q_j b_1 \Leftrightarrow x + n \in R_j$

Quindi $Y_1 := X_1 - k + 1 = R_j \cap [\delta - k + 1, 1[$

$Y_2 := X_2 - k = R_j \cap [0, \delta - k + 1[$

Di conseguenza $Y_1 \cap Y_2 \subseteq [\delta - k + 1, 1[\cap [0, \delta - k + 1[= \emptyset$ e

$Y_1 \cup Y_2 = R_j \cap ([\delta - k + 1, 1[\cup [0, \delta - k + 1[) = R_j \cap [0,1[= A_j$

Mettendo tutto insieme:

$\mu(A_j) = \mu(Y_1) + \mu(Y_2) = \mu(X_1) + \mu(X_2) = \mu(A_i + \delta) = \mu(A_i)$ □

Il teorema di Cantor-Bendixson

Promemoria Se $S \subseteq \mathbb{R}$, diciamo che $x \in \mathbb{R}$ è un punto di accumulazione di S se $x \in \overline{S \setminus \{x\}}$, ossia se esiste $\{x_i\}_{i\in\omega}$ di punti di $S \setminus \{x\}$ tale che $\lim_{i\to+\infty} x_i = x$
$S \subseteq \mathbb{R}$ si dice perfetto se S coincide con l'insieme dei suoi punti di accumulazione

esempio un intervallo chiuso è perfetto

OSS Se $S \subseteq [0,1]$ è perfetto e non vuoto allora esistono S_1 e S_2 sottoinsiemi di S perfetti, non vuoti e disgiunti.

DIMOSTRAZIONE

Un singoletto non è perfetto, quindi esistono $x_1, x_2 \in S$ con $x_1 < x_2$. Si hanno due casi:

- se $[x_1, x_2] \subseteq S$: consideriamo x_3, x_4 con $x_1 < x_3 < x_4 < x_2$ e definiamo $S_1 = S \cap [0, x_3]$ e $S_2 = S \cap [x_4, 1]$
- se esiste $x_3 \in [x_1, x_2] \setminus S$: definiamo $S_1 = S \cap [0, x_3[$ e $S_2 = S \cap]x_3, 1]$ $\square$

Proposizione Se $S \subseteq [0,1]$ è perfetto, allora $|S| = 2^{\aleph_0}$

DIMOSTRAZIONE

Sia P l'insieme dei sottoinsiemi perfetti di $[0,1]$.
Fissiamo $f : P \longrightarrow P \times P$

$$X \longmapsto (X_1, X_2) \text{ tali che } X_1 \cup X_2 \subseteq X \text{ e } X_1 \cap X_2 = \emptyset$$

Assegnamo ad ogni sequenza binaria finita $\sigma : n \longrightarrow \{0,1\}$ un sottoinsieme perfetto S_σ di S, per ricorsione su n. A questo scopo, data $\sigma : n \longrightarrow \{0,1\}$ e $b \in \{0,1\}$ indichiamo con $\sigma^\frown b$ la sequenza $\sigma \cup \{(n,b)\} : n+1 \longrightarrow \{0,1\}$. Ora definiamo:

$$S_\emptyset = S \qquad S_{\sigma^\frown b} = \begin{cases} X & \text{se } b = 0 \\ Y & \text{se } b = 1 \end{cases} \qquad \text{dove } (X,Y) = f(S_\sigma)$$

Data una successione infinita $\tau : \omega \longrightarrow \{0,1\}$, definiamo infine:

$$S_\tau = \bigcap \{ S_\sigma \mid \sigma = \tau|_n, n \in \omega \}$$

Osserviamo che per ogni successione τ, $S_\tau \neq \emptyset$, infatti per ogni $n \in \omega$ $S_{\tau|_{s(n)}} \subseteq S_{\tau|_n}$: quindi i compatti $S_{\tau|_n}$ costituiscono una catena di compatti non vuoti, per cui la loro intersezione non è vuota.
Inoltre, se $\tau \neq \rho$, allora $S_\tau \cap S_\rho = \emptyset$. Infatti, detto n il minimo indice tale che $\tau_n \neq \rho_n$, senza perdita di generalità $\tau_n = 0$ e $\rho_n = 1$, abbiamo $S_{\tau|_{s(n)}} = A$ e $S_{\rho|_{s(n)}} = B$ con $(A,B) = f(S_{\tau|_n}) = f(S_{\rho|_n})$, quindi $S_\tau \subseteq A$ e $S_\rho \subseteq B$ sono disgiunti perché $A \cap B = \emptyset$.
In conclusione, per ogni $\tau \in {}^\omega 2$ possiamo scegliere un punto in S_τ e questa funzione è iniettiva, quindi $2^{\aleph_0} \leq |S|$
Inoltre $|S| \leq |\mathbb{R}| = 2^{\aleph_0}$, quindi $|S| = 2^{\aleph_0}$ $\square$

Teorema di Cantor-Bendixson Sia $C \subseteq \mathbb{R}$ chiuso
Allora $C = N \cup P$ con $|N| \leq \aleph_0$ e P perfetto.

DIMOSTRAZIONE

Dato un insieme $X \subseteq \mathbb{R}$, definiamo il suo derivato

$X' := \{$punti di accumulazione di $X\} = \{a \in \mathbb{R} \mid \forall \varepsilon > 0 \ ]a-\varepsilon, a+\varepsilon[\cap (X \setminus \{a\}) \neq \emptyset\}$

Se X è chiuso: $X' = X \setminus \{$punti isolati di $X\}$

dove $a \in X$ è isolato se $\exists \varepsilon > 0 \ ]a-\varepsilon, a+\varepsilon[\cap X = \{a\}$

OSS $a \in X$ è un punto isolato di X se e solo se esiste un intervallo $]s,t[$ a estremi razionali che isola a in X, ossia

$$\exists s,t \in \mathbb{Q} \quad s<t \ \wedge \ ]s,t[\cap X = \{a\}$$

Costruiamo ora una successione transfinita di sottoinsiemi chiusi C_α di C, $\alpha \in \mathrm{Ord}$:

$$C_0 = C \qquad C_{\alpha+1} = C_\alpha' \qquad C_\lambda = \bigcap\{C_\alpha \mid \alpha < \lambda\}$$

Gli insiemi C_α sono chiusi perché il derivato di un chiuso è un chiuso e l'intersezione di chiusi è un chiuso. Osserviamo che $\alpha \leq \beta \longrightarrow C_\beta \subseteq C_\alpha$. Definiamo:

$$P = \bigcap_{\alpha \in \mathrm{Ord}} C_\alpha = \{a \in \mathbb{R} \mid \forall \alpha \in \mathrm{Ord} \ a \in C_\alpha\}$$
$$N = C \setminus P$$

① P è perfetto

P è chiuso perché intersezione di chiusi, occorre dimostrare che ogni $a \in P$ è punto di accumulazione di P. Per assurdo sia $\varepsilon > 0$ tale che $P \cap]a-\varepsilon, a+\varepsilon[= \{a\}$. Per ogni $x \in]a-\varepsilon, a+\varepsilon[\setminus \{a\}$, siccome $x \notin P$, esiste α tale che $x \notin C_\alpha$ e α_x sia il minimo tale che $x \notin C_{\alpha_x}$.

Sia $\beta = \sup\{\alpha_x \mid x \in]a-\varepsilon, a+\varepsilon[\setminus \{a\}\}$

Ora $C_\beta \cap]a-\varepsilon, a+\varepsilon[= \{a\}$, quindi a è un punto isolato di C_β.

Allora $a \notin C_{S(\beta)}$ e perciò $a \notin P$ ↯

② A è al più numerabile

Per ogni $x \in A$ possiamo considerare α_x minimo tale che $x \notin C_{\alpha_x}$.

Questo α_x è successore: infatti, se fosse limite, avremmo $C_{\alpha_x} = \bigcap\{C_\gamma \mid \gamma < \alpha_x\}$ ed esisterebbe $\gamma < \alpha_x$ tale che $x \notin C_\gamma$.

Allora $\alpha_x = S(\beta_x)$ e C_{β_x} è l'ultimo dei C_α a contenere x.

Siccome $x \in C_{\beta_x}$ ma $x \notin C_{\alpha_x} = C_{\beta_x}'$, x è un punto isolato di C_{β_x}.

Scegliamo un intervallo $]s_x, t_x[$ a estremi razionali che isola x in C_{β_x}.

Ci basta mostrare che la funzione seguente è iniettiva:

$$A \longrightarrow \mathbb{Q} \times \mathbb{Q}$$
$$x \longmapsto (s_x, t_x)$$

Siano x, y tali che $]s_x, t_x[=]s_y, t_y[$. Supponiamo, senza perdita di generalità, che $\beta_x \leq \beta_y$. Allora

$$y \in]s_y, t_y[\cap C_{\beta_y} \subseteq]s_x, t_x[\cap C_{\beta_x} = \{x\}$$

quindi $x = y$. $\square$

Corollario Se $C \subseteq \mathbb{R}$ è chiuso, allora o $|C| = 2^{\aleph_0}$ o $|C| \leq \aleph_0$

DIMOSTRAZIONE

Per Cantor-Bendixson, $C = N \cup P$

Se $P = \emptyset$, $|C| = |N| \leq \aleph_0$. Altrimenti $2^{\aleph_0} = |P| \leq |C| \leq 2^{\aleph_0}$ $\square$

esempio Esiste $S \subseteq \mathbb{R}$ non numerabile che non contiene alcun insieme perfetto non vuoto.

DIMOSTRAZIONE

Sia $|\mathbb{R}| = \aleph_\alpha$. Sia $f : \mathcal{P}^{\neq \emptyset}(\mathbb{R}) \longrightarrow \mathbb{R}$ una funzione di scelta.

Si vede che $2^{\aleph_0} = |\text{intervalli}| \leq |\text{perfetti non vuoti}| \leq |\text{chiusi}| = |\text{aperti}| = 2^{\aleph_0}$

Quindi esiste una funzione surgettiva
$$\begin{aligned} \omega_\alpha &\longrightarrow \text{perfetti non vuoti} \\ \beta &\longmapsto P_\beta \end{aligned}$$

Definiamo per ricorsione transfinita
$$\begin{aligned} g : \omega_\alpha &\longrightarrow \mathbb{R} \times \mathbb{R} \\ \beta &\longmapsto (g_1(\beta), g_2(\beta)) \end{aligned}$$

dove $g_1(\beta) = f(P_\beta \setminus (g_1[\beta] \cup g_2[\beta]))$

$g_2(\beta) = f(\mathbb{R} \setminus (g_1[\beta] \cup g_2[\beta] \cup \{g_1(\beta)\}))$

La funzione g è ben definita perché, per ogni $\beta < \omega_\alpha$, $|\beta| < \aleph_\alpha$ quindi $|g_1[\beta]| < \aleph_\alpha$ e $|g_2[\beta]| < \aleph_\alpha$ e $|P_\beta| = 2^{\aleph_0} = |\mathbb{R}| = \aleph_\alpha$.

Di conseguenza f è sempre applicata ad insiemi non vuoti

Dimostriamo che $S = g_2[\omega_\alpha]$ soddisfa la tesi.

La funzione $g_2 : \omega_\alpha \longrightarrow \mathbb{R}$ è iniettiva, perché, se $\gamma < \beta$, $g_2(\gamma) \in g_2[\beta]$ e $g_2(\beta) = f(\mathbb{R} \setminus (\dots g_2[\beta] \dots)) \neq g_2(\gamma)$ Per cui $|g_2[\omega_\alpha]| = 2^{\aleph_0}$

Fissiamo ora un perfetto non vuoto P_β. Dobbiamo mostrare $P_\beta \not\subseteq g_2[\omega_\alpha]$.

Ci basta dire che $g_1(\beta) \notin g_2[\omega_\alpha]$.

Supponiamo per assurdo $g_1(\beta) = g_2(\gamma)$ per qualche $\gamma < \omega_\alpha$.

Se $\gamma < \beta$, $g_1(\beta) = g_2(\gamma) \in g_1[\beta] \cup g_2[\beta]$ ↯

Se $\beta \leq \gamma$, $g_2(\gamma) = g_1(\beta) \in g_1[\gamma] \cup g_2[\gamma] \cup \{g_1(\gamma)\}$ ↯

□

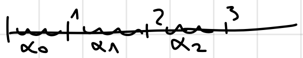
esercizio Ogni ordinale numerabile si immerge in $\mathbb{R}$.

DIMOSTRAZIONE (v. brutta)

Per assurdo, sia α minimo che non si immerge in $\mathbb{R}$

- $\alpha = S(\beta)$ ↯
- $\alpha = \lambda$ limite

$\lambda = \{\alpha_i \mid i \in \omega\}$ perché α numerabile



$\sup\{\alpha_0, \alpha_0 + \alpha_1, \alpha_0 + \alpha_1 + \alpha_2, \dots\} \hookrightarrow \mathbb{R}$

$\geq$

$\sup\{\alpha_0, \alpha_1, \dots\} = \alpha$

Aritmetica cardinale

NOTAZIONE κ è un cardinale $\equiv$ κ è un ordinale iniziale

$\kappa = \lambda^+$ $\equiv$ κ è il minimo cardinale $> \lambda$

Def. Sia I un insieme e $\{\kappa_i\}_{i\in I}$ una famiglia di cardinali:

$$\sum_{i\in I} \kappa_i = \left|\bigcup\{\kappa_i \times \{i\} \mid i\in I\}\right| \qquad \prod_{i\in I} \kappa_i = \left|\{f : I \to \sup_i \kappa_i \mid \forall i\in I\ f(i)\in \kappa_i\}\right|$$

OSS Se $\forall i\in I$ $\kappa_i = |X_i|$ e gli X_i sono a due a due disgiunti, allora

$$\sum_{i\in I} \kappa_i = \left|\bigcup\{X_i \mid i\in I\}\right|$$

DIMOSTRAZIONE (richiede AC)

Per ogni i scegliamo una bigezione $f_i : \kappa_i \times \{i\} \longrightarrow X_i$

Allora $f : \bigcup\{\kappa_i \times\{i\} \mid i\in I\} \longrightarrow \bigcup\{X_i \mid i\in I\}$

$$(a,i) \longmapsto f_i(a)$$

(ossia $f = \bigcup\{f_i \mid i \in I\}$) è una bigezione. $\square$

OSS Se $\forall i\in I$, $\kappa_i = |X_i|$

$$\sum_{i\in I}\kappa_i \geq \left|\bigcup\{X_i \mid i\in I\}\right| \qquad \prod_{i\in I} \kappa_i = \left|\{f : I \to \bigcup\{X_i \mid i\in I\} \mid \forall i\in I\ f(i)\in X_i\}\right|$$

DIMOSTRAZIONE

Per la prima si osserva che la funzione definita nella dimostrazione precedente è surgettiva.

La seconda è analoga: dette $g_i : \kappa_i \longrightarrow X_i$ bigezioni,

$$g : \{f : I \to \bigcup\{\kappa_i \mid i\in I\} \mid \forall i\ f(i)\in\kappa_i\} \longrightarrow \{f : I \to \bigcup\{X_i \mid i\in I\} \mid \forall i\ f(i)\in X_i\}$$

$$g(f)(i) = g_i(f(i)) \quad \text{è una bigezione} \qquad \square$$

OSS $$\kappa^{\sum_{i\in I}\lambda_i} = \prod_{i\in I} \kappa^{\lambda_i}$$

DIMOSTRAZIONE

Un elemento dell'insieme a sinistra è una funzione

$f : \bigcup\{\lambda_i \times\{i\} \mid i\in I\} \longrightarrow \kappa$ e possiamo identificarla con la funzione

$\tilde{f} : I \longrightarrow \bigcup\{\kappa^{\lambda_i} \mid i \in I\}$

$i \longmapsto \tilde{f}_i$ definita da $\tilde{f}_i(\alpha) = f(\alpha, i)$ $\square$

OSS Valgono le seguenti proprietà ragionevoli:

- se $\forall i\in I$ $\kappa_i \leq \lambda_i$: $\sum_{i\in I}\kappa_i \leq \sum_{i\in I}\lambda_i$
- $\forall i \in I$ $\kappa_i \leq \sum_{i\in I}\kappa_i$
- se $\forall i\in I$ $\kappa_i \neq 0$: $|I| \leq \sum_{i\in I}\kappa_i$ e $\forall i$ $\kappa_i \leq \prod_{i\in I}\kappa_i$

  se $I = I_1 \sqcup I_2$: $\sum_{i\in I}\kappa_i = \sum_{i\in I_1}\kappa_i + \sum_{i\in I_2}\kappa_i$ e $\prod_{i\in I}\kappa_i = \prod_{i\in I_1}\kappa_i \prod_{i\in I_2}\kappa_i$

  $\sum_{i\in \kappa}\lambda = \kappa\cdot\lambda$ $\qquad \prod_{i\in\kappa}\lambda = \lambda^\kappa$
- $\left(\prod_{i\in I}\kappa_i\right)^\lambda = \prod_{i\in I}\kappa_i^\lambda$

Proposizione Supponiamo che κ_i per $i \in I$ siano cardinali $\neq 0$. Allora
$$\sum_{i\in I} \kappa_i = |I| \cdot \sup_i \kappa_i = \max(|I|, \sup_i \kappa_i)$$

DIMOSTRAZIONE

$\leq$: $\sum_{i\in I} \kappa_i \leq \sum_{i \in I} \sup_i \kappa_i = |I| \cdot \sup_i \kappa_i$

$\geq$: abbiamo che $\sum_{i\in I} \kappa_i \geq |I|$ e $\forall j \in I$ $\sum_{i\in I} \kappa_i \geq \kappa_j$,
da cui $\sum_{i\in I} \kappa_i \geq \sup_i \kappa_i$. Perciò $\sum_{i\in I} \kappa_i \geq \max(|I|, \sup_i \kappa_i) = |I| \cdot \sup_i \kappa_i$ □

Teorema di König Se $\forall i \in I$ $\kappa_i < \lambda_i$, allora $\sum_{i\in I} \kappa_i < \prod_{i \in I} \lambda_i$

DIMOSTRAZIONE

Dimostriamo che non può valere il $\geq$.

Siano $A = \bigcup \{\kappa_i \times \{i\} \mid i \in I\}$ e $B = \{f : I \to \sup_i \lambda_i \mid \forall i \in I \ f(i) \in \lambda_i\}$

Data $f : A \to B$, dobbiamo mostrare che f non è surgettiva.

Consideriamo
$$f_i : \kappa_i \longrightarrow \lambda_i$$
$$\alpha \longmapsto f(\alpha, i)(i) \in \lambda_i$$

Siccome $\kappa_i < \lambda_i$, f_i non può essere surgettiva, quindi per ogni i, $\lambda_i \setminus Im(f_i) \neq \emptyset$. Per l'assioma di scelta, c'è
$$g : I \longrightarrow \sup_i \lambda_i$$
$$i \longmapsto g(i) \in \lambda_i \setminus Im(f_i)$$

Chiaramente $g \in B$, verifichiamo che $g \notin Im(f)$

Se fosse $g = f(\alpha, i)$ allora $g(i) = f(\alpha, i)(i) = f_i(\alpha) \in Im(f_i)$ ↯ □

Corollario (Teorema di Cantor) $\kappa < 2^\kappa$

DIMOSTRAZIONE

$\kappa = \sum_{i \in \kappa} 1 < \prod_{i \in \kappa} 2 = 2^\kappa$ □

Corollario $\aleph_\omega \neq 2^{\aleph_0}$

DIMOSTRAZIONE

$\aleph_\omega = \sum_{i \in \omega} \aleph_i < \prod_{i \in \omega} \aleph_{i+1} \leq \aleph_\omega^{\aleph_0}$ quindi in particolare $\aleph_\omega < \aleph_\omega^{\aleph_0}$

Ma abbiamo che $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$

perciò $2^{\aleph_0} \neq \aleph_\omega$ □

Def. Dato un cardinale infinito K, la cofinalità (V1) di K, $cof(K)$, è il minimo cardinale μ per cui esiste una famiglia $\{\lambda_i\}_{i\in\mu}$ di cardinali tale che $\forall i\in\mu$ $\lambda_i<K$ e $K=\sum_{i\in I}\lambda_i$

esempio
$cof(\aleph_0)=\aleph_0$ un'unione finita di insiemi finiti è finita
$cof(\aleph_\omega)=\aleph_0$ $\sum_{\alpha\in\omega}\aleph_\alpha=\aleph_\omega$; se $|I|<\aleph_0$, $\sum_{\alpha\in I}\aleph_\alpha=\aleph_{max(I)}<\aleph_\omega$
$cof(\aleph_{42})=\aleph_{42}$ $\aleph_{42}=\sum_{i\in I}K_i\leq\sum_{i\in I}\aleph_{41}=|I|\cdot\aleph_{41}=max(|I|,\aleph_{41})\longrightarrow|I|=\aleph_{42}$

Def. Dato un insieme ordinato $(S,<)$, diciamo che $A\subseteq S$ è cofinale in S se $\forall x\in S\ \exists y\in A\ x\leq y$ (ossia A non ha maggioranti stretti in S).
La cofinalità (V2) di $(S,<)$ è la minima cardinalità di un sottoinsieme cofinale di S.

esempio
$cof(\omega)=\aleph_0$ ω è cofinale in se stesso, un sottoinsieme finito ha massimo
$cof(\mathbb{R},<)=\aleph_0$ ω è cofinale in $(\mathbb{R},<)$
$cof(\omega+1)=1$ $\{\omega\}$ è cofinale in ω
$cof(\omega_\omega)=\aleph_0$ $\{\omega_0,\omega_1,\omega_2,\dots\}$ è cofinale in $\omega_\omega=\sup_{i\in\omega}\omega_i$

Proposizione Se K è un cardinale infinito, $cof^{(V1)}(K)=cof^{(V2)}(K)$

DIMOSTRAZIONE
$cof^{(V1)}\leq cof^{(V2)}$: Sia A cofinale in K con $|A|=cof^{(V2)}(K)$
Segue che $\sup A=K\longrightarrow K=\bigcup A$
Allora $K\leq\sum_{a\in A}|a|=max(|A|,\sup_{a\in A}|a|)\leq|K|$
Siccome $\forall a\in A$ $a<K$ e K è iniziale, vale $\forall a\in A$ $|a|<K$
Quindi $cof^{(V1)}(K)\leq|A|$
$cof^{(V2)}\leq cof^{(V1)}$: Sia $K=\sum_{i\in I}K_i$ con $|I|=cof^{(V1)}(K)$
Se $|I|=K$ la tesi è ovvia
Se $|I|<K$, $K=\sum_{i\in I}K_i=max(\sup_{i\in I}K_i,|I|)$
da cui $K=\sup_{i\in I}K_i$, cioè $\{K_i\}_{i\in I}$ è cofinale in K. □

OSS Sia $(S,<_S)$ totalmente ordinato e $T\subseteq S$ cofinale in S. Indichiamo con $<_T$ la restrizione di $<_S$ a T: $<_T=<_S\cap(T\times T)$.
Allora $cof(S,<_S)=cof(T,<_T)$

DIMOSTRAZIONE
Dimostriamo che se $A\subseteq T$ è cofinale in $(T,<_T)$, allora A è anche cofinale in S
Mentre se $B\subseteq S$ è cofinale in $(S,<_S)$, allora esiste $B'\subseteq T$ con $|B'|\leq|B|$ cofinale in T.
- Dato $A\subseteq T$ cofinale in T e $x\in S$, dato che T è cofinale in S $\exists t\in T$ $x\leq t$ e siccome A è cofinale in T $\exists y\in A$ $t\leq y$, per cui $x\leq y$, quindi A è cofinale in S.
- Dato $B\subseteq S$ cofinale, dato che T è cofinale in S, $\forall b\in B$ possiamo scegliere $y_b\in T$ con $b<y_b$. Sia $B'=\{y_b\mid b\in B\}\subseteq T$. La funzione $b\longmapsto y_b$ è surgettiva quindi $|B'|\leq|B|$
Inoltre, preso $x\in S$, esiste $b\in B$ con $x\leq b$, quindi $x\leq y_b\in B'$ □

OSS Sia K un cardinale infinito: $cof(K)\leq K$

DIMOSTRAZIONE
$K=\sum_{i\in K}1$ □

OSS Sia $(A,<)$ totalmente ordinato, allora
$$\mathrm{cof}(\mathrm{cof}(A,<)) = \mathrm{cof}(A,<)$$

DIMOSTRAZIONE

$\leq$: immediata dall'osservazione precedente

$\geq$: sia B cofinale in A di cardinalità minima, sia $\kappa = \mathrm{cof}(|B|)$

Cerchiamo un insieme $C \subseteq B$ cofinale in B con $|C| \leq \kappa$

Se $\kappa = |B|$, prendo $C = B$

Se $\kappa < |B|$, scrivo $B = \bigcup_{i\in I} B_i$ con $|B_i| < |B|$ e $|I| = \mathrm{cof}(|B|)$

Per ogni $i \in I$ sia $c_i \in A$ con $\forall b \in B_i \;\; b < c_i$

Definisco $C = \{c_i \mid i \in I\}$: $|C| \leq |I| = \mathrm{cof}(|B|)$

Inoltre $\forall a \in A \; \exists b \in B \;\; a \leq b \longrightarrow \exists i \;\; b \in B_i \longrightarrow a \leq b < c_i \in C$ □

corollario (del teorema di König) Per κ cardinale infinito e λ cardinale ≥ 2:
$$\kappa < \kappa^{\mathrm{cof}(\kappa)} \qquad \kappa < \mathrm{cof}(\lambda^\kappa)$$

DIMOSTRAZIONE

Sia $\mu = \mathrm{cof}(\kappa)$, esiste una famiglia $\{\kappa_i\}_{i\in\mu}$ tale che $\forall i \in \mu \;\; \kappa_i < \kappa$ e $\kappa = \sum_{i\in\mu} \kappa_i$

Per König: $\kappa = \sum_{i\in\mu} \kappa_i < \prod_{i\in\mu} \kappa = \kappa^\mu = \kappa^{\mathrm{cof}(\kappa)}$

Da questa segue $\lambda^\kappa < (\lambda^\kappa)^{\mathrm{cof}(\lambda^\kappa)} = \lambda^{\kappa\cdot\mathrm{cof}(\lambda^\kappa)}$ (perché $\lambda^\kappa \geq 2^{\aleph_0}$)

da cui $\kappa < \kappa \cdot \mathrm{cof}(\lambda^\kappa) = \max(\kappa, \mathrm{cof}(\lambda^\kappa))$

perciò, siccome $\kappa \not< \kappa$, $\kappa < \mathrm{cof}(\lambda^\kappa)$ □

DEF. La funzione $\gimel$ ("gimel") è definita sui cardinali infiniti da
$$\gimel(\kappa) = \kappa^{\mathrm{cof}(\kappa)}$$

DEF. Un cardinale κ è

- **regolare** se $\mathrm{cof}(\kappa) = \kappa$
- **singolare** se $\mathrm{cof}(\kappa) < \kappa$
- **successore** se $\kappa = \aleph_{\alpha+1}$ per qualche ordinale α
- **limite** se $\kappa = \aleph_\lambda$ con λ ordinale limite
- **limite forte** se $\aleph_0 < \kappa$ e $\forall \alpha \;\; \aleph_\alpha < \kappa \longrightarrow 2^{\aleph_\alpha} < \kappa$
- **debolmente inaccessibile** se è regolare e limite
- **fortemente inaccessibile** se è regolare e limite forte

OSS Un cardinale limite forte è anche limite

DIMOSTRAZIONE

Se fosse $\kappa = \aleph_{\alpha+1}$ allora $\kappa \leq 2^{\aleph_\alpha}$, quindi κ non sarebbe limite forte □

proposizione I cardinali successori sono regolari

DIMOSTRAZIONE

Sia $\kappa = \aleph_{\alpha+1}$. Supponiamo per assurdo $\lambda = \mathrm{cof}(\kappa) < \kappa$.

Allora esiste $\{\kappa_i\}_{i\in\lambda}$ con $\forall i \in \lambda \;\; \kappa_i < \kappa$ e $\sum_{i\in\lambda} \kappa_i = \kappa$

Quindi $\kappa = \sum_{i\in\lambda} \kappa_i \leq \sum_{i\in\lambda} \aleph_\alpha = \aleph_\alpha \cdot \lambda \leq \aleph_\alpha < \kappa$ ↯ □

Corollario Se κ è successore $\partial(\kappa) = 2^\kappa$

DIMOSTRAZIONE
$\partial(\kappa) = \kappa^\kappa = 2^\kappa \quad (2^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa)$ □

Proposizione Se λ è un ordinale limite $cof(\aleph_\lambda) = cof(\lambda)$

DIMOSTRAZIONE
Il sottoinsieme $\{\omega_\alpha \mid \alpha < \lambda\} \subseteq \omega_\lambda$ è cofinale ed isomorfo come ordine a λ. □

Proposizione (Formula di Hausdorff) Siano κ e λ cardinali infiniti, allora
$$(\kappa^+)^\lambda = \kappa^\lambda \cdot \kappa^+$$

DIMOSTRAZIONE
$\geq$: vale $(\kappa^+)^\lambda \geq \kappa^+$ e $(\kappa^+)^\lambda \geq \kappa^\lambda$, quindi $(\kappa^+)^\lambda \geq max(\kappa^\lambda, \kappa^+) = \kappa^\lambda \cdot \kappa^+$
$\leq$: se $\kappa^+ \leq \lambda / \kappa < \lambda$:
$$(\kappa^+)^\lambda \leq (2^\kappa)^\lambda \leq (\kappa^\lambda)^\lambda = \kappa^\lambda \leq \kappa^\lambda \cdot \kappa^+$$
se $\kappa \geq \lambda$:
$$(\kappa^+)^\lambda = |\{f : \lambda \to \kappa^+\}|$$
Data $f : \lambda \to \kappa^+$, $|Im f| \leq \lambda < \kappa^+$, quindi $Im(f)$ non è cofinale in κ^+:
$\exists \alpha \in \kappa^+ \ Im f \subseteq \alpha$
Allora $(\kappa^+)^\lambda = |\{f : \lambda \to \kappa^+\}| = |\bigcup_{\alpha \in \kappa^+} \{f : \lambda \to \alpha\}|$
quindi $(\kappa^+)^\lambda \leq \sum_{\alpha \in \kappa^+} |\{f : \lambda \to \alpha\}| = \sum_{\alpha \in \kappa^+} |\alpha|^\lambda \leq \sum_{\alpha \in \kappa^+} \kappa^\lambda = \kappa^\lambda \cdot \kappa^+$

<u>FATTO</u> La funzione esponenziale κ^λ è determinata ricorsivamente dalle funzioni cof e ∂

Def. Sia κ un cardinale limite. Definiamo
$$2^{<\kappa} := sup\{2^\lambda \mid \lambda \text{ cardinale} < \kappa\}$$

Lemma Dato κ cardinale limite
$$2^\kappa = (2^{<\kappa})^{cof(\kappa)}$$

DIMOSTRAZIONE
Sia $\lambda = cof(\kappa)$ e $\{\kappa_i\}_{i \in \lambda}$ tale che $\forall i \in \lambda \ \kappa_i < \kappa$ e $\sum_{i \in \lambda} \kappa_i = \kappa$. Allora
$$2^\kappa = 2^{\sum_{i \in \lambda} \kappa_i} = \prod_{i \in \lambda} 2^{\kappa_i} \leq \prod_{i \in \lambda} 2^{<\kappa} = (2^{<\kappa})^\lambda \leq (2^\kappa)^\lambda = 2^\kappa$$ □

Def. Sia κ un cardinale. Diciamo che la funzione $\lambda \mapsto 2^\lambda$ è definitivamente costante sotto κ se esiste un cardinale $\mu < \kappa$ tale che $\forall \nu$ cardinale $\mu \leq \nu < \kappa \to 2^\nu = 2^\mu$

Proposizione La funzione $\kappa \longmapsto 2^\kappa$ è determinata da $\gimel$ come segue:

$$2^\kappa = \begin{cases} \gimel(\kappa) & \text{se } \kappa \text{ è successore} \\ & \text{altrimenti:} \\ 2^{<\kappa} \cdot \gimel(\kappa) & \text{se } \lambda \mapsto 2^\lambda \text{ è definitivamente costante sotto } \kappa \\ \gimel(2^{<\kappa}) & \text{se } \lambda \mapsto 2^\lambda \text{ non è definitivamente costante sotto } \kappa \end{cases}$$

DIMOSTRAZIONE

Abbiamo già visto il caso successore. Supponiamo κ sia un cardinale limite.

- Caso $\lambda \mapsto 2^\lambda$ definitivamente costante sotto κ e κ regolare

$$2^{<\kappa} \cdot \gimel(\kappa) = 2^{<\kappa} \cdot \kappa^\kappa = 2^{<\kappa} \cdot 2^\kappa = 2^\kappa$$

- Caso $\lambda \mapsto 2^\lambda$ definitivamente costante sotto κ e κ singolare

  Sia μ tale che $\forall \nu$ cardinale $\mu \leq \nu < \kappa \longrightarrow 2^\nu = 2^\mu = 2^{<\kappa}$, allora

$$2^\kappa = (2^{<\kappa})^{\mathrm{cof}(\kappa)} = 2^{\mu \cdot \mathrm{cof}(\kappa)} = 2^\mu = 2^{<\kappa}$$

  e si conclude osservando che

$$\gimel(\kappa) = \kappa^{\mathrm{cof}(\kappa)} \leq (2^\kappa)^{\mathrm{cof}(\kappa)} = (2^{<\kappa})^{\mathrm{cof}(\kappa)} = 2^{\mu \cdot \mathrm{cof}(\kappa)} = 2^{<\kappa}$$

- Caso $\lambda \mapsto 2^\lambda$ non definitivamente costante sotto κ.

  Basta dimostrare che $\mathrm{cof}(2^{<\kappa}) = \mathrm{cof}(\kappa)$, da questo segue

$$2^\kappa = (2^{<\kappa})^{\mathrm{cof}(\kappa)} = (2^{<\kappa})^{\mathrm{cof}(2^{<\kappa})} = \gimel(2^{<\kappa})$$

  Dimostriamo che $\mathrm{cof}(2^{<\kappa}) \leq \mathrm{cof}(\kappa)$. Sia $A \subseteq \kappa$ cofinale.
  Consideriamo $B = \{2^\alpha \mid \alpha \in A\}$. Chiaramente $|B| \leq |A|$
  Mostriamo che B è cofinale in $2^{<\kappa}$. Se $x < 2^{<\kappa}$, allora esiste $\alpha < \kappa$ tale che $x < 2^\alpha$. Siccome A è cofinale in κ, esiste $\beta \in A$ tale che $\alpha \leq \beta$.
  Quindi $2^\beta \in B$ e $x < 2^\beta$.
  Mostriamo ora che $\mathrm{cof}(\kappa) \leq \mathrm{cof}(2^{<\kappa})$
  Per definizione, dato $\alpha < 2^{<\kappa}$, esiste $\beta < \kappa$ tale che $\alpha < 2^\beta$.
  Sia β_α il minimo di tali β. Sia ora $A \subseteq 2^{<\kappa}$ un insieme cofinale e definiamo $B = \{\beta_\alpha \mid \alpha \in A\}$. Di nuovo $|B| \leq |A|$: dimostriamo che B è cofinale in κ
  Preso $x \in \kappa$, $2^x \leq 2^{<\kappa}$. Però, siccome $\lambda \mapsto 2^\lambda$ non è definitivamente costante sotto κ, esiste y con $x < y < \kappa$ tale che $2^x < 2^y$, quindi $2^x < 2^{<\kappa}$. Sia $\alpha \in A$ con $2^x \leq \alpha$, che esiste perché A è cofinale.
  Allora $2^x \leq \alpha < 2^{\beta_\alpha}$, quindi $x < \beta_\alpha$ $\square$

LA GERARCHIA DI VON NEUMANN E L'ASSIOMA DI BUONA FONDAZIONE

DEF. Costruiamo per ricorsione transfinita

$V_0 = \emptyset$

$V_{s(\alpha)} = \mathcal{P}(V_\alpha)$

$V_\lambda = \bigcup \{V_\alpha \mid \alpha < \lambda\}$

La classe V_* è l'unione degli insiemi V_α, formalmente:

$$x \in V_* \equiv \exists \alpha \in Ord \ x \in V_\alpha$$

Lemma $\forall \alpha \in Ord$ V_α è transitivo

DIMOSTRAZIONE

Per induzione transfinita:

- Caso 0 : immediato perché $\emptyset$ è transitivo a vuoto
- Caso $s(\alpha)$: $x \in V_{s(\alpha)} = \mathcal{P}(V_\alpha) \longrightarrow x \subseteq V_\alpha$. Per hp. ind. V_α è transitivo, quindi $\forall y \in x \ y \subseteq V_\alpha \longrightarrow \forall y \in x \ y \in V_{s(\alpha)}$
- Caso λ: $x \in V_\lambda \longrightarrow x \in V_\alpha$ per qualche $\alpha < \lambda$ e V_α è transitivo per hp. ind quindi $x \subseteq V_\alpha \subseteq V_\lambda$

□

corollario V_* è una classe transitiva, ossia $\forall x \in V_* \ x \subseteq V_*$

Lemma $\forall \alpha, \beta \in Ord$ $\alpha \leq \beta \longrightarrow V_\alpha \subseteq V_\beta$

DIMOSTRAZIONE

Dimostriamo per induzione transfinita su β che $\forall \alpha < \beta \ V_\alpha \subseteq V_\beta$

- Caso $\beta = 0$ · vero a vuoto
- Caso successore: siccome $\alpha < s(\beta) \longleftrightarrow \alpha \leq \beta$, per hp. ind. abbiamo $V_\alpha \subseteq V_\beta$, quindi per def. $V_\alpha \in V_{s(\beta)} = \mathcal{P}(V_\beta)$
  Per la transitività di $V_{s(\beta)}$: $V_\alpha \subseteq V_{s(\beta)}$
- Caso limite: $\alpha < \lambda \longrightarrow V_\alpha \subseteq \bigcup \{V_\alpha \mid \alpha < \lambda\} = V_\lambda$

□

Lemma $\forall \alpha \in Ord$ $\alpha \subseteq V_\alpha$

DIMOSTRAZIONE

Per induzione transfinita:

- Caso base: $\emptyset \subseteq V_0 = \emptyset$
- Caso successore: $\left.\begin{array}{l} \alpha \subseteq V_\alpha \longrightarrow \alpha \subseteq V_{s(\alpha)} \\ \alpha \in \mathcal{P}(V_\alpha) = V_{s(\alpha)} \longrightarrow \{\alpha\} \subseteq V_{s(\alpha)} \end{array}\right\} \longrightarrow s(\alpha) = \alpha \cup \{\alpha\} \subseteq V_{s(\alpha)}$
- Caso limite: $\lambda = \bigcup \{\alpha \mid \alpha < \lambda\} \subseteq \bigcup \{V_\alpha \mid \alpha < \lambda\} = V_\lambda$

□

DEF. Data una formula insiemistica, la possiamo relativizzare a V_* rimpiazzando tutti i quantificatori $\exists\square$ con $\exists\square\in V_*$ e tutti i $\forall\square$ con $\forall\square\in V_*$

esempio Sia $\varphi\equiv\exists x\ \forall y\in x\ \exists z\in y\ \ z\cap x=\emptyset$

cioè $\varphi\equiv\exists x\ \forall y\,(y\in x\longrightarrow\exists z(z\in y\wedge\neg\exists t(t\in x\wedge t\in z)))$

φ relativizzata a V_* diventa:

$$\exists x\in V_*\ \forall y\in V_*\ (y\in x\longrightarrow\exists z\in V_*(z\in y\wedge\neg\exists t\in V_*(t\in x\wedge t\in z)))$$

Teorema Valgono gli assiomi della teoria degli insiemi relativizzati a V_*

DIMOSTRAZIONE

① Vuoto: $\exists x\in V_*\ \ \forall y\in V_*\ \ y\notin x$
Basta prendere $x=\emptyset\in V_1$

② Estensionalità: $\forall a,b\in V_*\ \ a=b\longleftrightarrow\forall x\in V_*\ (x\in a\longleftrightarrow x\in b)$
Per la transitività dei V_α, gli elementi di a e b sono anch'essi in V_*, quindi $\forall x\in V_*\ (x\in a\longleftrightarrow x\in b)$ equivale a $\forall x\ (x\in a\longleftrightarrow x\in b)$.
Si conclude per l'assioma di estensionalità.

③ Separazione: $\forall A\in V_*\ \exists B\in V_*\ \forall x\in V_*\ \ x\in B\longleftrightarrow(x\in A\wedge\varphi(x))$
Per separazione esiste $B=\{x\in A\mid x\in V_*\wedge\varphi(x)\}\subseteq A\in V_\alpha$ per qualche α.
Per transitività $B\subseteq V_\alpha$, cioè $B\in V_{S(\alpha)}$ e quindi $B\in V_*$

④ Paio: $\forall a,b\in V_*\ \exists B\in V_*\ \forall x\in V_*\ \ x\in B\longleftrightarrow(x=a\vee x=b)$
Se $a\in V_\alpha, b\in V_\beta$ e senza perdita di generalità $\alpha\le\beta$, allora $a,b\in V_\beta$, quindi $\{a,b\}\in\mathcal{P}(V_\beta)=V_{S(\beta)}$

⑤ Unione: $\forall A\in V_*\ \ \exists B\in V_*\ \ \forall x\in V_*\ \ x\in B\longleftrightarrow\exists y\in A\ \ x\in y$
Se $A\in V_\alpha$, per transitività $A\subseteq V_\alpha$ e quindi $\bigcup A\subseteq V_\alpha$, perciò $\bigcup A\in V_{S(\alpha)}$

⑥ Parti: $\forall A\in V_*\ \exists B\in V_*\ \forall x\in V_*\ \ x\in V_*\longleftrightarrow x\subseteq A$
Se $A\in V_\alpha$, per transitività $A\subseteq V_\alpha$, quindi $P(A)\subseteq P(V_\alpha)=V_{S(\alpha)}$, perciò $P(A)\in P(V_{S(\alpha)})=V_{\alpha+2}$

⑦ Infinito: $\exists X\in V_*\ \ \emptyset\in X\wedge\forall y\in V_*\ \ y\in X\longrightarrow y\cup\{y\}\in X$
Basta considerare $X=\omega\in V_{S(\omega)}$

⑧ Rimpiazzamento: $F.V_*\longrightarrow V_*$ funzione classe e $X\in V_*\ \longrightarrow F[X]\in V_*$
Se $X\in V_\alpha$, per transitività $a\in X\longrightarrow a\in V_\alpha$, quindi $F(a)$ è ben definito e $F(a)\in V_*$ per $a\in X$.
Sia α_a minimo con $F(a)\in V_{\alpha_a}$ e $\beta=\sup\{\alpha_a\mid a\in X\}$. Allora $F[X]\subseteq V_\beta$ e $F[X]\in V_{S(\beta)}$.

⑨ Scelta: $\forall X\in V_*\ \ (\forall y\in X\ \ y\neq\emptyset)\longrightarrow\exists f\in V_*$ funzione di scelta su X
Sia f una funzione di scelta su $X\in V_\alpha$. Osserviamo che $f\subseteq\mathcal{P}(\mathcal{P}(X\cup\bigcup X))\subseteq\mathcal{P}(\mathcal{P}(V_\alpha))=V_{\alpha+2}$, quindi $f\in V_{\alpha+3}$ e perciò $f\in V_*$. $\square$

OSS Dato $x\in V_*$, esiste il minimo α tale che $x\in V_\alpha$, e questo è necessariamente un ordinale successore, perché se $x\in V_\lambda=\bigcup\{V_\alpha\mid\alpha<\lambda\}$ allora $x\in V_\alpha$ per qualche $\alpha<\lambda$.

DEF. Dato $x\in V_*$, detto α il minimo ordinale tale che $x\in V_\alpha$, il rango di x, $\mathrm{rank}(x)$, è definito da $\alpha=\mathrm{rank}(x)+1$, ossia

$$x\in V_\alpha\longleftrightarrow\mathrm{rank}(x)<\alpha$$

Lemma Se $x \in y \in V_*$ allora $\mathrm{rank}(x) < \mathrm{rank}(y)$

DIMOSTRAZIONE

$y \in V_{s(\mathrm{rank}(y))} = \mathcal{P}(V_{\mathrm{rank}(y)})$, quindi $y \subseteq V_{\mathrm{rank}(y)}$,
da cui $x \in V_{\mathrm{rank}(y)}$ e perciò $\mathrm{rank}(x) < \mathrm{rank}(y)$ □

DEF. Una classe C si dice ben fondata se per ogni insieme S di elementi di C, S contiene un x minimale per appartenenza ($\in$-minimale), ossia tale che $x \cap S = \emptyset$

Proposizione La classe C è ben fondata se e solo se non esiste una famiglia $\{x_i\}_{i\in\omega}$ di elementi di C tale che $\forall i \in \omega$ $x_{i+1} \in x_i$,
ossia non esiste una catena infinita discendente per appartenenza

DIMOSTRAZIONE

Se $\{x_i\}_{i\in\omega}$ è una catena infinita discendente, allora $\{x_i \mid i \in \omega\}$ non ha un elemento $\in$-minimale
Invece se S non ha un elemento $\in$-minimale, fissata una funzione di scelta f su S, possiamo definire una catena discendente per ricorsione numerabile.
Fissiamo $\bar{x} \in S$: $x_0 = \bar{x}$ $\quad x_{n+1} = f(\{y \in S \mid y \in x_n\})$
dove l'insieme a cui è applicata f è non vuoto, altrimenti x_n sarebbe $\in$-minimale □

Proposizione La classe V_* è ben fondata.

DIMOSTRAZIONE

Dato un insieme S di elementi di V_*, consideriamo $x \in V_*$ di rango minimo.
Se esistesse $y \in S$ con $y \in x$ allora avremmo $\mathrm{rank}(y) < \mathrm{rank}(x)$ ↯ □

Teorema Se gli assiomi della teoria degli insiemi sono coerenti, essi non dimostrano l'esistenza di una catena infinita discendente per appartenenza

DIMOSTRAZIONE

Supponiamo di poter dimostrare che la catena esiste.
Siccome gli assiomi valgono relativizzati a V_*, possiamo svolgere la dimostrazione relativizzata ed ottenere che esiste una catena infinita discendente in V_*, ma V_* è ben fondata ↯ □

⑩ Assioma di buona fondazione

$\forall S \neq \emptyset \quad \exists x \in S \quad x \cap S = \emptyset$

Proposizione: Esistenza della chiusura transitiva Dato un insieme X, esiste il più piccolo insieme transitivo $tc(X)$ tale che $X \subseteq tc(X)$

DIMOSTRAZIONE

Costruiamo per ricorsione: $X_0 = X \qquad X_{n+1} = \bigcup X_n$

Si verifica immediatamente che $tc(X) = \bigcup\{X_n \mid n \in \omega\}$ □

Teorema: Principio di ε-induzione Se una classe C soddisfa

$\forall S \ (\forall x \in S \ \ x \in C) \longrightarrow S \in C$

allora $C = V$, ossia $\forall S \ S \in C$

DIMOSTRAZIONE

Sia per assurdo $S \notin C$. Sia $S' = \{x \in tc(\{S\}) \mid x \notin C\}$

Siccome $S \in S'$, S' non è vuoto, quindi per buona fondazione esiste $x \in S'$ tale che $\forall y \in x \ \ y \notin S'$. Siccome $x \in tc(\{S\})$ e quest'ultimo è transitivo, $\forall y \in x \ \ y \in tc(\{S\})$. È quindi necessario che $\forall y \in x \ \ y \in C$.

Ma allora per ipotesi $x \in C$ e $x \notin S'$ ↯ □

Proposizione $V = V_*$ ossia $\forall x \ \exists \alpha \in Ord \ \ x \in V_\alpha$

DIMOSTRAZIONE

Per ε-induzione, ci basta dire che, fissato un S, se $\forall x \in S \ x \in V_*$ allora $S \in V_*$.

Consideriamo $\alpha = \sup\{rank(x)+1 \mid x \in S\}$

Per ogni $x \in S$ abbiamo $x \in V_{rank(x)+1} \subseteq V_\alpha$, quindi $S \subseteq V_\alpha$.

Di conseguenza $S \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$ □

Corollario Non esistono catene infinite discendenti per appartenenza

ASSIOMI DI ZFC

① Assioma dell'insieme vuoto

$\exists x \ \forall y \ \ y \notin x$

② Assioma di estensionalità

$\forall a \ \forall b \ \ a = b \longleftrightarrow \forall x \ (x \in a \longleftrightarrow x \in b)$

③ Assioma di separazione

$\forall A \ \exists B \ \ \forall x \ \ x \in B \longleftrightarrow (x \in A \wedge \varphi(x))$

④ Assioma del paio

$\forall a \ \forall b \ \exists B \ \ \forall x \ \ x \in B \longleftrightarrow (x = a \vee x = b)$

⑤ Assioma dell'unione

$\forall A \ \exists B \ \forall x \ \ \ x \in B \longleftrightarrow \exists y \in A \ \ x \in y$

⑥ Assioma dell'insieme potenza

$\forall A \ \exists B \ \ \forall x \ \ x \in B \longleftrightarrow (\forall C \ \ C \in x \longrightarrow C \in A)$

⑦ Assioma dell'infinito

$\exists X \ \ \ \emptyset \in X \wedge \forall y \in X \ \ y \cup \{y\} \in X$

⑧ Assioma di rimpiazzamento

Data una funzione classe $F : V \longrightarrow V$

$\forall A \ \exists B \ \ \forall y \ \ y \in B \longleftrightarrow \exists x \in A \ \ \ F(x) = y$

⑨ Assioma della scelta (AC)

Dato X insieme di insiemi non vuoti,

allora esiste una funzione di scelta per X,

cioè $f : X \longrightarrow \bigcup X$, con $\forall A \in X \ \ f(A) \in A$

⑩ Assioma di buona fondazione

$\forall S \neq \emptyset \ \ \ \exists x \in S \ \ \ x \cap S = \emptyset$