Elementi di teoria degli insiemi

Pisa, a.a. 2021-22

docente: Marcello Mamino (marcello.mamino@unipi.it)

testo consigliato: Hrbacek-Jech, Introduction to set theory

sito del corso: https://ciovil.li/eti21

argomento: teoria degli insiemi di Zermelo-Fraenkel

Indice

6 Prologo nel XIX secolo

9 Digressione: insiemi numerabili

11 Tornando agli insiemi di unicità

16 Giochi di parole

18 Scopi del corso

19 Il linguaggio della teoria degli insiemi

22 Le regole di inferenza

25 Assiomi dell'insieme vuoto e di estensionalità

27 Assioma di separazione

29 Classi e classi proprie

30 Assioma del paio e coppia di Kuratowski

33 Assioma dell'unione e operazioni booleane

37 Assioma delle parti e prodotto cartesiano

39 Relazioni di equivalenza e di ordine, funzioni

43 Assioma dell'infinito e numeri naturali

46 Gli assiomi di Peano

48 L'ordine di ω

51 Induzione forte e principio del minimo

54 Ricorsione numerabile

63 Cardinalità

64 Teorema di Cantor-Bernstein

68 Teorema di Cantor

69 Operazioni fra cardinalità

71 Cardinalità finite

72 Principio dei cassetti

76 Operazioni fra le cardinalità finite

78 La cardinalità numerabile — $\aleph_0$

84 Insiemi numerabili in pratica

86 $\aleph_0 \cdot \aleph_0 = \aleph_0$

89 $\mathbb{Z}$ e $\mathbb{Q}$

97 Ordini densi numerabili

104 Il grafo random

106 $\mathbb{R}$ e la cardinalità del continuo

110 Caratterizzazione di $(\mathbb{R}, <)$

113 $|\mathbb{R}| = 2^{\aleph_0}$

114 Operazioni che coinvolgono $2^{\aleph_0}$

115 $2^{\aleph_0} - \aleph_0 = 2^{\aleph_0}$

118 Stato del corso

120 I buoni ordinamenti

128 Operazioni fra buoni ordinamenti

135 Gli ordinali di Von Neumann

144 Assioma del rimpiazzamento

148 Induzione e ricorsione transfinita

157 Operazioni fra gli ordinali

162 Aritmetica ordinale e forma normale di Cantor

167 Sottrazione e divisione euclidea

169 La forma normale di Cantor

171 Punti fissi e ε-numbers

173 Operazioni in forma normale di Cantor

177 Gli alef

178 Teorema di Hartogs

182 Somme e prodotti di alef

186 L'assioma di scelta

190 Buon ordinamento → AC

191 AC → buon ordinamento (idra)

192 Zorn → buon ordinamento

193 AC → Zorn

195 Conseguenze immediate di AC

199 Esempi di applicazione di AC

200 Basi di spazi vettoriali

202 Invariante di Dehn

205 Insieme di Vitali

209 Teorema di Cantor – Bendixson

216 $|X| = |X \times X| \rightarrow AC$ (Tarski)

217 Aritmetica cardinale

218 Somme e prodotti infiniti

220 Teorema di König

222 Cofinalità

227 Formula di Hausdorff

231 Gerarchia di Von Neumann

233 Formule relativizzate ad una classe

238 Assioma di buona fondazione

239 Principio di $\in$-induzione

Prologo nel ~~XIX~~ Secolo

La nascita della teoria degli insiemi è una storia complicata di cui so pochissimo. Però, persone che ne sanno molto più di me hanno sostenuto l'opinione che il problema seguente abbia avuto un ruolo. Come che sia, è almeno una introduzione possibile.

Problema Data una serie trigonometrica

$$S(x) = c_0 + \sum_{i=1}^{\infty} a_i \sin(ix) + b_i \cos(ix)$$

se, per ogni $x \in \mathbb{R}$, sappiamo che $S(x)$ converge a 0, possiamo dire che i coefficienti c_0, a_i, b_i sono tutti 0?

Risolto positivamente da Georg Cantor nel 1870.

Def. Diciamo che $X \subseteq \mathbb{R}$ è un *insieme di unicità* se, per ogni serie trigonometrica

$$S(x) = c_0 + \sum_{i=1}^{\infty} a_i \sin(ix) + b_i \cos(ix)$$

vale la seguente implicazione

$$\left.\begin{array}{l} S(x) \text{ converge a } 0 \text{ per} \\ \text{tutti gli } x \notin X \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{tutti i coefficienti } c_0, \\ a_i, b_i \text{ sono nulli} \end{array}\right.$$

Esempio per il risultato di Cantor, $\emptyset$ è di unicità.

Problema Quali sottoinsiemi di $\mathbb{R}$ sono di unicità?

Fatto $X \subseteq \mathbb{R}$ è di unicità se (ma non solo se):

(*) ogni funzione continua $f: \mathbb{R} \to \mathbb{R}$ che soddisfi le ipotesi seguenti è necessariamente lineare: $f(x) = ax + b$

- per ogni intervallo $]a,b[$ con $]a,b[\cap X = \emptyset$, $f|_{]a,b[}$ è lineare,
- per ogni $x \in \mathbb{R}$, se f ha derivate dx e sx in x, allora queste coincidono. "f non ha punti angolosi"

Esempio $X = \{\dots, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots\} = \{a_i \mid i \in \mathbb{Z}\}$ con $\dots < a_{-2} < a_{-1} < a_0 < a_1 < a_2 < \dots$, $\lim_{i \to +\infty} a_i = +\infty$, $\lim_{i \to -\infty} a_i = -\infty$ ha la proprietà (*), quindi è di unicità.

NON esempi: l'intervallo $[0,1]$ e $\mathbb{R}$ non hanno (*).

NON esempio buffo: l'insieme di Cantor non ha (*).

$C_0 = [0, 1]$

$C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$

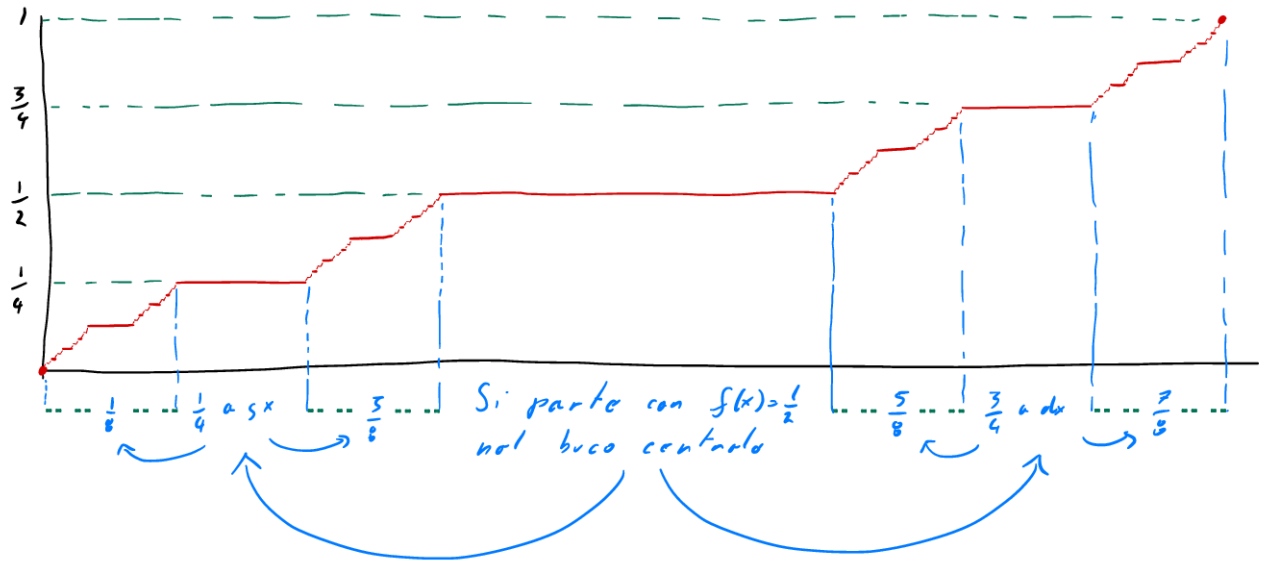
$C_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$

$C_3 = [0, \frac{1}{27}] \cup [\frac{2}{27}, \frac{1}{9}] \cup [\frac{2}{9}, \frac{7}{27}] \cup [\frac{8}{27}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{19}{27}] \cup [\frac{20}{27}, \frac{7}{9}] \cup [\frac{8}{9}, \frac{25}{27}] \cup [\frac{26}{27}, 1]$

etc.

$C = C_0 \cap C_1 \cap C_2 \cap C_3 \cap \dots$ ← detto insieme di Cantor.

Esiste una funzione continua $f: \mathbb{R} \to \mathbb{R}$, detta scala di Cantor — o del diavolo, tale che $f'(x) = 0$ per $x \notin C$ e non è derivabile in $x \in C$.



Nota $\mathbb{Q}$ e C non hanno $(*)$ ma, in realtà, sono di unicità.

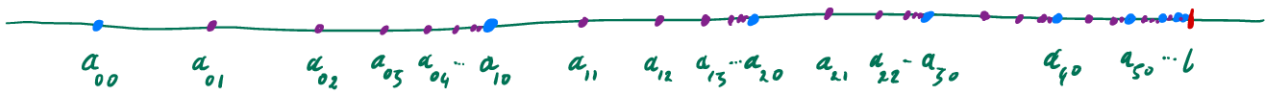
Esempio buffo (Una successione crescente col suo limite)



$X = \{a_0, a_1, a_2, \dots, l\} = \{a_i \mid i \in \mathbb{N}\} \cup \{l\}$ con $a_i \uparrow l$.

Dim La funzione f è lineare in $]-\infty, a_0[$, $]a_0, a_1[$, $]a_1, a_2[$, ... Quindi nei punti $a_0, a_1, a_2 \dots$ ammette derivata dx e sx. Siccome questi punti non possono essere angolosi, $f_{|]-\infty, a_0[}$, $f_{|]a_0, a_1[}$, etc. hanno lo stesso coefficiente angolare, quindi, sfruttando la continuità, $f_{|]-\infty, l[}$ è lineare. Siccome $f_{|]l, +\infty[}$ è lineare, usando nuovamente l'assenza di punti angolosi abbiamo la tesi.

Esempio più buffo (Una succ. crescente di succ. crescenti)



$X = \{ a_{ij} \mid i, j \in \mathbb{N} \} \cup \{l\}$

dove $a_{i0} \uparrow l$ per $i \to +\infty$

$a_{ij} \uparrow a_{(i+1)0}$ per $j \to +\infty$ con i fissato.

Dim. In ciascuno degli intervalli $]a_{i0}, a_{(i+1)0}[$, f è lineare ragionando come nell'esempio precedente, e ora ci siamo ridotti alla situazione — di nuovo — dell'esempio precedente con $a'_i = a_{i0}$.

Digressione: insiemi numerabili

Def Un insieme X è *numerabile* se è il supporto di una successione, $X = \{a_0, a_1, a_2, \dots\} = \{a_i \mid i \in \mathbb{N}\}$, con $a_i \neq a_j$ per ogni $i \neq j$.

Esempi

$\mathbb{N}$	$0, 1, 2, 3 \dots$	$a_i = i$
{n. dispari}	$1, 3, 5, 7 \dots$	$a_i = 2i + 1$
{n. primi}	$2, 3, 5, 7 \dots$	$a_i = b, h$? p_i ?
$\mathbb{Z}$	$0, -1, 1, -2, 2 \dots$	$a_i = (-1)^i \left\lceil \frac{i}{2} \right\rceil$

Esempio meno immediato: $\mathbb{N} \times \mathbb{N} = \{(x, y) \mid x, y \in \mathbb{N}\}$

Dim. La funzione $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$$(x, y) \longmapsto 2^x(1 + 2y) - 1$$

è biunivoca (perché?) quindi $a_i = f^{-1}(i)$ enumera $\mathbb{N} \times \mathbb{N}$.

Prop. Un sottoinsieme infinito di un insieme numerabile è, a sua volta, numerabile.

Dim Sia $Y \subseteq X$ con Y infinito e $X = \{a_i \mid i \in \mathbb{N}\}$.
La sottosuccessione $b_j = a_{i_j}$ degli a_i che appartengono a Y enumera Y. A essere precisi bisognerebbe dire esattamente chi sono gli indici i_j. Per ricorsione:

$$i_0 = \min\{i \mid a_i \in Y\} \qquad i_{j+1} = \min\{i > i_j \mid a_i \in Y\}$$

dove i minimi esistono perché Y non è finito.

Prop. Se X e Y sono numerabili, $X \times Y = \{(a,b) \mid a \in X, b \in Y\}$ è anch'esso numerabile

Dim Fissiamo $X = \{a_i \mid i \in \mathbb{N}\}$ $Y = \{b_j \mid j \in \mathbb{N}\}$.
Siccome $\mathbb{N} \times \mathbb{N}$ è numerabile, $\mathbb{N} \times \mathbb{N} = \{(i_t, j_t) \mid t \in \mathbb{N}\}$.
Quindi $X \times Y = \{(a_{i_t}, a_{j_t}) \mid t \in \mathbb{N}\}$

Esempio $\mathbb{Q}$ è numerabile

Dim $\mathbb{Q}$ è in corrispondenza biunivoca con

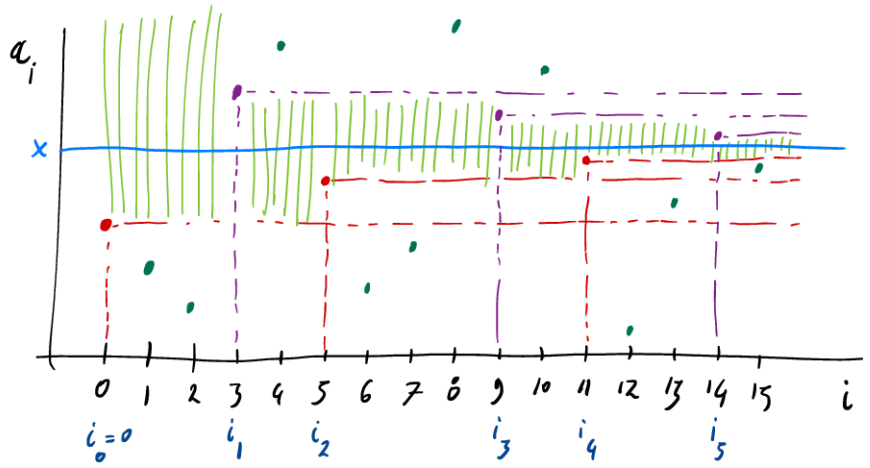
$$F = \{(num, den) \mid num \in \mathbb{Z} \wedge den \in \mathbb{N}^{>0} \wedge MCD(num, den) = 1\}$$
$$\subseteq \mathbb{Z} \times \mathbb{N}.$$

NON esempio $\mathbb{R}$ non è numerabile

Dim. Supponendo, per assurdo, che $\mathbb{R} = \{a_i \mid i \in \mathbb{N}\}$, cerchiamo un $x \in \mathbb{R}$ che non compare fra gli a_i. Allo scopo, costruiamo una la sottosuccessione a_{i_j} definita per ricorrenza da

$i_0 = 0 \qquad i_1 = \min\{i \mid a_i > a_0\}$

$i_{j+1} = \min\{i \mid a_i \text{ è compreso fra } a_{i_{j-1}} \text{ e } a_{i_j}\}$



Si vede facilmente (esercizio!) che la successione $\{a_{i_{2k}}\}_k$ è crescente, $\{a_{i_{2k+1}}\}_k$ è decrescente e $\lim_{k\to\infty} a_{i_{2k}} \leq \lim_{k\to\infty} a_{i_{2k+1}}$.
Fissiamo x tale che $\lim_{k\to\infty} a_{i_{2k}} \leq x \leq \lim_{k\to\infty} a_{i_{2k+1}}$. Chiaramente x non è nessuno degli a_{i_j}, perché $a_{i_{2k}} < x < a_{i_{2k+1}}$. Supponiamo $x = a_n$, allora ci sarà un j tale che $i_j < n < i_{j+1}$, ma questo è assurdo perché allora $x = a_n$ è compreso fra $a_{i_{j-1}}$ e a_{i_j}, però $n < i_{j+1}$ contro la minimalità di quest'ultimo.
(Esercizio: hai notato il caso $n < i_1$? Aggiustalo!)

Esercizio Dimostra che l'insieme di Cantor C non è numerabile.

Tornando agli insiemi di unicità

Teo (Cantor-Lebesgue) Se $X \subseteq \mathbb{R}$ è chiuso e numerabile, allora X soddisfa (*), ed è, quindi, di unicità.

La strategia dimostrativa passa attraverso una definizione.

Def Dato $X \subseteq \mathbb{R}$, il *derivato di Cantor-Bendixson* di X è

$$X' = X \setminus \{\text{punti isolati di } X\}$$

(Dove $a \in X$ è un punto isolato se $\exists \varepsilon > 0 \ ]a-\varepsilon, a+\varepsilon[\cap X = \{a\}$)

Oss Se X è chiuso e X' ha (*), allora anche X ha (*).

Dim Occorre dimostrare che se f è continua, lineare ristretta agli intervalli aperti che non intersecano X, e non ha punti angolosi, allora f è lineare ristretta agli intervalli aperti che non intersecano X'. Fatto questo, usando l'ipotesi su X', f è lineare — abbiamo quindi mostrato che X ha (*).

Sia $]a,b[\cap X' = \emptyset$, dobbiamo dire che $f|_{]a,b[}$ è lineare.

Ci basta dire che per ogni $\varepsilon > 0$ $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare.

Siccome $]a,b[\cap X' = \emptyset$, $]a,b[\cap X \subseteq \{\text{punti isolati di } X\}$.

Quindi $[a+\varepsilon, b-\varepsilon] \cap X$ è finito — se così non fosse, avrebbe un punto di accumulazione α che non può essere un punto isolato di X, per cui $f|_{[a+\varepsilon, b-\varepsilon]}$ è lineare a tratti, e, siccome non ha punti angolosi, è lineare.

Cor Sia $X^{(n)} = X^{\overbrace{\prime\prime\ldots}^{n \text{ volte}}}$. Se $X^{(n)} = \emptyset$ per qualche $n \in \mathbb{N}$, allora X ha (*).

Dim Induzione su n.

Il guaio è che ci sono chiusi numerabili per cui $X^{(n)} \neq \emptyset$ qualunque sia n.

Esempio Vogliamo costruire X chiuso e numerabile tale che $X^{(n)} \neq \emptyset$ per ogni $n \in \mathbb{N}$. Cominciamo col rivedere alcuni esempi già visti.

- $X = \{a_0, a_1, a_2, \dots\}$ con $a_i \uparrow +\infty$ per $i \to \infty$.



Tutti i punti sono isolati, $X' = \emptyset$.

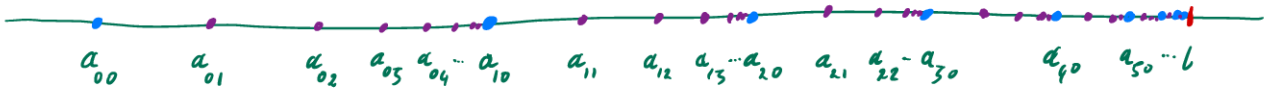
- $X = \{a_0, a_1, a_2, \dots, l\}$ con $a_i \uparrow l$ per $i \to \infty$.



"Successione con punto limite"

Tutti i punti sono isolati salvo l, quindi $X' = \{l\}$ e $X'' = \emptyset$.

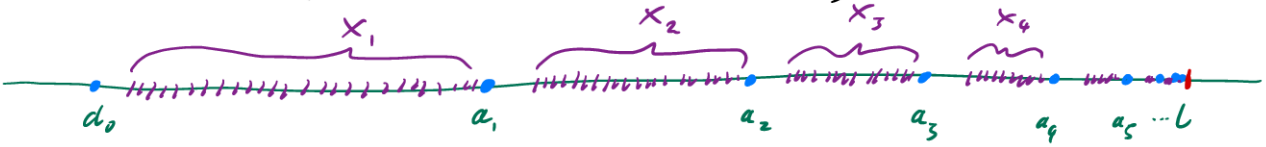
- $X = \{a_{ij} \mid i, j \in \mathbb{N}\} \cup \{l\}$ con $a_{i0} \uparrow l$ e $a_{ij} \uparrow a_{(i+1)0}$.



"Successione di successioni"

$X' = \{a_{10}, a_{20}, a_{30}, \dots, l\}$ $X'' = \{l\}$ $X''' = \emptyset$

Si vede che possiamo proseguire, in questo modo, costruendo una successione di successioni di successioni, etc. n volte, X_n. Avremo $X_n^{(n)} \neq \emptyset$, $X_n^{(n+1)} = \emptyset$. Ora costruiamo X_ω fatto così:



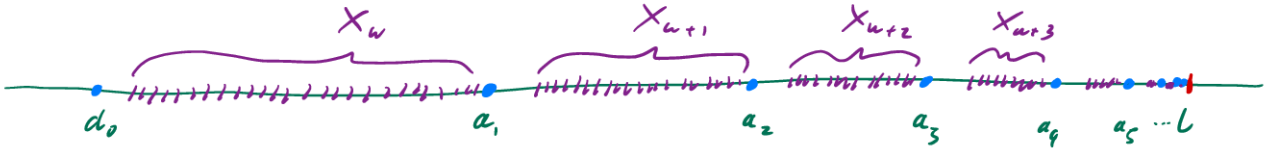
È chiaro che, per ogni n, $X_w^{(n)} \neq \emptyset$. D'altro canto, X_w soddisfa $(*)$, perché f deve essere lineare in ciascuno degli intervalli $[a_n, a_{n+1}]$, perché X_{n+1} soddisfa $(*)$, quindi ci si riduce al caso della successione.

Esercizio: perché X_w è numerabile?

Ora potremmo pensare che, pazienza se X_w non si smonta a furia di derivati, sarà un caso particolare. Però, adesso, possiamo fare una successione di insiemi come X_w, chiamiamola X_{w+1}, e una successione di questi X_{w+2}, etc.
Al diavolo, serve un nuovo corollario!

Cor 2 Se $X^{(n)}$ è "tipo X_w", allora X ha $(*)$.

Ok, questo corollario copre X_w, X_{w+1}, X_{w+2}, ma copre anche $X_{w\cdot 2}$?



No: occorre un nuovo corollario.

Cor 3 Se $X^{(n)}$ è "tipo $X_{w\cdot 2}$", allora X ha $(*)$.

E poi un altro per $X_{w\cdot 3}$, e un altro per $X_{w\cdot 4}$, etc.
E ora abbiamo finito? No, perché possiamo costruire una successione con X_w, $X_{w\cdot 2}$, $X_{w\cdot 3}$, etc.

Se chiamiamo questa follia $X_{w.w}$, ecco che si riparte a fare successioni di $X_{w.w}$. Ora si sarà capito che definiremo una specie di aritmetica di queste cose, per cui potremo fare anche w^w, w^{w^w}, etc.

È questa la soluzione, allora?

No, ogni sforzo di trovare l'induzione a capo delle induzioni è vano. Se ho X_w, X_{ww}, X_{www}, etc., allora, ecco che faccio una successione con questa cosa, la battezzo in qualche modo — chessò, X_{ε_0} — e si riparte!

Per smontare ogni possibile insieme chiuso e numerabile occorre *un nuovo tipo di induzione*, l'induzione transfinita, che è strettamente più potente dell'induzione aritmetica. Questa tecnica è stata sviluppata da Cantor, forse prendendo le mosse dal problema degli insiemi di unicità, e sarà uno degli argomenti centrali del corso.

Esercizio (per la fine del corso)
Dimostra il teorema di Cantor–Lebesgue.

Giochi di parole

Descrivere un oggetto matematico non basta per crearlo. Se bastasse, si incorrebbe in contraddizioni come questa.

Paradosso di Russell

Tipicamente le collezioni — uso questa parola perché daremo, al termine "insieme", un senso tecnico preciso — non sono membre di se stesse: la collezione di tutti i numeri primi non è un numero primo. Però ci sono anche collezioni che sono membre di se stesse: per esempio la collezione di tutte le collezioni. Consideriamo

$$N = \{ \text{collezioni } X \mid X \notin X \}$$

la collezione delle collezioni che non sono membre di se stesse — N per collezioni normali.

$N \in N$ oppure no?

$N \in N$ se e solo se, per definizione $N \notin N$. ↯

Il paradosso di Russell ci dice che, del principio di collezione — ossia l'idea che data una proprietà ben definita P si possa costruire la collezione $\{X \mid P(X)\}$ — non ci si può fidare.

Paradosso di Berry

L'Italiano annovera un numero finito di parole, è quindi possibile formare solo un numero finito di frasi di meno di cento parole. Alcune di queste descrivono un numero naturale, altre no. Comunque, solo un numero finito di numeri naturali può essere descritto con meno di cento parole. Per il principio del minimo, esiste

b = "il più piccolo numero naturale che l'Italiano non può descrivere con meno di cento parole".

Il guaio, chiaramente, è che lo abbiamo appena descritto con sedici parole. ∎

Quindi non ci si può fidare troppo neppure dell'Italiano, o meglio, non è possibile descrivere precisamente cosa sia una descrizione precisa.

In conclusione, occorre fissare un linguaggio formale in cui si esprimono le proposizioni della teoria degli insiemi, e occorre fissare un sistema di assiomi, espressi in questo linguaggio, che dicano quali costruzioni sono lecite: quali insiemi esistono. Il ruolo della teoria degli insiemi è, poi, di fondare l'edificio della matematica. L'ambizione, quindi, è che il linguaggio e gli assiomi della teoria degli insiemi siano, in realtà, il linguaggio e gli assiomi della matematica.

Scopi del corso

Questo corso persegue due obiettivi:

1. Studiare i *fondamenti della matematica*, nella forma più comunemente accettata nel ~~XX~~ secolo e fino ad ora, la teoria degli insiemi di Zermelo–Fraenkel con l'assioma della scelta (ZFC)
2. Studiare *tecniche e strumenti* che sono stati sviluppati grazie alla teoria degli insiemi, per esempio: la teoria delle cardinalità, la teoria dei numeri ordinali, l'induzione e la ricorsione transfinita.

In questo corso non ci occupiamo dei modelli della teoria degli insiemi. Mi spiego. Per esempio, in teoria dei gruppi, si assiomatizza cosa sia un gruppo, e poi si studia come possano essere fatti i diversi gruppi. In teoria degli insiemi, si assiomatizza l'universo di tutti gli insiemi, però, per il teorema di incompletezza di Gödel, questa assiomatizzazione non può essere completa. Quindi esistono tanti universi insiemistici possibili. Indagare queste possibilità — i *modelli della teoria degli insiemi* — è argomento di corsi più avanzati.

Il linguaggio della teoria degli insiemi

Per non incorrere in contraddizione, accettiamo che le sole proposizioni ad avere senso siano quelle esprimibili mediante **formule insiemistiche**. Le formule si costruiscono ricorsivamente.

- Le lettere $a, b, c \dots$, $A, B, C \dots$, $\alpha, \beta, \gamma, \dots$ rappresentano **variabili**. I valori delle variabili sono sempre insiemi, e non ci sono altri oggetti salvo gli insiemi
- Le **formule atomiche** sono

  variabile = variabile "appartiene a" variabile $\in$ variabile

  es. $x = y$, $x = x$, $\alpha = C$ es. $x \in y$, $x \in x$, $\alpha \in C$
- Le formule si combinano fra loro mediante
  - **connettivi logici**

    "non" $\neg$ formula formula "e" $\wedge$ formula formula "o" $\vee$ formula

    $\neg \Phi$ $\equiv$ "Φ è falsa"

    $\Phi \wedge \Psi$ $\equiv$ "Φ e Ψ sono entrambe vere"

    $\Phi \vee \Psi$ $\equiv$ "almeno una fra Φ e Ψ è vera"
  - **quantificatori**

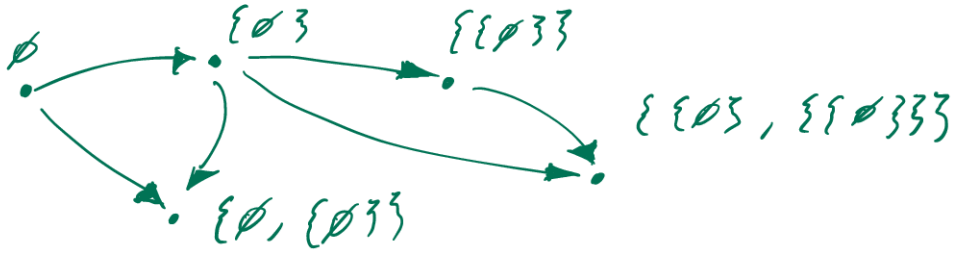
    "per ogni x" $\forall x$ formula "esiste x" $\exists x$ formula

    $\forall x \, \Phi$ $\equiv$ "Φ è vera qualunque sia l'insieme x"

    $\exists x \, \Phi$ $\equiv$ "c'è un insieme x che fa sì che Φ sia vera"

    Es. chiaramente varranno: $\forall x \; x = x$, $\forall x \exists y \; x = y$, $\neg \exists x \forall y \; x = y$

L'intuizione è che l'universo insiemistico sia un gigantesco grafo diretto (aciclico) i cui vertici sono gli insiemi, ed in cui le frecce rappresentano la relazione di appartenenza.



Possiamo solo fare affermazioni a proposito di vertici e frecce di questo grafo. Per esempio

"a è un elemento di un elemento di b" ≡

"c'è un percorso di due frecce fra a e b" ≡

$$\exists x \quad a \in x \wedge x \in b$$

"a è un sottoinsieme di b" ≡

"ogni elemento di a è un elemento di b" ≡

"non c'è un insieme che è elemento di a e non di b" ≡

"non c'è un vertice con una freccia verso a e non verso b" ≡

$$\neg \exists x \quad x \in a \wedge \neg x \in b$$

Parentesi. Ad essere precisi, avremmo dovuto definire le formule includendo un mucchio di parentesi, allo scopo di eliminare ogni possibilità di formare una combinazione di simboli ambigua. Per esempio $\Phi_1 \wedge \Phi_2 \vee \Phi_3$ è ambigua, perché si potrebbe leggere $(\Phi_1 \wedge \Phi_2) \vee \Phi_3$ o $\Phi_1 \wedge (\Phi_2 \vee \Phi_3)$.

In una notazione completamente parentesizzata, per esempio, la formula per "a è un sottoinsieme di b" sarebbe

$$\neg\left(\exists x\left((x\in a)\wedge(\neg(x\in b))\right)\right)$$

Non useremo, in generale, questa notazione, ma useremo le parentesi selettivamente per evitare ambiguità.

Abbreviazioni: Le formule appena descritte costituiscono il linguaggio della teoria degli insiemi *puro*. Durante il corso estenderemo più volte questo linguaggio mediante abbreviazioni, che semplicemente rimpiazzano formule più lunghe con scritture convenzionali più compatte, e quindi non alterano la potenza espressiva del linguaggio. Vediamo le prime abbreviazioni:

$x\neq y \overset{def.}{\equiv} \neg x=y$ $\quad x\notin y \overset{def.}{\equiv} \neg x\in y$ $\quad \exists x\,\Phi \overset{def.}{\equiv} \neg\exists x\,\Phi$

$\Phi\to\Psi \overset{def.}{\equiv} \Psi\vee\neg\Phi$ $\quad \Phi\leftrightarrow\Psi \overset{def.}{\equiv} (\Phi\to\Psi)\wedge(\Psi\to\Phi)$

$\exists x\in y\ \Phi \overset{def.}{\equiv} \exists x\,(x\in y\wedge\Phi)$ $\quad \forall x\in A\ \Phi \overset{def.}{\equiv} \forall x\,(x\in A\to\Phi)$

$\exists! x\,\Phi(x) \overset{def.}{\equiv} \exists x\,(\Phi(x)\wedge\forall y\,(\Phi(y)\to y=x))$

$\exists! x\in A\ \Phi(x) \overset{def.}{\equiv} \exists! x\,(x\in A\wedge\Phi(x))$

$A\subseteq B \overset{def.}{\equiv} \forall x\,(x\in A\to x\in B)$ $\quad A\subsetneq B \overset{def.}{\equiv} A\subseteq B\wedge A\neq B$

$C=A\cup B \overset{def.}{\equiv} \forall x\ \ x\in C\leftrightarrow(x\in A \vee x\in B)$

$C=A\cap B \overset{def.}{\equiv} \forall x\ \ x\in C\leftrightarrow(x\in A \wedge x\in B)$

Nota: il fatto che possiamo dire $C=A\cup B$ o $C=A\cap B$ non significa né che questi oggetti esistano né che siano unici. Dimostreremo fra poco l'esistenza e unicità di unione e intersezione.

Esercizi: esprimi queste proposizioni mediante formule insiemistiche pure

- gli elementi degli elelementi di A sono elementi di A
- B è l'insieme dei sottoinsiemi di A
- l'unione degli elementi di A è l'intersezione di quelli di B

  (qui assumi che unione e intersezione esistano e siano uniche)
- ogni insieme è disgiunto da uno dei suoi elementi

Le regole di inferenza

La teoria assiomatica degli insiemi si compone di tre parti: il linguaggio formale che abbiamo appena descritto, gli assiomi della teoria che studieremo durante il corso, ed un sistema di regole formali che specificano precisamente quali passaggi sono leciti nelle dimostrazioni. Possiamo immaginare quest'ultima componente come una specie di algebra dei ragionamenti, che permette di verificare i passaggi di una dimostrazione in maniera puramente meccanica, come se fossero semplici manipolazioni algebriche. Noi non vedremo le regole di inferenza, e voglio qui spiegare perché.

1. Sono argomento del corso di logica.
2. In realtà, scrivere le dimostrazioni in maniera formale, le renderebbe lunghissime e praticamente incomprensibili.

3. In pratica, non si sbaglia facendo ragionamenti che non reggono; si sbaglia dicendo cose fumose che non possono essere espresse nel linguaggio della teoria. Per esempio, le parole "e così via" sono assai pericolose.
4. Conoscere le regole — sidatori — non aiuta né a trovare né a capire le dimostrazioni.

Pur senza dare un sistema completo di regole, vediamo qualche manipolazione formale che potrebbe servire.

Tavole di verità Due combinazioni mediante connettivi logici ($\neg, \wedge, \vee, \to, \leftrightarrow$) delle stesse formule — "combinazioni booleane" — alle volte, dicono la stessa cosa. Per esempio, $\neg\Phi \vee \neg\Psi \overset{\text{"equivale a"}}{\equiv} \neg(\Phi \wedge \Psi)$. Per verificare questo fatto basta considerare tutte le possibili combinazioni di valori di verità che possono assumere le formule combinate — nello esempio Φ e Ψ — compilando una "tabella di verità"

Φ	Ψ	$\neg\Phi$	$\neg\Psi$	$\neg\Phi \vee \neg\Psi$	$\Phi \wedge \Psi$	$\neg(\Phi \wedge \Psi)$
V	V	F	F	F	V	F
V	F	F	V	V	F	V
F	V	V	F	V	F	V
F	F	V	V	V	F	V

Queste due colonne coincidono!

Conviene tenere a mente alcune equivalenze elementari

$$\neg\neg\Phi \equiv \Phi \qquad \Phi \wedge (\Psi \vee \Theta) \equiv (\Phi \wedge \Psi) \vee (\Phi \wedge \Theta)$$

$$\Phi \vee (\Psi \wedge \Theta) \equiv (\Phi \vee \Psi) \wedge (\Phi \vee \Theta)$$

$$\neg(\Phi \wedge \Psi) \equiv \neg\Phi \vee \neg\Psi \qquad \Phi \to \neg\Psi \equiv \Psi \to \neg\Phi$$

$$\neg(\Phi \vee \Psi) \equiv \neg\Phi \wedge \neg\Psi \qquad \Phi \to \Psi \equiv \neg\Psi \to \neg\Phi$$

Esercizio Dimostrale.

Per quanto riguarda i quantificatori ricordiamo le regole seguenti, che tuttavia non sono esaustive.

$$\neg\forall x\, \Phi \equiv \exists x \neg\Phi \qquad \neg\forall x \neg\Phi \equiv \exists x\, \Phi$$

$$\neg\exists x\, \Phi \equiv \forall x \neg\Phi \qquad \neg\exists x \neg\Phi \equiv \forall x\, \Phi$$

Esercizio Convinciti della validità delle equivalenze precedenti

Esercizio Dimostra che

$$\neg\forall x \in A\, \Phi \equiv \exists x \in A \neg\Phi \qquad \neg\exists x \in A\, \Phi \equiv \forall x \in A \neg\Phi$$

Esercizio Dimostra che

$$\forall x\,(x \in A \to x \in B) \equiv \neg\exists x\,(x \in A \wedge \neg x \in B)$$

Esercizio Secondo te, la seguente formula è vera?

$$\forall A\,((\exists x\; x \in A) \to \forall B\; \exists x \in A\,(x \in B \to \forall y \in A\; y \in B))$$

Infine vi sono regole per la relazione di uguaglianza, che dicono, in sostanza, che se $x = y$ allora x e y non sono distinguibili, ossia vale $\Phi(x) \leftrightarrow \Phi(y)$ qualunque sia Φ. Per quanto ci riguarda, se $x = y$ allora x e y sono nomi della stessa cosa.

I primi assiomi

① Assioma dell'insieme vuoto

"Esiste un insieme vuoto"

$\exists x \, \forall y \; y \notin x$

Nota: Questo assioma non sarebbe strettamente necessario, in quanto potremmo ottenere un insieme vuoto anche come sottoprodotto, per esempio, dall'assioma dell'infinito che vedremo in seguito. Tuttavia è bello poter partire avendo per le mani almeno un insieme.

② Assioma di estensionalità

"Un insieme è determinato dalla collezione dei suoi elementi"

"Due insiemi coincidono se e solo se hanno i medesimi elementi"

$\forall a \, \forall b \quad a = b \leftrightarrow \forall x \; (x \in a \leftrightarrow x \in b)$

Esercizio: dimostra che la freccia $a = b \to \forall x \dots$, in realtà, segue dal fatto che se $a = b$ allora a e b sono indistinguibili.

Convenzione Le variabili libere (= non quantificate), se non specificato altrimenti, si intendono implicitamente quantificate universalmente all'inizio della formula. Per cui possiamo scrivere l'assioma di estensionalità semplicemente nella forma:

$$a = b \leftrightarrow \forall x \; (x \in a \leftrightarrow x \in b)$$

Prop. C'è un unico insieme vuoto $\exists! x \, \forall y \; y \notin x$

Dim Consideriamo due insiemi vuoti x_1 e x_2, ossia supponiamo $\forall y \; y \notin x_1$ e $\forall y \; y \notin x_2$. Allora

$$\forall y \; y \in x_1 \leftrightarrow y \in x_2$$

perché $y \in x_1$ e $y \in x_2$ sono entrambe necessariamente false. Quindi, per estensionalità, $x_1 = x_2$. ∎

Dim 2 Questo livello di pedanteria non è necessario, ma, per una volta, proviamo a dimostrare in ogni dettaglio la formula $\exists! x \, \forall y \; y \notin x$. Per definizione di $\exists!$, questa equivale a

$$\exists x_1 \left[(\forall y \; y \notin x_1) \wedge \forall x_2 \, (\forall y \; y \notin x_2) \to x_2 = x_1 \right)$$

Per l'assioma del vuoto, $\exists x_1 \, \forall y \; y \notin x_1$: fissiamo questo x_1.

Resta da dimostrare che

$$(\forall y \; y \notin x_1) \wedge \forall x_2 \, (\forall y \; y \notin x_2) \to x_2 = x_1$$

Per costruzione, $\forall y \; y \notin x_1$ è vera, quindi resta

$$\forall x_2 \, (\forall y \; y \notin x_2) \to x_2 = x_1$$

Ora prendiamo un x_2 qualunque: dobbiamo dimostrare

$$(\forall y \; y \notin x_2) \to x_2 = x_1 \qquad (*)$$

Si danno due casi: o $\forall y \; y \notin x_2$ è vera o è falsa. Nel secondo caso l'implicazione $(*)$ è vera per via della tabella di verità. Nel primo abbiamo sia $\forall y \; y \notin x_1$ per costruzione, sia $\forall y \; y \notin x_2$ per ipotesi. Quindi, preso un qualunque y, $y \in x_1$ e $y \in x_2$ sono entrambe false.

La tabella di verità di $\leftrightarrow$ ci dice quindi che vale

$y \in x_1 \leftrightarrow y \in x_2$, e, per l'arbitrarietà di y

$$\forall y \ (y \in x_1 \leftrightarrow y \in x_2)$$

Dall'assioma di estensionalità

$$(\forall y \ (y \in x_1 \leftrightarrow y \in x_2)) \rightarrow x_1 = x_2$$

Abbiamo quindi $x_1 = x_2$, da cui segue $(*)$. ☕

Chiaramente, ho voluto scrivere questa dimostrazione delirante per convincervi che NON è UNA BUONA IDEA.

Notazione L'unicità dell'insieme vuoto ci giustifica ad introdurre una nuova abbreviazione

$$x = \emptyset \overset{\text{def.}}{\equiv} \forall y \ y \notin x \qquad \emptyset \in x \overset{\text{def.}}{\equiv} \exists z \ z = \emptyset \wedge z \in x$$

(3) Assioma* di separazione

"Se A è un insieme, e $\Psi(x)$ una formula insiemistica qualunque, allora $\{x \in A \mid \Psi(x)\}$ è un insieme"

$$\forall A \ \exists B \ \forall x \ x \in B \leftrightarrow (x \in A \wedge \Psi(x))$$

* Nota: tecnicamente l'assioma di separazione è uno schema di assiomi, ossia una regola che, per ogni possibile formula Ψ, ci permette di scrivere un assioma.

Prop Fissati A e $\Psi(x)$, l'insieme $\{x \in A \mid \Psi(x)\}$ è univocamente definito. Ossia

$$\forall A \ \exists! B \ \forall x \ x \in B \leftrightarrow (x \in A \wedge \Psi(x))$$

Dim Come per l'unicità dell'insieme vuoto, supponiamo di avere B_1 e B_2 tali che

$$\forall x \; x \in B_1 \leftrightarrow (x \in A \wedge \Psi(x)) \qquad \forall x \; x \in B_2 \leftrightarrow (x \in A \wedge \Psi(x))$$

Allora $x \in B_1 \leftrightarrow (x \in A \wedge \Psi(x)) \leftrightarrow x \in B_2$, quindi, per estensionalità, $B_1 = B_2$. ∎

Esercizio: Verifica che se $\Psi \rightarrow \Phi$ e $\Phi \rightarrow \Theta$, allora $\Psi \rightarrow \Theta$.

Notazione Vista l'unicità, scriviamo

$$B = \{x \in A \mid \Psi(x)\} \overset{\text{def.}}{\equiv} \forall x \; x \in B \leftrightarrow (x \in A \wedge \Psi(x))$$

Osserviamo che l'assioma di separazione è una forma indebolita del principio di collezione. Rimpiazzando questo con quello, il paradosso di Russell diventa una proposizione

Prop. Non esiste l'insieme di tutti gli insiemi. ~~$\exists$~~ $V \; \forall x \; x \in V$

Dim Supponiamo, per assurdo, che esista questo V. Allora, per separazione con la formula $\Psi(x) \equiv x \notin x$, esiste

$$N = \{x \in V \mid x \notin x\}$$

che ha, per definizione, la proprietà

$$\forall x \; x \in N \leftrightarrow (x \in V \wedge x \notin x)$$

Per ipotesi assurda, $x \in V$ è sempre vera, quindi

$$\forall x \; x \in N \leftrightarrow x \notin x$$

Prendendo, ora, $x = N$, abbiamo $N \in N \leftrightarrow N \notin N$ ↯

Classi e classi proprie

Sebbene, abbiamo detto, gli unici oggetti della teoria degli insiemi sono gli insiemi, usualmente ci si riferisce alla collezione di tutti gli insiemi che soddisfano una certa formula come ad una specie di insieme: una **classe**. Più precisamente, data una formula $\Psi(x)$, se diciamo:

"sia C la classe degli insiemi x tali che $\Psi(x)$"

intendiamo dire che useremo la scrittura $x \in C$ come una semplice abbreviazione per la formula $\Psi(x)$.

Non avrebbe senso scrivere $C \in$ qualcosa, perché il simbolo $\in$ in $x \in C$ non ha senso, se non nel tutt'uno $\in C$. In altri termini, se scriviamo $x \in C$ in luogo di $\Psi(x)$ è solo come ausilio all'intuizione: avremmo potuto decidere di scrivere x , o nient'altro che $\Psi(x)$.

Def V, la classe universale, è la classe di tutti gli insiemi.

$$x \in V \overset{def.}{\equiv} x = x$$

Insomma, scrivere $x \in V$ non dice molto: è una formula sempre vera.

Date due classi C e D, che, ricordiamo, non significa altro che "date due formule ...", definiamo l'abbreviazione

$$C = D \overset{def.}{\equiv} \forall x \; x \in C \leftrightarrow x \in D$$

Ora, dato un qualunque insieme A, possiamo definire la classe $\hat{A}$ degli x tali che $x \in A$. Se $\hat{A} = \hat{B}$, per definizione

$$\forall x \quad x \in A \iff x \in B$$

quindi $A = B$ per estensionalità. Ha quindi senso, con un leggero abuso di notazione, omettere il cappelletto $\hat{}$ e identificare la classe $\hat{A}$ semplicemente con A. In questo senso, abbiamo classi che sono insiemi — formalmente C è un insieme se $C = \hat{A}$ per qualche insieme A — e classi che non sono insiemi. Chiamiamo classe propria una classe che non è un insieme.

Esempio V è una classe propria.

L'intuizione, che sarà più chiara via via che procediamo nel corso, è che le classi proprie sono troppo grandi per essere insiemi.

L'assioma del paio e la coppia di Kuratowski

I primi assiomi ci dicono, a grandi linee, che, entro i limiti di quanto si può fare rinunciando al principio di collezione — che esiste $\{x \mid$ una qualunque proprietà$\}$ —, gli insiemi sono delle specie di collezioni. Sono determinati dai loro elementi, e li si può dividere in collezioni più

piccole in maniera arbitraria. Ci troviamo, però, adesso, nella necessità di procurarci qualche insieme con cui lavorare. I prossimi assiomi serviranno per giustificare le costruzioni con cui, usualmente, si definiscono nuovi insiemi. Per esempio, abbiamo bisogno di costruire certi insiemi di base, tipo l'insieme dei numeri interi o insiemi finiti i cui elementi siano elencati esplicitamente, fare prodotti di insiemi esistenti, considerare le funzioni fra insiemi esistenti, &c.

④ Assioma del paio

"Dati a e b esiste l'insieme $\{a, b\}$"

$$\forall a\, \forall b\, \exists P\, \forall x\ \ x \in P \leftrightarrow (x = a \vee x = b)$$

Prop. Fissati a e b, l'insieme $\{a, b\}$ è univocamente determinato

$$\forall a\, \forall b\, \exists! P\, \forall x\ \ x \in P \leftrightarrow (x = a \vee x = b)$$

Esercizio dimostra la proposizione precedente.

"singoletto di a"

Prop. Dato a, esiste ed è unico $\{a\}$.

$$\forall a\, \exists! S\, \forall x\ \ x \in S \leftrightarrow x = a$$

Dim Ponendo $b = a$ nella proposizione precedente

$$\exists! P\, \forall x\ \ x \in P \leftrightarrow (x = a \vee x = a)$$

Ora $x = a \vee x = a$ equivale semplicemente a $x = a$. ∎

Notazione. $P = \{a, b\} \overset{def.}{\equiv} \forall x \; x \in P \leftrightarrow (x = a \vee x = b)$

$S = \{a\} \overset{def.}{\equiv} \forall x \; x \in S \leftrightarrow x = a$

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

Dim Usiamo il fatto che la $\vee$ è commutativa

$$x \in \{a, b\} \leftrightarrow (x = a \vee x = b) \leftrightarrow (x = b \vee x = a) \leftrightarrow x \in \{b, a\}$$

Quindi, per estensionalità, $\{a, b\} = \{b, a\}$. ∎

Il paio $\{a, b\}$ è, quindi, una coppia non ordinata. È possibile codificare le coppie ordinate con questo trucco

Def (coppia di Kuratowski)

$(a, b) \overset{def.}{\equiv} \{\{a\}, \{a, b\}\}$

Prop La coppia di Kuratowski (a, b) rappresenta la coppia ordinata di a e b, ossia $(a, b) = (a', b') \leftrightarrow (a = a' \wedge b = b')$

Dim Dato $c = (a, b)$, vogliamo determinare univocamente a e b. Intanto, a è determinato da

$$x = a \leftrightarrow \forall y \in c \; x \in y$$

La freccia $\rightarrow$ è infatti immediata, mentre $\leftarrow$ segue da $\{a\} \in c$, per cui $\forall y \in c \; x \in y \Rightarrow x \in \{a\} \Rightarrow x = a$.

Veniamo ora a b. Studiamo prima il caso in cui $\exists! x \; x \in c$

$\exists! x \; x \in c \Leftrightarrow \{a\} = \{a, b\}$ in quanto $\{a\} \in c$ e $\{a, b\} \in c$

$\{a\} = \{a, b\} \Leftrightarrow b = a$ per estensionalità

In questo caso, b è quindi determinato.

Altrimenti, $x = \{a,b\} \leftrightarrow (x \in c \wedge x \neq \{a\})$, $\{a,b\}$ è quindi univocamente determinato da c, e $x = b \leftrightarrow (x \in \{a,b\} \wedge x \neq a)$. ∎

Def
$$(a,b,c) \overset{\text{def.}}{\equiv} ((a,b),c)$$
$$(a,b,c,d) \overset{\text{def.}}{\equiv} (((a,b),c),d)$$
$$(a_1, a_2, \dots, a_n) \overset{\text{def.}}{\equiv} ((a_1, \dots, a_{n-1}), a_n)$$

Nota Quest'ultima definizione è, in realtà, uno schema di definizioni: una per ogni n. Per ora, NON siamo in grado di scrivere, per esempio, una formula insiemistica che dica "Esiste un n ed una n-tupla $(a_1 \dots a_n)$ tale che ...". Però, per ogni n dato, diciamo 92, possiamo scrivere esplicitamente una formula che dice $x = (a_1, a_2, a_3, \dots, a_{92})$.

Prop
$$(a,b,c) = (a',b',c') \leftrightarrow a = a' \wedge b = b' \wedge c = c'$$
$$(a_1 \dots a_n) = (a_1' \dots a_n') \leftrightarrow a_1 = a_1' \wedge \dots \wedge a_n = a_n'$$

Dim Esercizio: dimostra la prima e convinciti che, dato un qualunque n esplicito, potresti dimostrare la seconda.

L'assioma dell'unione

⑤ Assioma dell'unione

"Dato un insieme A esiste un insieme B i cui elementi sono gli elementi degli elementi di A"

"Dato un insieme A esiste l'unione degli elementi di A"

$$\forall A\ \exists B\ \forall x\ x \in B \leftrightarrow \exists y \in A\ x \in y$$

Prop. $\forall A\ \exists! B\ \forall x\ x \in B \leftrightarrow \exists y \in A\ x \in y$

Dim Esercizio.

"unione di A"

Def. $B = \bigcup A \overset{\text{def.}}{\equiv} \forall x\ x \in B \leftrightarrow \exists y \in A\ x \in y$

Esercizio Dimostra che l'assioma dell'unione segue da

$$\forall A\ \exists B\ \forall y \in A\ \forall x \in y\ x \in B$$

Combinando l'assioma dell'unione e il paio possiamo definire $a \cup b$

Def. $a \cup b \overset{\text{def.}}{\equiv} \bigcup \{a, b\}$

Prop. $x \in a \cup b \leftrightarrow (x \in a \vee x \in b)$

Dim Dire che x è un elemento di $a \cup b$ significa dire che x è un elemento di un elemento di $\{a, b\}$, ossia che x è un elemento di uno fra a e b. ∎

Ora definiremo le intersezioni: riesci a vedere perché, a differenza delle unioni, non ci servirà un nuovo assioma?

quindi, in particolare, C può essere un insieme

Def Sia C una classe non vuota. L'insieme B è l'intersezione di C se $B = \bigcap C \overset{\text{def.}}{\equiv} \forall x\ x \in B \leftrightarrow \forall y \in C\ x \in y$

Prop. Data una classe non vuota C, l'intersezione $\bigcap C$ esiste ed è unica. In particolare, nel caso dell'intersezione di un insieme vale:

$$\forall A \left(A \neq \emptyset \to \exists! B \ \forall x \left(x \in B \leftrightarrow \forall y \in A \ x \in y \right) \right)$$

Nota: L'ipotesi $C \neq \emptyset$ è necessaria perché si avrebbe che $\bigcap \emptyset$ è la classe universale V, che non è un insieme.

Dim L'unicità segue per estensionalità al solito modo. Veniamo all'esistenza. Dal momento che C non è vuota, possiamo prendere uno $z \in C$. Ora consideriamo

$$B = \{ x \in z \mid \forall y \in C \ x \in y \}$$

Chiaramente $x \in B \to \forall y \in C \ x \in y$. D'altro canto, $\forall y \in C \ x \in y$ implica, in particolare, $x \in z$, quindi $x \in B$. Abbiamo così provato che $x \in B \leftrightarrow \forall y \in C \ x \in y$, ossia $B = \bigcap C$. ∎

Def. $a \cap b \overset{def.}{=} \bigcap \{a, b\}$

$a \setminus b \overset{def.}{=} \{ x \in a \mid x \notin b \}$

Prop. $x \in a \cap b \leftrightarrow (x \in a \wedge x \in b)$

$x \in a \setminus b \leftrightarrow (x \in a \wedge x \notin b)$

Dim Esercizio (La seconda è semplicemente la definizione)

Prop. Alcune proprietà delle operazioni $\cup$ $\cap$ $\setminus$

commutatività:

$$a \cup b = b \cup a$$

$$a \cap b = b \cap a$$

associatività:

$$a \cup (b \cup c) = (a \cup b) \cup c \overset{\text{def.}}{=} a \cup b \cup c$$

$$a \cap (b \cap c) = (a \cap b) \cap c \overset{\text{def.}}{=} a \cap b \cap c$$

distributività:

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

leggi di de Morgan:

$$a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c)$$

$$a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)$$

Dim Tutte queste proprietà si deducono immediatamente dalle corrispondenti proprietà dei connettivi logici, le quali, a loro volta, si vedono tramite le tabelle di verità. Per esempio, dimostriamo la prima delle leggi di de Morgan.

$$\begin{aligned}
x \in a \setminus (b \cup c) &\iff x \in a \wedge x \notin (b \cup c) \\
&\iff x \in a \wedge \neg (x \in b \vee x \in c) \\
&\iff x \in a \wedge x \notin b \wedge x \notin c \qquad \text{ripetiamo ovvero?} \\
&\iff x \in a \wedge x \notin b \wedge x \in a \wedge x \notin c \\
&\iff x \in a \setminus b \wedge x \in a \setminus c \\
&\iff x \in (a \setminus b) \cap (a \setminus c)
\end{aligned}$$

∎

Ora possiamo costruire insiemi finiti elencandone gli elementi, come si fa di solito, con la notazione $\{\dots\}$.

Def.

$$\{a, b, c\} \overset{\text{def.}}{=} \{a\} \cup \{b\} \cup \{c\}$$

$$\{a, b, c, d\} \overset{\text{def.}}{=} \{a\} \cup \{b\} \cup \{c\} \cup \{d\}$$

$$\{a_1, \dots, a_n\} \overset{\text{def.}}{=} \{a_1\} \cup \dots \cup \{a_n\}$$

Prop $x \in \{a, b, c\} \leftrightarrow (x = a \vee x = b \vee x = c)$

$x \in \{a_1, \dots, a_n\} \leftrightarrow (x = a_1 \vee \dots \vee x = a_n)$

Dim Esercizio

Assioma delle parti, prodotti cartesiani, &c.

Abbiamo definito la coppia (x,y), però, per esempio, ancora nulla ci assicura che dati A e B esista

$$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}$$

Le funzioni $A \to B$ saranno, poi, sottoinsiemi di $A \times B$, e vorremo parlare dell'insieme ^AB delle funzioni $A \to B$.
Per tutto questo ci manca un solo ingrediente: l'insieme delle parti.

⑥ Assioma delle parti

"Dato un insieme A esiste l'insieme $\mathcal{P}(A)$ i cui elementi sono i sottoinsiemi di A"

$$\forall A \, \exists B \, \forall x \; x \in B \leftrightarrow x \subseteq A$$

Prop: $\forall A \, \exists! B \, \forall x \; x \in B \leftrightarrow x \subseteq A$

Dim A questo punto, non vale neanche più la pena di fare l'esercizio.

Def ("insieme delle parti" o "insieme potenza" di A)

$$B = \mathcal{P}(A) \overset{\text{def.}}{\equiv} \forall x \; x \in B \leftrightarrow x \subseteq A$$

Prop Dati A e B esiste un unico insieme $A \times B$ tale che

$$\forall z \quad z \in A \times B \iff \exists x \in A \; \exists y \in B \; z = (x,y)$$

Ossia, informalmente, $A \times B = \{ (x,y) \mid x \in A \wedge y \in B \}$

Dim L'unicità è conseguenza immediata dell'assioma di estensionalità. Per l'esistenza, definiamo

$$A \times B \overset{def.}{=} \{ z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists x \in A \; \exists y \in B \; z = (x,y) \}$$

Dobbiamo dimostrare che ogni coppia (x,y) con $x \in A$ e $y \in B$ appartiene a questo insieme. Basta dimostrare che tutte queste coppie appartengono a $\mathcal{P}(\mathcal{P}(A \cup B))$.

$$a \in A \wedge b \in B \Rightarrow \{a\}, \{a,b\} \overset{*}{\subseteq} A \cup B$$

$$\overset{*}{\text{Notare}} \text{ poniamo} \Rightarrow \{a\}, \{a,b\} \in \mathcal{P}(A \cup B)$$

$$a, b, \ldots \in z \overset{def}{=} a \in z \wedge b \in z \wedge \ldots \Rightarrow (a,b) = \{\{a\}, \{a,b\}\} \subseteq \mathcal{P}(A \cup B)$$

$$a, b, \ldots \in z \overset{def.}{=} a \subseteq z \wedge b \subseteq z \wedge \ldots \Rightarrow (a,b) \in \mathcal{P}(\mathcal{P}(A \cup B))$$

■

Notare avremmo potuto costruire $A \times B$ usando, anziché l'assioma delle parti, l'assioma del rimpiazzamento, che vedremo più avanti.

Ora rivedremo alcuni concetti ben noti dai primi corsi del primo anno (o dalla scuola superiore?). Lo facciamo molto rapidamente, essenzialmente completezza, e per fissare le notazioni.

Def Una *relazione binaria* tra A e B è un sottoinsieme di $A \times B$

Notazione Data una relazione $R \subseteq A \times B$, $a \, R \, b \overset{def}{=} (a,b) \in R$.

Per esempio scriviamo $a < b$ per $(a,b) \in <$.

Def. Una relazione $\sim \subseteq A \times A$ è una *relazione di equivalenza* se è

riflessiva: $\forall x \in A \quad x \sim x$

simmetrica: $\forall x, y \overset{*}{\in} A \quad x \sim y \leftrightarrow y \sim x$ *Nota: $\forall x_1 \dots x_n \overset{\text{def.}}{=} \forall x_1 \dots \forall x_n$

transitiva: $\forall x, y, z \in A \quad (x \sim y \wedge y \sim z) \rightarrow x \sim z$ e lo stesso con $\exists$ e coi quantificatori limitati

Def. $\leq \subseteq A \times A$ è una *relazione d'ordine (largo)* se è

riflessiva: $\forall x \in A \quad x \leq x$

antisimmetrica: $\forall x, y \in A \quad (x \leq y \wedge y \leq x) \rightarrow x = y$

transitiva: $\forall x, y, z \in A \quad (x \leq y \wedge y \leq z) \rightarrow x \leq z$

Def. $< \subseteq A \times A$ è una *relazione d'ordine stretto* se è

irriflessiva: $\forall x \in A \quad \neg(x < x)$

transitiva: $\forall x, y, z \in A \quad (x < y \wedge y < z) \rightarrow x < z$

Esercizio Dimostra che una relazione di ordine stretto $<$ su A è automaticamente asimmetrica: $\forall x, y \in A \quad x < y \rightarrow \neg(y < x)$

Prop: Data una relazione di ordine stretto $<$ su A, la relazione

$$\leq \overset{*}{=} \{(x, y) \in A \times A \mid x < y \vee x = y\}$$

è una relazione di ordine largo. Viceversa, se $\leq$ è una relazione di ordine largo, la relazione seguente è di ordine stretto.

$$< \overset{*}{=} \{(x, y) \in A \times A \mid x \leq y \wedge x \neq y\}$$

Inoltre, in questo modo, le relazioni di ordine stretto e di ordine largo sono poste in corrispondenza uno-a-uno.

*Formalmente: $\{z \in A \times A \mid \exists x, y \in A \; z = (x, y) \wedge \dots\}$

Dim Definiamo la diagonale

$$\Delta_A \overset{\text{def.}}{=} \{(x,y) \in A \times A \mid x = y\}$$

Allora è facile verificare che, se $<$ è una relazione di ordine stretto, allora $< \cap \Delta_A = \emptyset$ e $< \cup \Delta_A$ è la relazione di ordine largo corrispondente. Vice versa, se $\leq$ è una relazione di ordine largo, allora $\Delta_A \subseteq \leq$ e $\leq \setminus \Delta_A$ è la relazione di ordine stretto corrispondente. ∎

Notazione Fissata una relazione di ordine largo $\leq$ su A, ci sentiremo liberi di usare la corrispondente relazione di ordine stretto $<$ sfidando che la scelta del simbolo sia indizio sufficiente dell'operazione. Inoltre scriveremo $x > y$ per $y < x$ e $x \geq y$ per $y \leq x$.

Def Una relazione di ordine totale su A è una relazione di ordine $\leq$ tale che $\forall x, y \in A \quad x \leq y \vee x = y \vee y \leq x$

Esercizio Formula la definizione precedente per ordini stretti.

Def Data una relazione $R \subseteq A \times B$, $A' \subseteq A$ e $B' \subseteq B$

$$R|_{A' \times B'} \overset{\text{def.}}{=} R \cap (A' \times B') \quad \text{"restrizione di } R \text{ a } A' \times B'\text{"}$$

Esercizio Data R relazione di equivalenza/ordine su A e $A' \subseteq A$ dimostra che $R|_{A' \times A'}$ è una relazione di equivalenza/ordine su A'.

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

$\mathrm{Dom}(R) \overset{\text{def}}{=} \{x \in A \mid \exists y \in B \ \ x R y\}$ dominio di R

$\mathrm{Im}(R) \overset{\text{def}}{=} \{y \in B \mid \exists x \in A \ \ x R y\}$ immagine di R

Def. Chiamiamo funzione $f : A \to B$ una relazione $f \subseteq A \times B$ tale che $\forall x \in A \ \exists! y \in B \ (x,y) \in f$.

Intuitivamente f è l'insieme delle coppie $(x, f(x))$ per $x \in A$.

Notazione Data una funzione f, scriviamo

$y = f(x) \overset{\text{def}}{=} (x,y) \in f$.

Dato $S \subseteq \mathrm{Dom}(f)$, scriviamo

$f[S] \overset{\text{def}}{=} \{y \in \mathrm{Im}(f) \mid \exists x \in S \ y = f(x)\} = \{f(x) \mid x \in S\}$ (informalmente)

Def Una funzione $f : A \to B$ è

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

suriettiva se $B = \mathrm{Im}(f)$ ossia $\forall y \in B \ \exists x \in A \ f(x) = y$

bigettiva se è sia iniettiva sia suriettiva.

Def Data f iniettiva

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

Oss Data f iniettiva, f^{-1} è una funzione: $\mathrm{Im}(f) \to \mathrm{Dom}(f)$ iniettiva. In particolare se f è bigettiva: $A \to B$, allora f^{-1} è bigettiva: $B \to A$.

Def Data $f : A \to B$ e $A' \subseteq A$

$$f|_{A'} \stackrel{def}{=} \{(x,y) \in A' \times B \mid f(x) = y\}$$

$f|_{A'}$ "f ristretta ad A'" è una funzione $A' \to B$.

Def Date $g : A \to B$ e $f : B \to C$

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

↳ o, più formalmente $\exists y (y = g(x) \wedge z = f(y))$

$f \circ g$ "f composta con g" è una funzione $A \to C$.

Notazione Indichiamo con Id_A la funzione identità su A

$$Id_A \stackrel{def}{=} \{(x,y) \in A \times A \mid x = y\} \quad (= \Delta_A)$$

Oss. Data $f : A \to B$ biiettiva e $g : B \to A$, sono equivalenti

$$g = f^{-1} \qquad g \circ f = Id_A \qquad f \circ g = Id_B$$

Esercizio Date $g : A \to B$ e $f : B \to C$, sotto quali condizioni $f \circ g$ è iniettiva, suriettiva, biiettiva?

Esercizio Data una relazione di equivalenza $\sim$ su A, dimostra che esiste un insieme $A/\sim$ ed una funzione suriettiva $i_\sim$ da A a $A/\sim$ tale che $\forall x,y \in A \quad x \sim y \leftrightarrow i_\sim(x) = i_\sim(y)$

Esercizio: Data una relazione di equivalenza $\sim$ su A e $f : A \to B$, affinché esista $\tilde{f} : A/\sim \to B$ tale che $f = \tilde{f} \circ i_\sim$, è necessario e sufficiente che $\forall x,y \in A \quad x \sim y \Rightarrow f(x) = f(y)$.

L'assioma dell'infinito e i numeri naturali

Il nostro prossimo obiettivo è definire i numeri naturali. I soli oggetti della teoria degli insiemi sono gli insiemi, per cui va da sé che i numeri saranno determinati insiemi. Il nostro scopo non è quindi tanto definire, quanto codificare i numeri naturali per mezzo di insiemi opportuni. La scelta della codifica non è obbligata: per esempio potremmo decidere che

n parentesi

$$\text{"codifica buffa di } n\text{"} = \{\{\{\dots\emptyset\dots\}\}\}$$

Sceglieremo, invece, quest'altra codifica

$$n = \{0, 1, \dots, n-1\} = \{x \in \mathbb{N} \mid x < n\}$$

$$0 = \emptyset \qquad 1 = \{0\} \qquad 2 = \{0, 1\} \qquad 3 = \{0, 1, 2\} \qquad \&c.$$

che presenta alcuni vantaggi: per esempio n è rappresentato da un insieme di n elementi; e dire $m < n$ equivale semplicemente a dire $m \in n$.

L'ostacolo è ora parlare di questi oggetti in maniera precisa nel linguaggio della teoria degli insiemi. A dire il vero, potremmo già scrivere una formula $\Phi(n)$ che dice "n è un numero naturale" si tratta di un esercizio difficile, che sarà reso più facile da idee che vedremo più avanti. Noi non scriviamo questa formula, ma, anche a farlo, non potremmo comunque dimostrare

che esiste un insieme i cui elementi sono i numeri naturali, questo perché gli assiomi visti finora non permettono di uscire dalla classe degli insiemi finiti (degli insiemi "evidentemente finiti", ad essere precisi: definiremo questo concetto a tempo debito).

Servirà un nuovo assioma. L'idea da sfruttare è che, siccome $n = \{0, \dots, n-1\}$, per ottenere il successore di n, ossia $n+1 = \{0, \dots, n-1, n\}$ dobbiamo aggiungere a n l'elemento n stesso: $n+1 = n \cup \{n\}$. Avendo una formula per denotare il successore, possiamo postulare l'esistenza di un insieme chiuso per successori, e questo ci darà $\mathbb{N}$.

Def. (successore) $\quad s(x) \overset{\text{def.}}{\equiv} x \cup \{x\}$

Def. (insiemi induttivi)
Diciamo che un insieme A è induttivo se contiene $\emptyset$ ed è chiuso per successori, ossia

$$A \text{ è induttivo} \overset{\text{def.}}{\iff} \emptyset \in A \wedge \forall x \in A \; s(x) \in A$$

⑦ Assioma dell'infinito

"Esiste un insieme induttivo"

$$\exists A \, (\emptyset \in A \wedge \forall x \in A \; s(x) \in A)$$

Finalmente definiamo l'insieme dei numeri naturali — che, per

qualche buffa ragione, chiamiamo w (omega) — come l'intersezione della classe, non vuota per l'assioma dell'infinito, di tutti gli insiemi induttivi.

Def. L'insieme w è l'intersezione di tutti gli insiemi induttivi, ossia w è l'unico insieme tale che

$$\forall x \left(x \in w \longleftrightarrow \left(\forall A \text{ "}A \text{ è induttivo"} \rightarrow x \in A \right) \right)$$

Adesso che abbiamo w, possiamo facilmente dimostrare che ogni dato numero naturale vi appartiene

Def $0 \overset{\text{def}}{\equiv} \emptyset$ $\quad 1 \overset{\text{def.}}{\equiv} s(0)$ $\quad 2 \overset{\text{def}}{\equiv} s(1)$ $\quad 3 \overset{\text{def.}}{\equiv} s(2)$ &c.

Esercizio Dimostra che $0, 1, 2, 3 \in w$.

Un esercizio un po' più difficile è esibire insiemi che non appartengano a w

Esercizio Dimostra che $\{\{\emptyset\}\} \notin w$

Idea Esibisci un insieme induttivo che non contiene $\{\{\emptyset\}\}$.

Per convincerci, però, che w è, a buon diritto, l'insieme dei numeri naturali, serve qualcosa di più. Classicamente, i numeri naturali si definiscono per mezzo degli assiomi di Peano. Questi assiomi, che caratterizzano a meno di isomorfismi l'insieme $\mathbb{N}$ dotato della funzione

successore, per noi diventano dei teoremi che dimostreremo a proposito dell'insieme ω. In questo senso, quindi, ω codifica legittimamente i numeri naturali.

Def (assiomi di Peano — al secondo ordine — Qualunque cosa questo significhi...)
Dato un insieme $\mathbb{N}$, un elemento $0 \in \mathbb{N}$, e una funzione $succ : \mathbb{N} \to \mathbb{N}$, diciamo che $(\mathbb{N}, 0, succ)$ soddisfa gli assiomi di Peano se

A. il successore è iniettivo

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

B. lo zero non è un successore

~~$\exists$~~ $n \in \mathbb{N} \quad succ(n) = 0$

C. principio di induzione

Data una qualunque formula insiemistica (proprietà) $\Phi(n)$

$\left(\varphi(0) \wedge \forall n \in \mathbb{N} \ \Phi(n) \to \Phi(succ(n)) \right) \to \forall n \in \mathbb{N} \ \Phi(n)$

Nota:

Qui ci deve essere un typo...

Axiomata.

1. $1 \in \mathrm{N}$.
2. $a \in \mathrm{N} . \supset . a = a$.
3. $a, b, c \in \mathrm{N} . \supset : a = b . = . b = a$.
4. $\cap$ $a, b \in \mathrm{N} . \supset \therefore a = b . b = c : \supset . a = c$.
5. $a = b . b \in \mathrm{N} : \supset . a \in \mathrm{N}$.
6. $a \in \mathrm{N} . \supset . a + 1 \in \mathrm{N}$.
7. $a, b \in \mathrm{N} . \supset : a = b . = . a + 1 = b + 1$.
8. $x \in \mathrm{N} . \supset . a + 1 - = 1$.
9. $k \in \mathrm{K} \therefore 1 \in k \therefore x \in \mathrm{N} . x \in k : \supset_x . x + 1 \in k :: \supset . \mathrm{N} \supset k$.

Apparivano così in "Arithmetices Principia", nel 1889.

Teo La funzione $succ : w \to w$, $succ(n) = s(n)$, è ben definita e $(w, \emptyset, succ)$ soddisfa gli assiomi di Peano.

Dim Per controllare che succ sia ben definita, occorre assicurarsi che se $n \in w$ allora $s(n) \in w$. Fissiamo $n \in w$ e consideriamo un qualunque insieme induttivo A. Siccome A è induttivo, $w \in A$, quindi $n \in A$, e, di conseguenza $s(n) \in A$. Per l'arbitrarietà di A, allora, $s(n)$ appartiene a ogni insieme induttivo. Quindi $s(n) \in w$.

Iniziamo ora col dimostrare B e C, poi passeremo ad A.

B. Supponiamo, per assurdo, $s(n) = \emptyset$. Abbiamo allora

$$n \in n \cup \{n\} = s(n) = \emptyset$$

contro la definizione di $\emptyset$.

C. Dimostriamo che l'insieme $A = \{n \in w \mid \Phi(n)\}$ è induttivo, da cui $w = A$, quindi $\forall n \in w \; \Phi(n)$.

1. Per ipotesi abbiamo $\Phi(\emptyset)$, quindi $\emptyset \in A$.
2. $n \in A \Rightarrow \Phi(n) \Rightarrow \Phi(s(n)) \Rightarrow s(n) \in A$.
   ($\Phi(n)$: per ipotesi; $\Phi(s(n))$: perché $n \in w \to s(n) \in w$)

A. Lemma 1: $\forall n \in w \; \bigcup n \subseteq n$

Dim. Per induzione (C.) con $\Phi(n) \overset{\text{def.}}{\equiv} \bigcup n \subseteq n$

$\Phi(\emptyset)$: $\bigcup \emptyset = \emptyset \subseteq \emptyset$

$\Phi(n) \to \Phi(s(n))$: $\bigcup(s(n)) = \bigcup(n \cup \{n\}) \overset{*}{=} (\bigcup n) \cup n \overset{\blacktriangle}{=} n \subseteq s(n)$

$$
\begin{aligned}
* \quad x \in \bigcup(n \cup \{n\}) &\iff \exists y \;\; x \in y \;\wedge\; y \in n \cup \{n\} \\
&\iff \exists y \;\; x \in y \;\wedge\; (y \in n \vee y = n) \\
&\iff \exists y \;\; (x \in y \wedge y \in n) \vee (x \in y \wedge y = n) \\
&\iff \exists y \;\; (x \in y \wedge y \in n) \vee \exists y \;\; (x \in y \wedge y = n) \\
&\iff \quad x \in \bigcup n \qquad \vee \qquad x \in n \\
&\iff \quad x \in (\bigcup n) \cup n
\end{aligned}
$$

▲ Per ipotesi induttiva $\bigcup n \subseteq n$, quindi $(\bigcup n) \cup n \subseteq n \cup n = n$.

□ Lemma 1

Lemma 2: $\forall\, n \in \omega \quad \bigcup s(n) = n$

Dim. Come nel passo induttivo della dimostrazione precedente

$$\bigcup(s(n)) = \bigcup(n \cup \{n\}) = (\bigcup n) \cup n \overset{\blacktriangle}{=} n$$

Dove in ▲ abbiamo $\bigcup n \subseteq n$, non per ipotesi induttiva, ma per il lemma 1.

□ Lemma 2.

Finalmente $s(m) = s(n) \Rightarrow m = \bigcup s(m) = \bigcup s(n) = n$. ■

Conviene, adesso, sviluppare un po' di tecnologia per manipolare i numeri interi. Dopo, dimostreremo altresì che gli assiomi di Peano hanno un unico modello $(\mathbb{N}, 0, \mathrm{succ})$ a meno di isomorfismi.

Def. Dati $m, n \in \omega$, scriviamo $m < n \overset{\text{def.}}{\equiv} m \in n$

Prop. La relazione $<$ è un ordine totale su ω.

Per dimostrare questa proposizione, sono comodi alcuni lemmi.

Osservazione

1. $m \in n \to m \in s(n)$ Infatti $n \subseteq n \cup \{n\} = s(n)$
2. $m \in s(n) \to (m \in n \vee m = n)$ Infatti $m \in n \cup \{n\} = s(n)$

$\iff m \in n \vee m \in \{n\}$

$\iff m \in n \vee m = n$

Lemma $\forall a, b \in \omega \quad a \in b \to (s(a) \in b \vee s(a) = b)$

Dim Induzione su b

- caso $b = 0$: $a \in \emptyset \to \dots$ vera a vuoto, perché $a \in \emptyset$ è falsa.
- caso $b = s(n)$: l'ipotesi induttiva è $a \in n \to (s(a) \in n \vee s(a) = n)$

Dobbiamo dimostrare $a \in s(n) \to (s(a) \in s(n) \vee s(a) = s(n))$

$a \in s(n) \Rightarrow a \in n \cup \{n\} \Rightarrow a \in n \vee a = n$

Due casi: $a \in n \Rightarrow s(a) \in n \vee s(a) = n \Rightarrow s(a) \in s(n)$

$a = n \Rightarrow s(a) = s(n)$ ∎

Dim (della proposizione)

transitività: $a \in b \wedge b \in c \to a \in c$ Induzione su c

- caso $c = 0$: la premessa $b \in c$ è falsa, quindi l'implicazione è vera a vuoto.
- caso $c = s(n)$: assumiamo l'ipotesi induttiva $a \in b \wedge b \in n \to a \in n$

Sapendo $a \in b \wedge b \in s(n)$ vogliamo dedurre $a \in s(n)$

Due casi: $b = n \Rightarrow a \in b = n \Rightarrow a \in s(n)$ (oss 2., oss 1.)

$b \in n \Rightarrow a \in b \in n \Rightarrow a \in n$ (oss 1.)

irriflessività: $\neg\, a \in a$

Per induzione

- caso $a = 0$: $\neg\, \emptyset \in \emptyset$ per definizione di $\emptyset$
- caso $a = s(n)$: assumiamo l'ipotesi induttiva $\neg\, n \in n$

  Per assurdo supponiamo $s(n) \in s(n)$

  Due casi: oss. 2
  - $s(n) = n \Rightarrow n \in n$ ↯
  - $s(n) \in n \Rightarrow n \in s(n) \in n \Rightarrow n \in n$ ↯ (transitiv.)

totalità: $a \in b \vee a = b \vee b \in a$

Per induzione su a

- caso $a = 0$: $\emptyset \in b \vee \emptyset = b \vee b \in \emptyset$ (impossibile)

  Induzione secondaria su b
  - caso $b = 0$: $0 \in \emptyset \vee \emptyset = \emptyset$ ✓
  - caso $b = s(m)$: ipotesi induttiva $\emptyset \in m \vee \emptyset = m$

    Due casi: oss. 1
    - $\emptyset \in m \Rightarrow \emptyset \in s(m) \Rightarrow \emptyset \in b$
    - $\emptyset = m \Rightarrow \emptyset \in \{\emptyset\} = s(m)$
- caso $a = s(n)$: L'ipotesi induttiva è $n \in b \vee n = b \vee b \in n$

  Tre casi:
  - $n \in b \Rightarrow$ lemma $s(n) \in b \vee s(n) = b$ ($a \in b$; $a = b$)
  - $n = b$, $b \in n$ $\Rightarrow$ oss. 1 $b \in s(n) \Rightarrow b \in a$

∎

Con: "Un numero naturale è l'insieme dei numeri naturali minori di lui" $\forall m \in \omega \quad m = \{n \in \omega \mid n < m\}$

Dim Vogliamo dire che $m = \{n \in w \mid n \in m\}$, ossia che $m \subseteq w$.

Per induzione. $\emptyset \subseteq w$. $m \in w \Rightarrow S(m) = m \cup \{m\} \in m$

$\subseteq w$ in quanto $m \in w$ ∎

Cor $\forall m, n \in w \quad m \leq n \longleftrightarrow m \subseteq n$

Dim Siccome w è totalmente ordinato, si danno due casi:

$m \leq n \Rightarrow \forall x \in w \; x < m \to x < n \Rightarrow \forall x \in w \; x \in m \to x \in n \Rightarrow m \subseteq n$

$n < m \Rightarrow n \in m$ tuttavia $n \notin n$ quindi $m \not\subseteq n$ ∎

Seconda forma dell'induzione, principio del minimo

Teo (principio di induzione — forma forte)

Data una formula insiemistica $\Phi(x)$, vale

$$\left(\forall n \in w \; \left(\forall x < n \; \Phi(x)\right) \to \Phi(n)\right) \longrightarrow \forall n \in w \; \Phi(n)$$

"Se, assumendo $\Phi(x)$ per tutti gli $x < n$, ho $\Phi(n)$. Allora $\Phi(n)$ è vera per tutti i numeri n"

Oss Chiamiamo questa forma "forte" perché permette di assumere un'ipotesi induttiva più forte dell'induzione di Peano. In quella, infatti, si deve dedurre $\Phi(n)$ a partire da Φ del numero precedente. Qui, invece, possiamo far conto di sapere Φ, non solo per il precedente, ma per tutti i numeri minori di n.

Dim Assumiamo l'antecedente

$$\forall n \in w \; \left(\forall x < n \; \Phi(x)\right) \to \Phi(n) \qquad (*)$$

Inizialmente, dimostriamo per induzione $\forall m \in \omega\ \Psi(m)$ dove

$$\Psi(m) \overset{\text{def.}}{\equiv} \forall x < m\ \Phi(x)$$

- caso $m = 0$. $\forall x < \emptyset\ \Phi(x)$ è vera a vuoto.
- caso $m = S(n)$. Per ipotesi induttiva $\forall x < n\ \Phi(x)$.

  Se $x < m = S(n)$, sappiamo già che $x < n \vee x = n$.

  - Nel caso $x < n$, abbiamo $\Phi(x)$ per ipotesi induttiva.
  - Nel caso $x = n$, l'ipotesi induttiva, combinata con $(*)$ ci dà $\Phi(n)$ ossia $\Phi(x)$.

  Per l'arbitrarietà di $x < m$ abbiamo dimostrato $\forall x < m\ \Phi(x)$

Ora sappiamo $\forall m \in \omega\ \forall x < m\ \Phi(x)$. Dato un $n \in \omega$ qualunque, considerando $m = n+1$ e $x = n$ otteniamo $\Phi(n)$. ∎

Teo (Principio del minimo)
Sia $A \subseteq \omega$. Se $A \neq \emptyset$ allora esiste $n \in A$ tale che $\forall x \in A\ n \leq x$.
"Ogni sottoinsieme non vuoto di ω ha un minimo elemento"

Dim (idea) Si dimostra per induzione forte che, se $n \in A$, allora A ha un minimo. Poi, siccome A non è vuoto, deve esserci qualche $n \in A$, quindi A ha minimo. L'induzione funziona così. Se $n \in A$, si danno due casi. O esiste $x < n$ con $x \in A$, e allora A ha minimo per ipotesi induttiva, oppure $\forall x < n\ x \notin A$, ma allora n è il minimo di A.

Dim Considerando la contronominale, dobbiamo dimostrare che se A non ha un minimo elemento, allora A è vuoto. Assumiamo quindi $\forall n \in A\ \exists x \in A\ x < n$, dobbiamo dimostrare che $\forall n \in \omega\ n \notin A$. Procediamo per induzione, forma forte. Ci serve dire che $(\forall x < n\ \ x \notin A) \to n \notin A$. Questa, però, è immediata, perché equivale a

$$(\neg \exists x < n\ \ x \in A) \to n \notin A$$
$$\Leftrightarrow\ (\neg \exists x\ \ x < n \wedge x \in A) \to n \notin A$$
$$\Leftrightarrow\ (\neg \exists x \in A\ \ x < n) \to n \notin A$$
$$\Leftrightarrow\ n \in A \to \exists x \in A\ x < n$$

che è appunto l'assunto. ∎

Def. Un insieme totalmente ordinato $(S, <)$ si dice **bene ordinato** se ogni suo sottoinsieme non vuoto ha un minimo.

$$\forall A \subseteq S\ \ A \neq \emptyset \to \exists m \in A\ \forall x \in A\ m \leq x$$

La nozione di buon ordine è stata introdotta da Cantor agli albori della teoria degli insiemi, e giocherà un ruolo centrale in questo corso.

Esempio $(\omega, <)$ è un insieme bene ordinato.

Esercizio Dimostra che $X = S(S(S(\omega)))$ è bene ordinato dalla relazione $a < b \overset{def.}{\equiv} a \in b$.

Ricorsione numerabile

La ricorsione è il procedimento per cui si costruisce una funzione $f: \omega \to$ quello che sia definendo $f(s(n))$ a partire da $f(n)$, o, più in generale da $f(\emptyset) \dots f(n)$. Questo è un procedimento fondamentale: potremmo dire che è il modo di precisare gli infidi puntini (...). Per esempio

Def. (operazioni aritmetiche)

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

Anziché $a+b = \underbrace{s(s(\dots a \dots))}_{b \text{ successori}}$ Anziché $a \cdot b = \underbrace{a + a + \dots + a}_{b \text{ volte}}$

Def. (potenza, fattoriale)

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

Anziché $a^b = \underbrace{a \cdot a \cdot \dots \cdot a}_{b \text{ volte}}$ Anziché $a! = 1 \cdot 2 \cdot \dots \cdot (a-1) \cdot a$

Def. (sommatoria)

$$\begin{cases} \sum_{i=0}^{0} f(i) = 0 \\ \sum_{i=0}^{s(a)} f(i) = \left(\sum_{i=0}^{a} f(i) \right) + f(s(a)) \end{cases}$$

Anziché $\sum_{i=0}^{a} f(i) = f(0) + f(1) + \dots + f(a)$

Altre successioni — ossia funzioni con dominio ω — sono definite nella maniera più naturale proprio per ricorsione.

Esempio In quanti modi posso coprire una sequenza di n caselle  con tessere di una o due caselle che non si sovrappongono e non lasciano caselle scoperte?

Sol. Detto F_n il numero di ricoprimenti di una sequenza lunga n, vediamo che la tessera più a sinistra può essere o . Nel primo caso, ci sono F_{n-1} modi di completare il ricoprimento, nel secondo caso F_{n-2}. Quindi

$$F_n = F_{n-1} + F_{n-2}$$

La sequenza risulta completamente determinata, per ricorsione, osservando che $F_0 = F_1 = 1$: sono i numeri di Fibonacci.

In un certo senso, induzione e ricorsione sono due facce della stessa medaglia: dove l'induzione dimostra $\Phi(s(n))$ assumendo di sapere $\Phi(n)$, la ricorsione calcola $f(s(n))$ assumendo di aver pure $f(n)$. Lo stesso parallelismo, vedremo, si presenterà per l'induzione e la ricorsione transfinita. Tornando al numerabile: come abbiamo enunciato due forme dell'induzione, enunceremo due forme parallele della ricorsione.

La semplice osservazione che segue dice che due funzioni sono uguali precisamente quando assumono gli stessi valori.

Oss. (estensionalità per funzioni)
Dato $f, g : A \to B$ $\quad f = g \iff \forall x \in A \; f(x) = g(x)$
Dim. $(x,y) \in f \iff y = f(x) \iff y = g(x) \iff (x,y) \in g$.

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

Teo (di ricorsione numerabile — prima forma)
Dato un insieme A, un elemento $k \in A$ e una funzione

$$h : \omega \times A \to A$$

esiste un'unica funzione $f : \omega \to A$ tale che

$$\forall n \in \omega \quad f(s(n)) = h(n, f(n))$$

Esempio Per definire a^b considero $k = 1$, $h(n,x) = a \cdot x$
Per definire il fattoriale $k = 1$, $h(n,x) = s(n) \cdot x$
Esercizio Come potrei costruire F_n usando questo teorema?

Dim. Il piano consiste nel trovare una formula $\Phi(x,y)$ che dice "$y = f(x)$" — questa è la vera difficoltà della dimostrazione — poi semplicemente otteniamo f per separazione nell'insieme $\omega \times A$ usando la formula Φ.
Per dire "$y = f(x)$" diremo "i primi x passaggi della ricorsione, partendo da k, conducono a y".
Dato $x \in \omega$ diciamo che g è una x-approssimazione

se vale la formula seguente.

$$g \in {}^{s(x)}A \wedge g(\emptyset) = k \wedge \forall n \in x \;\; g(s(n)) = h(n, g(n))$$

che dice che $g : \{0 \dots x\} \to A$ soddisfa la definizione ricorsiva di f, ristretta, naturalmente, al dominio $\{0 \dots x\}$.
Il vantaggio di tagliuzzare f in x-approssimazioni è che così ottenuamo un parametro, x, su cui impostare un'induzione.

Lemma $\forall x \in \omega \; \exists! g$ "g è una x-approssimazione"

Dim Induzione su x

caso $x = \emptyset$. Basta osservare che l'unica $\emptyset$-approssimazione è $\{(\emptyset, k)\}$. Infatti il dominio è $\{\emptyset\}$ per definizione, e abbiamo la condizione $g(\emptyset) = k$.

caso $x = s(a)$. Per ipotesi induttiva esiste un'unica a-approssimazione g. Poniamo $g' = g \cup \{(s(a), h(a, g(a)))\}$ ossia $g'(t) = g(t)$ per $t \leq a$, e $g'(s(a)) = h(a, g(a))$.
È immediato verificare che g' è una $s(a)$-approssimazione. Per verificare l'unicità, osserviamo che, date $s(a)$-approssimazioni g' e g'', la loro restrizione a $s(a)$ è una a-approssimazione, quindi, per ipotesi induttiva $g'|_{s(a)} = g = g''|_{s(a)}$. D'altro canto il dominio di una $s(a)$-approssimazione è $s(s(a)) = s(a) \cup \{s(a)\}$, abbiamo detto che g' e g'' coincidono su $s(a)$, e

$$g'(s(a)) = h(a, g'(a)) = h(a, g''(a)) = g''(s(a))$$

Stabilito il lemma, introduciamo la formula Φ

$\Phi(x,y) \overset{\text{def.}}{\equiv} \exists g \in {}^{s(x)}A$ "g è una x-approssimazione" $\wedge\ g(x) = y$

Per l'unicità della x-approssimazione $\forall x \in \omega\ \exists! y\ \Phi(x,y)$

possiamo quindi definire, per ogni $x \in \omega$ e $y \in A$

$$f(x) = y \overset{\text{def.}}{\equiv} \Phi(x,y)$$

$$\text{formalmente}\quad f = \{(x,y) \in \omega \times A \mid \Phi(x,y)\}$$

Occorre verificare che f soddisfa le condizioni della ricorsione.

$f(\emptyset) = k$. Immediata.

$f(s(n)) = \dots$ Per costruzione $f(s(n)) = g(s(n))$ per una $s(n)$-approssimazione g. D'altra canto $g(s(n)) = h(n, g(n))$.

Ora $g|_{s(n)}$ è una n-approssimazione, quindi

$g(n) = g|_{s(n)}(n) = f(n)$. Mettendo tutto insieme

$$f(s(n)) = g(s(n)) = h(n, g(n)) = h(n, f(n))$$

L'unicità di f segue facilmente per induzione. Dati f' e f'' che soddisfano la ricorsione abbiamo

$f'(\emptyset) = k = f''(\emptyset)$ $\qquad$ $f'(s(n)) = h(n, f'(n)) = h(n, f''(n)) = f''(s(n))$

($f'(n) = f''(n)$ per ip. induttiva)

∎

Procedendo come negli esempi all'inizio di questa sezione, il teorema di ricorsione numerabile ci consente di costruire le operazioni aritmetiche, la potenza &c. A titolo di esempio, vediamo la nel dettaglio il caso della somma.

Esempio (costruzione di $+ : \omega \times \omega \to \omega$)

Vogliamo formalizzare la definizione

$$\begin{cases} a + 0 = a \\ a + s(b) = s(a+b) \end{cases}$$

Per il teorema di ricorsione sappiamo che, per ogni $a \in \omega$ fissato, esiste un'unica $f : \omega \to \omega$ tale che

$$f(0) = a \;\wedge\; \forall b \in \omega \; f(s(b)) = s(f(b))$$

Scriviamo quindi

$$a + x = y \overset{\text{def.}}{\equiv} \exists f \in {}^{\omega}\omega \; f(0) = a \wedge f(x) = y \wedge \forall b \in \omega \; f(s(b)) = s(f(b))$$

L'applicazione che segue chiude il conto che abbiamo lasciato aperto con gli assiomi di Peano. Dimostriamo che essi identificano un'unica struttura a meno di isomorfismi, quindi ω è, a buon diritto, l'insieme dei numeri naturali.

Teo Supponiamo che $(\mathbb{N}, 0, succ)$ soddisfi gli assiomi di Peano, allora $(\mathbb{N}, 0, succ)$ e $(\omega, \emptyset, s)$ sono strutture isomorfe — ossia, formalmente, esiste $f : \omega \to \mathbb{N}$ biiettiva tale che $f(\emptyset) = 0$ e $\forall n \in \omega \; f(s(n)) = succ(f(n))$.

Fa comodo isolare la seguente osservazione.

Oss $\forall x \in \omega \; x \neq 0 \longrightarrow \exists y \in \omega \; x = s(y)$

Dim. Induzione su x. Il caso $x = 0$ è vero a vuoto. Nel caso $x = s(n)$ basta prendere $y = n$ e si ha $x = s(y)$. Ü

Dimostriamo ora il teorema.

Dim Per il teorema di ricorsione c'è un'unica f che soddisfa le condizioni $f(\emptyset) = 0$ e $\forall n \in \omega \; f(s(n)) = succ(f(n))$.
Resta da constatare che f è bigettiva.

Suriettività: Per ipotesi $(\mathbb{N}, 0, succ)$ soddisfa il principio di induzione. Dimostriamo quindi per induzione in $(\mathbb{N}, 0, succ)$ che $\forall y \in \mathbb{N} \; \exists x \in \omega \; f(x) = y$.

caso $y = 0$. Basta osservare che $f(\emptyset) = 0$ per costruzione.

caso $y = succ(n)$. Per ipotesi induttiva c'è $x \in \omega$ tale che $f(x) = n$.
Quindi $f(s(x)) = succ(n)$.

Iniettività: Consideriamo, per assurdo, il minimo $x \in \omega$ tale che, per qualche $y \in \omega$ con $y \neq x$, $f(x) = f(y)$.
Osserviamo che, per la minimalità di x, $x < y$, quindi, in particolare $y \neq \emptyset$, e possiamo scrivere $y = s(y')$.
Se $x = \emptyset$, allora $succ(f(y')) = f(s(y')) = f(y) = f(x) = 0$, contraddicendo l'assioma B. per $(\mathbb{N}, 0, succ)$.
Se $x \neq \emptyset$, allora possiamo scrivere $x = s(x')$, da cui

$$succ(f(x')) = f(s(x')) = f(x) = f(y) = f(s(y')) = succ(f(y'))$$

e, per l'assioma A. in $(\mathbb{N}, 0, succ)$, $f(x') = f(y')$. Allora, per la minimalità di x, siccome $x' < x$, dobbiamo avere $x' = y'$.
Ma da questo seguirebbe $x = s(x') = s(y') = y$ ↯ ∎

Se, infine, volgiamo la nostra attenzione all'esempio dei numeri di Fibonacci, vediamo che non è possibile definire questa sequenza applicando il teorema di ricorsione in maniera diretta, poiché F_n non dipende solo dal termine precedente della sequenza, F_{n-1}, ma anche da F_{n-2}. Ce la si potrebbe cavare con un trucco, per esempio definendo la funzione $n \longmapsto (F_n, F_{n+1})$ da ω a $\omega \times \omega$. È comodo, però, disporre di una versione più versatile del teorema.

Teo (di ricorsione numerabile — seconda forma)
Dato un insieme A, denotiamo con A^* l'insieme delle funzioni $g \subseteq \omega \times A$ con $Dom(g) \in \omega$. Sia $h: A^* \to A$, allora esiste un'unica funzione $f: \omega \to A$ tale che

$$\forall n \in \omega \quad f(n) = h(f|_n)$$

In altre parole, $f(n)$ può dipendere in maniera arbitraria dai valori assunti da f sui numeri minori di n.

Esempio di applicazione
Per costruire la successione di Fibonacci, definiamo $h(g)$ in questo modo. Sia $n = Dom(g)$. Se $n = \emptyset$ o $n = 1$, allora $h(g) = 1$. Altrimenti esistono $n-1, n-2 \in \omega$ tali che $s(n-1) = s(s(n-2)) = n$. Definiamo quindi $h(g) = g(n-1) + g(n-2)$.

Rif. L'idea è definire, mediante la prima forma del teorema di ricorsione, la successione delle troncate di f. Ossia la funzione $f' : n \longmapsto f|_n$. — Un modo alternativo, sarebbe ripetere la dimostrazione della prima forma.

Costruiamo per ricorsione — prima forma — la funzione $f' : \omega \to A^*$ tale che: $f'(\emptyset) = \emptyset$

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

Ora poniamo $f(n) = f'(s(n))(n)$.

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

caso $n = 0$. Immediato

caso $n = s(m)$. $f|_{s(m)} = f|_m \cup \{(m, f(m))\}$

$$= f'(m) \cup \{(m, f'(s(m))(m))\}$$

$$= f'(m) \cup \{(m, h(f'(m))\} = f'(s(m)).$$

Infine, quindi, $f(n) = f'(s(n))(n) = h(f'(n)) = h(f|_n)$. ∎

Abbiamo così terminato di dimostrare le proprietà di base dei numeri naturali. Da qui prende le mosse il corso di aritmetica. Nella prossima sezione, inizieremo lo studio di un concetto squisitamente insiemistico: la cardinalità.

Esercizio: dimostra commutatività associatività &c. di $+$ e $\cdot$.

Cardinalità

Il concetto di cardinalità è, forse, il modo più semplice di contare gli elementi di un insieme: diciamo che due insiemi hanno un uguale numero di elementi se esiste una corrispondenza biunivoca fra di essi.

Def Dati due insiemi A e B

$|A| = |B|$ $\overset{\text{def.}}{\equiv}$ $\exists f \in {}^{A}B$ "f è bigettiva $A \to B$"

"A ha la stessa cardinalità di B"

"A e B sono equipotenti"

$|A| \leq |B|$ $\overset{\text{def.}}{\equiv}$ $\exists B' \subseteq B \quad |A| = |B'|$

ossia: $\exists f \in {}^{A}B$ "f è iniettiva"

Note:

- La scrittura $|A| = |B|$ suggerisce che esistano insiemi — o oggetti di qualche genere — denotati $|A|$ e $|B|$ di cui si predica l'uguaglianza. Effettivamente costruiremo questi oggetti, ma, per ora, la scrittura $|A| = |B|$ è inscindibile, come (A, B).
- Potrebbe sorgere il sospetto che se $|A| < |B|$ quando $A \subsetneq B$, ma non è così, come mostra l'esempio di $A = \{x \in \omega \mid x > 0\}$ e $B = \omega$.

Oss. La relazione $|\cdot| = |\cdot|$ soddisfa le proprietà formali di una relazione di equivalenza.

riflessività: $|A| = |A|$

simmetria: $|A| = |B| \to |B| = |A|$

transitività: $|A| = |B| \wedge |B| = |C| \to |A| = |C|$

Dim Esercizio

Oss. La relazione $|\cdot| \leq |\cdot|$ è:

riflessiva: $|A| \leq |A|$

transitiva: $|A| \leq |B| \wedge |B| \leq |C| \to |A| \leq |C|$

Inoltre è compatibile con la relazione di equipotenza

$$|A| = |B| \to |A| \leq |B|$$

Dim Esercizio

Per stabilire che le cardinalità sono, formalmente, ordinate dalla relazione $|\cdot| \leq |\cdot|$, ci manca l'antisimmetria, che è appunto l'enunciato del teorema seguente.

Teo (Cantor - Bernstein)

$$\forall A, B \ (|A| \leq |B| \wedge |B| \leq |A|) \to |A| = |B|$$

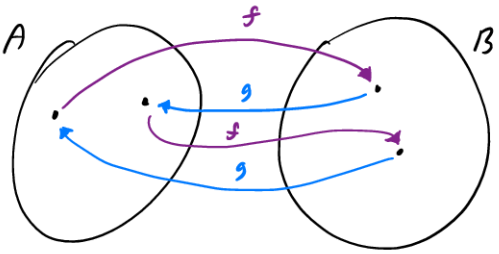
Ossia: se c'è una funzione iniettiva $A \to B$ e una funzione iniettiva $B \to A$, allora esiste una bigezione fra A e B.

Dim. Siano $f: A \to B$ e $g: B \to A$ iniettive. Il nostro obiettivo è costruire una nuova funzione $h: A \to B$ biiettiva. L'idea è che ogni elemento, poniamo, di A, è una tappa di un percorso: $a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$

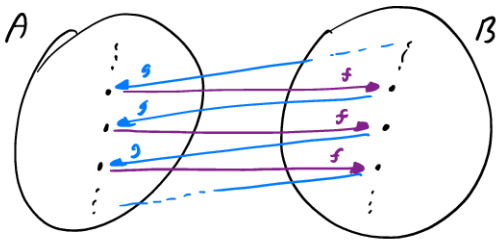
Siccome f e g sono iniettive, questo percorso ha all'indietro un'unica estensione all'indietro

$$f^{-1}(g^{-1}(a)) \xrightarrow{f} g^{-1}(a) \xrightarrow{g} a \xrightarrow{f} f(a) \xrightarrow{g} g(f(a)) \xrightarrow{f} f(g(f(a))) \xrightarrow{g} \dots$$

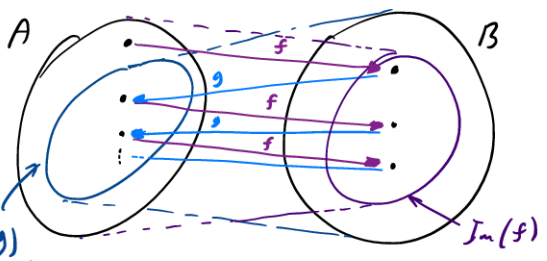
a patto che $a \in \mathrm{Im}(g)$, $g^{-1}(a) \in \mathrm{Im}(f)$, etc. Quando, e se, non possiamo più applicare la funzione inversa, il percorso si interrompe. Ci sono quindi percorsi di tre tipi:

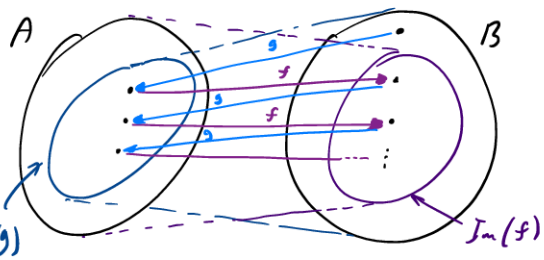


CIRCOLARI



ILLIMITATI IN AVANTI O INDIETRO

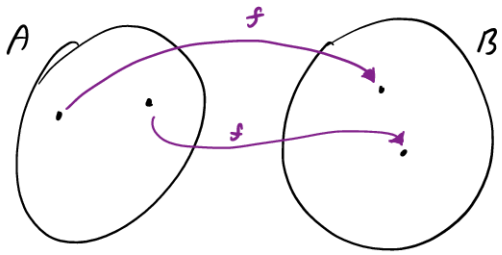




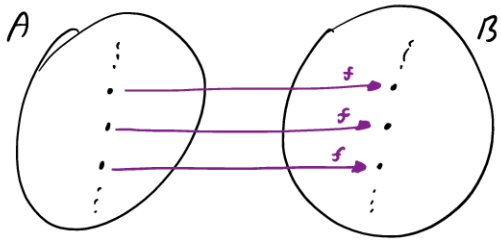
ILLIMITATI IN AVANTI MA NON INDIETRO

Per gli elementi che si trovano su un percorso circolare, o su un percorso illimitato avanti e indietro, f fornisce una biiezione, come la fornirebbe anche g^{-1} — la scelta è arbitraria a patto di

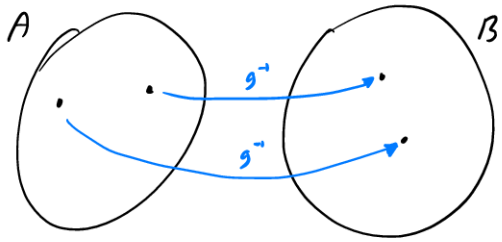
usare la medesima funzione per l'intero percorso.

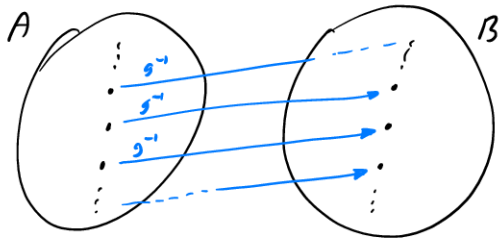


o anche

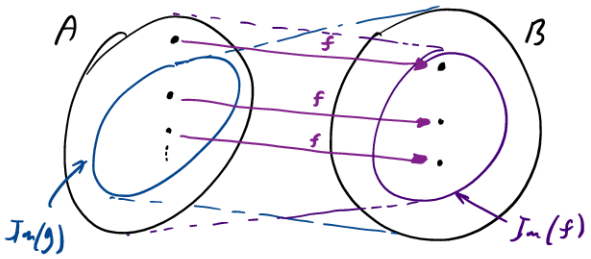


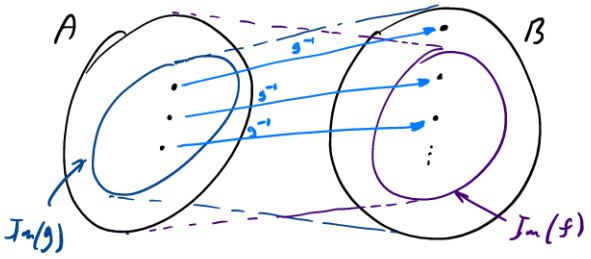
o anche





Per i percorsi, invece, illimitati solo a destra, occorre vedere in quale insieme sta l'elemento iniziale del percorso: se questo è in A, la biiezione è data da f, altrimenti da g^{-1}.





Per comodità, poniamo $h(x) = f(x)$ in ogni caso eccetto quando x è lungo un percorso che parte da B, nel cui caso $h(x) = g^{-1}(x)$.

Formalmente, definiamo per ricorsione le seguenti successioni di sottoinsiemi di B e A rispettivamente — ossia, tecnicamente, la funzione $w \to \mathcal{P}(B) \times \mathcal{P}(A)$, $i \mapsto (B_i, A_i)$

$$B_0 = B \setminus \mathrm{Im}(f) \qquad A_i = g[B_i] \qquad B_{s(i)} = f[A_i]$$

Definiamo quindi

$$B_* = \bigcup_{i\in\omega} B_i \overset{\text{def.}}{\equiv} \bigcup \{B_i \mid i\in\omega\} \qquad A_* = \bigcup_{i\in\omega} A_i$$

Questi sono i punti che appartengono a cammini che partono da B, definiamo quindi $h: A \to B$ e $k: B \to A$ come segue

$$h(x) = \begin{cases} g^{-1}(x) & \text{se } x \in A_* \\ f(x) & \text{altrimenti} \end{cases} \qquad k(y) = \begin{cases} g(y) & \text{se } y \in B_* \\ f^{-1}(y) & \text{altrimenti} \end{cases}$$

Ci basta dimostrare che h e k sono ben definite, $k \circ h = Id_A$ e $h \circ k = Id_B$.

① h e k sono ben definite.

Occorre verificare che stiamo applicando g^{-1} e f^{-1} a elementi della immagine di g e f rispettivamente. Nella definizione di h, se $x \in A_*$, allora $x \in A_i$ per qualche $i\in\omega$, quindi $x \in g[B_i] \subseteq Im(g)$. Nella definizione di k, se $y \notin B_*$, in particolare, $y \notin B_0$, per cui $y \in Im(f)$.

② $k \circ h = Id_A$

Se $x \in A_*$, allora $x \in A_i$ per qualche $i\in\omega$, quindi $x = g(y)$ con $y \in B_i$, per cui $k(h(x)) = k(g^{-1}(x)) = k(y) = g(y) = x$.

Per il caso $x \notin A_*$, osserviamo, intanto, che $x \notin A_* \to f(x) \notin B_*$. Infatti, se $f(x) \in B_i$ con $i\in\omega$, allora $i \neq 0$, perché $B_0 = B \setminus Im(f)$, quindi possiamo scrivere $i = s(\sigma)$, e $f(x) \in B_{s(\sigma)} = f[A_\sigma]$. Per l'iniettività di f, abbiamo allora $x \in A_\sigma$ ↯.

Di conseguenza, se $x \in A_*$, $k(h(x)) = k(f(x)) = f^{-1}(f(x)) = x$.

(3) $h \circ k = Id_B$

Se $y \in B_*$, allora $y \in B_i$ per qualche $i \in \omega$, quindi $g(y) \in A_i$.

Di conseguenza $h(k(y)) = h(g(y)) = g^{-1}(g(y)) = y$.

Altrimenti $y \notin B_*$ e, se $f^{-1}(y) \in A_*$, avremmo una contraddizione, poiché $f^{-1}(y) \in A_i \to y = f(f^{-1}(y)) \in A_{s(i)}$. Quindi $h(k(y)) = h(f^{-1}(y)) = f(f^{-1}(y)) = y$. ∎

Visto che $|\cdot| \leq |\cdot|$ ha le proprietà formali di una relazione d'ordine fra le classi di equivalenza della relazione $|\cdot| = |\cdot|$, possiamo definire il corrispondente ordine stretto.

Def Dati due insiemi A e B

$$|A| < |B| \overset{def.}{\equiv} |A| \leq |B| \wedge \underbrace{|A| \neq |B|}_{\overset{def.}{\equiv} \neg(|A| = |B|)}$$

Teo (Cantor)
Dato un insieme qualunque A, vale $|A| < |\mathcal{P}(A)|$

La dimostrazione di questo enunciato è, ancora una volta, il medesimo argomento del paradosso di Russell.

Dim La disuguaglianza $|A| \leq |\mathcal{P}(A)|$ è facile: basta considerare la funzione iniettiva $A \to \mathcal{P}(A)$, $x \longmapsto \{x\}$.

Consideriamo, ora, una qualunque $f: A \to \mathcal{P}(A)$ iniettiva.

Dobbiamo dimostrare che $\mathrm{Im}(f) \subsetneq \mathcal{P}(A)$. Consideriamo

$$B = \{x \in A \mid x \notin f(x)\}$$

Supponendo, per assurdo, $B = f(a)$, avremmo

$$a \in f(a) \iff a \in B \iff a \notin f(a)$$ ↯ ∎

Operazioni fra cardinalità

Def. $|A| + |B| \overset{\text{def}}{\equiv} |A \sqcup B| \overset{\text{def}}{\equiv} |A \times \{0\} \cup B \times \{1\}|$

$|A| \cdot |B| \overset{\text{def.}}{\equiv} |A \times B| \qquad |A|^{|B|} \overset{\text{def.}}{\equiv} |{}^B A|$

Prop: Le operazioni di somma, prodotto e potenza fra cardinalità sono ben definite, ossia dati A, B, A', B' con $|A| = |A'|$ e $|B| = |B'|$, vale:

$$|A| + |B| = |A'| + |B'| \qquad |A| \cdot |B| = |A'| \cdot |B'| \qquad |A|^{|B|} = |A'|^{|B'|}$$

Dim Date $f: A \to A'$ e $g: B \to B'$ biiettive, è immediato verificare che le seguenti sono biezioni:

$$A \cup B \to A' \cup B' \qquad A \times B \to A' \times B' \qquad {}^B A \to {}^{B'} A'$$

$$(a, 0) \mapsto (f(a), 0) \qquad (a, b) \mapsto (f(a), g(b)) \qquad h \mapsto f \circ h \circ g^{-1}$$

$$(b, 1) \mapsto (g(b), 1)$$ ∎

Notazione Riferendoci alle cardinalità finite $|\emptyset|, |1|, |2|, \dots$ se non c'è rischio di confusione, scriveremo semplicemente $0, 1, 2, \dots$

Oss. $|\mathcal{P}(A)| = 2^{|A|}$, per cui il teorema di Cantor può essere enunciato dicendo che, dato qualunque A, $|A| < 2^{|A|}$.

Dim La funzione che ad ogni $B \in \mathcal{P}(A)$ associa la sua funzione indicatrice $\chi_B : A \to 2$ definita da

$$\chi_B(x) = \begin{cases} 1 & \text{se } x \in B \\ 0 & \text{altrimenti} \end{cases}$$

è una bigezione $\mathcal{P}(A) \to {}^A2$.

Prop. Le operazioni fra cardinalità godono delle proprietà seguenti: denotando, per brevità, con α, β, γ i simboli $|A|, |B|, |C|$

$$\alpha + 0 = \alpha \qquad \alpha + \beta = \beta + \alpha \qquad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$

$$\alpha \cdot 0 = 0 \qquad \alpha \cdot \beta = \beta \cdot \alpha \qquad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

$$\alpha \cdot 1 = \alpha \qquad \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

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

$$\alpha^1 = \alpha \qquad \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$$

$$1^\alpha = 1$$

Dim In ciascun caso, si tratta semplicemente di esibire una bigezione esplicita fra il membro di sinistra e il membro di destra. Come esempio, vediamo uno dei casi più complicati, il resto è lasciato come esercizio.

Dimostriamo che $(|A|^{|B|})^{|C|} = |A|^{|C| \cdot |B|}$. Dobbiamo esibire una bigezione fra l'insieme ${}^C({}^BA)$ delle funzioni che ad ogni elemento di C associano una funzione $B \to A$, e l'insieme ${}^{C \times B}A$ delle funzioni che ad ogni coppia di elementi in $C \times B$ associano un elemento di A.

A $f \in {}^C({}^B A)$ associamo $\tilde{f} \in {}^{C\times B}A$ definita da

$$\tilde{f}(c,b) = f(c)(b)$$

Dimostriamo che l'inversa di questa applicazione associa a $g \in {}^{C\times B}A$ la funzione $\overline{g} \in {}^C({}^B A)$ definita da

$$\overline{g}(c) : B \to A$$
$$b \mapsto g(c,b)$$

La verifica è facilissima:

$\forall (c,b) \in C\times B \quad \tilde{\overline{g}}(c,b) = \overline{g}(c)(b) = g(c,b) \quad \Rightarrow \quad \tilde{\overline{g}} = g$

e, fissato un qualunque $c \in C$

$\forall b \in B \quad \overline{\tilde{f}}(c)(b) = \tilde{f}(c,b) = f(c)(b) \quad \Rightarrow \quad \overline{\tilde{f}}(c) = f(c)$

da cui, per l'arbitrarietà di c, $\overline{\tilde{f}} = f$. ∎

Cardinalità finite

Ora inizia una breve carrellata fra le cardinalità più facili da definire. Parliamo qui di cardinalità finite, poi introdurremo la cardinalità numerabile e la cardinalità del continuo.

Def Diciamo che A è *finito* se $\exists n \in \omega \; |A| = |n|$.
Se A non è finito, diciamo che A è *infinito*.

Storicamente, è rilevante una definizione alternativa di finitezza, data originariamente da Dedekind.

Def A è *Dedekind-finito* se non può essere messo in

corrispondenza biunivoca con un suo sottoinsieme proprio.
Ossia A è Dedekind-finito se $\forall B \subsetneq A \quad |B| < |A|$.

Con gli assiomi introdotti fino ad ora, possiamo solo dimostrare che finito $\to$ Dedekind-finito, mentre l'implicazione inversa è conseguenza dell'assioma della scelta.

Prop. (principio dei cassetti — ossia — finito $\to$ Dedekind-finito)
Dato A finito e $B \subsetneq A$, vale $|B| < |A|$.
Dim $\leq$ vale ovviamente perché l'identità è una funzione iniettiva $B \to A$. Occorre quindi dimostrare $|B| \neq |A|$.

Osserviamo che, senza perdita di generalità, possiamo assumere $A = n \in \omega$. Per ipotesi, infatti esiste $f : A \to n$ biiettiva, per un opportuno new. Quindi $f[B] \subsetneq n$. D'altro canto, per l'iniettività di f, $|f[B]| = |B| = |A| = n$.

Ci basta quindi dimostrare, per induzione su n, che

$$\forall n \in \omega \quad \forall B \subseteq n \quad |B| = |n| \to B = n.$$

Caso $n = \emptyset$. Necessariamente anche $B = \emptyset$, quindi $B = n$.

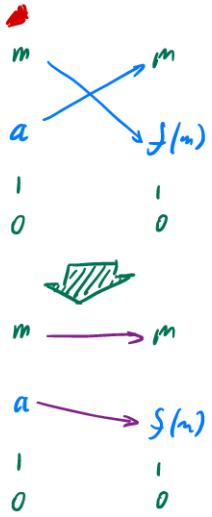
Caso $n = s(m)$ L'ipotesi induttiva è $\forall C \subseteq m \quad |C| = |m| \to C = m$



Prendiamo $f : s(m) \to B$ biiettiva. Si danno due casi. Se $f(m) = m$, allora $C \overset{\text{def.}}{=} \mathrm{Im}(f_{|m}) \subseteq m$, e, per l'iniettività di f, $|C| = |m|$, quindi, per

l'ipotesi induttiva, $C = m$. Ma $B = Im(f) =$

$= C \cup \{f(m)\} = m \cup \{m\} = n$.



Se $f(m) \neq m$, allora vediamo che esiste $a < m$ tale che $f(a) = m$. Se così non fosse, infatti, $f|_m$ sarebbe una bigezione fra m e $m \setminus \{f(m)\}$, contro l'ipotesi induttiva. Ora, però, possiamo costruire una nuova bigezione $f' : s(m) \to B$ che ricade nel caso precedente:

$$f'(x) = \begin{cases} m & \text{se } x = m \\ f(m) & \text{se } x = a \\ f(x) & \text{altrimenti} \end{cases}$$

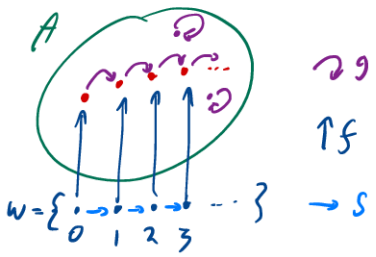
Cor Se A è un insieme finito, allora $\exists!\, n \in \omega \; |A| = |n|$

Dim Se $|m| = |A| = |n|$, possiamo assumere, senza perdita di generalità $m \in n$, ossia $m \subseteq n$, quindi $m = n$ per il principio dei cassetti.

Se adesso volessimo dimostrare il viceversa: che un insieme infinito non è Dedekind-finito, quale sarebbe l'ostacolo? Abbiamo già osservato che ω non è finito, poiché la funzione successore stabilisce una corrispondenza biunivoca fra ω e $\omega \setminus \{0\} \subsetneq \omega$. Ne segue la seguente osservazione.

Oss. Se esiste $f : \omega \to A$ iniettiva, allora A non è Dedekind-finito.

Dim Basta considerare la funzione iniettiva



$$g : A \to A$$

$$g(a) = \begin{cases} f(s(f^{-1}(a))) & \text{se } a \in f[w] \\ a & \text{altrimenti} \end{cases}$$

È immediato vedere che $Im(g) = A \setminus \{f(0)\} \subsetneq A$ ☒

Quindi ci basterebbe dimostrare che w si immerge in ogni insieme infinito. Un tentativo di dimostrazione potrebbe andare come segue.

Sia A infinito, costruiamo per ricorsione, seconda forma, una $f : w \to A$ iniettiva. Supponiamo di conoscere $f|_n$, il nostro scopo è definire il prossimo valore: $f(n)$. Siccome A è infinito, $f|_n$, che è iniettiva per costruzione, non può essere surgettiva, quindi esiste $a \in A$ con $a \notin Im(f|_n)$. Pongo $f(n) = a$.

Dov'è l'errore? Nell'ultima riga! Noi sappiamo che, data $f|_n$, esistono degli $a \in A$ con $a \notin Im(f|_n)$, questo è corretto. È anche corretto che ci basterebbe porre $f(n) =$ "uno qualunque di questi a". Il guaio è che, per applicare il teorema di ricorsione, ci serve una funzione che fissa uno degli a. A patto di averne una, ne andrebbe bene una qualunque.

Purtroppo, però, a partire dalla mera ipotesi che A è infinito, non abbiamo modo di procurarci nessuna funzione del genere. Potremmo cavarcela se avessimo qualche struttura su A, sulla quale far leva — per esempio per dire "prendo il minimo fra gli $a \notin \mathrm{Im}(f_n)$", o "prendo il più giallo" — ma di A non sappiamo nulla, e non abbiamo modo di indurre una struttura di questo genere.

Accettato che non possiamo dimostrare che ω si immerge in qualsiasi insieme infinito, possiamo però lambire questa soglia: dimostriamo che, in un insieme infinito, si immergono tutti i numeri naturali.

Prop. Sia A infinito. Allora $\forall n \in \omega \quad |n| < |A|$

Dim Basta dimostrare il $\leq$, infatti $|n| < |n+1| \leq |A|$.

Dimostriamo per induzione su n che c'è una funzione iniettiva da n ad A.

Caso $n=0$. La funzione vuota.

Caso $n=m+1$. Per ipotesi induttiva esiste $f : m \to A$ iniettiva. Siccome A è infinito, esiste $a \in A \setminus \mathrm{Im}(f)$. La funzione $f' = f \cup \{(m, a)\}$, che si ottiene estendendo f col mandare m in a, è iniettiva $n \to A$. ∎

Cor Un sottoinsieme di un insieme finito è finito.

Dim Sia A finito e $B \subseteq A$. Se, per assurdo, B fosse infinito, avremmo $|A| < |B| \leq |A|$ ↯

Esercizi Dimostra che:
- se $|A| < |n|$ con $n \in \omega$, allora $|A| = |m|$ per qualche $m < n$
- se A è finito e $f : A \to B$, allora $f[A]$ è finito.

Prop Dati $m, n \in \omega$

$$|m| + |n| = |m+n| \qquad |m| \cdot |n| = |m \cdot n| \qquad |m|^{|n|} = |m^n|$$

Dim Dimostriamo, intanto, che $|m| + |1| = |S(m)|$. A sinistra abbiamo, infatti, la cardinalità di $m \times \{0\} \cup \{(1,1)\}$ e a destra quella di $m \cup \{m\}$. Quest'ultimo insieme si mappa biiettivamente nel primo mandando $x \in m$ in $(x,0)$ e m in $(1,1)$.
Ora, le uguaglianze asserite seguono, per induzione su n, dalle proprietà delle operazioni sulle cardinalità e dalla definizione ricorsiva delle operazioni su ω.

$|m| + |n| = |m+n|$

caso $n = 0$. $|m| + |0| = |m| = |m + 0|$

caso $n = S(a)$.
$$\begin{aligned}
|m| + |S(a)| &= |m| + (|a| + |1|) && \text{osservazione iniziale}\\
&= (|m| + |a|) + |1| && \text{proprietà operazioni}\\
&= |m + a| + |1| && \text{ipotesi induttiva}\\
&= |S(m+a)| && \text{di nuovo l'osservazione}\\
&= |m + S(a)| && \text{definizione di } +
\end{aligned}$$

$|m| \cdot |n| = |m \cdot n|$

caso $n = 0$. $|m| \cdot |0| = |0| = |m \cdot 0|$

caso $n = s(a)$.

$$\begin{aligned}
|m| \cdot |s(a)| &= |m| \cdot (|a| + |1|) && \text{osservazione iniziale}\\
&= |m| \cdot |a| + |m| && \text{proprietà operazioni}\\
&= |m \cdot a| + |m| && \text{ipotesi induttiva}\\
&= |m \cdot a + m| && \text{identità per il } +\\
&= |m \cdot s(a)| && \text{definizione di } \cdot
\end{aligned}$$

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

caso $n = 0$. $|m|^{|0|} = |1| = |m^0|$

caso $n = s(a)$.

$$\begin{aligned}
|m|^{|s(a)|} &= |m|^{|a|+|1|} && \text{osservazione iniziale}\\
&= |m|^{|a|} \cdot |m| && \text{proprietà operazioni}\\
&= |m^a| \cdot |m| && \text{ipotesi induttiva}\\
&= |m^a \cdot m| && \text{identità per il } \cdot\\
&= |m^{s(a)}| && \text{definizione di potenza}
\end{aligned}$$

∎

Nota Questa proposizione ci fornisce una dimostrazione delle proprietà aritmetiche elementari delle operazioni su ω, alternativa a quella per induzione (che è stata lasciata come esercizio). Basta, infatti, applicare le corrispondenti proprietà delle operazioni sulle cardinalità.

Esercizio Dimostra che se $m, n \in \omega$ e $m \leq n$, esiste un unico $n - m \in \omega$ tale che $m + (n - m) = n$. In due modi diversi.

La cardinalità del numerabile — $\aleph_0$

Def Diciamo che A è *al più numerabile* se $|A| \leq |\omega|$ ed è *numerabile* se $|A| = |\omega|$. Il simbolo $\aleph_0$ — *alef con zero* — è semplicemente un'abbreviazione per $|\omega|$. Per cui $|A| \leq \aleph_0$ si può leggere "A è al più numerabile" e $|A| = \aleph_0$ si può leggere "A è numerabile".

Oss In altri termini, dire che A è al più numerabile significa dire che c'è una funzione iniettiva $A \to \omega$. Dire che è numerabile significa dire che è in biiezione con ω.

Prop Se A è al più numerabile, allora o A è finito o A è numerabile.
Ossia: $|A| < \aleph_0$ se e solo se A è finito.

Potremmo dimostrare la proposizione direttamente, ma ci conviene, invece, passare attraverso alcune considerazioni che saranno utili in seguito.
In generale, per costruire una biiezione fra due insiemi A e B — ossia per dimostrare $|A| = |B|$ — occorre appoggiarsi a qualche struttura definita sugli insiemi A e B. Per esempio, una funzione successore. In questo

corso, giocheranno un ruolo importante, in questa direzione, le relazioni d'ordine, e, in particolare — l'idea è di Cantor — i **buoni ordini**. Ricordiamo la definizione.

Def Un insieme totalmente ordinato $(S, <)$ si dice **ben ordinato** se ogni suo sottoinsieme non vuoto ha un minimo.

$$\forall A \subseteq S \quad A \neq \emptyset \to \exists m \in A \ \forall x \in A \ m \leq x$$

Il trucco è che un isomorfismo di ordini è, in particolare, una biiezione, e spesso, per costruire biiezioni, costruiamo isomorfismi di ordini.

Def Due insiemi (parzialmente) ordinati $(A, <_A)$ e $(B, <_B)$ sono **isomorfi**, in simboli $(A, <_A) \sim (B, <_B)$, se esiste una biiezione $f : A \to B$ tale che

$$\forall x, y \in A \quad x <_A y \iff f(x) <_B f(y)$$

Oss Due insiemi totalmente ordinati $(A, <_A)$ e $(B, <_B)$ sono isomorfi se e solo se esiste una funzione $f : A \to B$ surgettiva e **strettamente crescente** — cioè tale che

$$\forall x, y \in A \quad x <_A y \to f(x) <_B f(y)$$

Dim esercizio.

Oss. Sia $(A, <_A)$ totalmente ordinato con $|A| = n \in \omega$. Allora $(A, <_A) \sim (n, <)$, dove $<$ denota l'ordinamento indotto da ω.

Dim Per induzione su n.

caso $n=0$. $A=\emptyset$ quindi $(A, <_a) \sim (\emptyset, \emptyset)$.

caso $n=s(m)$. Se $m=0$, allora $A=\{a\}$ e $(A, <_a) \sim (1, <)$.

Assumiamo quindi $m>0$. Dimostriamo, intanto, che $(A, <_a)$ ha un massimo elemento. Fissiamo una biiezione $f: s(m) \to A$. Allora $|f[m]|=m$, quindi $f[m]$ con l'ordinamento indotto da $<_a$ è isomorfo a $(m, <)$ per ipotesi induttiva, e, in particolare, ha un massimo M. Ora, per la totalità di $<_A$, o $M < f(m)$ oppure $f(m) < M$. Si verifica immediatamente che, nel primo caso, $f(m)$ è il massimo di A, e nel secondo M è il massimo di A.

Stabilito che A ha un massimo N, osserviamo che, detto $A' = A - \{N\}$, siccome $|A'|=m$, usando nuovamente l'ipotesi induttiva abbiamo un isomorfismo $f: A' \to m$ fra A' con l'ordinamento indotto da $<_a$ e $(m, <)$. Si verifica facilmente che

$$f': A \to s(m) \qquad f'(x) = \begin{cases} f(x) & \text{se } x \in A' \\ m & \text{se } x = N \end{cases}$$

è l'isomorfismo cercato. ∎

Possiamo caratterizzare ω in termini delle proprietà del suo ordinamento naturale. Quelle che servono sono le seguenti:

Oss. 1. $(\omega, <)$ è un buon ordine

2. $(\omega, <)$ è illimitato — ossia $\forall x \in \omega \; \exists y \in \omega \; x < y$

3. Ogni $A \subseteq \omega$ superiormente limitato e non vuoto ha un massimo, ossia

$$\forall A \subseteq \omega \left(A \neq \emptyset \wedge \underbrace{(\exists L \in \omega \; \forall x \in A \; x \leq L)}_{\equiv \text{“}A \text{ è superiormente limitato”}} \right) \dots$$

$$\dots \longrightarrow (\exists M \in A \; \forall x \in A \; x \leq M)$$

Dim. 1. è il principio del minimo, e per 2. basta prendere $y = S(x)$. Per 3., osserviamo che, se A è superiormente limitato da $L \in \omega$, allora $A \subseteq S(L)$, quindi A è finito. Siccome A è finito, l'ordinamento totale su A definito da

$$x \preceq y \overset{\text{def.}}{\equiv} y < x$$

è buono, quindi, in particolare, c'è il minimo di A secondo l'ordinamento $\preceq$. Questo è il massimo di A. ∎

Prop. Sia $(A, \preceq)$, con $A \neq \emptyset$, un ordinamento

1. buono
2. illimitato
3. tale che ogni sottoinsieme superiormente limitato e non vuoto di A ha un massimo secondo $\preceq$

Allora $(A, \preceq) \sim (\omega, <)$.

Dimostriamo prima un facile lemma.

Lemma Sia $(A, \prec)$ un ordine, e sia $f : \omega \to A$ tale che

$$\forall n \in \omega \; f(n) \prec f(s(n))$$

Allora f è strettamente crescente, $\forall m, n \in \omega \; m < n \to f(m) \prec f(n)$, e, in particolare, iniettiva.

Dim Consideriamo, per assurdo, $m < n$ tali che $f(m) \not\prec f(n)$, con n minimo. Siccome $0 \leq m < n$, esiste n' tale che $n = s(n')$. O $n' = m$ o $m < n'$. Nel primo caso $f(m) \prec f(s(n')) = f(n)$ contraddicendo $f(m) \not\prec f(n)$. Nel secondo, per la minimalità di n, $f(m) \prec f(n')$, ma $f(n') \prec f(s(n')) = f(n)$, quindi abbiamo di nuovo la contraddizione $f(m) \prec f(n)$. ∎

Dim (proposizione) Costruiamo per ricorsione un isomorfismo f da $(\omega, <)$ a $(A, \prec)$.

$$f(0) = \min_{\prec} A \qquad f(s(n)) = \min_{\prec} \{a \in A \mid f(n) \prec a\}$$

dove $\min_{\prec}$ denota il minimo secondo $\prec$.

Occorre dimostrare, intanto, che f è ben definita.

$f(0)$ è ben definita perché $A \neq \emptyset$, quindi ha un minimo.

Per dire che $f(s(n))$ è ben definita, occorre dire che la funzione $h : A \to A$, $h(x) = \min_{\prec} \{a \in A \mid x \prec a\}$ è ben definita, ossia che $\{a \in A \mid x \prec a\}$ è non vuoto. Ma questo avviene, qualsiasi sia $x \in A$, perché altrimenti A sarebbe limitato da x.

Per come è costruita, e per il lemma, f è crescente, quindi

iniettiva. Di conseguenza, ci basta dimostrare la suriettività. Prendiamo $y \in A$ e cerchiamo x tale che $f(x) = y$.
Se, per ogni $x \in \omega$, avessimo $f(x) \prec y$, allora $f[\omega]$ sarebbe superiormente limitato da y, e tuttavia non avrebbe massimo perché ogni $f(x)$ è $\prec$ di $f(s(x))$. Quindi c'è il minimo $x \in \omega$ tale che $y \preceq f(x)$. Dimostriamo che $f(x) \preceq y$, da cui l'uguaglianza cercata.
Se $x = 0$, allora $f(x)$ è il minimo di A, quindi $f(x) \preceq y \in A$.
Se $x = s(x')$, $f(x') \prec y$ per la minimalità di x, ma allora, $y \in \{a \in A \mid f(x') \prec a\}$ quindi $f(x) = f(s(x')) = \min_{\prec}\{\dots\} \preceq y$ ∎

Tornando alla proposizione iniziale

Prop. Se A è al più numerabile, allora o A è finito o A è numerabile.

Dim Per ipotesi esiste $f : A \to \omega$ iniettiva, per cui abbiamo $|A| = |f[A]|$, e, siccome $f[A] \subseteq \omega$, ci basta dimostrare che dato $B \subseteq \omega$, o B è finito o è numerabile.

Sia $B \subseteq \omega$ infinito, dimostriamo che B, con l'ordinamento indotto dall'ordine naturale di ω, soddisfa le ipotesi della proposizione precedente.
1. e 2. valgono in quanto ogni sottoinsieme di B è, in particolare, sottoinsieme di ω. Per ottenere 3. dobbiamo dire

che $\mathcal{B}$ non ha un massimo elemento. Se, infatti, ci fosse un $M \in \mathcal{B}$ tale che $\forall b \in \mathcal{B}\ b \subseteq M$, allora avremmo che $\mathcal{B} \subseteq \mathcal{S}(M)$. $\mathcal{B}$ sarebbe dunque finito, contro l'ipotesi. ∎

Esercizio Dimostra che se $|A| \leq \aleph_0$ e $f: A \to B$ è una funzione surgettiva allora $|B| \leq \aleph_0$.

Insiemi numerabili in pratica

Sapere che, se $|A| \leq \aleph_0$, allora o A è finito o è numerabile, ci fornisce lo strumento essenziale per dimostrare la numerabilità di molti insiemi concreti. Spesso, infatti, è facile dimostrare che un insieme infinito è tale. Rimane poi da gestire un discorso di disuguaglianze per dire che esso è al più numerabile.
Cominciamo quindi con qualche considerazione generale a proposito delle disuguaglianze fra cardinalità

Oss. Dati A, B, C con $|B| \leq |C|$

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

Vale a dire che le operazioni sulle cardinalità sono monotone, nel senso delle disuguaglianze larghe. Attenzione però che, in generale, NON sono strettamente monotone!

Dim Detta $f : B \to C$ la funzione iniettiva che testimonia che $|B| \leq |C|$ e detto $B' = f[B]$ abbiamo $|B| = |B'|$, quindi basta dimostrare la disuguaglianza associata con B' al posto di B. Ora, giocando sul fatto che $B' \subseteq C$, si vede che queste disuguaglianze rappresentano, in realtà, relazioni di contenimento fra il membro di sinistra e il membro di destra. Per esempio:

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

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

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$|A| + |B'| \qquad\qquad |A| + |C|$$

Le altre si ottengono allo stesso modo. ∎

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

Dim La funzione seguente è iniettiva

$$f : A \cup B \to A \times \{0\} \cup B \times \{1\} \qquad f(x) = \begin{cases} (x,0) & \text{se } x \in A \\ (x,1) & \text{altrimenti} \end{cases}$$

∎

Veniamo ora a calcolare le operazioni aritmetiche. Già sappiamo, per il teorema di Cantor, che $2^{\aleph_0} > \aleph_0$, per cui mettere un $\aleph_0$ a esponente di qualunque cosa non sia uno 0 o un 1 conduce fuori dal numerabile. Tutto il resto invece no.

Prop $\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \aleph_0$ con $n \in \omega \setminus \{0\}$.

Dim Supponiamo di sapere già che $\aleph_0 \cdot \aleph_0 = \aleph_0$, allora possiamo formare la catena di disuguaglianze

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

Da cui, per il teorema di Cantor – Bernstein,

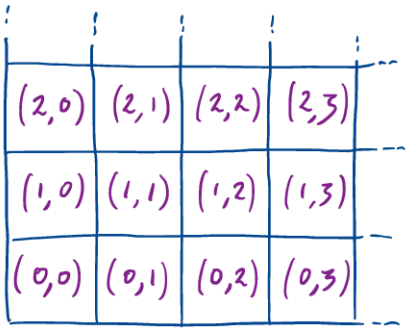
$$\aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$$

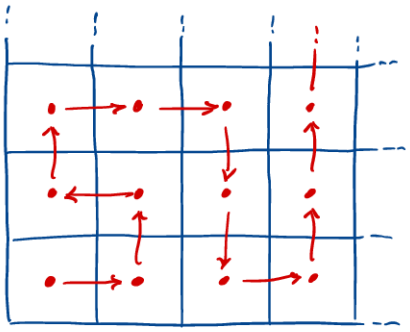
Ora è facile vedere per induzione che $n \in \omega \setminus \{0\} \to \aleph_0^n = \aleph_0$ infatti $\aleph_0^1 = \aleph_0$ e $\aleph_0^{n+1} = \aleph_0^n \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$.

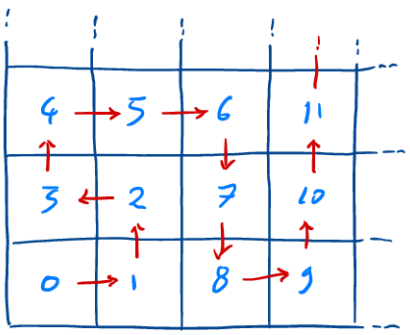
Resta quindi da dimostrare il lemma seguente

Lemma $\aleph_0 \cdot \aleph_0 = \aleph_0$ ossia esiste una bigezione fra $\omega \times \omega$ e ω

Ci sono diverse vie per illustrare questo risultato. Per esempio, possiamo rappresentare le coppie $(x,y) \in \omega \times \omega$ sotto la specie di una griglia a maglie quadrate. Poi disegnamo un percorso che pare visitare tutte le maglie della griglia, con sufficiente apparenza di regolarità, possibilmente, da convincere il lettore che vi debba essere un metodo. Infine numeriamo le maglie secondo l'ordine in cui sono visitate dal percorso. Avremo così numerato tutte le coppie di numeri naturali dal disegno.







Altrimenti, è possibile ossibire delle bigezioni esplicite, per esempio $f(x,y) = 2^x \cdot (2y+1) - 1$ $\quad g(x,y) = \dfrac{(x+y)^2 + 3x + y}{2}$

È possibile scrivere i due numeri della coppia in base 10 a cifre alternate, tipo: $(64, 4096) \mapsto 40009664$
E saranno possibili mille altre scelte, ma noi useremo, invece il tipo d'ordine di ω.

Dim (lemma)

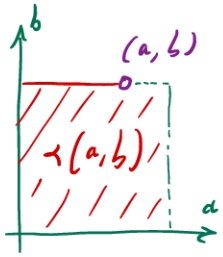
Consideriamo l'ordinamento seguente su $\omega \times \omega$

$(a,b) \prec (a',b') \overset{\text{def.}}{\equiv}$ $\max(a,b) < \max(a',b')$

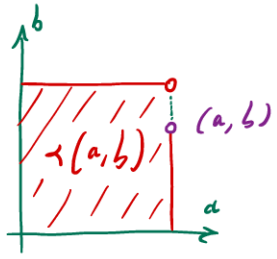
$\vee \left(\max(a,b) = \max(a',b') \wedge a < a' \right)$

$\vee \left(\max(a,b) = \max(a',b') \wedge a = a' \wedge b < b' \right)$

Ossia, per confrontare (a,b) con (a',b'), si confrontano prima



$\max(a,b)$ e $\max(a',b')$; a parità si confrontano a ed a'; se anche queste coincidono, si confrontano b e b'.



L'idea è che, in questo modo, la coppia $\prec$ di una certa (a,b) fissata sono tutte contenute nel quadrato $\{0 \dots \max(a,b)\} \times \{0 \dots \max(a,b)\}$, quindi sono in numero finito, e questo implica che $(\omega \times \omega, \prec)$ è isomorfo a $(\omega, <)$.

Formalmente, iniziamo col verificare che $\prec$ sia effettivamente un ordine stretto. La proprietà irriflessiva è immediata. Per verificare la proprietà transitiva, prendiamo $(a,b) \prec (a',b') \prec (a'',b'')$. Allora $\max(a,b) \leq \max(a',b') \leq \max(a'',b'')$. Se una di queste disuguaglianze è stretta allora $(a,b) \prec (a'',b'')$, altrimenti $\max(a,b) = \max(a',b') = \max(a'',b'')$ e segue dalla definizione che $a \leq a' \leq a''$. Nuovamente, se una disuguaglianza è stretta abbiamo concluso, altrimenti $a = a' = a''$, quindi $b < b' < b''$, da cui $(a,b) \prec (a'',b'')$. Per dire che l'ordine è totale osserviamo che se (a,b) e (a',b') non sono né $\prec$ né $\succ$ allora dobbiamo avere $\max(a,b) = \max(a',b')$, $a = a'$, $b = b'$, quindi $(a,b) = (a',b')$.

Ora vogliamo dire che $(\omega \times \omega, \prec) \sim (\omega, <)$. Partiamo dall'osservazione che se $(a,b) \in \omega \times \omega$ allora

$$(\omega \times \omega)_{(a,b)} \overset{\text{def.}}{\equiv} \{(x,y) \in \omega \times \omega \mid (x,y) \prec (a,b)\}$$

detto "il segmento iniziale determinato da (a,b) su $(\omega \times \omega, \prec)$" è finito. Infatti $(\omega \times \omega)_{(a,b)} \subseteq S(\max(a,b)) \times S(\max(a,b))$. Ci serve dire 1. $(\omega \times \omega, \prec)$ è ben ordinato. 2. $(\omega \times \omega, \prec)$ è illimitato 3. ogni sottoinsieme non vuoto e superiormente limitato di $\omega \times \omega$ ha un massimo.

1. Dato $A \subseteq \omega \times \omega$ con $A \neq \emptyset$, consideriamo $a \in A$. Se $(\omega \times \omega)_a \cap A = \emptyset$ allora a è il minimo di A. Altrimenti $A' = (\omega \times \omega)_a \cap A$

è non vuoto e finito, quindi ha minimo m. Questo deve essere anche il minimo di A, perché se $x \in A \setminus A'$ allora $m \prec a \preceq x$.

2. Dato $(a,b) \in \omega \times \omega$, $(a,b) \prec (s(a), s(b))$.
3. Dato $A \subseteq \omega \times \omega$ non vuoto e superiormente limitato da $(a,b) \in \omega \times \omega$, abbiamo che $A \subseteq (\omega \times \omega)_{(a+1, b+1)}$ è finito, quindi ammette massimo perché l'ordine $\prec$ è totale. ∎

Usando la proposizione appena dimostrata, potremmo dimostrare, per esempio, che $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili, se non fosse che non abbiamo ancora definito questi oggetti. Allo scopo, ricordiamo che — cfr. a pag. 38 delle note — una relazione di equivalenza induce un insieme di classi di equivalenza.

Def. ($\mathbb{Z}$) Definiamo $\mathbb{Z}$ come l'insieme delle classi di equivalenza su $\omega \times \omega$ indotte dalla relazione

$$(a,b) \sim_{\mathbb{Z}} (a',b') \overset{\text{def}}{\iff} a + b' = b + a' \qquad \text{morale: } "(a,b) = a - b"$$

Esercizio Dimostra che $\sim_{\mathbb{Z}}$ è una relazione di equivalenza

Esercizio Definiamo $+$, $-$ e $\cdot$ su $\mathbb{Z}$ mediante

$$[(a,b)]_{\mathbb{Z}} + [(a',b')]_{\mathbb{Z}} \overset{\text{def.}}{=} [(a+a', b+b')]_{\mathbb{Z}}$$

$$-[(a,b)]_{\mathbb{Z}} \overset{\text{def.}}{=} [(b,a)]_{\mathbb{Z}}$$

$$[(a,b)]_{\mathbb{Z}} \cdot [(a',b')]_{\mathbb{Z}} \overset{\text{def.}}{=} [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')]_{\mathbb{Z}}$$

dimostra che $\mathbb{Z}$, con queste operazioni, è un anello commutativo con identità $1 \overset{\text{def.}}{=} [(1,0)]_{\mathbb{Z}}$.

Def. ($\mathbb{Q}$) Definiamo $\mathbb{Q}$ come l'insieme delle classi di equivalenza su $\mathbb{Z} \times (\omega \setminus \{0\})$ indotta dalla relazione

$$(n,d) \sim_{\mathbb{Q}} (n',d') \overset{\text{def.}}{\equiv} n \cdot d' = d \cdot n' \quad \text{morale: } "(n,d) = \tfrac{n}{d}"$$

Esercizio Dimostra che $\sim_{\mathbb{Q}}$ è una relazione di equivalenza

Esercizio Definisci $+, -, \cdot$ e $\square^{-1}$ su $\mathbb{Q}$ nella maniera ragionevole e dimostra che $\mathbb{Q}$ è un campo.

Esercizio Definisci la relazione $<$ su $\mathbb{Q} \times \mathbb{Q}$ dicendo che $q \in \mathbb{Q}$ è positivo se $q = [(n,d)]_{\mathbb{Q}}$, con $n, d \in \omega \setminus \{0\}$, e dicendo che $a < b$ se e solo se $b - a$ è positivo. Dimostra che questo è un ordine totale e denso, cioè

$$\forall a, b \in \mathbb{Q} \quad a < b \to \exists c \in \mathbb{Q} \quad a < b < c.$$

Nota Gli esercizi precedenti sono tediosi, ma non sono difficili. Nel resto del corso daremo per scontate le proprietà aritmetiche elementari di $\mathbb{Z}$ e di $\mathbb{Q}$. D'ora innanzi scriveremo $a - b \overset{\text{def.}}{\equiv} [(a,b)]_{\mathbb{Z}}$ $\quad \frac{n}{d} \overset{\text{def.}}{\equiv} [(n,d)]_{\mathbb{Q}}$.

Per dimostrare la numerabilità di $\mathbb{Z}$ e $\mathbb{Q}$, è comodo richiamare ancora un esercizio, però, questa volta, lo risolviamo.

Esercizio Dimostra che se $|A| \leq \aleph_0$ e $f: A \to B$ è una funzione surgettiva allora $|B| \leq \aleph_0$.

Sol Per ipotesi esiste $g: A \to \omega$ iniettiva, e dobbiamo trovare una $h: B \to \omega$ iniettiva. Poniamo

$$h(b) = \min\left(g\left[\underbrace{\{a \in A \mid f(a) = b\}}_{\text{“}f^{-1}(b)\text{”}}\right]\right)$$

L'insieme fra graffe non è vuoto per la surgettività di f, quindi il minimo è ben definito. Inoltre, se $h(b) = h(b')$, allora $b = g(a)$ e $b' = g(a')$ con a e a' tali che $f(a) = b$ e $f(a') = b'$. Per l'iniettività di g, $a = a'$, quindi $b = f(a) = f(a') = b'$. ∎

Con Un insieme $A \neq \emptyset$ è al più numerabile se e solo se esiste $f: \omega \to A$ surgettiva.

Dim Il se è l'esercizio. Il solo se vale perché se $|A| = \aleph_0$ allora c'è f biiettiva, se $|A| < \aleph_0$ allora c'è $g: n \to A$ biiettiva per qualche $n \in \omega \setminus \{0\}$ e definiamo

$$f(x) = \begin{cases} g(x) & \text{se } x < n \\ g(0) & \text{altrimenti} \end{cases}$$

∎

Notazione Con successione (numerabile) intendiamo semplicemente una funzione con dominio ω, per cui

$$a = \{a_i\}_{i \in \omega} \overset{\text{def.}}{\equiv} a: \omega \to \dots, \quad a: i \longmapsto a_i$$

una enumerazione di A una successione $a = \{a_i\}_{i \in \omega}$ tale che $A = \mathrm{Im}(a)$, ossia, informalmente, $A = \{a_i \mid i \in \omega\}$.

Il corollario dice che $A \neq \emptyset$ è al più numerabile se e solo se ha una enumerazione.

Esempio $\mathbb{Z}$ è numerabile.

Dim La funzione $\omega \times \omega \to \mathbb{Z}$, $(a,b) \mapsto a-b$ è surgettiva per definizione, e $\omega \times \omega$ è numerabile, quindi $|\mathbb{Z}| \leq \aleph_0$.
D'altro canto la funzione $\omega \to \mathbb{Z}$ $n \mapsto n = [(n,0)]_{\mathbb{Z}}$ è iniettiva, quindi $\mathbb{Z}$ è infinito, quindi $|\mathbb{Z}| = \aleph_0$. ∎

Esempio $\mathbb{Q}$ è numerabile.
Come nell'esempio precedente $\mathbb{Z} \times (\omega \setminus \{0\}) \to \mathbb{Q}$, $(n,d) \mapsto \frac{n}{d}$ è surgettiva e $|\mathbb{Z} \times (\omega \setminus \{0\})| = \aleph_0 \cdot \aleph_0 = \aleph_0$. Inoltre $\mathbb{Q}$ è infinito perché $\omega \to \mathbb{Q}$, $n \mapsto \frac{n}{1}$ è iniettiva. ∎

Adesso, ci piacerebbe poter dire che, se abbiamo un insieme A al più numerabile, e tutti i suoi elementi sono, a loro volta, insiemi al più numerabili, allora $\bigcup A$ è al più numerabile. D'altro canto è ragionevole: se esiste una enumerazione $\{a_i\}_{i \in \omega}$ di A, e, per ogni $i \in \omega$, esiste una enumerazione $a_i = \{a_{i,j}\}_{j \in \omega}$ di a_i, allora possiamo mandare surgettivamente $\omega \times \omega$ in A: $(i,j) \mapsto a_{i,j}$, e, siccome $\omega \times \omega$ è al più numerabile, lo è anche A.

L'errore è credere di poter fissare una a_i per ogni $i \in \omega$.

Usando l'assioma della scelta potremo farlo, ma, per ora, non abbiamo modo, in generale, di procurarci la funzione $i \mapsto a_i$. Possiamo però assumere di averla, così si corregge il ragionamento impreciso di prima.

Prop: Sia $A = \{a_i \mid i \in \omega\}$ e sia $\{\alpha_i\}_{i\in\omega}$ una successione di funzioni tali che, per ogni $i \in \omega$, $\alpha_i : \omega \to a_i$ è una enumerazione di a_i. Allora $|\bigcup A| \leq \aleph_0$.

Dim Basta osservare che

$$f : \omega \times \omega \longrightarrow \bigcup A \qquad f : (i, j) \longmapsto \alpha_i(j)$$

è surgettiva. ∎

Notazione Data una funzione $f : I \to S$ definiamo

$$\bigcup_{i\in I} f(i) \overset{def.}{=} \bigcup f[I]$$

Così, per esempio, se $A = \{a_i \mid i \in \omega\}$

$$\bigcup_{i\in\omega} a_i = \bigcup A = \{x \mid \exists i \in \omega \; x \in a_i\}$$

Def. (parti finite)

$$\mathcal{P}^{fin}(A) \overset{def.}{=} \{X \in \mathcal{P}(A) \mid |X| < \aleph_0\}$$

Prop: $|A| \leq \aleph_0 \to |\mathcal{P}^{fin}(A)| \leq \aleph_0$

Dim Il caso $A = \emptyset$ è immediato. Assumiamo $A \neq \emptyset$. Sia

$$\mathcal{P}^{\leq n}(A) \overset{def.}{=} \{X \in \mathcal{P}(A) \mid |X| \leq n\}$$

siccome $\mathcal{P}^{fin}(A)$ è l'unione degli insiemi $\mathcal{P}^{\leq n}(A)$, basta

esibire una successione di enumerazioni a_n di $\mathcal{P}^{\leq n}(A)$.

Fissiamo $f : w \to w \times A$, $f : x \mapsto (f_1(x), f_2(x))$ surgettiva, che esiste perché A è al più numerabile. Costruiamo la successione $\{a_n\}_{n \in w}$ per ricorsione.

Per $n = 0$, $\mathcal{P}^{\leq 0}(A) = \{\emptyset\}$ e a_0 è la costante $\emptyset$.

Per $n = s(m)$

$$a_{s(m)}(x) = \begin{cases} \emptyset & \text{se } x = 0 \\ a_m(f_1(x-1)) \cup \{f_2(x-1)\} & \text{se } x > 0 \end{cases}$$

Dimostriamo per induzione che, per ogni $n \in w$, a_n è surgettiva $w \to \mathcal{P}^{\leq n}(A)$.

caso $n = 0$ Immediato.

caso $n = s(m)$. Per ipotesi induttiva $a_m : w \to \mathcal{P}^{\leq m}(A)$ è surgettiva. Dato $Y \in \mathcal{P}^{\leq s(m)}(A)$ si danno due casi. O $Y = \emptyset$, allora $Y = a_{s(m)}(0)$. Oppure esiste $y \in Y$. In questo caso $|Y \setminus \{y\}| \leq m$, quindi $Y \setminus \{y\} = a_m(t)$ per qualche $t \in w$. Per la surgettività di f, $(t, y) = f(x)$ per qualche $x \in w$. Quindi

$$\begin{aligned} a_{s(m)}(x+1) &= a_m(f_1(x)) \cup \{f_2(x)\} \\ &= (Y \setminus \{y\}) \cup \{y\} = Y. \end{aligned}$$

□

Applicazione Dimostriamo che l'insieme dei numeri reali algebrici $\mathbb{A}_{\mathbb{R}}$ è numerabile. Per questa applicazione, assumiamo le proprietà algebriche elementari di $\mathbb{R}$. L'insieme $\mathbb{A}_{\mathbb{R}}$ è definito come l'insieme degli $x \in \mathbb{R}$ che sono zeri di qualche polinomio non nullo a coefficienti razionali:

$$\mathbb{A}_{\mathbb{R}} \overset{\text{d.f.}}{=} \{ x \in \mathbb{R} \mid \exists p \in \mathbb{Q}[x] \setminus \{0\} \; p(x) = 0 \}$$

I numeri reali che non sono algebrici si dicono trascendenti, siccome — formalmente, vedremo questo risultato in seguito — $\mathbb{R}$ non è numerabile, deduciamo dalla numerabilità di $\mathbb{A}_{\mathbb{R}}$ che ci sono numeri reali trascendenti.

Dimostriamo, intanto, che l'insieme $\mathbb{Q}[x]$, dei polinomi a a coefficienti razionali nella indeterminata x, è numerabile. Possiamo identificare un polinomio

$$p(x) = a_0 + a_1 x^1 + a_2 x^2 + \dots + a_d x^d$$

con l'insieme dei suoi monomi

$$p(x) = \{ a_0, a_1 x^1, a_2 x^2, \dots, a_d x^d \}$$

e ciascun monomio con la coppia (grado, coefficiente)

$$p(x) = \{ (0, a_0), (1, a_1), (2, a_2), \dots, (d, a_d) \}$$

Formalmente, come accade per i numeri, le coppie ordinate, le funzioni, &c., anche i polinomi non sono oggetti atomici della teoria degli insiemi: occorre, in qualche modo, fissare

una codifica. Quella appena descritta è una codifica ragionevole. Rappresentando i polinomi in questo modo

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

per cui $\mathbb{Q}[x]$ è al più numerabile, quindi numerabile perché, per esempio, è elementare immergere $\mathbb{Q}$ in $\mathbb{Q}[x]$.

Venendo ad $\mathbb{A}_{\mathbb{R}}$ abbiamo una facile surgezione

$$f : (\mathbb{Q}[x] \setminus \{0\}) \times \omega \longrightarrow \mathbb{A}_{\mathbb{R}}$$

$$(p, i) \longmapsto \text{"la } i\text{-esima radice di } p \text{ se questa esiste, altrimenti } 0\text{"}$$

Vediamo, però, in maggior dettaglio come si può rappresentare f mediante una formula insiemistica.

"α è la i-esima radice di p" $\equiv$

$$p(\alpha) = 0 \wedge \left|\{x \in \mathbb{R} \mid x \leq \alpha \wedge p(x) = 0\}\right| = |i|$$

$y = f(p,i) \equiv$ "y è la i-esima radice di p"

$$\wedge \left(y = 0 \wedge \neg \exists \alpha \in \mathbb{R} \text{ "}\alpha \text{ è la } i\text{-esima radice di } p\text{"}\right)$$

Per separazione esiste, quindi, f, e, di conseguenza $|\mathbb{A}_{\mathbb{R}}| \leq \aleph_0$.

La disuguaglianza opposta è immediata perché $\mathbb{Q} \subseteq \mathbb{A}_{\mathbb{R}}$ ∎

Esercizio Dato un insieme X, una funzione $f : X^2 \to X$, e un sottoinsieme $A \subseteq X$ al più numerabile, dimostra che esiste un $\bar{A} \subseteq X$ al più numerabile tale che $f[\bar{A} \times \bar{A}] \subseteq \bar{A}$. (Concludi che un gruppo finitamente generato è al più numerabile.)

Ordini densi numerabili

Il prossimo risultato che vedremo è, come al solito, dovuto a Cantor, e caratterizza l'ordine di $\mathbb{Q}$ a meno di isomorfismi.

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

B è denso in $(A, <)$ $\overset{\text{def.}}{\equiv}$ $\forall x, y \in A \quad x < y \to \exists z \in B \quad x < z < y$

$(A, <)$ è denso $\overset{\text{def.}}{\equiv}$ A è denso in se stesso, cioè

$\forall x, y \in A \quad x < y \to \exists z \in A \quad x < z < y$

Esempio Abbiamo già osservato, in un esercizio, che $\mathbb{Q}$ è denso, infatti $x < y \to x < \frac{x+y}{2} < y$.

NON Esempio L'insieme ω con il suo ordinamento naturale non è denso, perché $\nexists z \in \omega \quad 0 < z < 1$.

Teorema (di isomorfismo di Cantor)

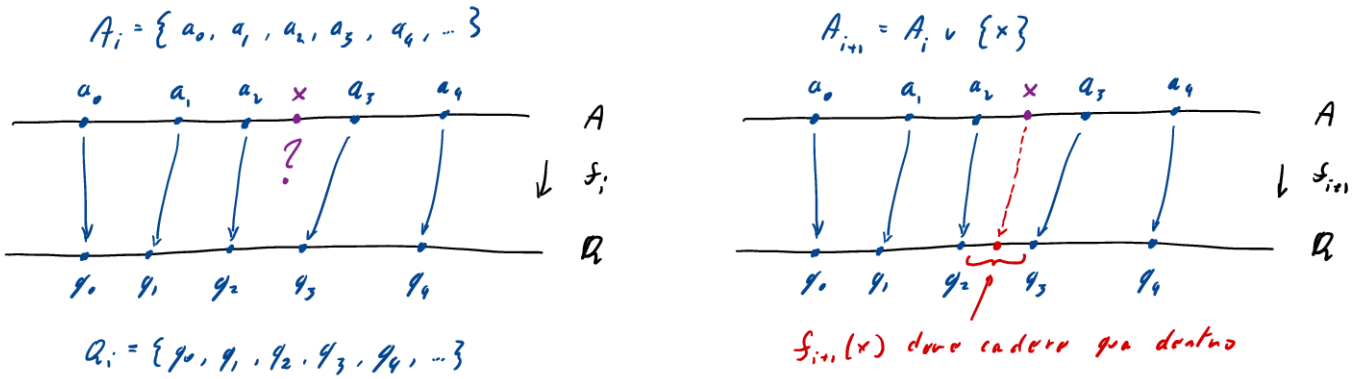
Sia $(A, <)$ un insieme totalmente ordinato tale che

- $|A| = \aleph_0$
- $(A, <)$ è denso
- $(A, <)$ non ha estremi, ossia non ha né massimo né minimo elemento.

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

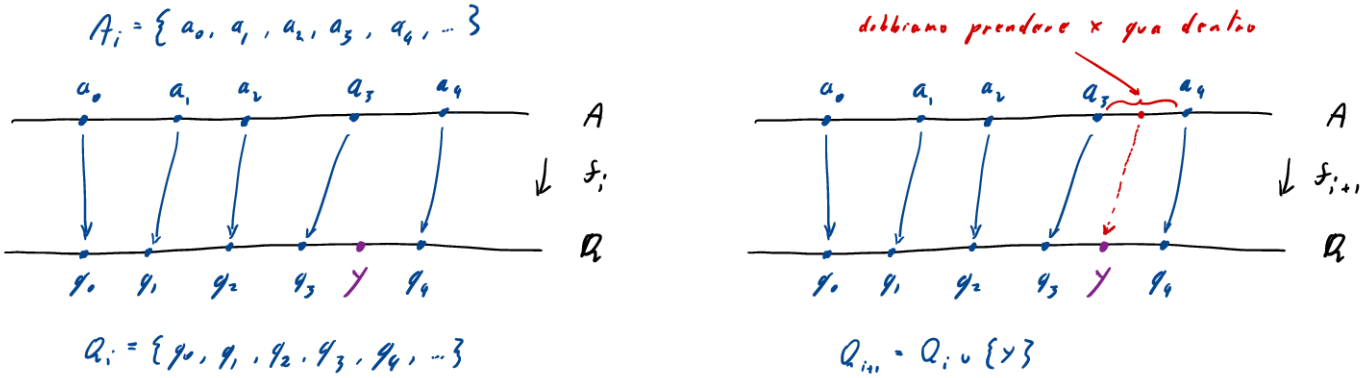
L'idea è di costruire l'isomorfismo per ricorsione. Ad

ogni passo della ricorsione avremo $f_i : A_i \to Q_i$ isomorfismo con $A_i \subseteq A$ finito e $Q_i \subseteq \mathbb{Q}$. Dovremo quindi estendere f_i ingrandendo il suo dominio. Supponiamo, per esempio, di



voler definire $f_{i+1}(x)$ con $x \notin A_i$. Allora, siccome A_i è finito, per sapere la posizione di x rispetto a ciascuno degli elementi di A_i, ci basta sapere quale sia l'ultimo elemento prima di x, e quale sia il primo dopo x — diciamo che, per esempio, sono a_2 e a_3 rispettivamente. Dovremo allora mandare x in un $f_{i+1}(x)$ con $f_i(a_2) < f_{i+1}(x) < f_i(a_3)$, e questo esiste per la densità di $\mathbb{Q}$.

Ragionando simmetricamente, possiamo anche estendere f_i, dato un $y \in \mathbb{Q}$ con $y \notin Q_i$, in modo tale che $y \in \mathrm{Im}(f_{i+1})$.



In definitiva, ci basta quindi fissare un'enumerazione di A e una di $\mathbb{Q}$, e fare questi passi di estensione in maniera alternata, assicurandoci così di aggiungere al dominio della f, uno per uno, tutti gli elementi di A, e di aggiungere all'immagine, uno per uno, tutti gli elementi di $\mathbb{Q}$.
Ci sarà comodo la seguente osservazione.

Oss. 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: $\bigcup \{Dom\, f \mid f \in F\} \to B$.

Dim Bisogna verificare che, se $(x, y_1) \in \bigcup F$ e $(x, y_2) \in \bigcup F$, allora $y_1 = y_2$. Dalla prima abbiamo che esiste $f_1 \in F$ con $y_1 = f_1(x)$ e dalla seconda abbiamo che esiste $f_2 \in F$ con $y_2 = f_2(x)$, ma quindi $x \in Dom(f_1) \cap Dom(f_2)$ e, per ipotesi, $y_1 = f_1(x) = f_2(x) = y_2$. ∎

Dim (Teorema)
Fissiamo due enumerazioni di A e $\mathbb{Q}$ rispettivamente

$$A = \{a_i \mid i \in \omega\} \qquad \mathbb{Q} = \{q_i \mid i \in \omega\}$$

Intendiamo costruire una successione di funzioni $\{f_i\}_{i \in \omega}$ tali che, per ogni $i \in \omega$

1. $f_i : A_i \to \mathbb{Q}_i$ con $|A_i| = |\mathbb{Q}_i| < \aleph_0$
2. f_i è un isomorfismo di ordini fra A_i e $\mathbb{Q}_i$

3. $f_i \subseteq f_{s(i)}$ ossia f_{i+1} estende f_i

4. $\forall j<i \quad a_j \in A_i \wedge q_j \in Q_i$ ossia $\{a_0 \dots a_{i-1}\} \subseteq Dom(f_i)$

$\{q_0 \dots q_{i-1}\} \subseteq Im(f_i)$

Verifichiamo, per cominciare, che da 1...4 segue che $f \overset{def}{=} \bigcup_{i \in \omega} f_i$ è un isomorfismo di ordini fra A e Q. Da 3. segue, con una facile induzione, che $\forall i,j \in \omega \; i \leq j \to f_i \subseteq f_j$. Quindi siamo nella situazione dell'osservazione, e, di conseguenza, f è una funzione. Inoltre 4. implica che $Dom(f) = A$ e $Im(f) = Q$.

Ci resta quindi da verificare che, date $x, y \in A$,

$$x < y \iff f(x) < f(y)$$

Siccome $\{a_i\}_{i \in \omega}$ enumera A, esistono $m, n \in \omega$ tali che $x = a_m$ $y = a_n$. Preso $t \in \omega$ con $m, n < t$, per la 4., $a_m, a_n \in Dom(f_t)$, e, siccome f_t è un isomorfismo di ordini per la 2., abbiamo

$$x = a_m < a_n = y \iff f(x) = f_t(a_m) < f_t(a_n) = f(y).$$

Descriviamo ora la costruzione per ricorsione numerabile della successione di funzioni f_i. Intanto poniamo $f_0 = \emptyset$.

Per costruire $f_{s(i)}$ definiamo prima un passo intermedio $f_{i+0.5}$:

Se $a_i \in Dom(f_i)$ allora $f_{i+0.5} = f_i$ ossia è strettamente crescente

Altrimenti sia $\bar{j} = \min \{ j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un iso.} \}$,

poniamo $f_{i+0.5} = f_i \cup \{(a_i, q_{\bar{j}})\}$

Ora definiamo $f_{s(i)}$

Se $q_i \in Im(f_{i+0.5})$ allora $f_{s(i)} = f_{i+0.5}$

Altrimenti: sia $\bar{l} = \min \{ l \in \omega \mid f_{i+0.5} \cup \{(a_l, q_i)\} \text{ è un iso} \}$

poniamo $f_{s(i)} = f_{i+0.5} \cup \{(a_{\bar{l}}, q_i)\}$

Le proprietà 1..4 seguono in maniera immediata per induzione, a patto che la costruzione sia ben posta, ossia i minimi esistano. Ad essere precisi, occorre quindi dimostrare, per induzione su i, la proposizione

$\forall i \in \omega$ "la costruzione di f_i è ben posta e valgono 1..4"

Vediamo che esiste il minimo nel primo passaggio:

$$\bar{j} = \min \{ j \in \omega \mid f_i \cup \{(a_i, q_j)\} \text{ è un iso.} \}$$

ossia che l'insieme di cui si prende il minimo non è vuoto. Il secondo caso è analogo. Per ipotesi induttiva A_i è finito. Se $A_i = \emptyset$ non c'è niente da dimostrare, altrimenti, detto $n = |A_i|$, e sfruttando il fatto che un ordine totale finito è isomorfo ad un numero naturale

$$A_i = \{ a_0, \dots, a_{n-1} \} \qquad \text{con} \qquad a_0 < \dots < a_{n-1}$$

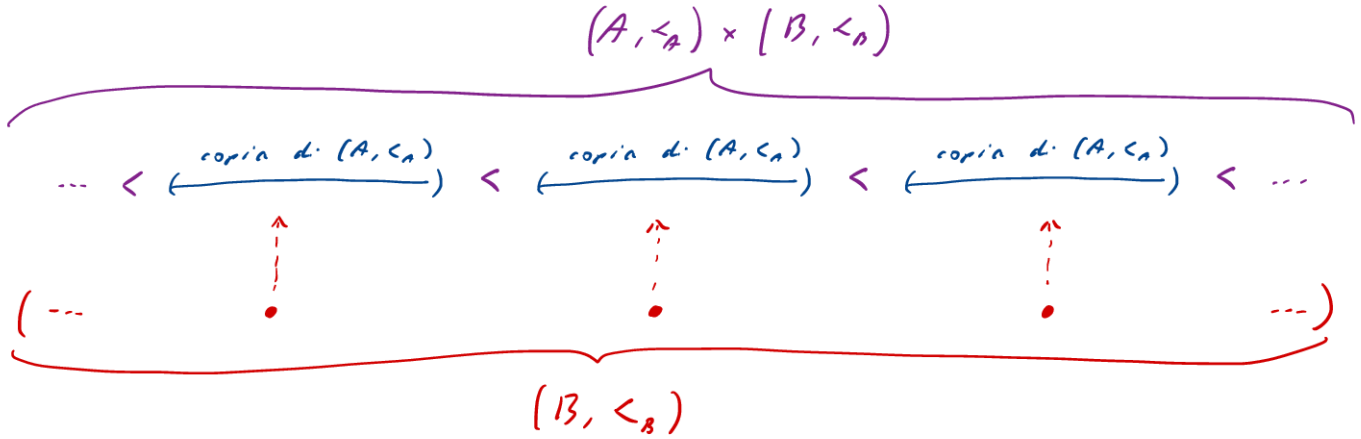
Ora, l'ipotesi è che $a_i \notin A_i$ quindi o $a_i < a_0$, o $a_k < a_i < a_{k+1}$ per qualche k, o $a_{n-1} < a_i$. Nel primo e nel terzo caso, rispettivamente, siccome $\mathbb{Q}$ non ha estremi, c'è un $q_j < f_i(a_0)$, o $q_j > f_i(a_n)$ rispettivamente. Nel secondo caso, per la densità di $\mathbb{Q}$, esiste q_j con $f_i(a_k) < q_j < f_i(a_{k+1})$. ∎

Cor Sia $(A, <)$ un ordine totale con $|A| \leq \aleph_0$.
Allora esiste $B \subseteq \mathbb{Q}$ tale che $(A, <) \sim (B, <)$ con l'ordinamento indotto su B da $\mathbb{Q}$.

Nota: Volendo, si potrebbe dimostrare questo corollario ripetendo, con qualche variazione, la dimostrazione del teorema. Ora daremo, però, un argomento che, invece, applica il teorema.
È comodo definire, prima, il prodotto di ordini.

Def (prodotto lessicografico di ordini)
Dati $(A, <_A)$ e $(B, <_B)$ definiamo $(A, <_A) \times (B, <_B) \overset{\text{def}}{\equiv} (A \times B, <_{A\times B})$
dove $(a, b) <_{A\times B} (a', b') \overset{\text{def}}{\equiv} b <_B b' \vee [b = b' \wedge a <_A a']$.

Ossia: $(A, <_A) \times (B, <_B)$ è il prodotto cartesiano $A \times B$ munito dell'ordine che CONFRONTA PRIMA LA SECONDA COMPONENTE.
Visualmente, si può immaginare $(A, <_A) \times (B, <_B)$ come "$(A, <_A)$ ripetuto $(B, <_B)$ volte"



Oss Il prodotto è un ordine. Inoltre se $(A, <_A)$ e $(B, <_B)$ sono ordini totali, allora anche $(A, <_A) \times (B, <_B)$ lo è.

Esercizio Dati $(A, <_A)$, $(B, <_B)$ e $(C, <_C)$ dimostrare che

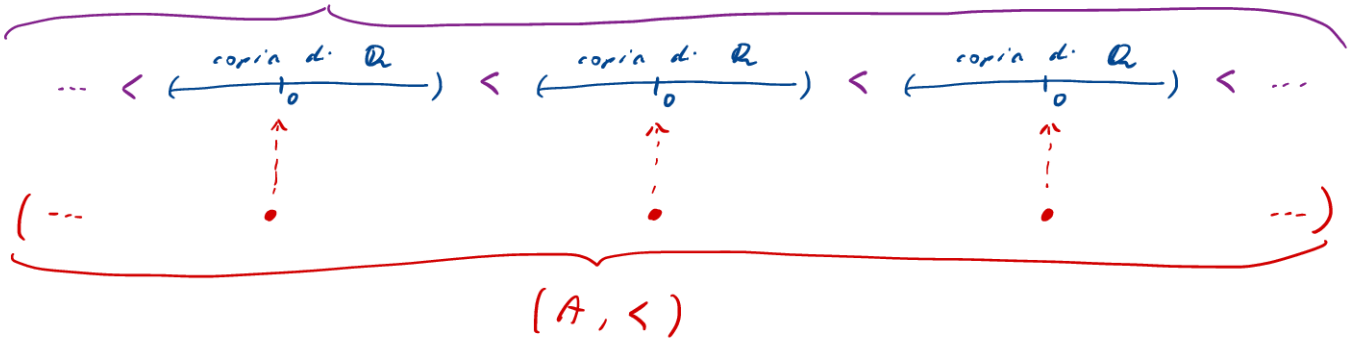
$$\big((A, <_A) \times (B, <_B)\big) \times (C, <_C) \sim (A, <_A) \times \big((B, <_B) \times (C, <_C)\big)$$

ossia che il prodotto di ordini è associativo a meno di isomorfismi.

Dim (corollario)

Il caso $A = \emptyset$ è banale. Supponiamo $A \neq \emptyset$ e consideriamo

$$(S, <) \overset{\text{def.}}{=} (\mathbb{Q}, <) \times (A, <)$$



$S = \mathbb{Q} \times A$ è numerabile. Inoltre, dato $(q, a) \in \mathbb{Q} \times A$ abbiamo $(q-1, a) < (q, a) < (q+1, a)$, quindi $\mathbb{Q} \times A$ non ha estremi. Per verificare che è denso, consideriamo $(q_1, a_1) < (q_2, a_2)$

Se $a_1 < a_2$, allora $(q_1, a_1) < (q_1 + 1, a_1) < (q_2, a_2)$

Se $a_1 = a_2$, allora $(q_1, a_1) < \left(\frac{q_1 + q_2}{2}, a_1\right) < (q_2, a_1) = (q_2, a_2)$. ∎

Esercizio Dimostra che se $(A, <)$ è denso e $2 \leq |A| \leq \aleph_0$, allora $(A, <)$ è isomorfo a uno dei seguenti intervalli di $\mathbb{Q}$.

$$[0, 1]_{\mathbb{Q}} \qquad]0, 1]_{\mathbb{Q}} \qquad [0, 1[_{\mathbb{Q}} \qquad]0, 1[_{\mathbb{Q}}$$

La tecnica di estendere indefinitamente isomorfismi parziali che ci ha permesso di dimostrare il teorema di isomorfismo

di Cantor si chiama back-and-forth, ed è un metodo fondamentale per trovare isomorfismi fra strutture.
Colgo questa occasione per suggerirne un esercizio di applicazione della medesima tecnica che è un po' complicato. Si tratta di definire il grafo random o grafo di Rado.

Def (grafo)
Un grafo (V, e) sull'insieme di vertici V è dato da una relazione e simmetrica e irriflessiva.

$$\forall x,y \in V \ (x,y) \in e \leftrightarrow (y,x) \in e \qquad \forall x \in V \ (x,x) \notin e$$

L'idea è che V può essere immaginato come un insieme di punti che possono essere connessi da archi. C'è un arco fra x e y se $(x,y) \in e$.

Partiamo da un'idea intuitiva — chi ha già seguito un corso di probabilità saprà formalizzare questa cosa in termini precisi. Data una probabilità $p \in]0,1[$ costruiamo un grafo G_p con insieme di vertici ω come segue. Per ogni coppia $(i,j) \in \omega \times \omega$ con $i<j$ lanciamo una moneta che fa testa con probabilità p — tutte queste monete indipendenti — e, se viene testa, mettiamo un arco fra i e j.

Potremmo pensare che i grafi $G_{0.01}$ e $G_{0.99}$ debbano venire molto diversi: uno ha l'1% degli archi possibili, l'altro

ha il 99%, insomma uno è quasi vuoto, l'altro quasi completo. Avviene, tuttavia, che, con probabilità 1, questi grafi sono isomorfi, dove, per essere precisi:

Def I grafi (V_1, e_1) e (V_2, e_2) sono *isomorfi* se esiste una biiezione $f: V_1 \to V_2$ tale che

$$\forall v, w \in V_1 \quad (v,w) \in e_1 \longleftrightarrow (f(v), f(w)) \in e_2$$

Vediamo perché: Dati due sottoinsiemi finiti X e Y di ω, e dato un vertice $v \notin X \cup Y$ la probabilità che v sia connesso da un arco a tutti i vertici di X e a nessuno di quelli di Y è $p^{|X|} \cdot (1-p)^{|Y|}$ — come che sia, è un certo numero >0 — e ci sono infiniti $v \notin X \cup Y$. Si capisce, quindi, che con probabilità 1 — ossia certamente — almeno uno di questi vincerà questa lotteria, ossia sarà connesso a tutti gli X e a nessuno degli Y. Usiamo l'esistenza di questo v per definire un grafo random.

Def Il grafo (ω, e) è un grafo random se

$$\forall X \subseteq \omega \; \forall Y \subseteq \omega \setminus X \; \exists v \in \omega \setminus (X \cup Y) \; \underbrace{X \times \{v\} \subseteq e}_{\forall x \in X \; (x,v) \in e} \wedge \underbrace{(Y \times \{v\}) \cap e = \emptyset}_{\neg \exists y \in Y \; (y,v) \in e}$$

Esercizio Dimostra che esiste un grafo random, ed è unico a meno di isomorfismi.

$\mathbb{R}$ e la cardinalità del continuo

In questa sezione daremo una definizione di $\mathbb{R}$ come insieme ordinato. Estenderemo, poi, la definizione ad includere le operazioni di campo, ma senza svolgere verifiche.

Definizioni
Sia $(A, <)$ un ordine totale.

- $m \in A$ è un *maggiorante* di $B \subseteq A$ se $\forall x \in B \; x \leq m$
- $B \subseteq A$ è *superiormente limitato* se ha un maggiorante
- $s \in A$ è l'*estremo superiore* di B — denotato $\sup B$ — se s è il minimo dei maggioranti di B.

Nota Non sempre gli estremi superiori esistono, e, se B ha un estremo superiore, questo è unico.

Def. Un ordine totale $(A, <)$ è *completo* se ogni $B \subseteq A$ superiormente limitato ha un estremo superiore $\sup B \in A$.

Esercizio Dimostra, usando solo le proprietà di $\mathbb{Q}$, che l'insieme $\{x \in \mathbb{Q} \mid x^2 < 2\}$ NON ha un estremo superiore in $\mathbb{Q}$.

In conseguenza dell'esercizio, possiamo dire che $\mathbb{Q}$ non è completo. Costruiamo ora un ordine completo $(\mathbb{R}, <)$ che contiene una copia isomorfa di $\mathbb{Q}$ come sottoinsieme denso.

Def. Sia $(A, <)$ un ordine totale. $B \subseteq A$ è un *segmento iniziale* di A se $\forall x \in B \; \forall y \in A \; y < x \to y \in B$.

Ossia B è un segmento iniziale di A se, ogniqualvolta B contiene un elemento, B contiene altresì tutti gli elementi minori di questo.

Un segmento iniziale B di A si dice *proprio* se $B \neq A$.

Esempi Dato $(A, <)$ ordine totale, A stesso e $\emptyset$ sono segmenti iniziali di A. Dato $x \in A$, l'insieme

$$A_x \overset{\text{def.}}{=} \{y \in A \mid y < x\}$$

è un segmento iniziale proprio di A — detto segmento iniziale *principale* determinato da x.

L'insieme $\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}$ è un segmento iniziale di $\mathbb{Q}$ che non è principale.

Nota: Useremo nuovamente il concetto di segmento iniziale studiando gli ordinali. Il prossimo concetto, quello di sezione di Dedekind, invece, ci serve unicamente per definire $\mathbb{R}$.

Def (Sezioni di Dedekind)

Una *sezione* sull'insieme totalmente ordinato $(A, <)$ è un segmento iniziale *proprio* e *non vuoto* di A che *non ha un maggiore* elemento. Ossia B segmento iniziale di A è una sezione se $B \neq A$, $B \neq \emptyset$ e $\forall x \in B \; \exists y \in B \; x < y$.

Def (di $\mathbb{R}$ come insieme ordinato)

$$\mathbb{R} \overset{\text{def.}}{\equiv} \{x \in \mathcal{P}(\mathbb{Q}) \mid x \text{ è una sezione su } \mathbb{Q}\}$$

Dati $x, y \in \mathbb{R}$

$$x \leq y \overset{\text{def.}}{\equiv} x \subseteq y$$

Prop. $(\mathbb{R}, <)$ è un ordine totale completo.

Prima della dimostrazione, isoliamo un semplice lemma.

Lemma Sia $(A, <)$ un ordine totale e X un insieme di segmenti iniziali di A. Allora $\bigcup X$ è un segmento iniziale di A.

Dim Sia $\alpha \in \bigcup X$ e $\beta \in A$ con $\beta < \alpha$. Dobbiamo dimostrare che $\beta \in \bigcup X$. Siccome $\alpha \in \bigcup X$, esiste $x \in X$ con $\alpha \in x$. Siccome x è segmento iniziale A, $\beta \in x \subseteq \bigcup X$. ∎

Dim (Prop.) Abbiamo un ordine parziale perché il contenimento, $\subseteq$, è un ordine parziale su $\mathcal{P}$(quello che sia). Supponiamo, per assurdo, che non sia totale, allora esistono $x, y \in \mathbb{R}$ con $x \not\subseteq y$ e $y \not\subseteq x$, per cui ci sono $a \in x \setminus y$ e $b \in y \setminus x$. Ora si danno due casi: se $a < b$ allora $b \in y \Rightarrow a \in y$ ~~↯~~ simmetricamente, se $b < a$ allora $a \in x \Rightarrow b \in x$ ~~↯~~

Resta da dimostrare la completezza. Sia $A \in \mathbb{R}$ non vuoto e superiormente limitato da $m \in \mathbb{R}$.

Dimostriamo che $\sup A = \bigcup A \in \mathbb{R}$.

Per il lemma, $\bigcup A$ è un segmento iniziale, siccome A non è vuoto $\bigcup A \neq \emptyset$, siccome m è un maggiorante di A, $\bigcup A \subseteq m$, quindi $\bigcup A \neq A$. In definitiva $\bigcup A$ è una sezione, e, di conseguenza, un elemento di $\mathbb{R}$.

Verifichiamo che $\bigcup A$ è un maggiorante di A. Se $x \in A$, allora $x \subseteq \bigcup A$, cioè, appunto $x \leq \bigcup A$.

Ora, se m è un maggiorante di A, allora $\forall x \in A \; x \subseteq m$, ma questo equivale a $\bigcup A \subseteq m$, quindi $\bigcup A$ è il minimo dei maggioranti di A. ∎

Oss. La funzione $\iota : \mathbb{Q} \to \mathbb{R}$ $\iota(a) = \mathbb{Q}_a = \{x \in \mathbb{Q} \mid x < a\}$ immerge $\mathbb{Q}$ in $\mathbb{R}$ in maniera strettamente crescente e densa. (Ossia $\mathrm{Im}(\iota)$ è densa in $\mathbb{R}$)

Dim. Dati $a, b \in \mathbb{Q}$ con $a < b$, abbiamo $\mathbb{Q}_a \subsetneq \mathbb{Q}_b$, quindi ι è strettamente crescente. Dati $x, y \in \mathbb{R}$ con $x < y$, per definizione $x \subsetneq y$, quindi esiste $a \in y \setminus x$. Siccome y non ha massimo, c'è un $b \in y$ con $a < b$. Ora $x \subsetneq \mathbb{Q}_b \subsetneq y$.

$a \notin x$ $a \in \mathbb{Q}_b$ $b \notin \mathbb{Q}_b$ $b \in y$ ∎

Notazione (abuso di) Siccome le immersioni

$$\omega \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$$

sono tutte iniettive e crescenti, quando non c'è pericolo di confusione, possiamo abusare della notazione immaginando che

questo siano vere e proprie inclusioni

$$\omega \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

In realtà non è vero: per esempio è $\iota[\mathbb{Q}]$, non $\mathbb{Q}$, ad essere sottoinsieme di $\mathbb{R}$, ma $\iota[\mathbb{Q}]$ è in corrispondenza biunivoca, in maniera canonica, tramite appunto ι, con $\mathbb{Q}$, e questa corrispondenza preserva tutta la struttura rilevante — l'ordine, come abbiamo verificato, ma anche le operazioni di campo.

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

Dim Per l'osservazione $\aleph_0 \leq |\mathbb{R}|$, inoltre $\mathbb{Q}$ è denso in $\mathbb{R}$, quindi $\mathbb{R}$ è denso. Si vede facilmente che $\mathbb{R}$ non ha massimo né minimo, quindi se $\mathbb{R}$ fosse numerabile sarebbe isomorfo a $\mathbb{Q}$. D'altro canto $\mathbb{R}$ è completo e $\mathbb{Q}$ no, quindi non possono essere isomorfi. ∎

Abbiamo stabilito che $(\mathbb{R}, <)$ è un ordine completo senza estremi con un sottoinsieme, $\mathbb{Q}$, denso e numerabile. Queste proprietà, a loro volta, caratterizzano l'insieme ordinato $(\mathbb{R}, <)$ a meno di isomorfismi.

Prop Sia $(A, <)$ un ordine totale completo senza estremi, supponiamo che esista $B \subseteq A$ numerabile e denso in A, allora $(A, <)$ è isomorfo a $(\mathbb{R}, <)$.

Dim Sia $\tilde{A}$ l'insieme delle sezioni su B. Osserviamo, inizialmente, che $(A, \leq) \sim (\tilde{A}, \subseteq)$. L'isomorfismo è infatti dato da

$$f : A \to \tilde{A} \qquad f(a) = B_a = \{x \in B \mid x < a\}$$

la cui inversa è

$$g : \tilde{A} \to A \qquad g(Y) = \sup Y$$

Verifichiamo: a è un maggiorante di B_a, ed è il minimo perché se $x < a$, per la densità di B, esiste $y \in B$ con $x < y < a$, quindi $y \in B_a$, e $x < y$ non può essere un maggiorante di B_a. Quindi $\sup B_a = a$ ossia $g(f(a)) = a$. Per ottenere la composizione opposta, $B_{\sup Y} = Y$, dimostriamo che $x \in B_{\sup Y} \leftrightarrow x \in Y$. Per costruzione, dato $x \in B$, $x \in B_{\sup Y} \Leftrightarrow x < \sup Y$. Ora, $x \in Y \to x \leq \sup Y$ perché $\sup Y$ è un maggiorante di Y, ma non può valere $x = \sup Y$ perché, per definizione di sezione, Y non ha un massimo. Per ottenere la freccia opposta, assumiamo $x < \sup Y$, allora x non può essere un maggiorante di Y — perché $\sup Y$ è il minimo di questi e $x < \sup Y$ — quindi esiste $y \in Y$ con $x < y$, ma Y è un segmento iniziale, quindi $x \in Y$.

Ora, per il teorema di Cantor, B con l'ordine indotto da $(A, <)$ è isomorfo a $\mathbb{Q}$, quindi le sezioni di B sono isomorfe alle sezioni di $\mathbb{Q}$, ossia $(\tilde{A}, \subseteq) \sim (\mathbb{R}, \leq)$. ∎

Per completezza, definiamo ora la struttura di campo di $\mathbb{R}$. Non verificheremo le proprietà, e neanche la correttezza di queste definizioni.

Def $(F, 0, 1, +, \cdot, <)$ è un campo ordinato se

- $(F, 0, 1, +, \cdot)$ è un campo
- $(F, <)$ è un ordine totale
- $\forall x,y,z \in F \quad x < y \to x + z < y + z$
- $\forall x,y \in F \quad (0 < x \wedge 0 < y) \to 0 < x \cdot y$

} l'ordine è compatibile con le operazioni

Def. (somma su $\mathbb{R}$)

Dati $x, y \subseteq \mathbb{R}$ $\quad x + y \overset{\text{def.}}{=} \{a + b \mid a \in x \wedge b \in y\}$

Dati $x, y \in \mathbb{R}$ con $x > 0$ e $y > 0$

$x \cdot y \overset{\text{def}}{=} \{q \in \mathbb{Q} \mid q \leq 0\} \cup \{a \cdot b \mid a \in x \wedge b \in y \wedge a > 0 \wedge b > 0\}$

Definiamo quindi $-x$ tramite l'inverso additivo ed il prodotto nei casi $x < 0$, $y > 0$ &c. tramite la regola dei segni.

Teo $\mathbb{R}$, dotato delle operazioni appena definite, è l'unico campo ordinato completo a meno di isomorfismi.

La dimostrazione di questo teorema, talvolta, si vede nei corsi di analisi 1, noi non la studieremo. Per chi fosse interessato: LIBRO DI TOSTO, cap. 10; NOTE DEL PROFESSOR DI NASSO, fascicolo 6; LEZIONE 16 DELL'A.A. 2020–21.

Torniamo ad una questione più strettamente insiemistica

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

Questo teorema ci dice, in un modo ancora diverso, che $\mathbb{R}$ è più che numerabile — poiché $\aleph_0 < 2^{\aleph_0}$ — ma, in più, caratterizza anche esattamente la cardinalità di $\mathbb{R}$.

Prima della dimostrazione formale, vediamo intuitivamente perché il risultato è vero. Per definizione, $\mathbb{R} \subseteq \mathcal{P}(\mathbb{R})$, quindi la disuguaglianza da dimostrare è $2^{\aleph_0} \leq |\mathbb{R}|$.
Esibiamo una funzione iniettiva $\mathcal{P}(\omega) \to \mathbb{R}$.

$$f : \mathcal{P}(\omega) \to \mathbb{R} \qquad f(S) = 0.a_0^S a_1^S a_2^S a_3^S \dots$$ (scrittura decimale)

$$\text{con } a_i^S = \begin{cases} 0 & \text{se } i \notin S \\ 1 & \text{se } i \in S \end{cases}$$

Per esempio $S = \{2, 3, 5, 7, 11, \dots\}$

$$\to f(S) = 0.001101010001\dots$$

È chiaro che

$$f(S) = f(T) \iff \forall i \in \omega \; a_i^S = a_i^T \iff \forall i \in \omega \; i \in S \leftrightarrow i \in T \iff S = T$$

Non è difficile formalizzare questa dimostrazione. Bisognerebbe definire $0.a_1 a_2 a_3 \dots$ come $\sum_{i=0}^{\infty} a_i 10^{-i}$, poi $\sum_{i=0}^{\infty}$ come $\sup\{\sum_{i=0}^{n}\}$, poi $\sum_{i=0}^{n}$ per ricorsione numerabile, poi dimostrare le proprietà aritmetiche rilevanti. Noi sfrutteremo la stessa idea, ma formulando la dimostrazione in termini di ordini.

Prima di dimostrare il teorema, sviluppiamo un po' di aritmetica della cardinalità $2^{\aleph_0}$. Questi lemmi sono importanti, e serviranno per calcolare la cardinalità di insiemi concreti.

Oss. $\left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0}$

Dim $\left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$

Lemma Siano α, β o "finito" o $\aleph_0$ o $2^{\aleph_0}$ allora

$$\alpha + \beta = \alpha \cdot \beta = \max(\alpha, \beta)$$

eccetto il caso $\alpha \cdot 0 = 0 \cdot \beta = 0$.

Dim Somme e prodotti di cardinalità finite sono finite.

Supponiamo quindi $\aleph_0 \leq \beta$ e, senza perdita di generalità, $\alpha < \beta$. Abbiamo:

$$\beta \leq \begin{matrix} \alpha+\beta \\ \alpha\cdot\beta \end{matrix} \leq \beta^2 = \beta$$

Dove l'ultima uguaglianza vale perché sia $\aleph_0^2 = \aleph_0$, sia $2^{\aleph_0} \leq \left(2^{\aleph_0}\right)^2 \leq \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0}$. ∎

Lemma Se $2 \leq \alpha \leq 2^{\aleph_0}$ allora $\alpha^{\aleph_0} = 2^{\aleph_0}$.

Dim. $2^{\aleph_0} \leq \alpha^{\aleph_0} \leq \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0}$ ∎

Ricordiamo un'osservazione riguardo al numerabile

Oss. Sia $|A| = \aleph_0$ e $B \subseteq A$ con $|B| < \aleph_0$. Allora $|A \setminus B| = \aleph_0$.

Dim Siccome $A \setminus B \subseteq A$, o $|A \setminus B| = \aleph_0$ o $|A \setminus B| < \aleph_0$. Se valesse la seconda $A = B \cup (A \setminus B)$ sarebbe unione di finiti, quindi finito. ∎

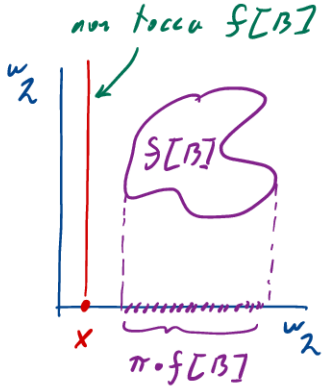
Vale una proposizione analoga per $2^{\aleph_0}$.

Lemma Sia $|A| = 2^{\aleph_0}$ e $B \subseteq A$ con $|B| \leq \aleph_0$. Allora $|A \setminus B| = 2^{\aleph_0}$.

Nota Varrebbe anche rimpiazzando questo con $< 2^{\aleph_0}$, però, per ora, possiamo dimostrare solo l'asserto più debole qua sopra.

Dim Chiaramente $|A \setminus B| \leq |A| = 2^{\aleph_0}$, basta quindi dimostrare $2^{\aleph_0} \leq |A \setminus B|$. Siccome $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$, esiste una bigezione

$$f : A \longrightarrow \omega_2 \times \omega_2$$



Sia $\pi : \omega_2 \times \omega_2 \longrightarrow \omega_2$, $\pi(x,y) = x$.

Siccome B è al più numerabile

$$|\pi \circ f[B]| \leq \aleph_0 < 2^{\aleph_0}$$

Quindi, in particolare $\pi \circ f[B] \neq \omega_2$

Prendiamo $x \in \omega_2 \setminus \pi \circ f[B]$. Dire che $x \notin \pi \circ f[B]$ significa che $(\{x\} \times \omega_2) \cap f[B] = \emptyset$. Quindi $f^{-1}(\{x\} \times \omega_2) \cap B = \emptyset$, ossia $f^{-1}(\{x\} \times \omega_2) \subseteq A \setminus B$, da cui $|f^{-1}(\{x\} \times \omega_2)| \leq |A \setminus B|$.

Usando il fatto che f è biunivoca

$$|f^{-1}(\{x\} \times \omega_2)| = |\{x\} \times \omega_2| = 1 \cdot 2^{\aleph_0} = 2^{\aleph_0}.$$

■

Dim ($|\mathbb{R}| = 2^{\aleph_0}$)

Siccome $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, la disuguaglianza $|\mathbb{R}| \leq 2^{\aleph_0}$ è immediata. Per dimostrare la disuguaglianza opposta definiamo

$$A \overset{\text{def.}}{=} \{ X \in \mathcal{P}(\omega) \mid X \neq \emptyset \wedge |\omega \setminus X| \geq \aleph_0 \}$$

ossia i sottoinsiemi di ω non vuoti e co-infiniti.

Intuitivamente, $X \in A$ rappresenta lo sviluppo in notazione binaria di un $x \in]0,1[$ — $x = 0.a_1 a_2 a_3 \ldots$ $a_i = 1 \leftrightarrow i \in X$ — la condizione $X \neq \emptyset$ serve a escludere lo 0, la condizione di co-infinitezza a escludere l'uno periodico.

Ci basta dimostrare che $|A| = 2^{\aleph_0}$ e che esiste $f : A \to \mathbb{R}$ iniettiva. La prima è più facile

$$A = \mathcal{P}(\omega) \setminus \left(\{\emptyset\} \cup \{ X \in \mathcal{P}(\omega) \mid |\omega \setminus X| < \aleph_0 \} \right)$$

L'insieme $S \overset{\text{def.}}{=}$ è in corrispondenza biunivoca con $\mathcal{P}^{\text{fin}}(\omega)$ tramite la funzione "complementare rispetto a ω"

$$\overline{\cdot} : S \to \mathcal{P}^{\text{fin}}(\omega) \qquad \overline{X} = \omega \setminus X$$

Quindi $|S| = |\mathcal{P}^{\text{fin}}(\omega)| = \aleph_0$, e, di conseguenza $|A| = 2^{\aleph_0}$ grazie al lemma precedente.

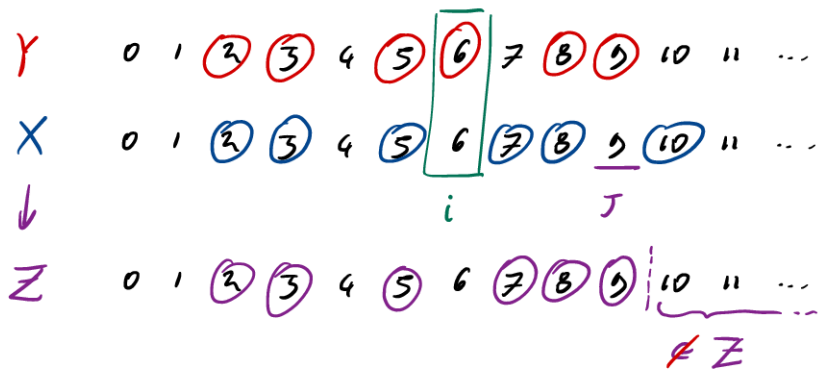
Resta da costruire $f : A \to \mathbb{R}$ iniettiva. Cominciamo col definire un ordine totale su A. Dati $X, Y \in A$

$$X < Y \overset{\text{def.}}{\iff} \exists i \in \omega \; \underbrace{\forall j < i \; j \in X \leftrightarrow j \in Y}_{in X = in Y} \wedge \underbrace{i \in Y \setminus X}_{i \in Y \wedge i \notin X}$$

In altri termini, detto i il minimo elemento della differenza simmetrica $X \triangle Y \overset{\text{def.}}{=} (X \setminus Y) \cup (Y \setminus X)$, se $i \in Y$ — per cui, chiaramente, $i \notin X$ — allora $X < Y$, se, invece, $i \in X$ — per cui $i \notin Y$ — allora $Y < X$. La verifica del fatto che questo è un ordine totale è immediata.

Consideriamo $B \overset{\text{def.}}{=} \mathcal{P}^{\text{fin}}(\omega) \setminus \{\emptyset\} \subseteq A$. Chiaramente $|B| = \aleph_0$. Dimostriamo che B è denso in A.

Dati $X, Y \in A$ con $X < Y$, sia $i = \min X \triangle Y$ e $j > i$ minimo tale che $j \notin X$, che esiste perché X è co-infinito. Sia $Z \overset{\text{def.}}{=} (X \cap j) \cup \{j\}$



Z è finito, quindi appartiene a B per costruzione. Inoltre, j è il minimo elemento di $X \triangle Z$ e $j \in Z$, quindi $X < Z$, e, similmente, i è il minimo di $Z \triangle Y$ e $i \in Y$, quindi $Z < Y$.

Stabilito che B è denso in A, B è, in particolare, denso, quindi, c'è un isomorfismo di ordini $g : B \to \mathbb{Q}$. Ora, siccome, nuovamente, B è denso in A, la funzione

$$h : A \to \text{sezioni su } B, \quad h(X) = \{Y \in B \mid Y < X\}$$

è iniettiva. Quindi $f : A \to \mathbb{R}$, $f(X) = g[h(X)]$ è una funzione iniettiva da A a $\mathbb{R}$. ∎

Stato del corso

È un dato di fatto — il primo teorema di incompletezza di Gödel — che ogni teoria calcolabile — i cui assiomi possano, cioè, essere elencati in maniera meccanica — è necessariamente incompleta. L'incompletezza non è quindi un difetto, o meglio, che lo sia oppure no è irrilevante, perché non può essere evitata.

Tuttavia, gli assiomi che abbiamo introdotto fino ad ora lasciano aperte lacune che sarebbe desiderabile colmare.

1. Sarebbe ragionevole che questi insiemi esistessero
   $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$
   $\{\omega, s(\omega), s(s(\omega)), s(s(s(\omega))), \dots\}$
   Però gli assiomi 1–7 non bastano per né per dimostrarne l'esistenza, né — e questo sarebbe disastroso — permettono di escluderla.

2. Alcune questioni sulle cardinalità, come per esempio la confrontabilità, non possono essere decise sulla base dei soli assiomi 1–7. Inoltre ci mancano risultati desiderabili per via delle applicazioni, segnatamente il lemma di Zorn.

3. Vi sono insiemi la cui esistenza vorremmo escludere. Per esempio vorremmo che l'equazione $X = \{X\}$ non avesse soluzioni, e sarebbe comodo escludere l'esistenza di qualcosa tipo $Y = \{\{\{\{\cdots\}\}\}\}$ con infinite parentesi annidate. Il guaio qui non è grave, ma questi oggetti contraddicono, in parte, l'intuizione che vorremmo concretizzare negli assiomi della teoria degli insiemi. Noi vorremmo che un insieme fosse identificato dalla sua struttura. Mi spiego, per esempio $\emptyset$ è identificato dal fatto di non avere elementi, $\{\emptyset\}$ è identificato dal fatto di aver un solo elemento che non ha elementi. &c. per tutti gli insiemi che conosciamo, ma cosa dire di Y? Y ha un elemento Y_1, che ha un elemento Y_2, che ha ... e la stessa descrizione si potrebbe applicare anche a Y_1, e anche a Y_2 ... Sono tutti uguali?

Queste tre lacune saranno colmate dai tre assiomi che ancora ci mancano: rispettivamente l'assioma del rimpiazzamento, l'assioma della scelta e l'assioma di buona fondazione. La teoria risultante sarà, inevitabilmente, incompleta — per esempio non decide il problema del continuo: l'esistenza di cardinalità intermedie fra $\aleph_0$ e $2^{\aleph_0}$ — ma è la fondazione meglio accettata della matematica.

I buoni ordinamenti

Il nostro prossimo obiettivo è definire e studiare la classe dei *numeri ordinali*. Questa può essere pensata come la più vasta classe — dotata di un ordinamento totale definito per mezzo di una formula — su cui sia corretto ragionare per induzione forte. Conteremo, quindi, sugli ordinali per formulare *l'induzione e la ricorsione transfinita*, procedimenti che superano la forza dimostrativa dell'induzione e della ricorsione aritmetica — per esempio permettendo di ottenere il teorema di Cantor – Lebesgue sugli insiemi di unicità.

Siccome l'induzione forte equivale al principio del minimo, studieremo i buoni ordini. In questa sezione, dimostreremo il risultato seguente. *nel seguito scriveremo semplicemente $(A, <)$ e $(B, <)$*

Teo Siano $(A, <_A)$ e $(B, <_B)$ insiemi bene ordinati, allora vale *una e una sola* delle seguenti

- $(A, <_A)$ è isomorfo a un segmento iniziale proprio di $(B, <_B)$
- $(A, <_A)$ e $(B, <_B)$ sono isomorfi
- $(B, <_B)$ è isomorfo a un segmento iniziale proprio di $(A, <_A)$

Ossia, se definiamo

$$(A, <_A) \prec (B, <_B) \overset{\text{dd.}}{\equiv} \exists\, C \text{ s.i proprio di } (B, <_B) \quad (A, <_A) \sim C$$

allora $\prec$ soddisfa le proprietà formali di un ordine totale

Sia la classe di isomorfismo di buoni ordini. Definiamo allora

$(A, <_A) \preceq (B, <_B) \overset{def.}{\iff} (A, <_A) \prec (B, <_B) \vee (A, <_A) \sim (B, <_B)$

ossia "$(A, <_A)$ è isomorfo a un segmento iniziale di $(B, <_B)$"

Richiamiamo le definizioni fondamentali

Def: $(A, <)$ è un *buon ordinamento* se ogni $B \subseteq A$ non vuoto ha un minimo elemento.

Def Dato un ordine totale $(A, <)$, $B \subseteq A$ è un *segmento iniziale* se $\forall b \in B \; \forall x \in A \; x < b \to x \in B$

Il segmento iniziale B è *proprio* se $B \neq A$

Il segmento iniziale B è *principale* se

$$B = A_a \overset{def.}{=} \{x \in A \mid x < a\}$$

per qualche $a \in A$, e, in questo caso, si dice *il segmento iniziale principale determinato da a*.

È chiaro che un segmento iniziale principale, A_a, è proprio, perché $a \notin A_a$, nel caso dei buoni ordini questa è una doppia implicazione

Prop: Ogni segmento iniziale proprio di un buon ordine è principale.

Dim Sia $(A, <)$ ben ordinato e $I \subsetneq A$ un segmento iniziale. Consideriamo $a = \min(A \setminus I)$. Allora $I = A_a$.

Verifichi: $x \in A_a \Rightarrow x < a \Rightarrow x \notin A \setminus I \Rightarrow x \in I$.

Supponiamo, per assurdo, $x \in I$ e $x \notin A_a$, la seconda equivale ad $a \leq x$, ma allora, siccome $x \in I$, $a \in I$ ma. Quindi $x \in I$ implica $x \in A_a$. ∎

Esercizio Dimostra che la proposizione precedente caratterizza i buoni ordini. Più precisamente, dato un ordine totale $(A, <)$, se ogni segmento iniziale proprio di A è principale, allora A è ben ordinato da $<$.

Lemma Sia $(A, <)$ un buon ordinamento e $f : A \to A$ una funzione crescente — def. $\forall x, y \in A \; x < y \to f(x) < f(y)$. — Allora $\forall x \in A \; x \leq f(x)$.

Dim Per assurdo, assumiamo la negazione della tesi. Quindi l'insieme $B = \{x \in A \mid f(x) < x\}$ non è vuoto. Sia $k = \min B$. Allora $f(k) < k$, e, siccome f è crescente, $f(f(k)) < f(k)$. Colorando diversamente $f(f(k)) < f(k)$, per cui $f(k) \in B$, che, ricordando $f(k) < k$, contraddice la minimalità di k.

Corollari

1. Un buon ordinamento non è isomorfo a un suo s.i. proprio.
2. L'identità è il solo isomorfismo fra un b.o. e se stesso
3. Se $(A, <)$ e $(B, <)$ sono b.o. isomorfi allora esiste un unico isomorfismo fra di essi.

Dim

1. Supponiamo che $(A, <)$ sia isomorfo al suo s.i proprio A_a, ordinato — si intende — dalla restrizione di $<$, e sia $f: A \to A_a$ un isomorfismo. Allora f è crescente per definizione. Tuttavia $f(a) < a$, poiché $f(a) \in A_a$, contraddicendo il lemma.

2. Sia $f: A \to A$ un automorfismo del buon ordine $(A, <)$, dobbiamo dimostrare che $f = Id_A$. Se così non fosse, ci sarebbe un $x \in A$ tale che $f(x) \neq x$.
Se $f(x) < x$ contraddiciamo il lemma perché f è crescente.
Se $x < f(x)$ idem considerando f^{-1}.

3. Se $f: A \to B$ e $g: A \to B$ fossero due isomorfismi diversi, allora $g^{-1} \circ f$ sarebbe un automorfismo di A diverso dall'identità, contraddicendo il punto 1. ∎

Oss Siano $(A, <)$, $(B, <)$, $(C, <)$ buoni ordini. Allora
$(A, <) \preceq (B, <) \wedge (B, <) \preceq (C, <) \longrightarrow (A, <) \preceq (C, <)$.

Dim Siano $f: A \to B$ e $g: B \to C$ isomorfismi fra A e un segmento iniziale di B e fra B e un segmento iniziale di C rispettivamente. Dimostriamo che $g \circ f$ è un isomorfismo fra A e un segmento iniziale di C.
$g \circ f$ è crescente in quanto composizione di funzioni crescenti.

Occorre verificare che l'immagine $g \circ f[A]$ è un segmento iniziale di C.

Verifica. Sia $g(f(a))$ un qualunque elemento di $g \circ f[A]$, e sia $x < g(f(a))$, dobbiamo dimostrare che $x \in g \circ f[A]$. $g(f(a)) \in g[B]$ e $g[B]$ è un s.i. di C per ipotesi, quindi $x \in g[B]$. Scriviamo $x = g(y)$. Ora, siccome g è un isomorfismo, da $x < g(f(a))$ deduciamo $y < f(a) \in f[A]$. Siccome $f[A]$ è un s.i. di B, quindi, $y = f(z)$ per qualche $z \in A$. In definitiva $x = g(f(z)) \in g \circ f[A]$. ☒

Oss. Siano $(A, <)$ e $(B, <)$ buoni ordini, allora

$$(A, <) \precsim (B, <) \wedge (B, <) \precsim (A, <) \rightarrow (A, <) \sim (B, <)$$

Dim Siano $f : A \to B$ e $g : B \to A$ isomorfismi fra A e un s.i. di B e fra B e un s.i. di A rispettivamente. Ricordando la dimostrazione dell'osservazione precedente, $g \circ f$ è un isomorfismo fra A e un s.i., $g \circ f[A]$, di A. Per il corollario 1., $g \circ f[A]$ non può essere un s.i. proprio, quindi $g \circ f[A] = A$. Ma allora, per il corollario 2. $g \circ f = Id_A$. Ragionando simmetricamente $f \circ g = Id_B$, quindi f è un isomorfismo fra A e B, con inversa g. ☒

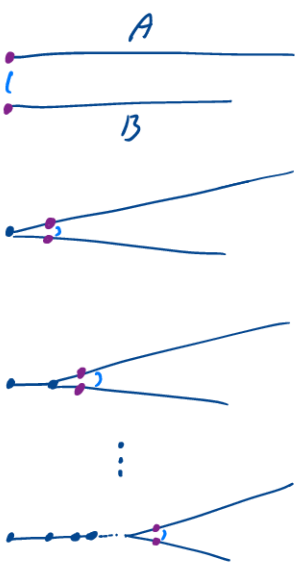
Possiamo finalmente passare alla dimostrazione del teorema.

Teo Siano $(A, <)$ e $(B, <)$ insiemi bene ordinati,

allora vale una e una sola delle seguenti

$$(A,<) \prec (B,<) \qquad (A,<) \sim (B,<) \qquad (B,<) \prec (A,<)$$

Idea Il corollario ci dice che vale al più una delle alternative, quindi la difficoltà risiede nel dimostrare che una



si verifica. Molto vagamente potremmo ragionare così. Identifichiamo, progressivamente, segmenti iniziali sempre più lunghi di A e B. All'inizio identifichiamo il minimo di A con il minimo di B, poi il secondo elemento di A con il secondo elemento di B, &c. Fatti ω passaggi avremo identificato un segmento iniziale di A, diciamo A_x, isomorfo a ω, con un B_y, anch'esso ovviamente isomorfo a ω. Bene: continuiamo identificando x con y. Quando potrebbe bloccarsi questo procedimento? Solo se, ad un certo punto, abbiamo identificato interamente uno dei due insiemi con un segmento iniziale dell'altro — poiché, altrimenti, abbiamo identificato due segmenti iniziali A_x e B_y e possiamo continuare attaccando x a y. È come la chiusura di una cerniera lampo: ad ogni istante c'è un prossimo dente.

Questo discorso, però, non è una dimostrazione. Se vogliamo, sarebbe un tentativo di costruire l'isomorfismo cercato per ricorsione transfinita. Il guaio è che i numeri che permettenobbero

di numerare i passaggi della costruzione, gli ordinali sono appunto l'oggetto che stiamo tentando di costruire.

Dim (quella vera)

Per il corollario, si può verificare al più una delle tre condizioni. Consideriamo ora f definita come segue

$$f \overset{\text{def.}}{=} \{(a,b) \in A \times B \mid A_a \sim B_b\}$$

Vogliamo dimostrare che f è una funzione crescente, che $\mathrm{Dom}\, f$ è un segmento iniziale di A, e che $\mathrm{Im}\, f$ è un segmento iniziale di B. Quindi f è un isomorfismo fra un segmento iniziale di A e uno di B. Infine dimostriamo che o $\mathrm{Dom}\, f = A$ o $\mathrm{Im}\, f = B$, e questo conclude la dimostrazione.

1. f è una funzione.

   Supponiamo per assurdo $(a,b) \in f$ e $(a,b') \in f$ con $b \neq b'$. Senza perdita di generalità $b < b'$, e, per definizione

   $$B_b \sim A_a \sim B_{b'}$$

   $B_{b'}$ sarebbe quindi isomorfo al suo segmento iniziale proprio B_b ↯

2. f è crescente

   Dati $a, a' \in A$ con $a < a'$, dobbiamo dimostrare $f(a) < f(a')$

   Supponiamo, per assurdo, $f(a') \leq f(a)$, abbiamo allora

$$A_{a'} \sim B_{f(a')} \subsetneq B_{f(a)} \sim A_a$$

dove i due isomorfismi vengono semplicemente dalla definizione di f, e $B_{f(a')} \subsetneq B_{f(a)}$ segue da $B_{f(a')} \subseteq B_{f(a)}$ che vale perché $f(a') \leq f(a)$ per ipotesi assurda.
Abbiamo quindi ottenuto $A_{a'} \sim A_a$ che è assurdo poiché A_a è un segmento iniziale proprio di $A_{a'}$.

3. $\mathrm{Dom}\, f$ è un segmento iniziale di A

Sia $a \in \mathrm{Dom}\, f$ e $a' < a$, vogliamo dimostrare $a' \in \mathrm{Dom}\, f$.
L'ipotesi $a \in \mathrm{Dom}\, f$ equivale a dire che esiste $b \in B$ tale che $A_a \sim B_b$, quindi, in particolare, $A_a \subsetneq B_b$.
Da $a' < a$ segue che $A_{a'} \subsetneq A_a$, quindi $A_{a'} \prec A_a$.
Per transitività $A_{a'} \prec B_b$ e, siccome ogni segmento iniziale è principale, esiste $b' \in B_b$ tale che $A_{a'} \sim (B_b)_{b'}$.
Si conclude osservando che $(B_b)_{b'} = B_{b'}$, quindi $f(a') = b'$.

4. $\mathrm{Im}\, f$ è un segmento iniziale di B

Dimostrazione simmetrica alla precedente.

5. O $\mathrm{Dom}\, f = A$ o $\mathrm{Im}\, f = B$

Se così non fosse, per 3. $\mathrm{Dom}\, f = A_a$ e per 4. $\mathrm{Im}\, f = B_b$ per opportuni $a \in A$ e $b \in B$. Per 2. f è crescente, quindi è un isomorfismo fra $\mathrm{Dom}\, f = A_a$ e $\mathrm{Im}\, f = B_b$. Ma allora $A_a \sim B_b$ e, per costruzione $(a, b) \in f$. Quindi $a \in \mathrm{Dom}\, f$ ↯

Esercizio Sia $(A, <)$ b.o. e sia $B \subsetneq A$. Dimostra che $B \leq A$, ma non necessariamente $B < A$.

Esercizio Sia $(A, \leq_A)$ un ordine totale con $A = \bigcup S$.
Supponiamo che: 1. ogni $X \in S$ è b.o. dalla restrizione di $\leq_A$
2. per ogni $X, Y \in S$, o X è s.i. di Y
o Y è s.i. di X

Dimostra che allora $(A, <)$ è un buon ordine.
Esibisci un controesempio eliminando la condizione 2.

Operazioni aritmetiche fra buoni ordinamenti

Per ora, non abbiamo visto molti esempi di buoni ordini. Le operazioni definite in questa sezione forniscono una prima sorgente di esempi concreti. Nel seguito del corso, vedremo buoni ordini assai più vasti di quelli ottenibili con queste operazioni.

Def Siano $(A, <_A)$ e $(B, <_B)$ ordini totali. Definiamo

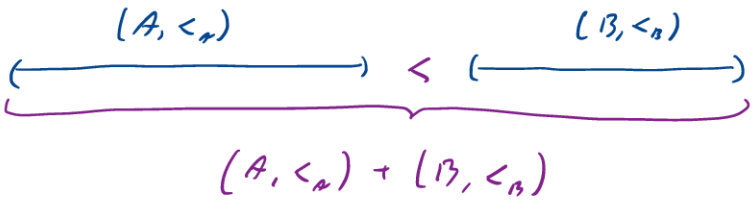
$$(A, <_A) + (B, <_B) \overset{\text{def.}}{=} (\underbrace{A \sqcup B}_{A \times \{0\} \cup B \times \{1\}}, <_+)$$

dove $<_+$ è definita da

$$(x, y) <_+ (x', y') \overset{\text{def.}}{\equiv} (y = 0 \wedge y' = 1)$$
$$\vee \; (y = 0 \wedge y' = 0 \wedge x <_A x')$$
$$\vee \; (y = 1 \wedge y' = 1 \wedge x <_B x')$$

Idea: $(A, <_A) + (B, <_B)$ si ottiene attaccando $(B, <_B)$ in

coda a $(A, <_A)$.



Ripetiamo, per completezza, la definizione di prodotto lessicografico

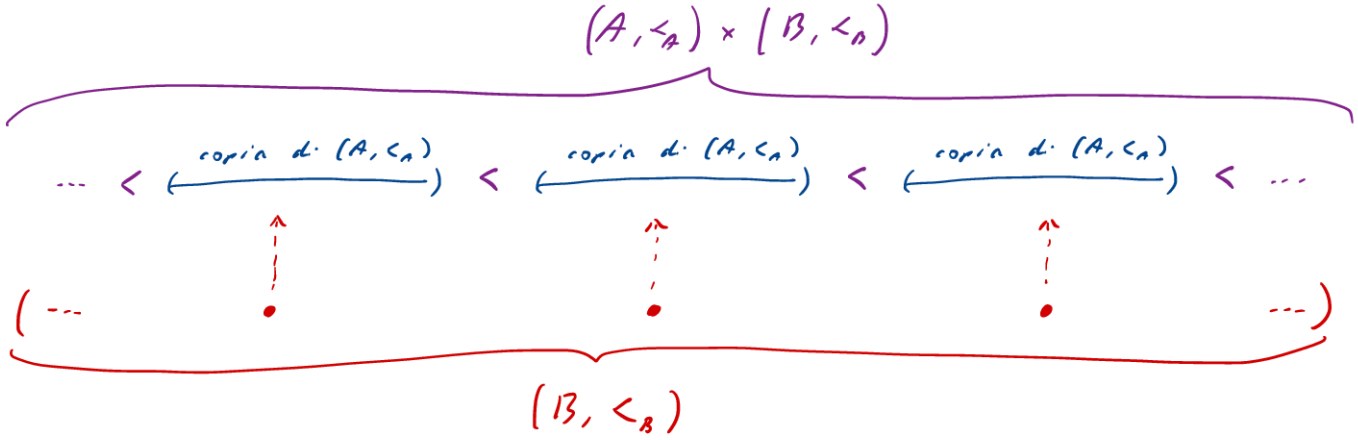
Def Siano $(A, <_A)$ e $(B, <_B)$ ordini totali. Definiamo

$$(A, <_A) \cdot (B, <_B) \overset{def.}{=} (A \times B, <_\times)$$

dove $<_\times$ è definito da

$$(x, y) <_\times (x', y') \overset{def.}{\equiv} (y <_B y') \wedge (y = y' \wedge x <_A x')$$

Idea: confronto prima la seconda componente. A parità decido la prima. Ossia: $(A, <_A) \cdot (B, <_B)$ sono tante copie di $(A, <_A)$ giustapposte, quanti sono gli elementi di B.



Per definire l'esponenziale, ci serve la nozione di supporto.

Def Dato un buon ordine $(B, <)$ e $f : A \to B$, il *supporto* di f è

$$Supp_B(f) \overset{def.}{=} \{x \in A \mid f(x) \neq \min B\}$$

Omettiamo il pedice B quando è chiaro cosa sia B.

Def Siano $(A, <_A)$ e $(B, <_B)$ ordini totali. Definiamo

$$(A, <_A)^{(B, <_B)} \overset{\text{def.}}{=} \left(\{ f \in {}^B A \mid |\operatorname{Supp} f| < \aleph_0 \}, <_{\text{exp}} \right)$$

funzioni a supporto finito

dove $<_{\text{exp}}$ è definito da

$$f <_{\text{exp}} g \overset{\text{def.}}{\iff} f \neq g \text{ e detto } m = \max_{<_B} \{ x \in B \mid f(x) \neq g(x) \}$$
$$\text{si ha } f(m) <_A g(m)$$

L'idea è che una funzione $B \to A$ può essere vista una specie di tupla con tante componenti quanti sono gli elementi di B. Ordinare questa tupla lessicograficamente significa che vince la componente diversa più a destra, ossia quella corrispondente all'elemento di B più grande.

Esercizio Verifica che $(\omega, <)^{(\omega, <)} \sim (\mathbb{N}[x], \prec)$ dove $\mathbb{N}[x]$ denota l'insieme dei polinomi a coefficienti in $\mathbb{N}$, e definiamo

$$p \prec q \overset{\text{def.}}{\iff} \exists N \in \mathbb{N} \; \forall x \in \mathbb{N} \; x > N \to p(x) < q(x)$$

Ossia $p \prec q$ se $p(x) < q(x)$ da un certo punto in poi.

Prop: Se $(A, <_A)$ e $(B, <_B)$ sono buoni ordini, allora anche $(A, <_A) + (B, <_B)$, $(A, <_A) \cdot (B, <_B)$ e $(A, <_A)^{(B, <_B)}$ sono buoni ordini.

Dim Si tratta di banali verifiche, eccetto la tenga.

La relazione $<_{\text{exp}}$ è irriflessiva per definizione. Occorre, intanto, verificare la transitività.

Assumiamo $f <_{rxp} g$ e $g <_{rxp} h$ con

$$m_1 = \max_{<_0} \{ x \in B \mid f(x) \neq g(x) \}$$
$$m_2 = \max_{<_B} \{ x \in B \mid g(x) \neq h(x) \}$$
$$m_3 = \max_{<_0} \{ x \in B \mid f(x) \neq h(x) \}$$

Detto $m = \max(m_1, m_2)$, abbiamo $f(m) \leq_A g(m) \leq_A h(m)$, dove la prima disuguaglianza è stretta se $m = m_1$ e la seconda se $m = m_2$. In ogni caso $f(m) <_A h(m)$. D'altra parte, se $m <_B x$, allora $f(x) = g(x) = h(x)$, quindi $m = m_3$ e la transitività è dimostrata.

La relazione $<_{rxp}$ è un ordine totale perché, se $f \neq g$, allora esiste $m = \max_{<_B} \{ x \in B \mid f(x) \neq g(x) \}$, e o $f(m) <_A g(m)$ o $g(m) <_A f(m)$. Nel primo caso $f <_{rxp} g$, nel secondo $g <_{rxp} f$.

Resta da verificare che l'ordine è buono. Per assurdo, supponiamo che non lo sia, allora, detto S l'insieme delle funzioni $B \to A$ a supporto finito, abbiamo

$$\exists f \in S \; \exists A \subseteq S \left(\underbrace{f \in A}_{\text{c'è un } A \subseteq S \text{ non vuoto}} \wedge \underbrace{\forall g \in A \; \exists h \in A \; h <_{rxp} g}_{\text{che non ha minimo}} \right)$$

Ora, fissiamo una $f \in S$ tale che $\exists A \subseteq S$ &c. con queste proprietà: che $\max_{<_0}(\mathrm{Supp}\, f)$ sia minimo, e che, a parità di $m = \max_{<_0}(\mathrm{Supp}\, f)$ il valore di $f(m)$ sia minimo. Fissiamo una A in modo tale che $f \in A$ ed A non abbia minimo. Il nostro scopo è costruire un $\tilde{A} \subseteq S$ che non ha minimo e contiene

una funzione $\tilde{f}$ con $\max(Supp\ \tilde{f}) <_B m$, in questo modo neghiamo la minimalità di m ed otteniamo la contraddizione voluta.

Osserviamo, intanto che A può essere ripartito in

$$A_1 = \{ g \in A \mid \max_{<_D}(Supp\ g) <_B m \}$$
$$A_2 = \{ g \in A \mid \max_{<_D}(Supp\ g) = m \wedge g(m) = f(m) \}$$
$$A_3 = \{ g \in A \mid \max_{<_D}(Supp\ g) = m \wedge f(m) <_A g(m) \}$$
$$A_4 = \{ g \in A \mid m <_D \max(Supp\ g) \}$$

e segue dalla definizione che le funzioni in A_1 sono $<_{exp}$ di quelle in A_2, che sono $<_{exp}$ &c. fino ad A_4. Però A_1 è vuoto, perché altrimenti, presa $f' \in A_1$, abbiamo $f' \in A$ e $\max(Supp\ f') < m$ contro la minimalità di m. Allora A_2, che non è vuoto poiché contiene f non ha minimo, se, infatti, l'avesse, questo dovrebbe essere anche minimo di A.

Concentriamoci ora su A_2. Tutte le $g \in A_2$ assumono il medesimo valore su m, quindi, comparando due di queste funzioni con $<_{exp}$, il valore assunto da entrambe su m è irrilevante. Ossia la funzione

$$H : A_2 \longrightarrow S$$
$$g \longmapsto \hat{g} \quad \text{con} \quad \hat{g}(x) = \begin{cases} \min A & \text{se } x = m \\ g(x) & \text{altrimenti} \end{cases}$$

è strettamente crescente. Per cui $\tilde{A} \overset{def.}{=} H[A_2]$ non ha minimo.

Ora, però, segue dalla definizione che, fissata $g \in A_\alpha$, $\operatorname{Supp} \hat{g} = (\operatorname{Supp} g) \setminus \{m\}$, quindi, ponendo $\hat{f} \overset{\text{def.}}{=} \hat{g}$, abbiamo $\max(\operatorname{Supp} \hat{f}) < m$, e questo contraddice la minimalità di m. ∎

Prop. Le operazioni aritmetiche sui buoni ordini passano al quoziente modulo isomorfismi. Ossia, dati due buoni ordinamenti $\mathcal{A} = (A, <_A)$ e $\mathcal{B} = (B, <_B)$, e dati $\mathcal{A}' = (A', <_{A'}) \sim \mathcal{A}$ e $\mathcal{B}' = (B', <_{B'}) \sim \mathcal{B}$, si ha

$$\mathcal{A} + \mathcal{B} \sim \mathcal{A}' + \mathcal{B}' \qquad \mathcal{A} \cdot \mathcal{B} \sim \mathcal{A}' \cdot \mathcal{B}' \qquad \mathcal{A}^{\mathcal{B}} \sim \mathcal{A}'^{\mathcal{B}'}$$

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

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

Esercizio svolgere qualcuna delle verifiche. ∎

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

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

Dim Facili verifiche. Esercizio: Farne qualcuna. ∎

È importante notare che non tutte le proprietà delle operazioni aritmetiche su ω valgono per i buoni ordini

Esercizio Esibire CONTROESEMPI alle seguenti

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

Un altro tranello in cui si potrebbe cadere è credere che le operazioni sui buoni ordini generalizzino quelle sulle cardinalità. Questo è vero per le cardinalità finite, e anche in generale per somma e prodotto — come è ovvio dalla definizione — ma fallisce per l'esponenziale quando l'esponente è infinito.

Esercizio Dimostra che se $\mathcal{A}=(A,<_A)$ e $\mathcal{B}=(B,<_B)$ sono buoni ordini con $|A|=|B|=\aleph_0$ e $(C,<_C)=\mathcal{A}^{\mathcal{B}}$ allora $|C|=\aleph_0$.

Gli ordinali di Von Neumann

In questa sezione definiremo gli ordinali di Von Neumann. L'idea che vogliamo concretizzare è che, siccome abbiamo visto che, a meno di isomorfismi, due buoni ordinamenti sono sempre uno nell'altro, unendo fra loro tutti i buoni ordinamenti — o tutte le classi di isomorfismo di questi — dovrebbe potersi costruire un buon ordinamento più grande di tutti. Questa vasta struttura sarà inevitabilmente una classe propria: la classe dei numeri ordinali, i cui elementi sono rappresentanti di tutte le possibili classi di isomorfismo di buoni ordini.

Def L'insieme α è *transitivo* se $\forall x \in \alpha \; x \subseteq \alpha$, o, equivalentemente, se $\forall x \alpha \; \forall y \in x \; y \in \alpha$.

Ossia: α è transitivo se gli elementi degli elementi di α sono, a loro volta, elementi di α.

Def (ordinali di Von Neumann)
L'insieme α è un *ordinale* se è *transitivo e ben ordinato dalla relazione di appartenenza*. Formalmente, l'insieme transitivo α è un ordinale se $(\alpha, <_\alpha)$ è un buon ordine, con

$$<_\alpha \overset{\text{def.}}{=} \{ (x,y) \in \alpha \times \alpha \mid x \in y \}$$

Denotiamo con Ord la classe degli ordinali, per cui

$$\alpha \in Ord \overset{\text{def.}}{\iff} \text{“}\alpha \text{ è transitivo e b.o. da } \in\text{”}$$

Esempi:

- ω è un ordinale
- gli elementi di ω sono ordinali
- $S(\omega) = \omega \cup \{\omega\}$ è un ordinale

Oss) Se $\alpha \in Ord$ e $\beta \in \alpha$ allora $\beta \in Ord$ e $\beta = \alpha_\beta$.

Nota: in particolare, la classe degli ordinali è transitiva.

Dim Siccome $\beta \in \alpha$, per la transitività di α, $\beta \subseteq \alpha$, quindi β è bene ordinato da $\in$. La transitività di β segue dalla transitività della relazione di ordine $<_\alpha$. Prendiamo, infatti, $\delta \in \gamma$ con $\gamma \in \beta$. Dobbiamo dimostrare $\delta \in \beta$. Siccome $\gamma \in \beta$, per la transitività di α, $\gamma \in \alpha$, e, da questa, nuovamente per la transitività di α, $\delta \in \alpha$. Ora $\delta, \gamma, \beta \in \alpha$, e abbiamo l'ipotesi $\delta \in \gamma \wedge \gamma \in \beta$, ossia $\delta <_\alpha \gamma \wedge \gamma <_\alpha \beta$, da cui $\delta <_\alpha \beta$. Quest'ultima dice, appunto, che $\delta \in \beta$.

Resta da dire che $\beta = \alpha_\beta$. Per definizione

$$x \in \alpha_\beta \iff x \in \alpha \wedge x <_\alpha \beta \iff x \in \alpha \wedge x \in \beta$$

Ora, $x \in \beta \to x \in \alpha$ per la transitività di α, quindi

$$x \in \alpha \wedge x \in \beta \iff x \in \beta$$

E concludiamo per estensionalità. ∎

La proposizione seguente ci dice che due ordinali non possono essere nella stessa classe di isomorfismo. Vorremmo poi dimostrare

che ogni classe di isomorfismo contiene un ordinale. Enunciamo prima una semplice osservazione.

Oss. Se $f: A \to B$ è un isomorfismo fra $(A, <_A)$ e $(B, <_B)$, allora preso qualunque $a \in A$ abbiamo $f[A_a] = B_{f(a)}$

Dim

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

Prop. Dati $\alpha, \beta \in Ord$, se $(\alpha, <_\alpha) \simeq (\beta, <_\beta)$ allora $\alpha = \beta$.

Dim Sia $f: \alpha \to \beta$ un isomorfismo. Ci basta dimostrare che $\forall \gamma < \alpha \; f(\gamma) = \gamma$. Sia, per assurdo, γ il minimo elemento di α tale che $f(\gamma) \neq \gamma$. Allora

$$\gamma = \alpha_\gamma = f[\alpha_\gamma] = \beta_{f(\gamma)} = f(\gamma) \quad \text{↯}$$ ∎

Possiamo ora chiederci come si rifletta l'ordinamento totale delle classi di isomorfismo di buoni ordini, dato dalla relazione "essere segmento iniziale di", sugli ordinali. La risposta è che diventa la relazione di appartenenza.

Teo Dati $\alpha, \beta \in Ord$, vale **una e una sola** delle seguenti:

$\alpha \in \beta$ che vale se e solo se $(\alpha, <_\alpha) \lhd (\beta, <_\beta)$

$\alpha = \beta$ ——— " ——— $(\alpha, <_\alpha) \simeq (\beta, <_\beta)$

$\beta \in \alpha$ ——— " ——— $(\beta, <_\beta) \lhd (\alpha, <_\alpha)$

Notazione: d'ora in poi $\alpha \lhd \beta$, $\alpha \simeq \beta$, $\beta \lhd \alpha$.

Dim

Se $\alpha \lhd \beta$ allora, per la definizione di $\lhd$, esiste $\gamma \in \beta$ tale che $\alpha \sim \beta_\gamma$. Però $\beta_\gamma = \gamma$, e, per la proposizione $\alpha \sim \gamma \to \alpha = \gamma$. Abbiamo quindi dimostrato che $\alpha = \gamma \in \beta$. D'altro canto, se $\alpha \in \beta$ allora $\alpha = \beta_\alpha$ quindi $\alpha \lhd \beta$.

Se $\alpha \sim \beta$ la proposizione ci da immediatamente $\alpha = \beta$, ed il viceversa è immediato.

Il caso $\beta \lhd \alpha$ è, infine, simmetrico al primo. ∎

Notazione Dati $\alpha, \beta \in Ord$, $\alpha < \beta \overset{def.}{\equiv} \alpha \in \beta$.

Il teorema precedente ci dice che la relazione $<$ gode delle proprietà di un ordine totale stretto sulla classe degli ordinali.

Esercizio Dimostra che α è un ordinale finito se e solo se $\alpha \in \omega$.

Prop. Siano $\alpha, \beta \in Ord$. $\alpha \leq \beta \overset{def.}{\equiv} \alpha < \beta \vee \alpha = \beta \iff \alpha \subseteq \beta$

Dim

$\to$ Se $\alpha < \beta$ allora $\alpha \in \beta$ quindi $\alpha \subseteq \beta$ per transitività di β.
Se $\alpha = \beta$ allora $\alpha \subseteq \beta$ immediatamente.

$\leftarrow$ Supponiamo per assurdo $\alpha \subseteq \beta$ e $\beta < \alpha$. Allora $\beta \in \alpha \subseteq \beta$.
Ma quindi $\beta \in \beta$ ↯ ∎

Facilissimo esercizio: perché?

Ricordiamo che $S(\alpha) \overset{\text{def.}}{=} \alpha \cup \{\alpha\}$. La proposizione seguente dice che $S(\alpha)$ è, a buon diritto, il successore di α, anche quando α è un ordinale.

Prop. Dato $\alpha \in Ord$, $S(\alpha)$ è il minimo ordinale $> \alpha$.

Dim Occorre inizialmente verificare che $S(\alpha)$ è un ordinale.

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. Siccome $S(\alpha)$ è un insieme di ordinali, $\in$ è un ordine totale su $S(\alpha)$. Dato $X \subseteq S(\alpha)$, con $X \neq \emptyset$, abbiamo che o $X = \{\alpha\}$ o $X \cap \alpha \neq \emptyset$. Nel primo caso X ha chiaramente un minimo, nel secondo, $\min(X \cap \alpha)$ è il minimo di X.

Supponiamo, ora $\alpha < \beta$, dobbiamo dimostrare $S(\alpha) \leq \beta$.

$$\begin{array}{ccccc} \alpha < \beta & \Rightarrow & \alpha \in \beta & \Rightarrow & \alpha \subseteq \beta \\ & & \Downarrow & & \Downarrow \\ & & \{\alpha\} \subseteq \beta & \Rightarrow & \alpha \cup \{\alpha\} \subseteq \beta \Rightarrow S(\alpha) \leq \beta. \end{array}$$ ∎

Cor. $\forall \alpha, \beta \in Ord \quad \beta \leq \alpha \leftrightarrow \beta < S(\alpha)$

Prop. Dato un insieme di ordinali X

1. Se $X \neq \emptyset$, allora esiste il minimo di X, detto $\min X$, inoltre $\min X = \bigcap X$.
2. Esiste il minimo dei maggioranti di X, detto $\sup X$, inoltre $\sup X = \bigcup X$. (gli $\alpha \in Ord$ tali che $\forall \beta \in X \ \beta \leq \alpha$)

3. C'è un ordinale che non appartiene a X.

Dim

1. Dimostriamo, prima, che il minimo esiste. Sia $\alpha \in X$ fissato, che c'è perché $X \neq \emptyset$. Consideriamo $\mu \overset{\text{def.}}{=} \min_{\leq S(\alpha)} (X \cap S(\alpha))$. Questo esiste perché $X \cap S(\alpha) \neq \emptyset$ in quanto α vi appartiene. Vediamo che $\mu = \min X$. Infatti, preso $\beta \in X$, se $\beta \leq \alpha$ allora $\beta \in X \cap S(\alpha)$, quindi $\beta \geq \mu$. Se, però $\alpha < \beta$, allora $\mu < S(\alpha) \in \beta$.

   Ora verifichiamo che $\mu = \bigcap X$. Chiaramente $\forall y \in X \ \mu \leq y$, quindi $\forall y \in X \ \mu \leq y$, ossia $\mu \in \bigcap X$. D'altro canto $\mu \in X$, quindi $\bigcap X \subseteq \mu$.

2. Dimostriamo prima che $\bigcup X$ è un ordinale.

   Transitività: Dato $\alpha \in \bigcup X$ esiste $\beta \in X$ tale che $\alpha \in \beta$. Per la transitività di β, $\alpha \subseteq \beta$. Da cui $\alpha \subseteq \bigcup X$.

   Buon ordine. Ogni $\alpha \in \bigcup X$ appartiene a qualche ordinale $\beta \in X$, ed è, quindi, un ordinale. Stabilito che $\bigcup X$ è un insieme di ordinali, è chiaro che un suo sottoinsieme non vuoto è un insieme non vuoto di ordinali. Quindi ha minimo per il punto 1.

   Dimostriamo ora che $\alpha \in \mathrm{Ord}$ è un maggiorante di X se e solo se $\bigcup X \leq \alpha$.

$\forall \alpha \in X\ \alpha \leq \sigma \Leftrightarrow \forall \alpha \in X\ \alpha \leq \sigma \Leftrightarrow \bigcup X \leq \sigma \Leftrightarrow \bigcup X \leq \sigma$

σ è un maggiorante di X

3. Immediata, basta prendere $s(\sup X)$. ∎

Con Un insieme di ordinali è un ordinale se e solo se è transitivo.

Dim Il buon ordinamento vale per il punto 2. della proposizione. ∎

Con (paradosso di Burali-Forti)
Ord è una classe propria.
Ossia non esiste l'insieme di tutti gli ordinali.

Dim Per il punto 3. della proposizione, se Ord fosse un insieme, esisterebbe un ordinale che non vi appartiene. ∎

Nota Cosa c'è di paradossale nel paradosso di Burali-Forti?

UNA QUESTIONE SUI NUMERI TRANSFINITI.

Nota di **C. Burali-Forti**, in Torino.

Adunanza del 28 marzo 1897.

Scopo principale di questa Nota è di dimostrare, che effettivamente esistono dei *numeri transfiniti* (*) (o *tipi d'ordine*) a, b tali che, a non è eguale, non è minore e non è maggiore di b.

Nel 1897, Cesare Burali-Forti era assolutamente convinto della esistenza dell'insieme di tutti gli ordinali — definiti allora come le classi di isomorfismo di buoni ordini — quello che non sapeva

è se la relazione $\prec$ fosse un ordine totale su questa classe. Burali-Forti credette di poter negare la totalità dell'ordine $\prec$ ragionando per assurdo. Se $\prec$ fosse un ordine totale, si può dimostrare che sarebbe buono, ma allora $\Omega \stackrel{def}{=} [(Ord, \prec)]$, la classe di isomorfismo di $(Ord, \prec)$, sarebbe uno dei membri della classe Ord, e, considerando il suo successore $S(\Omega)$, avremmo $\Omega \prec S(\Omega)$, ma anche $S(\Omega) \prec \Omega$, poiché $S(\Omega) \in Ord$. ⇝

Il guaio è che, nello stesso anno, Cantor ha pubblicato una dimostrazione del fatto che la relazione $\prec$ è totale — esattamente l'argomento dei segmenti iniziali isomorfi che abbiamo illustrato nel corso. Come è stata risolta la contraddizione? Concludendo che l'insieme di tutti gli ordinali non esiste? No. Sfortunatamente Burali-Forti aveva capito male la definizione di buon ordine, e ancora così, forse, nessuno se ne sarebbe accorto, ma, quel che è peggio, aveva tentato di correggerla, facendo, in realtà un gran pasticcio. La contraddizione è stata quindi imputata, da Burali-Forti stesso e da Cantor, al bisticcio di definizioni ed il paradosso è stato dimenticato. Cinque anni dopo, Russell si rese conto del fatto che l'assurdo sussiste anche se si usa la definizione corretta di buon ordine, e fu così che il paradosso di Burali-Forti acquisì il suo nome. E tutti vissero felici e contenti.

L'assioma del rimpiazzamento

Gli ordinali di Von Neumann sono eleganti, ma quanti ne abbiamo di questi arnesi? Si può dimostrare che, assumendo i soli assiomi 1-7, il gran totale degli ordinali potrebbe essere

$$Ord \stackrel{?}{=} \{\underbrace{\emptyset, S(\emptyset), \dots S^n(\emptyset), \dots \omega, S(\omega), \dots S^n(\omega), \dots}_{\text{In realtà, questo si chiamerà } \omega+\omega.}\}$$

la classe degli ordinali raggiungibili a partire da $\emptyset$ o da ω con un numero finito di applicazioni della mappa successore.

Esercizio Dimostra che la classe descritta sopra è effettivamente una classe, ossia è definita da una formula.

Se vogliamo poter rispondere alla domanda "quali ordinali esistono?" occorre un nuovo assioma: l'assioma del rimpiazzamento. Sotto questa ipotesi addizionale, la risposta sarà "tutti quelli che potrebbero esistere", ossia avremo un ordinale per ogni classe di isomorfismo di buoni ordini.

Per formulare l'assioma, ci serve il concetto di funzione classe.

Def Date due classi A e B una **funzione classe** da A a B è una formula insiemistica $\varphi(x,y)$ tale che

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

Ossia, una funzione classe è una proprietà, espressa nel linguaggio della teoria degli insiemi, che ad ogni $x \in A$ associa un unico $y \in B$.

Notazione Possiamo denotare una funzione classe $\varphi(x,y)$ da A a B mediante la notazione più familiare

$$F : A \to B$$

In questo caso, la scrittura $y = F(x)$ è una semplice abbreviazione:

$$y = F(x) \overset{\text{def.}}{\equiv} y \in B \wedge \varphi(x,y)$$

Esempi Le seguenti sono funzioni classe $V \to V$

$F_1(x) = x$ $\quad F_2(x) = \{x\}$ $\quad F_3(x) = \mathcal{P}(x)$ $\quad F_4(x) = S(x)$

La funzione classe $F_5(x) = \sup(\underbrace{x \cap Ord}_{\overset{\text{def.}}{\equiv} \{\alpha \in x \mid \alpha \in Ord\}})$ è $V \to Ord$.

(8) Assioma* del rimpiazzamento

"Se A è un insieme e $F : V \to V$ è una funzione classe, allora $F[A] \overset{\text{def.}}{\equiv} \{F(x) \mid x \in A\}$ è un insieme."

$$\forall A \; \exists B \; \forall y \quad y \in B \leftrightarrow \exists x \in A \quad y = F(x)$$

*Nota: come per la separazione, questo è uno schema di

assiomi, uno per ogni possibile funzione classe F.

Prop. Data una funzione classe $F: V \to V$

$$\forall A\ \exists! B\ \forall y\quad y \in B \iff \exists x \in A\quad y = F(x)$$

Quindi l'insieme $F[A]$ è univocamente determinato.

Dim. Estensionalità. ∎

Oss. Dato un insieme A e una funzione classe $G: A \to V$, esiste ed è unico l'insieme $G[A]$ tale che

$$\forall y\quad y \in G[A] \iff \exists x \in A\quad y = G(x)$$

Dim Basta applicare l'assioma alla funzione classe $F: V \to V$

$$y = F(x) \overset{\text{def.}}{\equiv} (x \in A \wedge y = G(x)) \vee (x \notin A \wedge y = \emptyset)$$

Notate che insieme mettiamo qui è irrilevante.

ossia

$$F(x) \overset{\text{def.}}{=} \begin{cases} G(x) & \text{se } x \in A \\ \emptyset & \text{altrimenti} \end{cases}$$

Infatti $x \in A$ implica $G(x) = F(x)$, per cui $G[A] = F[A]$. ∎

Esercizio Dimostra che, dati due insiemi A e B, esiste il loro prodotto cartesiano $A \times B$, usando l'assioma del rimpiazzamento ma senza usare l'assioma delle parti.

Teo Dato un buon ordine $(A, <)$, esiste un unico ordinale α tale che $(A, <) \sim \alpha$.

Dim L'unicità segue perché $\alpha \sim \alpha' \to \alpha = \alpha'$.

Basta dimostrare l'esistenza di α.

Sia $A' = \{x \in A \mid \exists \gamma \in Ord \ A_x \sim \gamma\}$

Consideriamo la funzione classe $F : A' \longrightarrow Ord$

$$F(x) = \text{l'unico } \gamma \in Ord \text{ tale che } A_x \sim \gamma$$

dove l'unicità vale perché

$$A_x \sim \gamma \wedge A_x \sim \gamma' \Rightarrow \gamma \sim \gamma' \Rightarrow \gamma = \gamma'.$$

Vogliamo dimostrare che $\alpha \overset{def.}{=} F[A'] \sim (A, <)$.

Dimostriamo che α è un ordinale, A' è un segmento iniziale di A e $\alpha \sim A'$. Infine concludiamo dimostrando $A' = A$.

1. **α è un ordinale.** α è un insieme di ordinali, ci basta, quindi, dire che è transitivo. Supponiamo $\beta < \gamma \in \alpha$, dobbiamo dire che $\beta \in \alpha$. Sia $f : \gamma \to A_x$ un isomorfismo, allora $f|_\beta : \beta \to A_{f(\beta)}$ è un isomorfismo, quindi $\beta = F(f(\beta))$.

2. **A' è un segmento iniziale di A.** Se $y < x \in A'$, allora esiste un isomorfismo $f : A_x \to \gamma$ quindi $f|_{A_y} : A_y \to \gamma_{f(y)}$ è un isomorfismo, e, siccome $\gamma_{f(y)} = f(y)$, abbiamo $A_y \sim f(y)$ per cui $y \in A'$.

3. **α ed A' sono isomorfi.** Sia $f : A' \to \alpha$ la funzione definita da $f(x) = F(x)$, che esiste per l'assioma di separazione applicato in $A' \times \alpha$. Dimostriamo che f è un isomorfismo di ordini.

La surgettività è immediata perché, per costruzione, abbiamo $\alpha = F[A'] = f[A']$. Verifichiamo la monotonia

$$x < y \Rightarrow A_x \prec A_y$$

$$f(x) \prec f(y) \Rightarrow f(x) < f(y)$$

4. $A' = A$. Se così non fosse A' sarebbe un segmento iniziale proprio di A, avremmo quindi $A' = A_k$ per qualche $k \in A$. Ma allora, per i punti 1-3, $A_k = A' \sim \alpha \in Ord$, quindi, per la definizione di A', $k \in A'$. Però questo contraddice $A' = A_k$. ∎

Una conseguenza del risultato precedente è che possiamo definire le operazioni sugli ordinali come semplice riflesso di quelle sui buoni ordini.

Def. (operazioni sugli ordinali — v.1)
Dati $\alpha, \beta \in Ord$, definiamo $\alpha + \beta$, $\alpha \cdot \beta$ e α^β come, rispettivamente, l'unico ordinale tale che

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

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

Esercizio Dimostra che l'insieme introdotto all'inizio della sezione è effettivamente $\omega + \omega$, ossia, più precisamente

$$\forall x \quad x \in \omega + \omega \longleftrightarrow (\exists m \in \omega \; x = m) \vee (\exists n \in \omega \; x = \omega + n)$$

Induzione e ricorsione transfinita

Il piatto forte di questa sezione è una seconda applicazione dell'assioma di rimpiazzamento: il teorema di ricorsione transfinita. Questo risultato sarà più chiaro a chi ha, in precedenza, risolto questo esercizio.

Esercizio Dimostra che esiste un insieme A tale che

$$\forall x \quad x \in A \leftrightarrow x = \emptyset \vee \exists y \in A \quad x = \{y\}$$

ossia, in sostanza, dimostra che esiste

$$A = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$$

L'idea chiave per risolvere questo esercizio è contenuta nella dimostrazione del teorema di ricorsione numerabile, che abbiamo già visto. Attenzione, però, che questo teorema non si può applicare direttamente alla situazione dell'esercizio. La soluzione è alla prossima pagina: qui riprendiamo con lo studio della teoria: in particolare, l'induzione transfinita.

Prop (induzione transfinita — v. 1)
Data una formula insiemistica $\varphi(x)$.
Se vale $\forall \alpha \in Ord \ (\forall \beta < \alpha \ \varphi(\beta)) \to \varphi(\alpha)$
Allora $\forall \alpha \in Ord \ \varphi(\alpha)$.
In termini di classi, rappresentando con C la classe

Soluzione dell'esercizio

Vorremmo definire la funzione classe $F(w) \to V$

$F(n) =$ singoletto n volte di $\emptyset$

a questo punto potremmo verificare che $A = F[w]$ soddisfa la richiesta. Occorre quindi dimostrare che la definizione informale di F data sopra è esprimibile nel linguaggio formale della teoria degli insiemi.

Diamo la seguente definizione, per n ew

$$y = F(n) \overset{def.}{\equiv} \exists f \begin{cases} f \text{ è una funzione} \\ Dom(f) = S(n) \\ f(0) = \emptyset \\ f(n) = y \\ \forall i \in n \quad f(S(i)) = \{f(i)\} \end{cases}$$

Per dimostrare che F è una funzione classe, ci basta dimostrare che $\forall n \, e w \; \exists! f \{ \ldots$, infatti, a questo punto, anche $y = f(n)$ è univocamente determinato. SENZA LA CONDIZIONE $f(n) = y$

1. Esistenza. Procediamo per induzione. Il caso $n = 0$ è immediato, basta considerare $f = \{(0, \emptyset)\}$. Nel caso $n = S(m)$, per ipotesi induttiva, abbiamo una funzione f' con $Dom\, f' = n$ $f'(0) = \emptyset$, $\forall i < n \; f'(S(i)) = \{f'(i)\}$.

Ora prendiamo $f = f' \cup \{(n, \{f'(m)\})\}$. Abbiamo

$\mathrm{Dom}\, f = (\mathrm{Dom}\, f') \cup \{n\} = s(n)$. $f(0) = f'(0) = \emptyset$.

Inoltre, preso $i < n = s(m)$, o $i < m$ o $i = m$.

Nel primo caso $f(s(i)) = f'(s(i)) = \{f'(i)\} = \{f(i)\}$.

Nel secondo $f(s(i)) = f(n) = \{f'(m)\} = \{f(m)\} = \{f(i)\}$.

2. Unicità. Dati f_1 e f_2 che soddisfano le condizioni

$\mathrm{Dom}(f_x) = s(n)$, $f_x(0) = \emptyset$, $\forall i < n \; f_x(s(i)) = \{f_x(i)\}$

dimostriamo, per induzione su i, che $\forall i \leq n \to f_1(i) = f_2(i)$

Caso $i = 0$: $f_1(0) = \emptyset = f_2(0)$.

Caso $i = s(j)$: $f_1(i) = \{f_1(j)\} = \{f_2(j)\} = f_2(i)$. ($= $ per ipotesi induttiva.)

Ora abbiamo la funzione classe F. È immediato verificare che $F(0) = \emptyset$. Inoltre, dato $n \in \omega$, $F(s(n)) = \{F(n)\}$. Infatti, detta $y = F(s(n))$, e detta f la funzione con $\mathrm{Dom}(f) = s(s(n))$ che testimonia $y = F(s(n))$, vediamo che $f_{|s(n)}$ testimonia che $F(n) = f_{|s(n)}(n) = f(n)$. Abbiamo quindi

$$F(s(n)) = f(s(n)) = \{f(n)\} = \{F(n)\}$$

Possiamo finalmente dimostrare che $A \overset{\text{def.}}{=} F[\omega]$ soddisfa la richiesta dell'esercizio. Infatti, $\emptyset = F(0) \in A$. Inoltre, preso $y \in A$, abbiamo $y = F(n)$ e $n \neq 0$, quindi $n = s(m)$ per qualche m, e, detto $x = F(m) \in A$, abbiamo $y = F(s(m)) = \{F(m)\} = \{x\}$.

definita da $\varphi(x)$, abbiamo che

se vale $\forall \alpha \in Ord \quad (\forall \beta \in \alpha \; \beta \in C) \to \alpha \in C$

allora $\forall \alpha \in Ord \quad \alpha \in C$

oppure ancora, in forma più concisa

$$(\forall \alpha \in Ord \quad \alpha \subseteq C \to \alpha \in C) \to Ord \subseteq C$$

Dim Per assurdo assumiamo $\neg\varphi(\alpha)$, per l'ipotesi abbiamo $\neg(\forall \beta < \alpha \; \varphi(\beta))$ ossia $\exists \beta < \alpha \; \neg\varphi(\beta)$. Consideriamo il minimo di questi β, ossia $\beta_0 = \min\{\beta \in \alpha \mid \neg\varphi(\beta)\}$. Di nuovo per l'ipotesi $\exists \beta < \beta_0 \; \neg\varphi(\beta)$ contro la minimalità di β. □

Nota Il principio di induzione transfinita non è, letteralmente, un teorema della teoria degli insiemi, quanto piuttosto uno schema di teoremi — o metateorema — che ci permette di costruire un diverso teorema per ogni possibile formula φ.

C'è una chiara analogia fra la forma precedente del principio di induzione transfinita e la forma forte della induzione aritmetica. A volte, però, è comodo esprimere l'induzione transfinita in una forma che meglio ricorda il principio di induzione di Peano.

Def Diciamo che $\alpha \in Ord$ è un ordinale successore se $\exists \beta \in Ord \; \alpha = S(\beta)$. Un ordinale $\alpha > 0$ che non è successore è detto ordinale limite.

Oss. Un ordinale α è successore se e solo se ha un massimo elemento.

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

Prop (induzione transfinita – v.2)

Sia $\varphi(x)$ una formula insiemistica. (ipotesi induttiva)

Se
- $\varphi(0)$ "caso base"
- $\forall \gamma \in Ord \quad \varphi(\gamma) \to \varphi(S(\gamma))$ "caso successore"
- Per ogni ordinale limite λ, $(\forall \beta < \lambda \ \varphi(\beta)) \to \varphi(\lambda)$ "caso limite"

allora $\forall \alpha \in Ord \ \varphi(\alpha)$.

Dim

Basta verificare l'ipotesi della v1., ossia che, fissato $\alpha \in Ord$

$$(\forall \beta < \alpha \ \varphi(\beta)) \to \varphi(\alpha)$$

Se α è limite o 0 abbiamo questa formula tout court.

Altrimenti $\alpha = S(\gamma)$ e abbiamo

$$\forall \beta < \alpha \ \varphi(\beta) \implies \varphi(\gamma) \implies \varphi(S(\gamma)) \equiv \varphi(\alpha)$$ ☐

Ora possiamo dimostrare il teorema di ricorsione transfinita. Faremo uso della notazione introdotta qui sotto.

Nota Data una funzione classe $F : A \to B$ e un insieme $X \subseteq A$ esiste la funzione $f = F|_X : X \to F[X]$

$$a \mapsto F(a)$$

Teo (ricorsione transfinita)

Data una funzione classe $G: V \to V$ esiste un'unica* funzione classe $F: Ord \to V$ tale che

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

*dove l'unicità va intesa nel senso seguente: date F_1, F_2 come sopra, vale $\forall \alpha \in Ord \; F_1(\alpha) = F_2(\alpha)$.

Dim

L'idea è di costruire una funzione classe $H: Ord \to V$ in maniera tale che, a posteriori, avremo $F_{|\alpha} = H(\alpha)$. Poi, semplicemente, porremo $F(\alpha) \overset{def.}{=} H(s(\alpha))(\alpha)$.
$H(\alpha)$ è l'analogo transfinito di una α-approssimazione nella dimostrazione del teorema di ricorsione numerabile.

Definiamo la funzione classe $H: Ord \to V$ con

$$f = H(\alpha) \overset{def.}{\equiv} \begin{cases} f \text{ è una funzione} \\ \wedge \; Dom(f) = \alpha \\ \wedge \; \forall \beta \in \alpha \quad f(\beta) = G(f_{|\beta}) \end{cases}$$

Verifichiamo, per induzione transfinita su α, che H sia realmente una funzione classe $Ord \to V$, ossia che

$$\forall \alpha \in Ord \quad \exists! f \; f = H(\alpha).$$

- Caso base. $f = H(0) \iff f = \emptyset$.

- Caso $\alpha = s(\gamma)$. Per ipotesi induttiva esiste ed è unica

$f = H(\gamma)$. Sia $f' = f \cup \{(\gamma, G(f))\}$.
Dimostriamo che $f' = H(\alpha)$. Si vede immediatamente che f' è una funzione e $Dom(f') = Dom(f) \cup \{\gamma\} = \gamma \cup \{\gamma\} = S(\gamma)$.
Preso $\beta \in \alpha$
se $\beta < \gamma$ allora $f'(\beta) = f(\beta) = G(f_{|\beta}) = G(f'_{|\beta})$
se $\beta = \gamma$ allora $f'(\gamma) = G(f) = G(f'_{|\gamma})$

Occorre ora dimostrare l'unicità, ossia che se $g = H(\alpha)$ allora $g = f'$. Siccome $Dom(g) = Dom(f') = \alpha$, ci basta verificare che, dato $\delta \in \alpha$, $g(\delta) = f'(\delta)$. Segue dalla definizione che $g_{|\gamma} = H(\gamma)$, e, per l'unicità di $H(\gamma)$, $g_{|\gamma} = f$. Quindi, se $\delta < \gamma$, allora $g(\delta) = g_{|\gamma}(\delta) = f(\delta) = f'(\delta)$. Altrimenti $\delta = \gamma$ e $g(\gamma) = G(g_{|\gamma}) = G(f) = f'(\gamma)$.

- Caso limite. Sia λ un ordinale limite. Assumiamo, per ipotesi induttiva, $\forall \beta < \lambda \; \exists! f \; f = H(\beta)$. Dobbiamo dimostrare $\exists! g \; g = H(\lambda)$. Per l'assioma di rimpiazzamento esiste l'insieme $H[\lambda]$. Poniamo $h = \bigcup H[\lambda]$. Vogliamo dimostrare che $g = H(\lambda) \leftrightarrow g = h$.

Per cominciare, dimostriamo che $h = H(\lambda)$.

- h è una funzione.

  Dobbiamo dire che dati $f_1, f_2 \in H[\lambda]$, questi coincidono sull'intersezione dei loro domini. Siano $f_1 = H(\beta_1)$

$f_2 = H(\beta_2)$. Senza perdita di generalità $\beta_1 < \beta_2$.
Ora, segue dalla definizione che $f_{2|\beta_1} = H(\beta_1)$, per cui, sfruttando l'ipotesi induttiva, $f_{2|\beta_1} = f_1$.

- $\mathrm{Dom}\ h = \lambda$

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

dove, nell'ultima uguaglianza, abbiamo sfruttato il fatto che λ è un ordinale limite

- $\forall \beta < \lambda \quad h(\beta) = G(h_{|\beta})$.

Dato $\beta < \lambda$, siccome λ è limite, $s(\beta) < \lambda$, quindi, detta $f = H(s(\beta))$ abbiamo $h(\beta) = f(\beta) = G(f_{|\beta}) = G(h_{|\beta})$.

Supponiamo, ora, $g = H(\lambda)$, dobbiamo dimostrare $g = h$. Dato $\beta < \lambda$, abbiamo $g_{|\beta} = h_{|\beta} = H(\beta)$ per l'unicità di $H(\beta)$, che abbiamo per ipotesi induttiva. Quindi

$$g(\beta) = G(g_{|\beta}) = G(h_{|\beta}) = h(\beta)$$

Abbiamo stabilito che H è una funzione classe. Definiamo

$$y = F(\alpha) \overset{\text{def.}}{\equiv} \exists f \quad f = H(s(\alpha)) \wedge y = f(\alpha)$$

Dobbiamo verificare che $F(\alpha) = G(F_{|\alpha})$. Detta $f = H(s(\alpha))$ osserviamo che $F_{|\alpha} = f_{|\alpha}$. Preso, infatti, $\beta < \alpha$, e $f' = H(s(\beta))$, abbiamo $F(\beta) = f'(\beta) = f(\beta)$ dove l'ultima uguaglianza vale perché le funzioni $H(-)$ coincidono sull'intersezione dei loro domini.

A questo punto $F(\alpha) = f(\alpha) = G(f_{|\alpha}) = G(F_{|\alpha})$.

Resta da dimostrare l'unicità di F. Ossia che date F_1 e F_2 tali che $\forall \alpha \in Ord \quad F_1(\alpha) = G(F_{1|\alpha})$

$\forall \alpha \in Ord \quad F_2(\alpha) = G(F_{2|\alpha})$

allora $\forall \alpha \in Ord \quad F_1(\alpha) = F_2(\alpha)$.

Per induzione transfinita (v. 1) possiamo assumere che $\forall \beta < \alpha \quad F_1(\beta) = F_2(\beta)$. Ma allora $F_{1|\alpha} = F_{2|\alpha}$, quindi

$$F_1(\alpha) = G(F_{1|\alpha}) = G(F_{2|\alpha}) = F_2(\alpha).$$ ∎

Come per l'induzione, possiamo esprimere la ricorsione transfinita separando i casi zero, successore e limite.

Def Date due classi A, B definiamo la classe $A \times B$

$$x \in A \times B \overset{def}{\equiv} \exists a \in A \; b \in B \; x = (a, b)$$

Con (del teorema di ricorsione transfinita)
Date funzioni classe $G_1 : Ord \times V \to V$ e $G_2 : V \to V$. Dato x_0 un insieme. Esiste un'unica funzione classe F tale che

$$F(0) = x_0$$
$$\forall \alpha \in Ord \quad F(S(\alpha)) = G_1(\alpha, F(\alpha))$$
$$\forall \lambda \in Ord \quad \lambda \text{ limite} \to F(\lambda) = G_2(F|_\lambda)$$

Dim

Applichiamo il teorema con la seguente funzione G

$$G(f) = \begin{cases} \emptyset & \text{se } f \text{ non è funzione con } Dom(f) \in Ord \\ x_0 & \text{se } f = \emptyset \\ G_1(\alpha, f(\alpha)) & \text{se } Dom(f) = \alpha + 1 \text{ per qualche } \alpha \in Ord \\ G_2(f) & \text{altrimenti.} \end{cases}$$

Con. Esistono le funzioni (classe!) di somma, prodotto e potenza di ordinali così definite:

$$\alpha + 0 = \alpha$$
$$\alpha + (s(\beta)) = s(\alpha + \beta)$$
$$\alpha + \lambda = \sup \{ \alpha + \beta \mid \beta < \lambda \}$$

$$\alpha \cdot 0 = 0$$
$$\alpha \cdot s(\beta) = \alpha \cdot \beta + \alpha$$
$$\alpha \cdot \lambda = \sup \{ \alpha \cdot \beta \mid \beta < \lambda \}$$

$$\alpha^0 = 1$$
$$\alpha^{s(\beta)} = \alpha^\beta \cdot \alpha$$
$$\alpha^\lambda = \sup \{ \alpha^\beta \mid \beta < \lambda \}$$

Ossia, le operazioni aritmetiche sugli ordinali si possono definire in modo analogo alle operazioni aritmetiche su ω nei casi 0 e successore, estendendo con continuità nel caso limite.

Def Una funzione classe $F : Ord \to Ord$ mai decrescente — $\alpha < \beta \to F(\alpha) \leq F(\beta)$ — si dice continua se, per ogni ordinale limite λ vale $F(\lambda) = \sup F[\lambda]$.

Nota Sarebbe corretto osservare che, letteralmente, il teorema di ricorsione transfinita non pare sufficiente a garantire l'esistenza, per esempio, della funzione classe

$+ : Ord \times Ord \to Ord$. Il problema è che, fissato α, possiamo costruire ricorsivamente la funzione classe "$\alpha +$" $Ord \to Ord$, ma abbiamo, a quanto pare, una diversa funzione per ogni possibile α. Ci sono due vie di uscita da questo impasse.

La più solida è, forse, dimostrare una versione parametrica del teorema, in cui sia G sia F hanno un argomento in più, un parametro, per accomodare α. Questa è una operazione del tutto elementare, ma aggiunge burocrazia alla dimostrazione, che è già complicata abbastanza.

La seconda strada è, tuttavia, osservare che il teorema si trova già in forma parametrica, anche se non si vede. Una funzione classe non è, infatti, altro che una formula insiemistica — con determinate proprietà — e nulla vieta che questa formula contenga una variabile libera α. Il teorema di ricorsione transfinita dice che, se una certa formula — quella che definisce G — è una funzione classe, allora un'altra formula — quella di F — scritta esplicitamente nella dimostrazione è anch'essa una funzione classe. Ebbene, se la formula per G ha una variabile libera α, questa variabile comparirà altresì nella formula di F, ed avremo così,

in realtà, una funzione classe di due argomenti: α e l'argomento di F.

Comunque sia, questa dei parametri è una sottigliezza che, al livello del nostro corso, si può trascurare. Sono sicuro che, chiunque sia giunto a padroneggiare la materia abbastanza da rendersi conto del problema, capirà anche che la sua soluzione non presenta difficoltà.

Prop: $\alpha+\beta \sim (\alpha, <_\alpha) + (\beta, <_\beta)$

$\alpha \cdot \beta \sim (\alpha, <_\alpha) \cdot (\beta, <_\beta)$

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

Ossia: che si definiscano le operazioni sugli ordinali per ricorsione, o che lo si faccia mediante le corrispondenti operazioni sui buoni ordini, il risultato è il medesimo.

Dim

Per induzione transfinita (seconda versione) su β.

I casi 0 e successore sono conseguenza immediata della definizione delle operazioni sui buoni ordini. Vediamo i limiti.

$\alpha + \lambda \sim (\alpha, <_\alpha) + (\lambda, <_\lambda)$ ← per def. $\sim (\alpha \sqcup \lambda, <_+)$

Fissiamo l'ordinale $\gamma \sim (\alpha, <_\alpha) + (\lambda, <_\lambda)$ e l'isomorfismo $f : \alpha \sqcup \lambda \to \gamma$. Vogliamo calcolare $\alpha + \lambda = \bigcup \{\alpha+\beta \mid \beta < \lambda\}$.

Ora, per ipotesi induttiva, se $\beta < \lambda$ allora $\alpha+\beta \sim \alpha \sqcup \beta$ dove

$\alpha \cup \beta$ è inteso ordinato dall'ordine lessicografico, che coincide con l'ordinamento indotto da $(\alpha, <_\alpha) + (\lambda, <_\lambda)$. Siccome $\alpha \cup \beta$ è segmento iniziale di $\alpha \cup \lambda$, $f[\alpha \cup \beta] = \alpha + \beta$. Ora, siccome λ è limite, $\lambda = \bigcup \{\beta \mid \beta < \lambda\}$. Quindi

$$\gamma = f[\alpha \cup \lambda] = \bigcup \{f[\alpha \cup \beta] \mid \beta < \lambda\}$$

$$\alpha \cup \lambda = \bigcup \{\alpha \cup \beta \mid \beta < \lambda\}$$

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

$\alpha \cdot \lambda \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$ ← per def. $\sim (\alpha \times \lambda, <_\times)$

Procediamo, come prima, fissando

$\gamma \sim (\alpha, <_\alpha) \cdot (\lambda, <_\lambda)$ e $f : \alpha \times \lambda \to \gamma$ isomorfismo

Nuovamente $\beta < \lambda \to f[\alpha \times \beta] = \alpha \cdot \beta$ e

$$\gamma = f[\alpha \times \lambda] = \bigcup \{f[\alpha \times \beta] \mid \beta < \lambda\}$$

$$\alpha \times \lambda = \bigcup \{\alpha \times \beta \mid \beta < \lambda\}$$

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

$\alpha^\lambda \sim (\alpha, <_\alpha)^{(\lambda, <_\lambda)}$

In questo caso, si ripropone il ragionamento dei due casi precedenti, con un leggero problema tecnico. Dato $\beta < \lambda$, nei due casi precedenti, abbiamo usato il fatto che $\alpha \cup \beta$ e $\alpha \times \beta$ sono, rispettivamente, segmenti iniziali di $\alpha \cup \lambda$ e $\alpha \times \lambda$, che poi scriviamo come unione, appunto, di questi sottoinsiemi. Il guaio, adesso, è che l'insieme delle funzioni $\beta \to \alpha$ a sup-
porto

finito non è neppure sottoinsieme dell'insieme delle funzioni $\lambda \to \alpha$ a supporto finito. La soluzione è semplice: detti

$$SF(\Pi \to \alpha) \equiv \{ g : \Pi \to \alpha \text{ a supporto finito} \}$$

$$\bar{E}xT^{\alpha}_{\beta} : SF(\beta \to \alpha) \longrightarrow SF(\lambda \to \alpha)$$

$$g \longmapsto h \quad \text{con} \quad h_{\restriction \beta} = g$$

Ossia l'operatore che estende a $\forall \delta \in \lambda \setminus \beta \; h(\delta) = 0$ una $g : \beta \to \alpha$ con 0 su $\lambda \setminus \beta$.

È chiaro che $\bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)] \sim SF(\beta \to \alpha)$, perché l'ordine $g_1 <_{Lex} g_2$ su $SF(\Pi \to \alpha)$ è definito confrontando le immagini del massimo x tale che $g_1(x) \neq g_2(x)$, e, sugli $x \in \lambda \setminus \beta$, le funzioni nell'immagine di $\bar{E}xT^{\alpha}_{\beta}$ sono identicamente 0. Inoltre, $\bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)]$ è un segmento iniziale di $SF(\beta \to \alpha)$. Possiamo quindi replicare l'argomento dei punti precedenti.

Fissiamo $\gamma \sim (\alpha, <_\alpha)^{(\lambda, <_\lambda)}$ e l'isomorfismo $f : SF(\lambda \to \alpha) \to \gamma$. Per ipotesi induttiva, dato $\beta < \lambda$,

$$\bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)] \sim SF(\beta \to \alpha) \sim \alpha^{\beta}$$

quindi, sfruttando il fatto che $\bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)]$ è un segmento iniziale di $SF(\lambda \to \alpha)$, abbiamo

$$f[\bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)]] = \alpha^{\beta}$$

Ora, data una $g \in SF(\lambda \to \alpha)$, detto $\delta = \max(\mathrm{Supp}\, g)$, siccome λ è limite, $\delta < s(\delta) < \lambda$, e $g \in \bar{E}xT^{\alpha}_{s(\delta)}[SF(s(\delta) \to \alpha)]$, quindi

$$SF(\lambda \to \alpha) = \bigcup \{ \bar{E}xT^{\alpha}_{\beta}[SF(\beta \to \alpha)] \mid \beta < \alpha \}$$

Di conseguenza

$$\gamma = f[SF(\lambda \to \alpha)] = \bigcup \{ f[\mathrm{EXT}^{\alpha}_{\beta}[SF(\beta \to \alpha)]] \mid \beta < \alpha \}$$
$$= \bigcup \{ \alpha^{\beta} \mid \beta < \alpha \} = \alpha^{\lambda}$$ ☐

Per la proposizione precedente, la definizione ricorsiva delle operazioni aritmetiche fra ordinali equivale a quella basata sulle operazioni fra buoni ordini. Quella ricorsiva è una definizione intensionale — il termine è parente più prossimo di intendere che di intenso — ossia specifica le proprietà che caratterizzano un certo oggetto, in questo caso le operazioni ordinali. L'altra è una definizione estensionale — ossia descrive l'oggetto definito. Generalmente, la difficoltà con le definizioni intensionali è dimostrare che il definiendo esiste, con le definizioni estensionali è, invece, ricavarne le proprietà.

Aritmetica ordinale & forma normale di Cantor

In questa sezione studieremo nel dettaglio le proprietà delle operazioni aritmetiche fra gli ordinali. Il risultato principale sarà che ogni ordinale α si scrive, in modo unico, nella forma

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

con $n \in \omega$, $k_1, k_2, \dots, k_n \in \omega \setminus \{0\}$ e $\beta_1 > \beta_2 > \dots > \beta_n$.

Con queste forme normali di Cantor è possibile calcolare le operazioni aritmetiche in modo esplicito.

Nota Per procedere con ordine, assumeremo la definizione ricorsiva delle operazioni ordinali e procederemo unicamente da quella.

Prop Le funzioni $(\alpha,\beta)\mapsto \alpha+\beta$ $(\alpha,\beta)\mapsto \alpha\cdot\beta$ $(\alpha,\beta)\mapsto \alpha^\beta$ sono strettamente crescenti nel secondo argomento — per $\alpha+\beta$ assumendo $\alpha\neq 0$, per α^β assumendo $1<\alpha$ — e mai-decrescenti nel primo argomento.

Per dimostrare la proposizione, ci serviranno queste note.

Nota: Dati due insiemi di ordinali X, Y non vuoti:

$$\forall \alpha\in X\ \exists \beta\in Y\ \alpha\leq\beta \longrightarrow \sup X \leq \sup Y$$

Dim (nota)
Basta osservare che se γ è un maggiorante di Y, allora è anche un maggiorante di X. Infatti, preso $\alpha\in X$ esiste $\beta\in Y$ con $\alpha\leq\beta$, e, siccome $\beta\leq\gamma$, abbiamo $\alpha\leq\gamma$.
Ora $\sup Y$ è un maggiorante di Y, quindi di X, quindi è $\geq \sup X$. ∎

Nota La funzione $\alpha\mapsto s(\alpha)$ è crescente.

Dim (nota) $\alpha<\beta \leftrightarrow s(\alpha)\leq\beta \leftrightarrow s(\alpha)<s(\beta)$ ∎

Dim (proposizione)

$\beta \mapsto \alpha+\beta$ è strettamente crescente

Dobbiamo dire che dati $\beta<\gamma$ vale $\alpha+\beta<\alpha+\gamma$. Procediamo per induzione transfinita (v. 2) su γ.

Caso $\gamma=0$. Vero a vuoto.

Caso $\gamma=s(\delta)$. Siccome $\beta<s(\delta)$, abbiamo $\beta\leq\delta$, quindi

$$\alpha+\beta \leq \alpha+\delta < s(\alpha+\delta) = \alpha+s(\delta) = \alpha+\gamma$$

Dove la prima disuguaglianza si ha perché o $\beta=\delta$ o $\beta<\delta$. Nel primo caso $\alpha+\beta=\alpha+\delta$, nel secondo, per ipotesi induttiva, $\alpha+\beta<\alpha+\delta$.

Caso $\gamma=\lambda$ limite. Dato $\beta<\lambda$, abbiamo $s(\beta)<\lambda$, quindi

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

Dove la prima disuguaglianza vale per ipotesi induttiva.

$\alpha \mapsto \alpha+\beta$ è mai-decrescente.

Dobbiamo dire che se $\alpha<\gamma$, allora $\alpha+\beta\leq\gamma+\beta$. Procediamo per induzione transfinita su β.

Caso $\beta=0$. Immediato.

Caso $\beta=s(\delta)$. Per ipotesi induttiva $\alpha+\delta\leq\gamma+\delta$, e

$$\alpha+\beta = s(\alpha+\delta) \leq s(\gamma+\delta) = \beta+\delta$$

Caso $\beta = \lambda$ limite. Dobbiamo dimostrare che

$$\alpha + \lambda = \sup\{\alpha + \delta \mid \delta < \lambda\} \leq \sup\{\gamma + \delta \mid \delta < \lambda\} = \gamma + \lambda$$

Basta applicare la prima nota osservando che $\alpha + \delta \leq \gamma + \delta$ per ipotesi induttiva.

Le dimostrazioni per il prodotto e l'esponenziale ripetono per disgraziamente lo schema delle precedenti, restano quindi per esercizio. Unica osservazione: nel passo induttivo del prodotto si deve usare il risultato per la somma, e nel passo induttivo dell'esponenziale si deve usare il prodotto. ∎

Esercizio Le ipotesi che $\alpha \neq 0$ per il prodotto e $1 < \alpha$ per l'esponenziale dove sono usate?

Prop: Dati $\alpha, \beta, \gamma \in Ord$

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

Nota: Abbiamo già asserito la proposizione corrispondente per i buoni ordinamenti, ma lasciando la dimostrazione per esercizio. Lasceremo comunque parte della dimostrazione per esercizio, ma non invano: è un esercizio più facile.

Oss Dato $X \subseteq Ord$, se $\sup X \notin X$, allora $\sup X$ è limite.

Dim Se, per assurdo $\sup X = s(\alpha)$, allora, siccome $\sup X$ non è elemento di X, $\forall \beta \in X \ \beta < \sup X$, quindi abbiamo anche $\forall \beta \in X \ \beta \leq \alpha$, per cui α è un maggiorante di X. ☐

Oss. Dati $X \subseteq Ord$ e $\alpha \in Ord$

$$\alpha + \sup X = \sup \{\alpha + \beta \mid \beta \in X\}$$
$$\alpha \cdot \sup X = \sup \{\alpha \cdot \beta \mid \beta \in X\}$$
$$\alpha^{\sup X} = \sup \{\alpha^{\beta} \mid \beta \in X\}$$

Dim Le dimostrazioni sono uguali. Vediamo la prima.
Se $\sup X \in X$, l'enunciato è immediato.
Supponiamo, quindi $\lambda = \sup X \notin X$. Dobbiamo dimostrare che

$$\alpha + \lambda = \sup \underbrace{\{\alpha + \gamma \mid \gamma < \lambda\}}_{A} = \sup \underbrace{\{\alpha + \beta \mid \beta \in X\}}_{B}$$

Basta dire che dato $\gamma_1 < \lambda$ esiste $\beta_1 \in X$ con $\alpha + \gamma_1 \leq \alpha + \beta_1$ e, viceversa, dato $\beta_2 \in X$ esiste $\gamma_2 < \lambda$ con $\alpha + \beta_2 \leq \alpha + \gamma_2$. Preso $\gamma_1 < \lambda$, γ_1 non è un maggiorante di X, quindi esiste $\beta_1 \in X$ con $\gamma_1 < \beta_1$, e, per la monotonia di $+$, $\alpha + \gamma_1 < \alpha + \beta_1$. Preso $\beta_2 \in X$, siccome $\lambda = \sup X$ è limite, $\beta_2 < s(\beta_2) < \lambda$, quindi, ponendo $\gamma_2 = s(\beta_2)$ $\alpha + \beta_2 < \alpha + \gamma_2$. ☐

Dim (proposizione) Sono tutte facili induzioni su γ. Vediamo la prima, le altre restano come esercizio. Conviene affrontarle nell'ordine in cui sono scritte, sinistra - destra, alto - basso.

Dimostriamo $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ per induzione su γ.

Caso $\gamma = 0$. $(\alpha+\beta)+0 = \alpha+\beta = \alpha+(\beta+0)$.

Caso $\gamma = s(\delta)$.

$$(\alpha+\beta)+s(\delta) = s\big(\underbrace{(\alpha+\beta)+\delta}_{\text{Ipotesi induttiva}}\big) = s\big(\underbrace{\alpha+(\beta+\delta)}_{\text{Ipotesi induttiva}}\big)$$
$$= \alpha + s(\beta+\delta) = \alpha+(\beta+s(\delta))$$

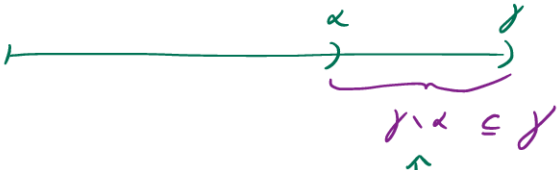
Caso $\gamma = \lambda$ limite.

$$(\alpha+\beta)+\lambda = \sup\{(\alpha+\beta)+\delta \mid \delta<\lambda\}$$
$$= \sup\{\alpha+(\beta+\delta) \mid \delta<\lambda\} \quad \text{(per ipotesi induttiva)}$$
$$= \alpha+\sup\{\beta+\delta \mid \delta<\lambda\} = \alpha+(\beta+\lambda)$$ ∎

Introduciamo, ora, due lemmi che serviranno per calcolare la forma normale di Cantor di un ordinale: la sottrazione e la divisione di ordinali.

<u>Lemma</u> (sottrazione di ordinali)
Dati $\alpha, \gamma \in \mathrm{Ord}$, con $\alpha \leq \gamma$, esiste un unico β tale che $\alpha+\beta=\gamma$.

Intuitivamente: $\gamma \sim \alpha \sqcup (\gamma \setminus \alpha)$ dove $\gamma \setminus \alpha = \{\delta \in \gamma \mid \delta \notin \alpha\}$.



β è il tipo d'ordine di questo.

Vediamo ora una dimostrazione formale.

Dim Abbiamo l'unicità perché la funzione + è crescente nel secondo argomento. Dimostriamo l'esistenza. Se $\alpha = \gamma$ l'enunciato è ovvio. Assumiamo quindi $\alpha < \gamma$. Consideriamo il minimo δ tale che $\gamma < \alpha + \delta$ — δ esiste poiché $\gamma < s(\gamma) \leq \alpha + s(\gamma)$. Se δ è successore, sia $\delta = s(\beta)$. Allora $\alpha + \beta \leq \gamma < s(\alpha + \beta)$, e $\gamma = \alpha + \beta$.

Ci basta quindi mostrare che δ non è limite (ovviamente non è 0). Se lo fosse, $\gamma < \alpha + \delta = \sup \{\alpha + \varepsilon \mid \varepsilon < \delta\}$, ma allora esiste $\varepsilon < \delta$ tale che $\gamma < \alpha + \varepsilon$ contro la minimalità di δ. ▪

Lemma (divisione euclidea di ordinali)
Dati $\alpha, \gamma \in Ord$, con $\alpha \neq 0$, esistono e sono unici $\beta, \rho \in Ord$ tali che $\rho < \alpha$ e $\alpha \cdot \beta + \rho = \gamma$.

Dim
Unicità: per il lemma precedente, fissato β, ρ è unico. Dobbiamo quindi dimostrare l'unicità di β. Supponiamo per assurdo $\alpha \cdot \beta + \rho = \alpha \cdot \beta' + \rho'$ con $\beta < \beta'$ e $\rho, \rho' < \alpha$. Allora
$\alpha \cdot \beta + \rho < \alpha \cdot \beta + \alpha = \alpha \cdot s(\beta) \leq \alpha \cdot \beta' \leq \alpha \cdot \beta' + \rho' = \alpha \cdot \beta + \rho$ ▪

Esistenza: Come nella dimostrazione del lemma precedente, consideriamo il minimo δ tale che $\gamma < \alpha \cdot \delta$ — che esiste in quanto $\gamma \leq \alpha \cdot \gamma < \alpha \cdot s(\gamma)$. Se δ è successore, sia $\delta = s(\beta)$. Allora $\alpha \cdot \beta \leq \gamma$ quindi esiste ρ tale che $\alpha \cdot \beta + \rho = \gamma$. Per concludere il caso δ successore, ci basta quindi dimostrare

che $\rho < \alpha$. Se, per assurdo, $\alpha \leq \rho$, allora

$$\gamma < \alpha \cdot s(\beta) = \alpha \cdot \beta + \alpha \leq \alpha \cdot \beta + \rho = \gamma \quad \lightning$$

Dobbiamo infine escludere che δ sia limite. Se lo fosse, avremmo $\gamma < \alpha \cdot \delta = \sup\{\alpha \cdot \varepsilon \mid \varepsilon < \delta\}$, ma allora esiste $\varepsilon < \delta$ tale che $\gamma < \alpha \cdot \varepsilon$ contro la minimalità di δ. ∎

Teo (forma normale di Cantor)
Ogni ordinale α può essere espresso in maniera unica come somma finita

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \ldots + \omega^{\beta_n} \cdot k_n$$

con $\beta_1 > \beta_2 > \ldots > \beta_n$ ordinali e $k_1, k_2, \ldots, k_n \in \omega \setminus \{0\}$.

Dim
Esistenza: Per induzione transfinita, supponiamo che ogni ordinale $< \alpha$ abbia una forma normale, dobbiamo dimostrare che α ha una forma normale. Sia γ minimo tale che $\alpha < \omega^\gamma$, che c'è perché $\alpha < \omega^{s(\alpha)}$. Come nei lemmi precedenti, consideriamo il caso γ successore. Sia $\gamma = s(\beta_1)$, allora

$$\alpha = \omega^{\beta_1} \cdot k_1 + \rho$$

con $\rho < \omega^{\beta_1}$. Osserviamo intanto che $0 < k_1 < \omega$. Infatti

$0 = k_1 \Rightarrow \alpha = \rho < \omega^{\beta_1}$ contro la minimalità di γ $\lightning$

$\omega \leq k_1 \Rightarrow \omega^\gamma = \omega^{s(\beta_1)} \leq \omega^{\beta_1} \cdot k_1 + \rho = \alpha$ $\lightning$

Ora, $\rho < \omega^{\beta_1} \leq \alpha$, quindi, per ipotesi induttiva, ρ si può

scrivere come somma finita

$$\rho = \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} k_n$$

Siccome $\rho < \omega^{\beta_1}$, abbiamo $\beta_2 < \beta_1$. Quindi

$$\alpha = \omega^{\beta_1} \cdot k_1 + \rho = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} \cdot k_n$$

è una forma normale.

Il caso γ limite si esclude, come al solito, osservando che, altrimenti, $\alpha < \omega^\gamma = \sup \{ \omega^\varepsilon \mid \varepsilon < \gamma \}$ implica che $\alpha < \omega^\varepsilon$ per qualche $\varepsilon < \gamma$, contro la minimalità di γ.

Unicità: Sia α minimo che non ha un'unica forma normale.

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} k_n$$
$$= \omega^{\beta_1'} k_1' + \omega^{\beta_2'} \cdot k_2' + \dots + \omega^{\beta_{n'}'} k_{n'}'$$

Ci basta dire che $\beta_1 = \beta_1'$ e $k_1 = k_1'$, infatti allora

$$\omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} k_n = \omega^{\beta_2'} \cdot k_2' + \dots + \omega^{\beta_{n'}'} k_{n'}' < \omega^{\beta_1}$$

contro la minimalità di α.

Supponiamo $\beta_1 = \beta_1'$, allora $\omega^{\beta_1} \cdot k_1 + \underbrace{\dots}_{< \omega^{\beta_1}} = \omega^{\beta_1} \cdot k_1' + \underbrace{\dots}_{< \omega^{\beta_1}}$ quindi $k_1 = k_1'$ per la divisione euclidea.

Se infine $\beta_1 < \beta_1'$ abbiamo

$$\omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \dots + \omega^{\beta_n} k_n < \omega^{s(\beta_1)} \leq \omega^{\beta_1'} k_1' + \dots$$

Esercizio: dimostrare la disuguaglianza in viola (sono tutte uguali). ∎

Si potrebbe credere che il teorema precedente, applicato ricorsivamente agli esponenti $\beta_1 \dots \beta_n$, implichi ogni ordinale si

può scrivere sotto forma di un'espressione finita composta di somme, prodotti e potenze delle costanti 0, 1, 2, ..., ω. Effettivamente, se valesse $\alpha > \beta_1 > \beta_2 > \dots > \beta_n$ per ogni α, allora questa conclusione sarebbe corretta. Però è possibile esibire un ordinale ε_0 — e, in realtà, un'intera classe propria di ordinali come questo — tale che $\varepsilon_0 = \omega^{\varepsilon_0}$. La forma normale di Cantor di ε_0 è quindi, chiaramente, ω^{ε_0}, e procedere ricorsivamente sull'esponente $\omega^{\omega^{\varepsilon_0}}$, $\omega^{\omega^{\omega^{\varepsilon_0}}}$, &c. non conduce ad un'espressione finita.

Tipo questa:

$$\omega^{\omega^4 \cdot 7 + \omega^2 \cdot 1} \cdot 9 + \omega^{75} + 9$$

Intuitivamente

$$\varepsilon_0 = \omega^{\omega^{\omega^{\cdots}}} \quad \omega \text{ volte}$$

La proposizione seguente è interessante di per sé, ma, in particolare, ci permetterà ora di dimostrare l'esistenza degli ε-number.

Prop Sia $F : Ord \to Ord$ una funzione classe crescente e continua — ossia $F(\lambda) = \sup F[\lambda]$ per λ limite.
Allora, per ogni $\alpha \in Ord$, F ha un punto fisso $\geq \alpha$.
Ossia $\exists \pi \in Ord \; \alpha \leq \pi \wedge F(\pi) = \pi$.

Dim

Definiamo per ricorsione $\pi_0 = \alpha$, $\pi_{S(n)} = F(\pi_n)$ per $n \in \omega$.
Se $F(0) = 0$, allora $\pi = 0$ è un punto fisso.

Se $0 < F(0)$, allora, per induzione, $\forall n\ \pi_n < \pi_{s(n)}$ per cui la funzione $n \mapsto \pi_n$ è crescente. Di conseguenza

$$\pi \overset{def.}{=} \sup\{\pi_n \mid n \in \omega\}$$

è limite (perché $\pi \notin \{\pi_n \mid n \in \omega\}$). Quindi

$$F(\pi) = \sup F[\pi] = \sup\{F(\pi_n) \mid n \in \omega\} = \sup\{\pi_{s(n)} \mid n \in \omega\} = \pi$$ ∎

Esempio Sia ε un punto fisso di $x \mapsto \omega^x$, allora la forma normale di ε è $\varepsilon = \omega^\varepsilon$.

Esercizio Sia $\varepsilon_0 = \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\}$
Formalmente definiamo per ricorsione $\alpha_0 = 1$ $\alpha_{n+1} = \omega^{\alpha_n}$, allora $\varepsilon_0 \overset{def.}{=} \sup\{\alpha_n \mid n \in \omega\}$. Dimostrare che ε_0 è il più piccolo punto fisso della funzione $x \mapsto \omega^x$.

Esercizio Sia $F : Ord \to Ord$ crescente continua. Allora esiste $G : Ord \to Ord$ crescente tale che

$$\forall \alpha \in Ord \quad F(\alpha) = \alpha \iff \exists \beta \in Ord \quad \alpha = G(\beta)$$

Ossia F ha una classe propria di punti fissi.

Esercizio La G dell'esercizio precedente è univocamente determinata da F e continua.

Def (ε-number)
Se negli esercizi precedenti: $F(\alpha) = \omega^\alpha$, allora $\varepsilon_\alpha \overset{def.}{=} G(\alpha)$.
L'α-esimo ε-number ε_α è l'α-esimo punto fisso di $x \to \omega^x$.

I primi due esercizi seguenti saranno assai più facili quando, usando l'assioma della scelta, dimostreremo che l'unione di un insieme numerabile di insiemi numerabili è numerabile

Esercizio * difficile (senza leggere l'idea qua sotto) $|\varepsilon_0| = \aleph_0$

Idea: dimostrare che $\alpha < \varepsilon_0$ se e solo se α può essere scritto a partire da $0, 1, \omega$, applicando le operazioni di somma, prodotto, ed esponente ordinale un numero finito di volte.

Esercizio ** ostico Sia ζ_0 minimo t.c. $\varepsilon_{\zeta_0} = \zeta_0$, allora $|\zeta_0| = \aleph_0$.

Esercizio Sia γ un qualunque ordinale ≥ 2. Ogni ordinale α si scrive in modo unico come somma finita

$$\alpha = \gamma^{\beta_1} k_1 + \ldots + \gamma^{\beta_n} k_n$$

con $\beta_1 > \ldots > \beta_n$ e $k_1 \ldots k_n < \gamma$.

Le operazioni in forma normale di Cantor

È facile ridurre l'aritmetica ordinale, in forma normale di Cantor, ad una piccola collezione di regole meccaniche. Nel contesto del corso, queste regole hanno un'importanza limitata, è però utile sapere che ci sono, ed avere una idea del loro aspetto. Il lemma seguente è un caso particolare, ma è semplice e vale la pena di ricordarlo.

Lemma Siano $\alpha, \beta, \gamma \in Ord$ tali che $\alpha < \omega^\beta \leq \gamma$

Allora $\alpha + \gamma = \gamma$.

Ossia fare $\alpha + \gamma$ assorbe tutti gli α abbastanza piccoli, ossia quelli $<$ di qualche potenza di ω che sia $\leq \gamma$.

Dim

Ci basta dimostrare $\alpha + \gamma \leq \gamma$.

Scrivendo α in forma normale di Cantor otteniamo

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

con $\beta_1 > \ldots > \beta_n$. Quindi $\alpha \leq \omega^{\beta_1} \cdot k$ per qualche $k \in \omega$, infatti:

$$\alpha = \omega^{\beta_1} k_1 + \ldots + \omega^{\beta_n} k_n \leq \omega^{\beta_1} k_1 + \omega^{\beta_1} k_2 + \ldots + \omega^{\beta_1} k_n = \omega^{\beta_1} (k_1 + \ldots + k_n)$$

Ora, da $\alpha < \omega^\beta$ deduciamo $\beta_1 < \beta$ quindi $s(\beta_1) \leq \beta$ e possiamo scrivere $\gamma = \omega^{s(\beta_1)} + \gamma' = \omega^{\beta_1} \cdot \omega + \gamma'$. Da cui

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

dove l'uguaglianza in rosso segue da $k + \omega = \omega$ che segue da

$$k + \omega = \sup \{ k + n \mid n < \omega \} = \omega$$

□

Prop (regole di calcolo in forma normale)

Per le somme ($c \neq 0$, $d \neq 0$):

$$\omega^\alpha \cdot c + \omega^\beta \cdot d = \begin{cases} \omega^\beta \cdot d & \text{se } \alpha < \beta \\ \omega^\alpha (c + d) & \text{se } \alpha = \beta \\ \omega^\alpha \cdot c + \omega^\beta \cdot d & \text{se } \beta < \alpha \end{cases}$$

già in forma normale

Per i prodotti si applica la proprietà distributiva, poi

$$\beta > 0 \to \left(\omega^{\alpha_1}\cdot k_1 + \omega^{\alpha_2}\cdot k_2 + \dots\right)\cdot \omega^{\beta} = \omega^{\alpha_1+\beta}$$

$$n \in \omega\setminus\{0\} \to \left(\omega^{\alpha_1}\cdot k_1 + \omega^{\alpha_2}\cdot k_2 + \dots\right)\cdot n = \omega^{\alpha_1}\cdot k_1 n + \omega^{\alpha_2}\cdot k_2 + \omega^{\alpha_3}\cdot k_3 + \dots$$

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

$$k^{\omega\cdot\alpha} = \omega^{\omega\cdot\alpha}$$

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

Dim

La regola per la somma è immediata.

Per dimostrare

$$\beta > 0 \to \left(\omega^{\alpha_1}\cdot k_1 + \omega^{\alpha_2}\cdot k_2 + \dots\right)\cdot \omega^{\beta} = \omega^{\alpha_1+\beta}$$

osserviamo intanto il caso particolare $n\cdot\omega = \omega$ per $n \in \omega\setminus\{0\}$.

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

Ora, scrivendo $\beta = 1+\gamma$

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

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

La regola

$$n \in \omega\setminus\{0\} \to \left(\omega^{\alpha_1}\cdot k_1 + \omega^{\alpha_2}\cdot k_2 + \dots\right)\cdot n = \omega^{\alpha_1}\cdot k_1 n + \omega^{\alpha_2}\cdot k_2 + \omega^{\alpha_3}\cdot k_3 + \dots$$

si ottiene facilmente per induzione su n.

Questa è immediata: $k^{\omega\cdot\alpha} = k^{\omega\cdot\omega^{\alpha}} = \left(\sup\{k^n \mid n\in\omega\}\right)^{\omega^{\alpha}} = \omega^{\omega^{\alpha}}$

Per dimostrare

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

Partiamo dal caso particolare $(\omega^\alpha \cdot k)^\omega = \omega^{\alpha\omega}$.

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

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

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

Esempi:

- $(\omega+1)^2 = (\omega+1)\cdot(\omega+1) = (\omega+1)\cdot\omega + \omega + 1 = \omega^2 + \omega + 1$
- $(\omega+1)^2\cdot n = \omega^2\cdot n + \omega + 1$ con $n\in\omega\setminus\{0\}$
- $(\omega+1)^2\cdot\omega = (\omega^2+\omega+1)\cdot\omega = \omega^3$
- $(\omega+1)^3 = (\omega^2+\omega+1)(\omega+1) = (\omega^2+\omega+1)\cdot\omega + \omega^2+\omega+1 = \omega^3+\omega^2+\omega+1$
- $(\omega+1)^n = \omega^n + \omega^{n-1} + \dots + 1 = \sum_{i=n}^{0}\omega^i$ con $n\in\omega$

  Per induzione su n. Il passo induttivo è come sopra

$$(\omega+1)^{n+1} = (\omega+1)^n(\omega+1) = \left(\sum_{i=n}^{0}\omega^i\right)\omega + \sum_{i=n}^{0}\omega^i = \omega^{n+1} + \sum_{i=n}^{0}\omega^i = \sum_{i=n+1}^{0}\omega^i$$

- $(\omega+1)^\omega = \omega^\omega$ applicando direttamente la regola.
- $(2\cdot\omega^2 + \omega\cdot 3 + 7)^3$ esame del 27.1.2020

$$(\omega^2 + \omega\cdot 3 + 7)^3 = \underbrace{(\omega^2+\omega\cdot 3+7)\cdot(\omega^2+\omega\cdot 3+7)}\cdot(\omega^2+\omega\cdot 3+7) =$$
$$(\ )\cdot\omega^2 + (\ )\cdot\omega\cdot 3 + (\ )\cdot 7 =$$
$$= \omega^4 + \omega^3\cdot 3 + \omega^2\cdot 7 + \omega\cdot 3 + 7$$

$$= (\omega^4+\dots)\omega^2 + (\omega^4+\dots)\omega\cdot 3 + (\omega^4+\dots)\cdot 7$$
$$= \omega^6 + \omega^5\cdot 3 + \omega^4\cdot 7 + \omega^3\cdot 3 + \omega^2\cdot 7 + \omega\cdot 3 + 7$$

Gli aleph

In questa sezione costruiremo una funzione classe dagli ordinali in sé, $\alpha \mapsto \omega_\alpha$, la cui immagine contiene precisamente un ordinale per ogni cardinalità infinita. Definiremo quindi la scrittura $|X| = \aleph_\alpha$ come $|X| = |\omega_\alpha|$. Ed indagheremo l'aritmetica, che è molto semplice, di somme e prodotti di cardinalità: $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\max(\alpha,\beta)}$. Tratteremo, invece, in seguito l'esponenziale di cardinalità, che non è affatto semplice.

Formalmente, in realtà, dimostreremo che ogni cardinalità infinita che sia la cardinalità di qualche ordinale è un aleph. Resterà quindi da dimostrare che ogni cardinalità è la cardinalità di qualche ordinale, ma per far questo occorre l'assioma della scelta. La cardinalità degli ordinali fanno comodo, per esempio, perché sono confrontabili:

Oss. Dati $\alpha, \beta \in \mathrm{Ord}$, o $|\alpha| < |\beta|$ o $|\alpha| = |\beta|$ o $|\beta| < |\alpha|$.

Dim Basta osservare che o $\alpha \subseteq \beta$ o $\beta \subseteq \alpha$, quindi o $|\alpha| \leq |\beta|$ o $|\beta| \leq |\alpha|$.

Ad ogni cardinalità associamo un rappresentante canonico: il minimo ordinale di quella cardinalità.

Def. $\alpha \in Ord$ è un *ordinale iniziale* se $\forall \beta < \alpha \; |\beta| < |\alpha|$

Esercizio Dimostra che se α è un ordinale iniziale infinito, allora α è limite.

Il nostro scopo è, ora, dimostrare che gli ordinali iniziali sono una classe propria, e quindi enumerabili per mezzo di una funzione classe $Ord \to Ord$, $\alpha \mapsto \omega_\alpha$. Questo è lo strumento tecnico fondamentale

Teo (Hartogs)
Dato un insieme X esiste un ordinale α che non è equipotente ad alcun sottoinsieme di X — ossia $|\alpha| \not\leq |X|$.

Dim Consideriamo l'insieme

$$Y = \{ R \in \mathcal{P}(X \times X) \mid \exists X' \subseteq X \; R \text{ è un buon ordine su } X' \}$$

Sia F la funzione classe che associa, ad ogni buon ordine, l'unico ordinale ad esso isomorfo. Per rimpiazzamento, esiste l'insieme $F[Y]$. Sia α un ordinale con $\alpha \notin F[Y]$. Supponiamo, per assurdo, $|\alpha| = |X'|$ per qualche $X' \subseteq X$. Allora, per definizione, abbiamo una biiezione $f : X' \to \alpha$. Questa, però, ci fornisce un buon ordinamento su X' isomorfo ad α — basta porre $x < y \overset{def.}{\equiv} f(x) < f(y)$ — contrariamente al fatto che $\alpha \notin F[Y]$, ossia non è isomorfo ad alcun buon ordinamento su un sottoinsieme di X. ∎

Def. Dato un insieme X, il **numero di Hartogs** di X, $H(X)$ è il più piccolo ordinale che non è equipotente ad alcun sottoinsieme di X — ossia $H(X) \in Ord$ è minimo tale che $|H(X)| \not\leq |X|$.

Oss. $H(X)$ è un ordinale iniziale.

Dim Per assurdo, se esistesse $\beta < H(X)$ tale che $|\beta| = |H(X)|$, avremmo, per la minimalità di $H(X)$, $|\beta| \leq |X|$, quindi $|H(X)| \leq |X|$ ↯ ∎

Cor La classe degli ordinali iniziali è una classe propria.

Dim Se, per assurdo, esistesse l'insieme X degli ordinali iniziali, allora per ogni α iniziale $|\alpha| \leq |\bigcup X|$, ma $|\bigcup X| < |H(\bigcup X)|$ ↯ ∎

Oss. Dato $\alpha \in Ord$, $H(\alpha)$ è il minimo ordinale tale che $|\alpha| < |H(\alpha)|$.

Dim Siccome la cardinalità degli ordinali sono confrontabili $|\alpha| < |H(\alpha)| \iff |H(\alpha)| \not\leq |\alpha|$. ∎

Il teorema di Hartogs ci permette, per esempio, di esibire un ordinale più che numerabile: $H(\omega)$. Per l'osservazione precedente, infatti, $\aleph_0 = |\omega| < |H(\omega)|$.

Esercizio Cosa c'è di SBAGLIATO nella dimostrazione

seguente dall'esistenza di un $\alpha \in Ord$ più che numerabile? — Sia $\alpha \overset{def.}{=} \sup\{\beta \in Ord \mid |\beta| \leq \aleph_0\}$. Se, per assurdo $|\alpha| \leq \aleph_0$, allora $|s(\alpha)| = |\alpha| + 1 \leq \aleph_0$ quindi, per la definizione di α, $s(\alpha) \leq \alpha$ ma

Gli ordinali iniziali possono essere elencati per mezzo di una funzione classe $\alpha \mapsto \omega_\alpha$, semplicemente, in conseguenza del fatto che sono una classe propria, abbiamo infatti il lemma seguente.

Lemma Sia C una classe propria di ordinali, allora esiste un'unica $F : Ord \to C$ crescente e biunivoca.

Dim
Sia $G : Ord \to C$ definita per ricorsione da
$G(\alpha) =$ il minimo $\beta \in C$ maggiore di tutti gli elementi di $G[\alpha]$
Ci basta dire che F soddisfa la richiesta se e solo se $F(\alpha) = G(\alpha)$ per ogni $\alpha \in Ord$.

Si vede immediatamente che G è crescente, quindi iniettiva. Per verificare la suriettività, sia $\beta \in C$, siccome G è crescente $\beta < s(\beta) \leq G(s(\beta))$. Quindi, per la minimalità di $G(s(\beta))$, $\beta \in G[s(\beta)]$, ed, in particolare, β è nell'immagine di G.

D'altro canto, data F come nell'enunciato, $F(\alpha)$ è maggiore di tutti gli elementi di $F[\alpha]$ poiché F è crescente. Se ci fosse $\beta \in C$ minore di $F(\alpha)$ con questa proprietà, allora avremmo $\beta < F(\gamma)$ per $\gamma < \alpha$ e $\beta > F(\gamma)$ per $\gamma \geq \alpha$, quindi $\beta \neq F(\gamma)$ per ogni γ, contro la suriettività di F. Di conseguenza F soddisfa la definizione ricorsiva di G, e, per il teorema di ricorsione transfinita, $\forall \alpha \in Ord \quad F(\alpha) = G(\alpha)$. □

Def La funzione classe dagli ordinali agli ordinali iniziali infiniti $\alpha \longmapsto \omega_\alpha$ è definita come l'unica crescente e biunivoca fra queste classi.

Prop.
$$\omega_0 = \omega$$
$$\omega_{S(\alpha)} = H(\omega_\alpha)$$
$$\omega_\lambda = \sup\{\omega_\alpha \mid \alpha \in \lambda\} \quad \text{per } \lambda \text{ limite}$$

Dim

I casi 0 e successore sono immediati, vediamo il caso limite. Per la dimostrazione del lemma precedente, ω_λ è il minimo ordinale iniziale maggiore di ogni ω_α con $\alpha \in \lambda$. Basta quindi dimostrare che $\beta \overset{def.}{=} \sup\{\omega_\alpha \mid \alpha \in \lambda\}$ è iniziale. Se così non fosse esisterebbe $\gamma < \beta$ con $|\gamma| = |\beta|$. Ma, per la definizione di estremo superiore, dovrebbe

anche esserci un $\alpha < \lambda$ con $\gamma < \omega_\alpha$. Quindi

$$|\gamma| \leq |\omega_\alpha| < |\omega_{s(\alpha)}| \leq |\lambda|$$

Notazione Usiamo il simbolo $\aleph_\alpha$ come abbreviazione per $|\omega_\alpha|$

Così, per esempio, X è numerabile $\equiv |X| = |\omega_0| \equiv |X| = \aleph_0$

Prop. (Somma e prodotti di aleph)

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

OPERAZIONI TRA CARDINALITÀ

$$\aleph_\alpha + |n| = \aleph_\alpha \cdot |n| = \aleph_\alpha \quad \text{per } n \in \omega \setminus \{0\}$$

Assumiamo per un istante il seguente lemma

Lemma $\forall \alpha \in Ord \quad \aleph_\alpha^2 = \aleph_\alpha$

Dim (proposizione)

Assumiamo, senza perdita di generalità, $\alpha \leq \beta$. Allora

$$\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq 2 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$$

Inoltre $\aleph_\alpha \leq \aleph_\alpha + |n| \leq \aleph_\alpha + \aleph_0 = \aleph_\alpha$

$$\aleph_\alpha \leq \aleph_\alpha \cdot |n| \leq \aleph_\alpha \cdot \aleph_0 = \aleph_\alpha$$

Oss. Se $|X| = \aleph_\alpha$ e $\aleph_0 \leq |Y| \leq |X|$, allora $|Y| = \aleph_\beta$, per qualche $\beta \leq \alpha$.

Dim Senza perdita di generalità possiamo assumere $X = \omega_\alpha$ e $Y \subseteq X$. Allora Y è ben ordinato dall'ordinamento indotto.

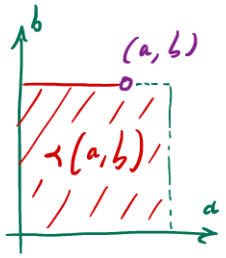
Sia γ il minimo ordinale con $|\gamma| = |\Upsilon|$ — che esiste perché l'ordinale di $(\Upsilon, <_{w_\alpha})$ ha questa proprietà. Siccome γ è il minimo della sua cardinalità, γ è iniziale, quindi esiste β tale che $\gamma = w_\beta$. La monotonia di $x \mapsto w_x$ implica che $\beta \leq \alpha$. ∎

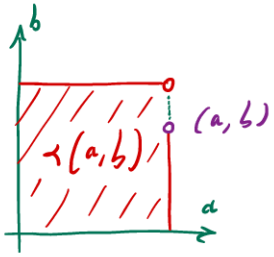
Dim (lemma)

Per induzione transfinita, possiamo assumere $\forall \beta < \alpha \quad \aleph_\beta^2 = \aleph_\beta$ e dobbiamo dimostrare $\aleph_\alpha^2 = \aleph_\alpha$. Strategia: diamo un buon ordine $\prec$ su $w_\alpha \times w_\alpha$ in modo tale che $(w_\alpha \times w_\alpha, \prec) \sim w_\alpha$.

Definiamo

$$(a,b) \prec (a',b') \overset{\text{def.}}{\equiv} \max(a,b) < \max(a',b') \vee \left(\max(a,b) = \max(a',b') \wedge a < a' \right) \vee \left(\max(a,b) = \max(a',b') \wedge a = a' \wedge b < b' \right)$$





Che è il medesimo ordinamento che abbiamo usato per dimostrare $\aleph_0^2 = \aleph_0$.

In pratica, per confrontare (a,b) con (a',b'), si confrontano prima $\max(a,b)$ e $\max(a',b')$; a parità si confrontano a ed a'; se anche queste coincidono, si confrontano b e b'.

Abbiamo già verificato, nella dimostrazione di $\aleph_0^2 = \aleph_0$,

che $\prec$ è un buon ordine (con ω al posto di ω_α, ma le verifiche non cambiano). Resta da verificare che

$$X \overset{\text{def.}}{=} (\omega_\alpha \times \omega_\alpha, \prec) \sim \omega_\alpha.$$

Sia β l'ordinale di $(\omega_\alpha \times \omega_\alpha, \prec)$. Dobbiamo mostrare che $\beta = \omega_\alpha$. Siccome $|\omega_\alpha| \leq |\omega_\alpha \times \omega_\alpha| = |\beta|$, e ω_α è iniziale, abbiamo $\omega_\alpha \leq \beta$, resta quindi da dimostrare che non vale $\omega_\alpha < \beta$, ossia che ω_α non è isomorfo a un segmento iniziale proprio di X.

Fissiamo un segmento iniziale proprio $X_{(a,b)}$ di X, e dimostriamo $|X_{(a,b)}| < \aleph_\alpha$ — quindi, necessariamente, $X_{(a,b)} \not\sim \omega_\alpha$.
Sia $\mu = \max(a,b)$. Siccome $\mu < \omega_\alpha$ e ω_α è iniziale, $s(\mu) < \omega_\alpha$, quindi $|s(\mu)| < \aleph_\alpha$. Di conseguenza, o $|s(\mu)| = \aleph_\gamma$ per qualche $\gamma < \alpha$, oppure $s(\mu) \in \omega$. Nel primo caso $|s(\mu) \times s(\mu)| = \aleph_\gamma^2 = \aleph_\gamma$ per ipotesi induttiva, nel secondo $s(\mu) \times s(\mu)$ è finito, e, in ogni caso $|s(\mu) \times s(\mu)| < \aleph_\alpha$. Siccome $X_{(a,b)} \subseteq s(\mu) \times s(\mu)$, abbiamo allora $|X_{(a,b)}| \leq |s(\mu) \times s(\mu)| < \aleph_\alpha$. ∎

Esercizi: Dimostra che:

- Per ogni n sia $\mathcal{P}^{=n}(X) \overset{\text{def.}}{=} \{Y \in \mathcal{P}(X) \mid |Y| = n\}$
  $\forall n \in \omega \quad |\mathcal{P}^{=n}(\omega_\alpha)| = \aleph_\alpha$
- $|\mathcal{P}^{\text{fin}}(\omega_\alpha)| = \aleph_\alpha$

  Suggerimento: $|\text{sottoins. finiti di } \omega_\alpha| \leq |\{f : n \to \alpha \mid n \in \omega\}|$
  fissa $g : \omega_\alpha \times (\omega_\alpha \cup \{\spadesuit\}) \to \omega_\alpha \cup \{\spadesuit\}$ biunivoca. Definisci $h : \dot{=} \to \omega_\alpha$

con $h(\emptyset) = \ldots$, $h(f) = g(f(0), h(x \mapsto f(x+1)))$.

- $\forall \alpha, \beta \in Ord \quad |\alpha| = |\beta| = \aleph_\gamma \longrightarrow |\alpha+\beta| = |\alpha \cdot \beta| = |\alpha^\beta| = \aleph_\gamma$.
- Se $|X| = \aleph_\alpha$ e $f : X \to Y$ è una funzione, $|f[X]| \leq \aleph_\alpha$.
- Se $|X \cup Y| = \aleph_\alpha$ e $|Y| < \aleph_\alpha$ allora $|X| = \aleph_\alpha$.
- $\forall \alpha \in Ord \quad \aleph_{\alpha+1} < 2^{2^{\aleph_\alpha}}$

L'assioma della scelta

L'assioma della scelta è stato introdotto da Ernst Zermelo, nel 1904, per dimostrare che ogni insieme è bene ordinabile. Si potrebbe dubitare del valore di una dimostrazione ottenuta introducendo un assioma ad hoc, è tuttavia opportuno osservare che l'assioma della scelta è stato usato prima di Zermelo, ma senza accorgersene. Quindi Zermelo non ha tanto costruito un nuovo principio, quanto piuttosto riconosciuto la necessità di codificare un principio già applicato, ma in modo impreciso. Inoltre, gli assiomi che abbiamo introdotto finora non permettono, per esempio, né di affermare né di negare la bene ordinabilità di $\mathbb{R}$. Quindi, se si vuole dare una risposta al problema dell'esistenza di un buon ordine di $\mathbb{R}$, che sia positiva o negativa, questa deve per forza venire da un nuovo assioma. In questo senso, Zermelo dice che il teorema del buon ordinamento è ragionevole perché segue da una ipotesi — l'assioma della scelta — ragionevole. Anzi, così ragionevole che i matematici l'hanno usato senza neppure accorgersi che questo assioma è effettivamente un'ipotesi.

nove e non gi ← ⑨ Assioma della scelta (AC) → Axiom of Choice

"Dato un insieme X di insiemi non vuoti, esiste una funzione di scelta $f: X \to \bigcup X$ tale che $\forall a \in X \quad f(a) \in a$.

In simboli: $\forall X \left(\emptyset \notin X\right) \to \left(\exists f \in {}^{X}(\bigcup X)\ \forall a \in X\ f(a) \in a\right)$.

L'assioma della scelta è di frequente applicato per fissare infiniti elementi. Per esempio, dovendo costruire una successione x_n che tende a $+\infty$, capita di ragionare dicendo *per ogni $n \in \mathbb{N}$ fisso $x_n > n$ che abbia inoltre questa o quella proprietà che mi interessano.* Formalmente, in questo ragionamento, stiamo dicendo *consideno*

$$X = \{\,]n, +\infty[\mid n \in \mathbb{N} \,\}$$

e considero $f : X \to \bigcup X \subseteq \mathbb{R}$ una funzione di scelta per X. Ora, *pongo* $x_n = f(]n, +\infty[)$. Si pone quindi la domanda: perché non ci serve alcun assioma per fissare un elemento — come a dire *consideno un numero ε tale che etc.* — ma ci serve per fissarne infiniti?

Il principio che, sapendo che ci sono oggetti che godono di una certa proprietà, ci permette di fissarne uno, è una legge logica. Questa legge, da un lato, è valida in ogni teoria del primo ordine, non solo nella teoria degli insiemi. D'altro canto, può essere vista come una mera scorciatoia nei ragionamenti, perché se da $\exists x\, \varphi(x)$ possiamo dedurre una ψ che non menziona x, fissando un x che soddisfa $\varphi(x)$, allora si può dimostrare che, a patto di presentare il ragionamento nella maniera opportuna, la conclusione ψ può essere raggiunta senza bisogno di fissare x. In questo senso, la possibilità

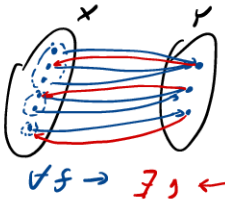
di fissare un oggetto — cioè dare un nome ad un oggetto — è una legge del pensiero: una caratteristica del modo in cui ragioniamo. Tecnicamente, questa legge è rivendicata dal teorema di completezza di Gödel, che dice che la logica del primo ordine è quella giusta per catturare una nozione molto naturale di modello.

L'assioma della scelta, d'altra parte, si può vedere come un modo per fissare infiniti elementi, ma si concretizza in un enunciato insiemistico, che asserisce l'esistenza di un certo insieme: la funzione di scelta. Non si tratta dunque di una caratteristica del nostro modo di ragionare — di una legge del pensiero — perché nulla ci obbliga a pensare in termini insiemistici, e, d'altro canto, nulla obbliga gli insiemi a fare quello che il nostro intuito dice che dovrebbero fare. Insomma, questo è l'intoppo: che non sappiamo esprimere il concetto di fissare infinite variabili se non tramite l'espediente di fissare una singola funzione di scelta. Tuttavia, per fare questo dobbiamo assumere l'esistenza di un certo insieme, appunto la funzione di scelta, che, si può dimostrare, non segue dagli assiomi 1–8.

Dando alle ciance.

Nota: AC equivale all'affermazione che ogni funzione surgettiva ha un'inversa destra, ossia

$\forall f : X \to Y$ surgettiva $\exists g : Y \to X$ $f \circ g = Id$



Dim.

($\to$) Consideriamo $A = f^{-1}(y)$

$$Z \overset{\text{def}}{=} \{ A \in \mathcal{P}(X) \mid \exists y \in Y \ \forall x \in X \ x \in A \leftrightarrow f(x) = y \}$$

Per la suriettività di f gli elementi di Z non sono vuoti; per AC esiste $h : Z \to X$ funzione di scelta. Definiamo

$g(y) \overset{\text{def}}{=} h(f^{-1}(y))$ — più precisamente $g(y) = h(\{x \in X \mid f(x) = y\})$.

Segue immediatamente da questa definizione che $f \circ g(y) = f(g(y)) = y$.

($\leftarrow$) Sia X un insieme di insiemi non vuoti, consideriamo l'insieme $X' = \{(a, A) \in (\bigcup X) \times X \mid a \in A\}$. La funzione

$$f : X' \to X$$
$$(a, A) \longmapsto A$$

è suriettiva, quindi ammette un'inversa destra g.

Ora, la funzione $h : X \to \bigcup(X)$

$$A \longmapsto \text{prima componente di } g(A)$$

è una funzione di scelta per X. ∎

L'assioma della scelta forma, insieme ai due enunciati seguenti — il teorema del buon ordinamento ed il lemma di Zorn — una terna classica di proposizioni equivalenti, nel senso che gli assiomi 1–8 unitamente ad una qualunque delle tre proposizioni implicano le altre due.

Tro (del buon ordinamento — o di Zermelo)

Ogni insieme è ben ordinabile

$$\forall S \; \exists < \in S \times S \quad (S, <) \text{ è un buon ordinamento}$$

Lemma (di Zorn)

Ogni insieme parzialmente ordinato in cui ogni sottocatena* ammetta un maggiorante* ha elementi massimali.*

* Definizioni: Dato $(S, <)$ ordine parziale

- una sottocatena è un $A \in S$ tale che la restrizione di $<$ ad A è un ordine totale
- un maggiorante di $A \subseteq S$ è un $x \in S$ tale che $\forall y \in A \; y \leq x$
- $x \in S$ è un elemento massimale se $\neg \exists y \in S \; x < y$

Tro

Le tre affermazioni precedenti sono equivalenti — ossia si implicano vicendevolmente assumendo gli assiomi 1–8.

Dim (Buon ordinamento → AC)

Dato S insieme di insiemi non vuoti, fissiamo un buon ordinamento $\prec$ su $\bigcup S$. Allora la funzione $f : S \to \bigcup S$

$$x \mapsto \min_{\prec}(x)$$

è una funzione di scelta per S. ∎

Dim (AC → Buon ordinamento — IDEA)

Dimostreremo questo risultato tramite la catena di deduzioni AC → Zorn → Buon ordinamento. Tuttavia conviene studiare l'idea di una dimostrazione diretta.

Fissiamo un insieme X, per AC, esiste una funzione di scelta

$$f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$$
$$A \longmapsto f(A) \in A$$

Ora vorremmo mettere in ordine gli elementi di X così

$x_0 = f(X)$ $x_1 = f(X \setminus \{x_0\})$ $x_2 = f(X \setminus \{x_0, x_1\})$ ...

ogni volta scegliendo un elemento nuovo fra quelli che ancora rimangono da elencare. Chiaramente, non è detto che questo procedimento termini in una quantità numerabile di passi, per cui dovremo definire $x_\omega = f(X \setminus \{x_0, x_1, x_2, \dots\})$ o, più in generale, per ricorsione transfinita

$$x_\alpha = f(X \setminus \{x_\beta \mid \beta < \alpha\})$$

Se supponiamo, per assurdo, che X non sia l'immagine di un ordinale, allora $X \setminus \{x_\beta \mid \beta < \alpha\}$ è necessariamente sempre non vuoto, per cui la costruzione ricorsiva ha senso. Ora, però avremmo una funzione iniettiva $\mathrm{Ord} \to X$, $\alpha \mapsto x_\alpha$, e questa non può esistere per il teorema di Hartogs — infatti non c'è neppure una funzione iniettiva $H(X) \to X$.

Così cade l'ipotesi assurda, e X è ben ordinabile. ∎

Dim (Zorn → Buon ordinamento)

Vogliamo dimostrare che un insieme S è ben ordinabile. Consideriamo

$T = \{\text{funzioni iniettive da un ordinale a } S\}$

$= \{f \in \mathcal{P}(H(S)\times S) \mid f \text{ è una funzione iniettiva} \wedge Dom(f) \in Ord\}$

T è parzialmente ordinato dalla relazione $f < g \overset{def.}{\iff} f \subseteq g$

Ci questo ordine parziale soddisfa l'ipotesi del lemma di Zorn.

Dando per buona la verifica, esiste un elemento massimale f di T.

Se f non fosse surgettiva, esisterebbe $y \in S \setminus Im(f)$, per cui

$f' = f \cup \{(Dom(f), y)\} > f$ contro la massimalità di f. Pertanto

f è una bigezione, quindi S è ben ordinabile.

Verifica dell'ipotesi di Zorn. Se $P \subseteq T$ è una sottocatena, $f = \bigcup P$

è un maggiorante di P. Per controllare che f sia una funzione

basta, infatti, osservare che date $g_1, g_2 \in P$ con $g_1 < g_2$,

$$\forall x \in Dom(g_1) \cap Dom(g_2) \quad g_1(x) = g_2(x)$$

Inoltre f è iniettiva, perché, se $f(x) = f(y)$ allora esistono $g_1, g_2 \in P$

tali che $g_1(x) = g_2(y)$, però, siccome P è una sottocatena, una fra g_1

e g_2 è $\leq$ dell'altra. Ponendo $g_1 \leq g_2$, $g_2(x) = g_1(x) = g_2(y)$ e $x = y$ per

l'iniettività di g_2.

Il dominio di f è un ordinale in quanto

$$Dom(f) = \bigcup \{Dom(g) \mid g \in P\} = \sup \{Dom(g) \mid g \in P\}$$

Infine, f è un maggiorante di P perché, per costruzione, se

$g \in P$ allora $g \subseteq f$ ossia $g \leq f$. ∎

Dim (AC → Zorn)

Sia $(S, <)$ un insieme parzialmente ordinato. Supponiamo che ogni sottocatena di S abbia un maggiorante e che, per assurdo, S non abbia elementi massimali. Questa assunzione implica che ogni sottocatena A ammette un maggiorante stretto, ossia un $x \in S$ tale che $\forall y \in A \; y < x$ — se avessimo infatti una sottocatena che non ammette un maggiorante stretto, allora un maggiorante di quella sottocatena non potrebbe essere $<$ di alcun elemento di S, e quindi sarebbe un elemento massimale.

Denotiamo con $\mathcal{P}^{\neq\emptyset}(S)$ l'insieme delle parti non vuote di S. Consideriamo una funzione di scelta f su $\mathcal{P}^{\neq\emptyset}(S)$.

L'idea, ora, è di costruire per induzione transfinita una funzione classe crescente $F : Ord \to S$ — che chiaramente non può esistere perché altrimenti $F_{|\aleph(S)}$ sarebbe un'immersione di $\aleph(S)$ in S. Vorremmo costruire F tramite la ricorsione:

$$F(\alpha) = f(\{\text{maggioranti stretti di } F[\alpha]\})$$

perché questa costruzione abbia senso, conviene che $F_{|\alpha}$ sia crescente, in questo modo $F[\alpha]$ è una sottocatena, per cui l'insieme dei maggioranti stretti non è vuoto, ed ha senso applicare ad esso la funzione di scelta f. Per assurdo, consideriamo il minimo α tale che $F_{|\alpha}$ non è crescente. Quindi esistono

$\gamma < \delta < \alpha$ tali che $F(\gamma) \not< F(\delta)$. Però siccome $\delta < \alpha$, $F|_\delta$ è crescente, per cui $F(\delta)$ è ben definita ed è un maggiorante stretto di $F[\delta]$, quindi, in particolare, $F(\gamma) < F(\delta)$ $\lightning$.

Questo modo di procedere contiene, però, un'imprecisione formale. Per applicare il teorema di ricorsione transfinita alla costruzione di F dobbiamo scrivere $F(\alpha) = G(F|_\alpha)$. La G della costruzione precedente è

$$G(h) = f(\{\text{maggioranti stretti dell'immagine di } h\})$$

Questa però non è una funzione classe $V \to V$, perché non è definita se l'immagine di h non ha maggioranti stretti in S. Il ragionamento si arrangia così: si fissa $\clubsuit \notin S$ e si definisce

$$F(\alpha) = \begin{cases} f(\{\text{magg. stretti di } F[\alpha]\}) & \text{se } F|_\alpha \text{ è } \alpha \to S \text{ crescente} \\ \clubsuit & \text{altrimenti} \end{cases}$$

ora tutti i casi sono coperti ed è lecito applicare il teorema di ricorsione transfinita. Se F non fosse una funzione classe crescente $\mathrm{Ord} \to S$, ci sarebbe il minimo α tale che $F|_\alpha$ non è $\alpha \to S$ crescente, e, ragionando come prima si ottiene un assurdo.

Ricapitolando, negando la tesi, abbiamo costruito una funzione classe crescente, dunque iniettiva: $\mathrm{Ord} \to S$, che non può esistere per il teorema di Hartogs. La tesi è quindi provata. $\square$

Conseguenze immediate di AC

Prop Ogni insieme è equipotente ad un ordinale iniziale. In particolare, ogni cardinalità infinita è un aleph.

Dim Per il teorema del buon ordinamento ogni insieme è ben ordinabile, quindi, per le proprietà degli ordinali iniziali, equipotente ad un unico ordinale iniziale. La seconda affermazione segue dal fatto che gli ω_α sono tutti e soli gli ordinali iniziali infiniti ∎

Oss Viceversa, assumere che ogni insieme è equipotente ad un ordinale implica AC.

Dim Dal fatto ogni X è equipotente ad un ordinale deduciamo il teorema del buon ordinamento. Se $|X| = |\alpha|$ con $\alpha \in Ord$, è una biiezione fra X e α, quindi un buon ordinamento di X. ∎

Cor Tutte le cardinalità sono confrontabili

$$\forall X, Y \quad |X| < |Y| \vee |X| = |Y| \vee |Y| < |X|$$

Dim Segue dal fatto che le cardinalità degli ordinali sono confrontabili. ∎

Oss La confrontabilità delle cardinalità implica AC.

Dim Dimostriamo il teorema del buon ordinamento. Consideriamo il confronto fra $|X|$ e $|\mathcal{H}(X)|$. Per la definizione di

$H(X)$ non può valere $|H(X)| \leq |X|$. Quindi $|X| < |H(X)|$.
Ossia esiste $f: X \to H(X) \in Ord$ iniettiva. □

Cor $\forall X$ infinito $|X \times X| = |X|$

Dim Se $|X| = \aleph_\alpha$ abbiamo $|X \times X| = |\omega_\alpha \times \omega_\alpha| = |\omega_\alpha| = |X|$ □

Nota Anche $|X \times X| = |X|$ implica AC. Questo però è un teorema di Tarski che vedremo più avanti

Cor $\forall X$ X infinito $\iff \aleph_0 \leq |X|$

Ossia ogni insieme infinito ha un sottoinsieme numerabile

Dim Abbiamo già dimostrato la freccia $\leftarrow$, mentre la freccia opposta segue dal fatto che $\aleph_0$ è il minimo altef infinito. □

Ricordiamo che un insieme si dice **finito secondo Dedekind** se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Prop X è finito $\longleftrightarrow$ X è finito secondo Dedekind

Dim $\longrightarrow$ risultato già dimostrato.

$\leftarrow$ Supponiamo che X non sia finito, allora $|X| = \aleph_\alpha$ per qualche α, quindi esiste $f: \omega_\alpha \to X$ biunivoca.

$$g: X \to X \setminus \{f(0)\}$$
$$x \mapsto f \circ g \circ f^{-1}(x)$$

è una bigezione fra X e $X \setminus \{f(0)\} \subsetneq X$. □

Prop $0 < |X| \leq |Y| \iff \exists f : Y \to X$ surgettiva

Dim. $\to$ Data $g : X \to Y$ iniettiva e $a \in X$, la funzione

$$f : Y \to X$$
$$y \mapsto \begin{cases} g^{-1}(y) & \text{se } y \in g[X] \\ a & \text{altrimenti} \end{cases}$$

è surgettiva.

$\leftarrow$ Data $f : Y \to X$ surgettiva, un'inversa destra di f è iniettiva. ∎

Prop Se $|S| \leq \aleph_\alpha$ e $\forall A \in S \; |A| \leq \aleph_\alpha$, allora $|\bigcup S| \leq \aleph_\alpha$.

Dim. Possiamo assumere che $\emptyset \notin S \neq \emptyset$. Basta esibire una funzione surgettiva $f : \omega_\alpha \times \omega_\alpha \to \bigcup S$. Sia $g : \omega_\alpha \to S$ surgettiva. Per ipotesi, per ogni $A \in S$, l'insieme $H_A \overset{\text{def.}}{=} \{h : \omega_\alpha \to A \mid h \text{ è surgettiva}\}$ è non vuoto. Sia l una funzione di scelta per $\{H_A \mid A \in S\}$. Allora

$$f : \omega_\alpha \times \omega_\alpha \to \bigcup S$$
$$(x, y) \mapsto (l(H_{g(x)}))(y) \quad \text{è surgettiva.}$$

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 $h = l(H_A)$ è surgettiva $\omega_\alpha \to A$, esiste y tale che $z = h(y) = (l(H_{g(x)}))(y)$. ∎

Cor L'unione numerabile (risp. al più numerabile) di insiemi numerabili (risp. al più numerabili) è numerabile (risp. al più numerabile).

Oss Sia $\mathcal{P}^{\leq n}(X) \overset{\text{def}}{=} \{A \in \mathcal{P}(X) \mid |A| \leq n\}$

Se X è infinito e $0 < n < \omega$, allora $|\mathcal{P}^{\leq n}(X)| = |X|$

Dim La disuguaglianza $|X| \leq |\mathcal{P}^{\leq n}(X)|$ segue dal fatto che la funzione $X \to \mathcal{P}^{\leq n}(X)$, $a \mapsto \{a\}$ è iniettiva.

Per dimostrare la disuguaglianza opposta, sia $|X| = \aleph_\alpha$, allora $|{}^n X| = \aleph_\alpha^n = \aleph_\alpha$, quindi basta osservare che la funzione seguente è surjettiva: $X^n \to \{A \in \mathcal{P}(X) \mid 0 < |A| \leq n\} \subseteq \mathcal{P}^{\leq n}(A)$

$f \mapsto \mathrm{Im}(f)$ ∎

Esercizio Se X è infinito e $0 < n < \omega$, $|\{A \in \mathcal{P}(X) \mid |A| = n\}| = |X|$

Prop Se X è infinito, $|\mathcal{P}^{\text{fin}}(X)| = |X|$

Dim $\mathcal{P}^{\text{fin}}(X) = \bigcup \{\mathcal{P}^{\leq n}(X) \mid n \in \omega\}$ è unione di $\aleph_0 < |X|$ insiemi di cardinalità $|X|$. ∎

Prop 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.

Dim

Da un lato, 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.

Per il viceversa, se $(A, <)$ non è un buon ordine sia $S \subseteq A$ con $S \neq \emptyset$ che non ha minimo. Consideriamo una funzione di

scelta $f: \mathcal{P}^{\neq\emptyset}(S) \to S$, e, fissato un $a_0 \in S$ 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 ∎

Esempi di applicazione di AC

Vediamo qui alcuni esempi di applicazione di AC al di fuori del contesto, strettamente, della teoria degli insiemi. Un primo esempio, molto facile, è dimostrare che, in uno spazio primo-numerabile (ossia, ogni punto ha una base di intorni numerabile, per esempio uno spazio metrico, per via delle palle di raggio $\frac{1}{n}$) un punto x è nella chiusura $\bar{A}$ di A se è limite di una successione di punti di A.
Considerando, per concretezza, lo spazio $\mathbb{R}$, abbiamo:

Prop. Sia $A \subseteq \mathbb{R}$, allora

$$x \in \bar{A} \iff \exists \{x_i\}_{i\in\omega} \left(\forall i \in \omega\ x_i \in A\right) \wedge \left(\lim_{i\to\infty} x_i = x\right)$$

$$\overset{\text{def.}}{=} \forall \varepsilon > 0 \quad]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$$

Dim.

$\leftarrow$ $\forall \varepsilon > 0 \ \exists i \ x_i \in]x-\varepsilon, x+\varepsilon[\cap A$

quindi $\forall \varepsilon > 0 \quad]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$ ossia, per definizione, $x \in \bar{A}$.

$\rightarrow$ Sia f una funzione di scelta per $\mathcal{P}(A) - \{\emptyset\}$.
Definiamo $x_i = f\left(A \cap \left]x - \frac{1}{i+1}, x + \frac{1}{i+1}\right[\right)$ ∎

Un'altra applicazione è l'esistenza di basi degli spazi vettoriali

infinito-dimensionali. Questo ragionamento, in realtà, si applica non solo alla dipendenza lineare, ma a qualunque relazione di dipendenza che soddisfi il lemma dello scambio di Steinitz, per esempio la dipendenza algebrica.

Promemoria.

Sia F un campo e V uno spazio vettoriale su F.

$A \subseteq V$ è linearmente indipendente se per ogni $a_1 \dots a_n \in A$ e $x_1 \dots x_n \in F$ $\quad x_1 a_1 + \dots + x_n a_n = 0 \leftrightarrow x_1 = \dots = x_n = 0$

$B \subseteq V$ linearmente indipendente è una base se dato qualunque $v \in V$ esistono $b_1 \dots b_n \in B$ $x_1 \dots x_n \in F$ tali che $v = x_1 b_1 + \dots + x_n b_n$

Ossia B è una base di V se ogni elemento di V si scrive in modo unico come combinazione lineare FINITA di elementi di B.

Non avrebbe senso, in generale, parlare di combinazioni lineari se non finite.

L'osservazione seguente è la chiave per applicare il lemma di Zorn

Oss. B è una base se e solo se è un sottoinsieme linearmente indipendente di V massimale rispetto all'inclusione.

Dim

(base $\to$ massimale) Se B non fosse massimale, ci sarebbe $v \in V$ tale che $B \cup \{v\}$ è linearmente indipendente. Ma $v = b_1 x_1 + \dots + b_n x_n$

per opportuni $b_1 \dots b_n \in B$ e $x_1 \dots x_n \in F$. Quindi $B \cup \{v\}$ non è indipendente perché $b_1 x_1 + \dots + b_n x_n + v \cdot (-1) = 0$ ■

(massimale → base) Sia B massimale, $v \in V$. Se $v \in B$, chiaramente $v = v \cdot 1$. Altrimenti, per la massimalità di B, $B \cup \{v\}$ non è indipendente. Di conseguenza esistono $b_1 \dots b_n \in B$ $x_1 \dots x_n, y \in F$ tali che $x_1 b_1 + \dots + x_n b_n + y v = 0$ ma non $x_1 = \dots = x_n = y = 0$.
Se y fosse $= 0$, avremmo $x_1 = \dots = x_n = 0$ per l'indipendenza di B.
Quindi $y \neq 0$ e $v = \left(-\frac{x_1}{y}\right) b_1 + \dots + \left(-\frac{x_n}{y}\right) b_n$ ■

Prop Dato uno spazio vettoriale V e $X \subseteq V$ linearmente indipendente, esiste una base B di V tale che $X \subseteq B$.
Dim 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 $a_1 \dots a_n \in \bigcup C$. Consideriamo $A_1 \dots A_n \in C$ 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,

$x_1 a_1 + \dots + x_n a_n = 0 \iff x_1 = \dots = x_n = 0$ ■

Esercizio Sia B una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale, determina $|B|$.

Esempio Esiste una funzione $f : \mathbb{R} \to \mathbb{R}$ tale che

$$\forall x, y \in \mathbb{R} \quad f(x+y) = f(x) + f(y)$$

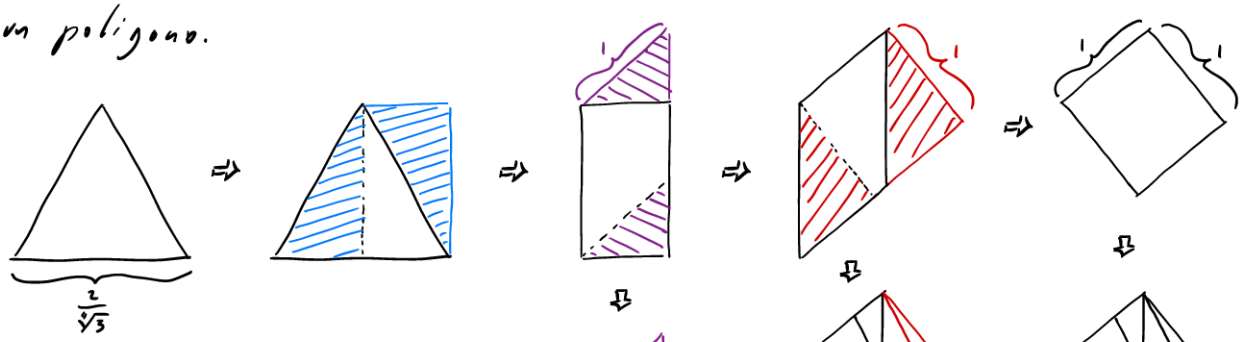
tuttavia f **non** è della forma $f(x) = k \cdot x$.

Dim Sia B una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale. Fissiamo $b_1 \in B$. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{Q}$$

$$x \longmapsto y_1 \text{ tale che } \exists y_2 \dots y_n \; x = b_1 y_1 + \dots + b_n y_n.$$ ∎

È noto dall'antichità che due poligoni aventi la stessa area sono scomponibili in un numero finito di poligoni congruenti — *equiscomponibili* — questa si può considerare, anzi, la definizione stessa di area di un poligono.



Per passare da un poligono ad un quadrato equivalente, spezzalo in triangoli, poi trasforma i triangoli in rettangoli, poi passando per un parallelogramma, poi trasforma un rettangolo in un altro con uno dei due lati arbitrario. Porta tutti i rettangoli ad avere un

lato uguale, unisci li, e trasforma il nuovo rettangolo in un quadrato, di nuovo col trucco del parallelogramma.

Nota Curiosamente, Euclide non definisce l'area, ma, dal momento che ci ragiona aggiungendo e togliendo pezzi congruenti, possiamo adattare, a posteriori, una definizione basata sull'equiscomponibilità alla matematica classica. Ancora più curiosamente, i ragionamenti di Euclide richiedono, in realtà di definire $Area(A) = Area(B)$ se e solo se esistono due poligoni C e D, rispettivamente non sovrapposti ad A e B, equiscomponibili fra loro, tali che $A \cup C$ e $B \cup D$ sono equiscomponibili. Per dedurre che, in realtà, due poligoni con la stessa area sono equiscomponibili serve l'assioma di Archimede, che Euclide non aveva. La sistemazione formale di questi concetti è dovuta a Hilbert, e al XIX secolo.

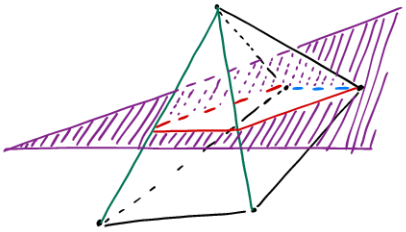
Ebbene, tutti questi anacronismi solo per dire che in tre dimensioni non funziona.

Teo (Dehn)
Un cubo ed un tetraedro regolare (sia pure aventi il medesimo volume) non si possono scomporre in un numero finito di poliedri congruenti.

Dim
Supponiamo di avere una funzione $f: \mathbb{R} \to \mathbb{R}$ additiva tale che $f(x) = 0$ se e solo se x è un multiplo razionale di π — $x = k\pi$ con $k \in \mathbb{Q}$.

Definiamo il valore di un poliedro come la somma dei valori dei suoi spigoli, definiti, a loro volta, dicendo che il valore di uno spigolo di lunghezza l che forma un angolo diedro di ampiezza α è $l \cdot f(\alpha)$.

Quando tagliamo un poliedro A con un piano, ottenendo così due nuovi poliedri B e C, la somma dei valori di B e C equivale al valore di A. Infatti, il taglio dà luogo ad alcuni spigoli nuovi, in rosso, ma la somma dei due angoli diedri, poniamo α_1 e α_2, che insistono su uno qualunque di essi è π e $l \cdot f(\alpha_1) + l \cdot f(\alpha_2) = l \cdot f(\alpha_1 + \alpha_2) = 0$. Può dividere spigoli vecchi, in verde, in due, poniamo di lunghezza l_1 e l_2, senza alterare l'angolo diedro, per cui $(l_1 + l_2) f(\alpha) = l_1 f(\alpha) + l_2 f(\alpha)$. Infine, in azzurro, può spezzare l'angolo diedro lasciando inalterata la lunghezza, e si conclude similmente.



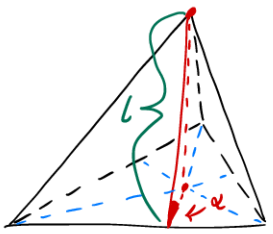
Abbiamo concluso che il valore è invariante per equiscomposizioni, ci resta da costruire f. Fissiamo una base B di $\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$ tale che $\pi \in B$ — ossia estendendo l'insieme linearmente indipendente $\{\pi\}$. Definiamo

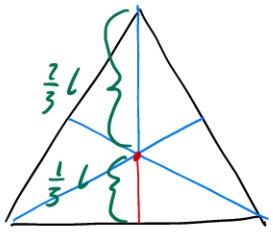
$$f(\pi q_0 + b_1 q_1 + \dots + b_n q_n) = b_1 q_1 + \dots + b_n q_n$$

per ogni $q_0 \dots q_n \in \mathbb{Q}$ e $b_1 \dots b_n \in B \setminus \{\pi\}$

f è quindi la proiezione su un complementale del sottospazio $\pi\mathbb{Q}$.
L'additività di f è conseguenza immediata della $\mathbb{Q}$-linearità.
Inoltre, per definizione, $f(x)=0$ se e solo se x si scrive nella forma πq_0 con $q_0 \in \mathbb{Q}$.

Ora si chiama che il valore di un cubo è nullo, perché tutti i diedri hanno ampiezza $\frac{1}{2}\pi$. Occorre quindi dimostrare che il valore di un tetraedro regolare è non nullo. Si vede facilmente che i diedri del tetraedro valgono $\alpha = \arccos\frac{1}{3}$ quindi basta dire che questo α non è multiplo razionale di π. In altri termini, che, se $n \in \mathbb{N}$, $n\alpha$ non è multiplo intero di π.





Questo fatto si può esprimere, altresì, dicendo che $z^n \neq \mathbb{R}$ dove $z \overset{def}{=} \cos\alpha + i\cdot\sin\alpha \in \mathbb{C}$. Ora, $z = \frac{1}{3}(1+2i\sqrt{2})$. Si vede immediatamente, per induzione, che $(1+2i\sqrt{2})^n = x_n + y_n i\sqrt{2}$ per qualche $x_n, y_n \in \mathbb{Z}$. Inoltre, sempre per induzione, riducendo x_n e y_n modulo 3, otteniamo che, per n dispari $x_n \equiv 1\ (3)$ $y_n \equiv 2\ (3)$, per n pari e $\neq 0$ $x_n \equiv 2\ (3)$ $y_n \equiv 1\ (3)$. In nessun caso, in particolare $y_n = 0$. ∎

Veniamo ora ad un'altra applicazione che da luogo ad un risultato negativo: il controesempio di Vitali.

Premessa Una misura σ-additiva su $\mathcal{P}(\mathbb{R})$ è una funzione $\mu : \mathcal{P}(\mathbb{R}) \to \mathbb{R}^{\geq 0} \cup \{+\infty\}$ tale che $\mu(\emptyset) = 0$ e, se $\{A_i\}_{i\in\omega}$ è una

successione di elementi **disgiunti** di $\mathcal{P}(\mathbb{R})$ allora

$$\mu\left(\bigcup\{A_i \mid i\in\omega\}\right) = \sum_{i=0}^{+\infty} \mu(A_i)$$

μ si dice **invariante per traslazioni** se $\forall x\in\mathbb{R}$, $A\in\mathcal{P}(\mathbb{R})$

$$\mu(A) = \mu\left(\{y\in\mathbb{R} \mid y-x\in A\}\right) \overset{\text{def}}{=} A+x$$

Oss. (monotonia) Se $A\subseteq B\subseteq\mathbb{R}$, $\mu(A)\leq\mu(B)$.

Dim $\mu(B) = \mu(A\cup(B\setminus A)) = \mu(B)+\mu(B\setminus A) \geq \mu(A)$.

Esercizio Esibire una misura σ-additiva ed invariante per traslazioni su $\mathcal{P}(\mathbb{R})$.

Prop. Non esiste una misura σ-additiva ed invariante per traslazioni μ su $\mathcal{P}(\mathbb{R})$ tale che $\mu([0,1[)=1$

Dim. Supponiamo, per assurdo, che 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 ci, infatti, assurdo perché se $\mu(A_i)-\mu(A_j)=0$, allora $\mu([0,1[) = \sum_{i=0}^{\infty} 0 = 0 \neq 1$, ma se $\mu(A_i)=\mu(A_j)=k>0$, allora $\mu([0,1[) = \sum_{i=0}^{\infty} k = +\infty \neq 1$.

Sia $i\mapsto q_i$ un'enumerazione di $\mathbb{Q}$. Fissiamo una base B di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale. Possiamo assumere $b_0 = 1\in B$ — altrimenti prendiamo $b_0\in B$ e moltiplichiamo tutti gli elementi di B per $\frac{1}{b_0}$. Definiamo

$$R_i \overset{\text{def}}{=} \{x\in\mathbb{R} \mid x = r_0\cdot 1 + q_i\cdot b_1 + r_2\cdot b_2 + \dots + r_n\cdot b_n \text{ con } r_0, r_2 \dots r_n\in\mathbb{Q}\}$$

$A_i \overset{\text{def.}}{=} R_i \cap [0,1[$

Ossia $x \in R_i$ se e solo se la componente b_1 di x è q_i. Siccome la successione $\{q_i\}_{i\in\omega}$ enumera i razionali, gli insiemi $\{R_i\}_{i\in\omega}$ sono una partizione di $\mathbb{R}$. Di conseguenza gli insiemi $\{A_i\}_{i\in\omega}$ sono 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 $A_i + \delta$.

$$x \in R_i \iff x \in \mathrm{Span}(\mathcal{B}\setminus\{b_1\}) + q_i b_1 \qquad = q_i b_1 + (q_j - q_i) b_1$$
$$\iff x + \delta \in \mathrm{Span}(\mathcal{B}\setminus\{b_1\}) + q_j b_1 \iff x + \delta \in R_j$$

Quindi $A_i + \delta = (R_i + \delta) \cap [\delta, \delta+1[= R_j \cap [\delta, \delta+1[$
$$= \underbrace{(R_j \cap [\delta, k[)}_{\overset{\text{def}}{=} X_1} \cup \underbrace{(R_j \cap [k, \delta+1[)}_{\overset{\text{def}}{=} X_2}$$

Similmente a prima, per $n \in \mathbb{N}$

$$x \in R_j \iff x \in \mathrm{Span}(\mathcal{B}\setminus\{b_1\}) + \mathbb{Q} + q_j b_1 \qquad \mathbb{Q} + n = \mathbb{Q}$$
$$\iff x + n \in \mathrm{Span}(\mathcal{B}\setminus\{b_1\}) + \mathbb{Q} + q_j b_1 \iff x + n \in R_j$$

Quindi $Y_1 \overset{\text{def}}{=} X_1 - k + 1 = R_j \cap [\delta - k + 1, 1[$
$Y_2 \overset{\text{def}}{=} X_2 - k = R_j \cap [0, \delta - k + 1[$

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

$$\mu(A_j) = \mu(Y_1) + \mu(Y_2) = \mu(X_1) + \mu(X_2) = \mu(A_i + \delta) = \mu(A_i)$$ ∎

Esercizio Una maniera alternativa di dimostrare la proposizione

precedente è come segue:

- considerare la relazione di equivalenza su $[0,1[$ data da $x \sim y \overset{\text{def.}}{\iff} x-y \in \mathbb{Q}$.
- fissare un $V \subseteq [0,1[$ che contiene uno ed un solo elemento per ogni classe di equivalenza — qui si usa AC
- dimostrare $[0,1[\subseteq S \overset{\text{def.}}{=} \bigcup \{ V+r \mid r \in \mathbb{Q} \cap]-1,1[\} \subseteq [-1,2[$ per cui $1 \leq \mu(S) \leq 3$
- osservare, tuttavia, che se $\mu(V)=0$ allora $\mu(S)=0$ e se $\mu(V)>0$ allora $\mu(S)=+\infty$.

Il teorema di Cantor-Bendixson

Il teorema di Cantor-Bendixson, che permette di dimostrare l'ipotesi del continuo limitatamente ai sottoinsiemi chiusi di $\mathbb{R}$, non è, tecnicamente, un'applicazione di AC. Tuttavia è un esempio di come le tecniche insiemistiche — segnatamente la ricorsione transfinita — hanno conseguenze in matematica.

Come abbiamo osservato all'inizio del corso, quello di indagare la struttura dei sottoinsiemi chiusi di $\mathbb{R}$ è stato, forse, uno dei problemi che hanno motivato lo sviluppo della teoria di Cantor. In questa sezione ne vedremo, in qualche misura, la soluzione.

Promemoria Se $S \subseteq \mathbb{R}$ diciamo che $x \in \mathbb{R}$ è un *punto di accumulazione* di S se $x \in (S \setminus \{x\})$ — ossia se esiste una successione $\{x_i\}_{i \in \omega}$ di punti di $S \setminus \{x\}$ tale che $\lim_{i \to \infty} x_i = x$.
Diciamo che $S \subseteq \mathbb{R}$ è *perfetto* se S coincide con l'insieme dei suoi punti di accumulazione.

Esempio Un intervallo chiuso è perfetto.

Esercizio Esibire un insieme perfetto non vuoto avente *parte interna** vuota. → $\stackrel{\text{def}}{=} \{x \in S \mid \exists \varepsilon > 0 \;]x-\varepsilon, x+\varepsilon[\subseteq S\}$

Prop Se $S \subseteq [0,1]$ è perfetto allora $|S| = 2^{\aleph_0}$

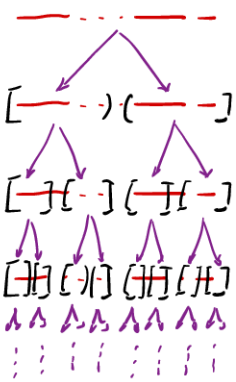
Per dimostrare questa proposizione, è comoda l'osservazione seguente.

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.

Dim Un singoletto non è perfetto, quindi esistono $x_1, x_2 \in S$ con $x_1 < x_2$. Ora si danno 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 $S_1 = S \cap [0, x_3]$, $S_2 = S \cap [x_4, 1]$.
- Se esiste $x_3 \in [x_1, x_2] \setminus S$: definiamo $S_1 = S \cap [0, x_3[$ e $S_2 = S \cap]x_3, 1]$. ∎

Dim (proposizione) L'idea è di usare l'osservazione per dividere l'insieme S in due, poi, ricorsivamente ciascuna delle due parti nuovamente in due, e così via. Si ottiene un albero binario di sottoinsiemi perfetti di S. Quest'albero ha $2^{\aleph_0}$ rami infiniti,



uno per ogni successione di cifre binarie, e l'intersezione degli insiemi di ogni ramo è un'intersezione di compatti uno nell'altro, quindi non vuota. Per cui abbiamo una funzione iniettiva dalle successioni di cifre binarie a S.

Sia $\mathcal{P}$ l'insieme dei sottoinsiemi perfetti di $[0,1]$. Fissiamo $f : \mathcal{P} \to \mathcal{P} \times \mathcal{P}$ che manda ogni $X \in \mathcal{P}$ in una coppia (X_1, X_2)

con $X_1 \cup X_2 \subseteq X$ e $X_1 \cap X_2 = \emptyset$. Assegnamo ad ogni sequenza binaria finita $\alpha : n \to \{0,1\}$, un sottoinsieme perfetto S_α di S, procedendo per ricorsione su n. A questo scopo, data $\alpha : n \to \{0,1\}$ e $b \in \{0,1\}$ indichiamo con $\alpha^\frown b$ la sequenza $\alpha \cup \{(n,b)\} : n+1 \to \{0,1\}$. Allora definiamo

$$S_\emptyset = S \qquad S_{\alpha^\frown b} = \begin{cases} X & \text{se } b=0 \\ Y & \text{se } b=1 \end{cases} \quad \text{dove } (X,Y) = f(S_\alpha)$$

Data una successione infinita $\tau : \omega \to \{0,1\}$, definiamo infine

$$S_\tau = \bigcap \{ S_\alpha \mid \alpha = \tau_{\restriction n}, n \in \omega \}$$

Osserviamo che, per ogni successione τ, $S_\tau \neq \emptyset$, infatti, per ogni $n \in \omega$, $S_{\tau_{\restriction S(n)}} \subseteq S_{\tau_{\restriction n}}$, i compatti $S_{\tau_{\restriction n}}$ costituiscono, quindi, una catena di compatti non vuoti, per cui la loro intersezione, che è S_τ, non è vuota. Inoltre, se $\tau \neq \rho$ allora $S_\tau \cap S_\rho = \emptyset$. Infatti, detto n il minimo indice per cui $\tau_n \neq \rho_n$ — senza perdita di generalità assumiamo $\tau_n = 0$ e $\rho_n = 1$ — abbiamo quindi $S_{\tau_{\restriction S(n)}} = A$ e $S_{\rho_{\restriction S(n)}} = B$ con $(A,B) = f(S_{\tau_{\restriction n}}) = f(S_{\rho_{\restriction n}})$, quindi $S_\tau \subseteq A$ e $S_\rho \subseteq B$ sono disgiunti poiché $A \cap B = \emptyset$.

In conclusione, per ogni $\tau \in 2^\omega$ possiamo scegliere un punto in S_τ e questa funzione è iniettiva, quindi $2^{\aleph_0} \leq |S|$. D'altro canto $|S| \leq |\mathbb{R}| = 2^{\aleph_0}$, quindi $|S| = 2^{\aleph_0}$. ☐

Esercizio Dimostrare la proposizione con $\mathbb{R}$ al posto di $[0,1]$.

Esercizio In quali passaggi della dimostrazione precedente abbiamo fatto uso dell'assioma della scelta?

Esercizio Dimostrare la proposizione senza fare uso di AC.

Teo (Cantor–Bendixson)
Sia $C \subseteq \mathbb{R}$ chiuso. Allora $C = A \cup P$ con $|A| \leq \aleph_0$ e P perfetto

Dim

Dato un insieme $X \subseteq \mathbb{R}$ definiamo il suo derivato

$$X' \overset{\text{def}}{=} \{\text{punti di accumulazione di } X\}$$
$$= \{a \in \mathbb{R} \mid \forall \varepsilon > 0 \ \ ]a-\varepsilon, a+\varepsilon[\cap (X \setminus \{a\}) \neq \emptyset\}$$

Chiaramente, se X è chiuso

$$X' = X \setminus \{\text{punti isolati di } X\}$$

dove un punto $a \in X$ è isolato se $\exists \varepsilon > 0 \ \ ]a-\varepsilon, a+\varepsilon[\cap X = \{a\}$.

Ci servirà l'osservazione seguente: $a \in X$ è un punto isolato di X se e solo se esiste un intervallo $]s,t[$ avente 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, per $\alpha \in \mathrm{Ord}$, tramite la seguente ricorsione

$$C_0 = C \qquad C_{\alpha+1} = C'_\alpha \qquad C_\lambda = \bigcap \{C_\alpha \mid \alpha < \lambda\}$$

Per vedere che tutti gli insiemi C_α sono chiusi basta osservare

che il derivato di un chiuso è chiuso ed un'intersezione di chiusi è chiusa. Osserviamo, inoltre, che $\alpha \leq \beta \to C_\beta \subseteq C_\alpha$. Definiamo

$$P = \bigcap_{\alpha \in Ord} C_\alpha = \{ a \in \mathbb{R} \mid \forall \alpha \in Ord \ \ a \in C_\alpha \}$$
$$A = C \setminus P$$

Dobbiamo dimostrare che P è perfetto e $|A| \leq \aleph_0$.

P è perfetto.

P è chiuso in quanto intersezione di chiusi, occorre quindi 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 $x \notin C_\alpha$ abbiamo, quindi α_x 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 e $a \notin C_{s(\beta)}$ che implica $a \notin P$ ↯

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 deve essere successore, perché, se fosse limite, avremmo $C_{\alpha_x} = \bigcap \{ C_y \mid y < \alpha_x \}$ ed esisterebbe $y < \alpha_x$ tale che $x \notin C_y$. Possiamo quindi definire β_x tramite $\alpha_x = s(\beta_x)$. Per cui C_{β_x} è l'ultimo dei C_α a contenere x.

Siccome $x \in C_{\beta_x}$ ma $x \notin C_{s(\beta_x)} = C'_{\beta_x}$, x deve essere un punto

isolato di C_{n_x}. Scegliamo un intervallo $]s_x, t_x[$ avente estremi razionali che isola x in C_{n_x}.
Ci basta dimostrare 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, $n_x \leq n_y$. Allora

$$y \in]s_y, t_y[\cap C_{n_y} \subseteq]s_x, t_x[\cap C_{n_x} = \{x\}$$

Di conseguenza $y = x$. ∎

Cor Se $C \subseteq \mathbb{R}$ è chiuso allora o $|C| = 2^{\aleph_0}$ o $|C| \leq \aleph_0$.
"Vale l'ipotesi del continuo per i sottoinsiemi chiusi di $\mathbb{R}$"

Dim Scriviamo $C = A \cup P$ usando il teorema. Se $P = \emptyset$ allora $|C| = |A| \leq \aleph_0$. Altrimenti $2^{\aleph_0} = |P| \leq |C| \leq 2^{\aleph_0}$ ∎

L'esempio seguente mostra che l'ipotesi che C sia chiuso non può essere omessa.

Esempio Esiste $S \subseteq \mathbb{R}$ non numerabile che non contiene alcun insieme perfetto non vuoto.

Dim Sia $|\mathbb{R}| = \aleph_\alpha$. E sia $f : \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\} \to \mathbb{R}$ una funzione di scelta. È facile vedere che

$$2^{\aleph_0} = |\text{intervalli}| \leq |\text{perfetti non vuoti}| \leq |\text{chiusi}| = |\text{aperti}| = 2^{\aleph_0}$$

Quindi esiste una funzione surgettiva

$$\omega_\alpha \longrightarrow \text{perfetti non vuoti}$$
$$\beta \longmapsto P_\beta$$

Definiamo per ricorsione transfinita

$$g : \omega_\alpha \longrightarrow \mathbb{R} \times \mathbb{R}$$
$$\beta \longmapsto (g_1(\beta), g_2(\beta))$$

con

$$g_1(\beta) = f\left(P_\beta \setminus (g_1[\beta] \cup g_2[\beta])\right)$$
$$g_2(\beta) = f\left(\mathbb{R} \setminus (g_1[\beta] \cup g_2[\beta] \cup \{g_1(\beta)\})\right)$$

La funzione g è ben definita perché, per ogni $\beta < \omega_\alpha$, $|\beta| < \aleph_\alpha$, quindi $|g_1[\beta]| < \aleph_\alpha$ e $|g_2[\beta]| < \aleph_\alpha$. D'altro canto $|P_\beta| = 2^{\aleph_0} = |\mathbb{R}| = \aleph_\alpha$. Di conseguenza, f è sempre applicata ad insiemi non vuoti.

Dimostriamo che $S = g_2[\omega_\alpha]$ soddisfa la tesi:
La funzione $g_2 : \omega_\alpha \to \mathbb{R}$ è iniettiva, perché, se $\gamma < \beta$, $g_2(\gamma) \in g_2[\beta]$ e $g_2(\beta) = f\left(\mathbb{R} \setminus (\ldots g_2[\beta] \ldots)\right) \neq g_2(\gamma)$.
Per cui $|g_2[\omega_\alpha]| = 2^{\aleph_0}$.

Fissiamo ora un perfetto non vuoto P_β. Dobbiamo dimostrare che $P_\beta \not\subseteq g_2[\omega_\alpha]$. 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 $\beta \leq \gamma$, $g_2(\gamma) = g_1(\beta) \in g_1[\gamma] \cup g_2[\gamma] \cup \{g_1(\gamma)\}$ ↯ ∎

Riepilogo delle forme equivalenti di AC

Abbiamo visto che diverse proposizioni sono equivalenti allo assioma della scelta. Per esempio, fissati gli altri assiomi, AC e l'affermazione che ogni insieme è ben ordinabile si implicano vicendevolmente. Elenchiamo le principali forme equivalenti dell'assioma della scelta.

Prop Assumendo gli assiomi di estensionalità, insieme vuoto, separazione, paio, unione, parti, infinito e rimpiazzamento, le seguenti proposizioni sono equivalenti:

- l'assioma della scelta
- ogni funzione surgettiva ha un'inversa destra
- il teorema del buon ordinamento
- il lemma di Zorn
- ogni cardinalità infinita è un aleph
- $\forall X, Y \ |X| \leq |Y| \vee |Y| \leq |X|$
- $\forall X \ |X| \geq \aleph_0 \to |X \times X| = |X|$ ← Dobbiamo ancora dimostrare questo!

Teo (Tarski)
Se per ogni X infinito $|X \times X| = |X|$, allora vale AC.

Dim

Dato un insieme infinito X cerchiamo un buon ordinamento di X. Basta costruire una funzione γ che immerge X negli ordinali.

Applicando l'ipotesi a $X \sqcup H(X)$ otteniamo

$$|X \times H(X)| \leq |(X \sqcup H(X)) \times (X \sqcup H(X))| = |X \sqcup H(X)|$$

Quindi esiste una funzione iniettiva $f : X \times H(X) \to X \sqcup H(X)$.

Per ogni $a \in X$ consideriamo la funzione

$$\begin{aligned} f_a : H(X) &\to X \sqcup H(X) \\ b &\mapsto f(a,b) \end{aligned}$$

Se l'immagine $f_a[H(X)]$ di f_a fosse contenuta in X, allora avremmo una funzione iniettiva da $H(X)$ a X, che non può esistere. Quindi $f_a[H(X)] \cap H(X) \neq \emptyset$. Definiamo

$$\begin{aligned} g : X &\to H(X) \\ a &\mapsto \min\left(f_a[H(X)] \cap H(X)\right) \end{aligned}$$

Questa funzione è ben definita perché $f_a[H(X)] \cap H(X) \subseteq H(X)$ è un insieme di ordinali, dunque ha un minimo. Inoltre g è iniettiva perché, se $a \neq b$, $g(a) = f(a, \text{qualcosa})$ e, per l'iniettività di f, $f(a, \text{qualcosa}) \neq f(b, \text{qualcosa}) = g(b)$. ∎

Aritmetica cardinale

Notazione κ è un cardinale $\overset{\text{def.}}{\equiv}$ κ è un ordinale iniziale

$\kappa = \lambda^+ \overset{\text{def.}}{\equiv}$ κ è il minimo cardinale $> \lambda$ $\left(\omega_\alpha^+ = \omega_{\alpha+1}\right)$

Possiamo definire le operazioni di prodotto, somma e potenza cardinale, per cui se $\kappa = \omega_\alpha$ $\lambda = \omega_\beta$ $\mu = \omega_\gamma$ scriviamo

$k = \lambda + \mu$, $k = \lambda \cdot \mu$, $k = \lambda^{\mu}$ per $\aleph_\alpha = \aleph_\beta + \aleph_\gamma$, $\aleph_\alpha = \aleph_\beta \cdot \aleph_\gamma$, $\aleph_\alpha = \aleph_\beta^{\aleph_\gamma}$.

Occorre fare attenzione a non confondere le operazioni cardinali con quelle ordinali. In questa sezione, ci occupiamo di operazioni cardinali

Siccome ad ogni cardinalità corrisponde un unico ordinale iniziale che abbia quella cardinalità, possiamo scrivere

$$k = |X| \overset{\text{def.}}{\iff} k \text{ è un cardinale e } |k| = |X|$$

Def (Somme e prodotti infiniti)
Sia I un insieme e $\{k_i\}_{i \in I}$ una famiglia di cardinali.
Formalmente, la famiglia $\{k_i\}_{i \in I}$ è una funzione f tale che $\mathrm{Dom}(f) = I$ e $\forall i \in I \; f(i)$ è un cardinale, k_i è un'abbreviazione per $f(i)$.

$$\sum_{i \in I} k_i \overset{\text{def.}}{=} \left| \bigcup \{ k_i \times \{i\} \mid i \in I \} \right|$$

$$\prod_{i \in I} k_i \overset{\text{def.}}{=} \left| \{ f : I \to \sup_i k_i \mid \forall i \in I \; f(i) \in k_i \} \right|$$

Nota Se $\forall i \in I \; k_i = |X_i|$ e gli insiemi X_i sono a due a due disgiunti allora

$$\sum_{i \in I} k_i = \left| \bigcup \{ X_i \mid i \in I \} \right|$$

Dim (richiede AC!) $|k_i \times \{i\}| = |k_i| \cdot 1 = |k_i| = |X_i|$
Per ogni i scegliamo una biezione $f_i : k_i \times \{i\} \to X_i$.

Allora $f : \bigcup \{ k_i \times \{i\} \mid i \in I \} \longrightarrow \bigcup \{ X_i \mid i \in I \}$

$(a, i) \longmapsto f_i(a)$

(ossia $f = \bigcup \{ f_i \mid i \in I \}$) è una biiezione. ∎

Nota Se $\forall i \in I \;\; k_i = |X_i|$

$$\sum_{i \in I} k_i \geq \left| \bigcup \{ X_i \mid i \in I \} \right|$$

$$\prod_{i \in I} k_i = \left| \{ f : I \to \bigcup \{ X_i \mid i \in I \} \mid \forall i \; f(i) \in X_i \} \right|$$

Dim Per la prima disuguaglianza si osserva che la funzione definita nella dimostrazione precedente è surgettiva — solo l'iniettività richiede, infatti, che gli insiemi X_i siano disgiunti.

La seconda è del tutto analoga. Date $g_i : k_i \to X_i$ biiezioni

$$g : \{ f : I \to \dots \mid \forall i \; f(i) \in k_i \} \longrightarrow \{ f : I \to \dots \mid \forall i \; f(i) \in X_i \}$$

$$g(f)(i) = g_i(f(i))$$

è una biiezione. ∎

Oss

$$k^{\sum_{i \in I} \lambda_i} = \prod_{i \in I} k^{\lambda_i}$$

Dim Un elemento dell'insieme a sinistra è una funzione $f : \bigcup \{ \lambda_i \times \{i\} \mid i \in I \} \to k$ e possiamo identificarla con la funzione $\tilde{f} : I \to \bigcup \{ k^{\lambda_i} \mid i \in I \}$

$i \mapsto \tilde{f}_i$ definita da $\tilde{f}_i(a) = f(a, i)$ ∎

Esercizio Valgono le proprietà ragionevoli, per esempio

- Se $\forall i \in I \quad k_i \leq \lambda_i$

$$\sum_{i\in I} k_i \leq \sum_{i\in I} \lambda_i \qquad \prod_{i\in I} k_i \leq \prod_{i\in I} \lambda_i$$

- $\forall i \in I \quad k_i \leq \sum_{i\in I} k_i$
- Se $\forall i \in I \quad k_i \neq 0$

$$|I| \leq \sum_{i\in I} k_i \qquad \forall i \in I \quad k_i \leq \prod_{i\in I} k_i$$

- Se $I = I_1 \cup I_2$

$$\sum_{i\in I} k_i = \left(\sum_{i\in I_1} k_i\right) + \left(\sum_{i\in I_2} k_i\right) \qquad \prod_{i\in I} k_i = \left(\prod_{i\in I_1} k_i\right)\cdot\left(\prod_{i\in I_2} k_i\right)$$

- $\sum_{i\in k} \lambda = k \cdot \lambda \qquad \prod_{i\in k} \lambda = \lambda^k$
- $\left(\prod_{i\in I} k_i\right)^\lambda = \prod_{i\in I} k_i^\lambda$

Prop: Supponiamo che k_i per $i \in I$ siano cardinali $\neq 0$. Allora

$$\sum_{i\in I} k_i = |I| \cdot \sup_{i\in I} k_i = \max\left(|I|, \sup_{i\in I} k_i\right)$$

Dim $(\leq)$ $\sum_{i\in I} k_i \leq \sum_{i\in I}\left(\sup_{j\in I} k_j\right) = |I| \cdot \sup_{i\in I} k_i$

$(\geq)$ Siccome $|I| \cdot \sup_{i\in I} k_i$ è il massimo fra $|I|$ e $\sup_{i\in I} k_i$, basta verificare che $\sum_{i\in I} k_i \geq |I|$ e $\sum_{i\in I} k_i \geq \sup_{i\in I} k_i$.

La prima è conseguenza dell'esercizio precedente.

La seconda segue osservando che $\forall j \in I \quad \sum_{i\in I} k_i \geq k_j$. ∎

Teo (König) Se $\forall i \in I \quad k_i < \lambda_i$ allora $\sum_{i\in I} k_i < \prod_{i\in I} \lambda_i$

Dim Dimostriamo che non può valere il $\geq$.

Siano: $A = \{ f : I \to \sup_i \lambda_i \mid \forall i \in I \ f(i) \in \lambda_i \}$

$B = \bigcup \{ k_i \times \{i\} \mid i \in I \}$

Data $f : A \to B$, dobbiamo dimostrare che f non è surgettiva.

Consideriamo $f_i : k_i \longrightarrow \lambda_i$

$\alpha \longmapsto f(\alpha, i)(i) \in \lambda_i$

Siccome $k_i \in \lambda_i$, f_i non può essere surgettiva, quindi, per ogni i, $\lambda_i \setminus \mathrm{Im}(f_i) \neq \emptyset$. Per l'assioma di scelta, c'è

$g : I \longrightarrow \sup_{i \in I} \lambda_i$

$i \longmapsto g(i) \in \lambda_i \setminus \mathrm{Im}(f_i)$.

Chiaramente $g \in B$, verifichiamo che $g \notin \mathrm{Im}(f)$.

Se $g = f(\alpha, i)$ allora $g(i) = f(\alpha, i)(i) = f_i(\alpha) \in \mathrm{Im}(f_i)$ ↯

Esempio

$$k = \sum_{i \in k} 1 < \prod_{i \in k} 2 = 2^k$$

Quindi il teorema di Cantor ($|X| < |\mathcal{P}(X)|$) si può vedere come conseguenza della disuguaglianza di König.

Esempio

$$\aleph_w = \sum_{\alpha \in w} w_\alpha < \prod_{\alpha \in w} w_{\alpha+1} \leq \aleph_w^{\aleph_0}$$

Quindi, in particolare, possiamo dedurre che $2^{\aleph_0} \neq \aleph_w$

infatti vale

$$2^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0}$$

mentre avremmo $<$ se, per assurdo, $2^{\aleph_0} = \aleph_w$.

Def (cofinalità – v.1)

Dato un cardinale infinito k, la cofinalità di k, $\mathrm{cof}(k)$, 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 $k=\sum_{i\in\mu}\lambda_i$.

In altri termini, $\mathrm{cof}(k)$ è il minimo numero di parti $<k$ in cui può essere diviso un insieme di cardinalità k.

Esempi

$\mathrm{cof}(\aleph_0)=\aleph_0$ un'unione finita di insiemi finiti è finita

$\mathrm{cof}(\aleph_\omega)=\aleph_0$ $\sum_{\alpha<\omega}\aleph_\alpha=\aleph_\omega$, se $|I|<\aleph_0$, $\sum_{\alpha\in I}\aleph_\alpha=\aleph_{\max(I)}<\aleph_\omega$

$\mathrm{cof}(\aleph_{\omega_2})=\aleph_{\omega_2}$ $\aleph_{\omega_2}=\sum_{i\in I}k_i\le\sum_{i\in I}\aleph_{\omega_1}=\max(|I|,\aleph_{\omega_1})\longrightarrow|I|=\aleph_{\omega_2}$

Def (cofinalità – v.2)

Dato un insieme ordinato $(S,<)$, diciamo che $A\subseteq S$ è cofinale in S se $\forall x\in S\ \exists y\in A\ x\le y$ — ossia A non ha maggioranti stretti in S. La cofinalità di $(S,<)$ è la minima cardinalità di un sottoinsieme cofinale di S.

Esempi

$\mathrm{cof}(\omega)=\aleph_0$ ω è cofinale in se stesso, un sottoins. finito ha massimo

$\mathrm{cof}(\mathbb{R},<)=\aleph_0$ $\mathbb{N}$ è cofinale in $\mathbb{R}$

$\mathrm{cof}(\omega+1)=1$ $\{\omega\}$ è cofinale in $\omega+1$

$\mathrm{cof}(\omega_\omega)=\aleph_0$ $\{\omega_0,\omega_1,\omega_2,\dots\}$ è cofinale in $\omega_\omega=\sup_{i\in\omega}\omega_i$

$\mathrm{cof}(\omega_{\omega_2})=\aleph_{\omega_2}$ Per la proposizione segnata

Prop. Se k è un cardinale infinito $\mathrm{cof}^{(V.1)}(k) = \mathrm{cof}^{(V.2)}(k)$.

Dim Siano $\lambda_1 = \mathrm{cof}^{(V.1)}(k)$ e $\lambda_2 = \mathrm{cof}^{(V.2)}(k)$.

$(\lambda_1 \leq \lambda_2)$ Sia A cofinale in k. Siccome k è limite $\alpha \in k \to s(\alpha) \in k$ quindi $\forall \alpha \in k \; \exists \beta \in A \; s(\alpha) \leq \beta$ da cui $\forall \alpha \in k \; \exists \beta \in A \; \alpha \in \beta$ ossia $k = \bigcup A$. Abbiamo quindi $k \leq \sum_{\beta \in A} |\beta| \leq \sum_{\beta \in A} k = k$. Siccome $\forall \beta \in A \; \beta < k$ e k è iniziale, vale anche $\forall \beta \in A \; |\beta| < k$.
L'identità $\sum_{\alpha \in A} |\alpha| = k$ dimostra quindi che $\lambda_1 \leq |A|$.

$(\lambda_2 \leq \lambda_1)$ Se $\lambda_1 = k$ non c'è niente da dimostrare, perché k stesso è cofinale in sé. Assumiamo quindi $\lambda_1 < k$. Per ipotesi, esiste $\{k_i\}_{i \in I}$ con $|I| = \lambda_1$, tale che

$$k = \sum_{i \in I} k_i = \max\left(|I|, \sup_{i \in I} k_i\right) = \sup_{i \in I} k_i$$

(perché $|I| = \lambda_1 < k$)

Dimostriamo che $A \overset{\text{def.}}{=} \{k_i \mid i \in I\}$ è cofinale in k. Da questo segue l'asserto in quanto $|A| \leq |I| = \lambda_1$. Dato $x < k$, se x non fosse un maggiorante di A, avremmo $\forall i \in I \; k_i < x$ ma allora

$$\sup_{i \in I} k_i \leq x < k \quad \rightsquigarrow \quad \blacksquare$$

Oss. Sia $(S, <_S)$ totalmente ordinato e $T \subseteq S$ cofinale in S. Indichiamo con $<_T$ la restrizione di $<_S$ a T $\quad <_T \overset{\text{def.}}{=} <_S \cap (T \times T)$
Allora $\mathrm{cof}(S, <_S) = \mathrm{cof}(T, <_T)$.

Dim 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 $x \in S$ dobbiamo trovare un $y \in A$ con $x \leq y$. Siccome T è cofinale in S esiste $t \in T$ con $x \leq t$, e, siccome A è cofinale in T, esiste $y \in A$ con $t \leq y$, per cui $x \leq y$.

- Dato $B \subseteq S$ cofinale, siccome T è cofinale in S, per ogni $b \in B$ possiamo scegliere un $y_b \in T$ con $b < y_b$. Sia $B' = \{y_b \mid b \in B\} \subseteq T$. Siccome la funzione $b \mapsto y_b$ è suriettiva da B a B' abbiamo $|B'| \leq |B|$. Inoltre preso un qualunque $x \in S$ esiste $b \in B$ con $x \leq b$, quindi $x \leq y_b \in B'$. ∎

Oss. Sia k un cardinale infinito, $\mathrm{cof}(k) \leq k$

Dim $k = \sum_{i \in k} 1$

Oss. Sia $(S, <)$ totalmente ordinato, allora

$$\mathrm{cof}(\mathrm{cof}(S, <)) = \mathrm{cof}(S, <)$$

e, in particolare, per ogni cardinale k, $\mathrm{cof}(\mathrm{cof}(k)) = \mathrm{cof}(k)$.

Dim Sia $k = \mathrm{cof}(S, <)$ e $A \subseteq S$ cofinale con $|A| = k$. Supponiamo, per assurdo, $\mathrm{cof}(k) < k$, quindi esistono $\{k_i\}_{i \in I}$ con $|I| = \mathrm{cof}(k)$ e $\forall i \in I \; k_i < k$ tali che $\sum_{i \in I} k_i = k$. Fissiamo allora una famiglia $\{A_i\}_{i \in I}$ di sottoinsiemi di A disgiunti tali che $\forall i \in I \; |A_i| = k_i$ e $\bigcup \{A_i \mid i \in I\} = A$. Per ogni $i \in I$, A_i non è cofinale in S, siccome $|A_i| = k_i < k = \mathrm{cof}(S)$, quindi possiamo scegliere un maggiorante stretto $y_i \in S$ di A_i.

Detto $B = \{a_i \mid i \in S\}$, abbiamo $|B| \leq |I| < k$. D'altra canto, B è cofinale in S, infatti, preso un $x \in S$, siccome A è cofinale, esiste $a \in A$ con $x \leq a$, questo a deve appartenere ad uno degli insiemi A_i, quindi $x \leq a \leq y_i \in B$. Per cui abbiamo trovato un insieme B cofinale in S con $|B| < k = \text{cof}(S)$. ↯

Vedremo ora alcune applicazioni della cofinalità

Corollari (del teorema di König)

Per k cardinale infinito, e λ cardinale ≥ 2.

$$k < k^{\text{cof}(k)} \qquad\qquad k < \text{cof}(\lambda^k)$$

Dim Cominciamo dalla prima. Detta $\mu = \text{cof}(k)$, esiste una famiglia $\{k_i\}_{i \in \mu}$ tale che $\forall i \; k_i < k$ e $k = \sum_{i \in \mu} k_i$.

Per König abbiamo

$$k = \sum_{i \in \mu} k_i < \prod_{i \in \mu} k = k^{\mu} = k^{\text{cof}(k)}$$

Passando alla seconda, assumiamo, per assurdo, $\text{cof}(\lambda^k) \leq k$, e applichiamo la prima a λ^k, che è infinito perché $\geq 2^{\aleph_0}$:

$$\lambda^k < (\lambda^k)^{\text{cof}(\lambda^k)} = \lambda^{k \cdot \text{cof}(\lambda^k)} \leq \lambda^{k \cdot k} = \lambda^k$$ ↯

Def La funzione $\beth$ "ghimel" è definita sui cardinali infiniti da

$$\beth(k) = k^{\text{cof}(k)}$$

Con $\qquad k < \beth(k) \qquad\qquad \text{cof}(k) < \text{cof}(\beth(k))$

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 $\forall \alpha \ \aleph_\alpha < \kappa \to 2^{\aleph_\alpha} < \kappa$
- *debolmente inaccessibile* se è regolare e limite
- *(fortemente) inaccessibile* se è regolare e limite forte

Oss. Un cardinale limite forte è anche limite

Dim Se $\kappa = \aleph_{\alpha+1}$ allora $\kappa \leq 2^{\aleph_\alpha}$, quindi κ non è limite forte. ∎

Prop I cardinali successori sono regolari.

Dim Sia $\kappa = \aleph_{\alpha+1}$. Supponiamo per assurdo $\lambda = \mathrm{cof}(\kappa) < \kappa$.
Allora esiste $\{\kappa_i\}_{i<\lambda}$ con $\forall i < \lambda \ \kappa_i < \kappa$ e $\sum_{i<\lambda} \kappa_i = \kappa$.
Quindi:

$$\kappa = \sum_{i<\lambda} \kappa_i \leq \sum_{i<\lambda} \aleph_\alpha = \aleph_\alpha \cdot \lambda \leq \aleph_\alpha < \kappa$$ ↯

∎

Cor Se κ è successore $\beth(\kappa) = 2^\kappa$

Dim $\beth(\kappa) = \kappa^\kappa = 2^\kappa$ $\quad \left(2^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa\right)$ ∎

Prop. Se λ è un ordinale limite. $\mathrm{cof}(\aleph_\lambda) = \mathrm{cof}(\lambda)$

Dim Il sottoinsieme $\{\omega_\alpha \mid \alpha < \lambda\} \subseteq \omega_\lambda$ è cofinale ed isomorfo, come ordine, a λ. ∎

Per esempio $\mathrm{cof}(\aleph_\omega) = \mathrm{cof}(\omega) = \aleph_0$.

Fatto In generale, un cardinale limite potrebbe essere regolare o singolare. Tuttavia, benché sia facile esibire cardinali limiti singolari, gli assiomi di ZFC non implicano l'esistenza di un cardinale limite e regolare — che si chiama, appunto, debolmente inaccessibile. Insomma, non si può dimostrare che tutti i cardinali limite sono singolari — e non c'è una buona ragione per assumere che lo siano — ma sarebbe coerente con gli assiomi della teoria degli insiemi che tutti i cardinali limite fossero singolari.

Prop (formula di Hausdorff)
Siano κ e λ cardinali infiniti, allora

$$(\kappa^+)^\lambda = \kappa^\lambda \cdot \kappa^+$$

Dim Dimostriamo le due disuguaglianze.

($\geq$) Siccome $\kappa^\lambda \cdot \kappa^+ = \max(\kappa^\lambda, \kappa^+)$ basta notare che valgono sia $(\kappa^+)^\lambda \geq \kappa^\lambda$ sia $(\kappa^+)^\lambda \geq \kappa^+$.

($\leq$) Distinguiamo due casi:

- se $\kappa < \lambda$ $\quad (\kappa^+)^\lambda \leq (2^\kappa)^\lambda \leq (\kappa^\lambda)^\lambda = \kappa^\lambda \leq \kappa^\lambda \cdot \kappa^+$
- se $\kappa \geq \lambda$ Sia $S_\alpha = \{f : \lambda \to \alpha\}$ per cui $|S_\alpha| = |\alpha|^\lambda$ e, in particolare, $(\kappa^+)^\lambda = |S_{\kappa^+}|$. Presa una $f \in S_{\kappa^+}$, osserviamo che $|Im(f)| = \lambda < \kappa^+$ Tuttavia κ^+ è regolare, quindi $Im(f)$ non è cofinale in κ^+, e, di conseguenza, esiste un ordinale $\alpha < \kappa^+$

tale che $\forall x \in \lambda \; f(x) < \alpha$, ossia $f \in S_\alpha$.

Abbiamo dunque dimostrato che $S_{\kappa^+} = \bigcup \{ S_\alpha \mid \alpha \in \kappa^+ \}$

Per cui $|S_{\kappa^+}| \leq \sum_{\alpha \in \kappa^+} |S_\alpha| \leq \sum_{\alpha \in \kappa^+} |\alpha|^\lambda \leq \kappa^\lambda \cdot \kappa^+$ ∎

Esercizio Dimostrare che $\aleph_\omega^{\aleph_1} = \beth(\aleph_1) \cdot \beth(\aleph_\omega)$

(* Suggerimento alla pagina successiva)

Fatto La funzione esponenziale κ^λ è determinata ricorsivamente dalle funzioni cof e $\beth$.

Non dimostriamo questo fatto, dimostriamo tuttavia il seguente caso particolare, che basta ad illustrare le tecniche necessarie: la funzione del continuo $\kappa \mapsto 2^\kappa$ è determinata ricorsivamente dalla funzione $\beth$.

Def. Sia κ un cardinale limite. Definiamo

$$2^{<\kappa} \overset{\text{def.}}{=} \sup \{ 2^\lambda \mid \lambda \text{ cardinale } < \kappa \}$$

Lemma Dato κ cardinale limite

$$2^\kappa = \left(2^{<\kappa}\right)^{\text{cof}(\kappa)}$$

Dim. Sia $\lambda = \text{cof}(\kappa)$ e $\{\kappa_i\}_{i \in \lambda}$ tale che $\forall i \in \lambda \; \kappa_i < \kappa$ e $\sum_{i \in \lambda} \kappa_i = \kappa$. Allora

$$2^\kappa = 2^{\sum_{i \in \lambda} \kappa_i} = \prod_{i \in \lambda} 2^{\kappa_i} \leq \prod_{i \in \lambda} 2^{<\kappa} = \left(2^{<\kappa}\right)^\lambda \leq \left(2^\kappa\right)^\lambda = 2^\kappa$$ ∎

Def Sia k un cardinale, diciamo che la funzione $\lambda \mapsto 2^\lambda$ è *definitivamente costante sotto* k se esiste un cardinale $\mu < k$ tale che $\forall \nu$ cardinale $\mu \leq \nu < k \to 2^\nu = 2^\mu$.

Prop. La funzione $k \mapsto 2^k$ è determinata da ∂ come segue:

$$2^k = \begin{cases} \partial(k) & \text{se } k \text{ è successore} \\ & \text{altrimenti:} \\ 2^{<k} \cdot \partial(k) & \text{se } \lambda \mapsto 2^\lambda \text{ è def. costante sotto } k \\ \partial(2^{<k}) & \text{se } \lambda \mapsto 2^\lambda \text{ NON è def. cost. sotto } k \end{cases}$$

Dim Abbiamo già visto il caso successore. Supponiamo che k sia un cardinale limite.

- Caso $\lambda \mapsto 2^\lambda$ definitivamente costante sotto k e k regolare

$$2^{<k} \cdot \partial(k) = 2^{<k} \cdot k^k = 2^{<k} \cdot 2^k = 2^k$$

- Caso $\lambda \mapsto 2^\lambda$ definitivamente costante sotto k e k singolare

Sia μ tale che $\forall \nu$ cardinale $\mu \leq \nu < k \to 2^\nu = 2^\mu = 2^{<k}$

allora

$$2^k = \left(2^{<k}\right)^{\mathrm{cof}(k)} = 2^{\mu \cdot \mathrm{cof}(k)} = 2^\mu = 2^{<k}$$

e si conclude osservando che

$$\partial(k) = k^{\mathrm{cof}(k)} \leq \left(2^k\right)^{\mathrm{cof}(k)} = \left(2^{<k}\right)^{\mathrm{cof}(k)} = 2^{\mu \,\mathrm{cof}(k)} = 2^{<k}$$

---

* Suggerimento per l'esercizio: studiare $\left(\prod_{n \in \omega} \aleph_n\right)^{\aleph_1}$

- Caso $\lambda \mapsto 2^\lambda$ non definitivamente costante sotto κ.

Basta dimostrare che $\mathrm{cof}(2^{<\kappa}) = \mathrm{cof}(\kappa)$, da questo segue

$$2^\kappa = \left(2^{<\kappa}\right)^{\mathrm{cof}(\kappa)} = \left(2^{<\kappa}\right)^{\mathrm{cof}(2^{<\kappa})} = \exists\left(2^{<\kappa}\right)$$

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 $x < 2^\beta$.

Dimostriamo, ora, la disuguaglianza opposta: $\mathrm{cof}(\kappa) \leq \mathrm{cof}(2^{<\kappa})$. Per definizione, dato $\alpha < 2^{<\kappa}$, esiste $\beta < \kappa$ tale che $\alpha < 2^\beta$. Chiamiamo β_α il minimo di questi β. Sia, ora, $A \subseteq 2^{<\kappa}$ un insieme cofinale e definiamo $B = \{\beta_\alpha \mid \alpha \in A\}$. Come al caso precedente $|B| \leq |A|$: 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 $x < \beta_\alpha$.

∎

La gerarchia di Von Neumann & l'assioma di buona fondazione

Insiemi come questi sono (forse?) nostri indesiderabili

$\{\{\{\{\{\dots\}\}\}\}\}$ $\quad x = \{x\}$ $\quad y = \{z\}$ $\quad z = \{y\}$



LEGENDA:
$\rightarrow = \in$

Desideriamo dimostrare, intanto, che, a patto che gli assiomi della teoria degli insiemi non si contraddicano — nel qual caso dimostrerebbero qualunque cosa — essi non dimostrano la esistenza di insiemi del genere.

Strategia: costruiamo un universo insiemistico V_*, che è una classe propria, al cui interno gli assiomi sono veri, e che, tuttavia, non contiene quella robaccia.

Def Costruiamo per ricorsione transfinita

$$V_0 = \emptyset$$
$$V_{s(\alpha)} = \mathcal{P}(V_\alpha)$$
$$V_\lambda = \bigcup \{V_\alpha \mid \alpha < \lambda\} \quad \text{per } \lambda \text{ limite}$$

La classe V_* è l'unione degli insiemi V_α, formalmente:

$$x \in V_* \overset{\text{def.}}{\equiv} \exists \alpha \in Ord \; x \in V_\alpha$$

Lemma $\forall \alpha \in Ord \; V_\alpha$ è transitivo

Dim Per induzione transfinita.

- Caso V_0: immediato poiché $\emptyset$ è transitivo a vuoto.

- Caso successore:

$$x \in V_{s(\alpha)} = \mathcal{P}(V_\alpha) \Rightarrow x \subseteq V_\alpha \Rightarrow \forall y \in x \; y \subseteq V_\alpha \Rightarrow \forall y \in x \; y \in V_{s(\alpha)}$$

($\uparrow$ poiché V_α è transitivo per ipotesi induttiva)

- Caso limite: $x \in V_\lambda \Leftrightarrow x \in V_\alpha$ per qualche $\alpha < \lambda$ ($\downarrow$) $\Rightarrow x \subseteq V_\alpha \subseteq V_\lambda$ ∎

Con V_* è una classe transitiva, ossia $\forall x \in V_* \; x \subseteq V_*$

Lemma $\forall \alpha, \beta \in Ord \quad \alpha \leq \beta \to V_\alpha \subseteq V_\beta$

Dim Dimostriamo per induzione transfinita su β che

$$\forall \alpha < \beta \quad V_\alpha \subseteq V_\beta$$

- Caso $\beta = 0$: vero a vuoto

- Caso successore: dobbiamo dimostrare $\forall \alpha < \beta + 1 \quad V_\alpha \subseteq V_{s(\beta)}$.
Siccome $\alpha < s(\beta) \hookrightarrow \alpha \leq \beta$, applicando l'ipotesi induttiva, abbiamo $V_\alpha \subseteq V_\beta$ — questa conclusione è, infatti, immediata se $\alpha = \beta$.
Per definizione, quindi: $V_\alpha \in V_{s(\beta)} = \mathcal{P}(V_\beta)$. Infine, per la transitività di $V_{s(\beta)}$, $V_\alpha \in V_{s(\beta)}$.

- Caso limite: $\alpha < \lambda \Rightarrow V_\alpha \subseteq \bigcup \{ V_\alpha \mid \alpha < \lambda \} = V_\lambda$ ∎

Lemma $\forall \alpha \in Ord \quad \alpha \subseteq V_\alpha$.

Dim Per induzione transfinita.

- Caso base: $\emptyset \subseteq V_0 = \emptyset$

- Caso successore:

$$\left.\begin{array}{lll} \alpha \subseteq V_\alpha & \Rightarrow & \alpha \subseteq V_{s(\alpha)} \\ \alpha \in \mathcal{P}(V_\alpha) = V_{s(\alpha)} & \Rightarrow & \{\alpha\} \subseteq V_{s(\alpha)} \end{array}\right\} \Rightarrow s(\alpha) = \alpha \cup \{\alpha\} \subseteq V_{s(\alpha)}$$

- 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 Supponiamo di voler relativizzare a V^* la formula

$$\varphi \equiv \exists x \, \forall y \in x \, \exists z \in y \; z \cap x = \emptyset$$

Dobbiamo intanto ridurla al linguaggio della teoria degli insiemi puro, ossia rimuovere tutte le abbreviazioni

$$\exists x \, \forall y \in x \, \exists z \in x \; z \cap x = \emptyset$$

$$\exists x \, \forall y \, (y \in x \to \exists z \, (z \in y \wedge \neg \exists t \; t \in z \cap x))$$

$$\exists x \, \forall y \, (y \in x \to \exists z \, (z \in y \wedge \neg \exists t \; t \in z \cap x))$$

$$\exists x \, \forall y \, (y \in x \to \exists z \, (z \in y \wedge \neg \exists t \; (t \in x \wedge t \in y)))$$

A questo punto rimpiazziamo meccanicamente tutti i quantificatori con quantificatori limitati a V^*

$$\exists x \, \forall y \, (y \in x \to \exists z \, (z \in y \wedge \neg \exists t \; (t \in x \wedge t \in y)))$$

$$\exists x \in V^* \, \forall y \in V^* \, (y \in x \to \exists z \in V^* \, (z \in y \wedge \neg \exists t \in V^* \, (t \in x \wedge t \in y)))$$

Questa nuova formula, φ relativizzata a V^*, come è scritta qua sopra, non è espressa nel linguaggio della teoria degli insiemi puro,

per via dei quantificatori limitati $\forall \square \in V^*$ e $\exists \square \in V^*$, tuttavia, se volessimo, potremmo semplicemente rimpiazzare questi quantificatori con le loro rispettive definizioni.

Teo Valgono gli assiomi della teoria degli insiemi relativizzati a V_*.

Dim

(1) Vuoto: $\exists x \in V_* \ \forall y \in V_* \ y \notin x$

Basta prendere $x = \emptyset \in V_1$

(2) Estensionalità $\forall a, b \in V_* \ a = b \leftrightarrow \forall x \in V_* \ (x \in a \leftrightarrow x \in b)$

Per la transitività dei V_α, dati $a, b \in V_*$, gli elementi di a e b sono anch'essi in V_*, quindi dire $\forall x \in V_* \ (x \in a \leftrightarrow x \in b)$ equivale a dire $\forall x \ (x \in a \leftrightarrow x \in b)$. Si conclude quindi per l'assioma di estensionalità.

(3) Separazione $\forall A \in V_* \ \exists B \in V_* \ \forall x \in V_* \ x \in B \leftrightarrow (x \in A \wedge p(x))$

Per separazione esiste $B = \{x \in A \mid x \in V_* \wedge \varphi(x)\}$. Siccome $B \subseteq A \in V_\alpha$ per qualche α, $B \subseteq V_\alpha$ per transitività, quindi $B \in V_{S(\alpha)}$, quindi $B \in V_*$.

(4) Paio: $\forall a, b \in V_* \ \exists B \in V_* \ \forall x \in V_* \ x \in B \leftrightarrow (x = a \vee x = b)$

Se $a \in V_\alpha$ e $b \in V_\beta$ e, senza perdita di generalità, $\alpha \leq \beta$,

allora $a, b \in V_n$, quindi $\{a, b\} \in \mathcal{P}(V_n) = V_{s(n)}$.

(5) Unione: $\forall A \in V_* \; \exists B \in V_* \; \forall x \in V_* \; x \in B \leftrightarrow \exists y \in A \; x \in y$

Se $A \in V_\alpha$, per la transitività di V_α, $A \subseteq V_\alpha$, e, di nuovo per transitività, $\bigcup A \subseteq V_\alpha$. Quindi $\bigcup A \in V_{s(\alpha)}$.

(6) Parti: $\forall A \in V_* \; \exists B \in V_* \; \forall x \in V_* \; x \in B \leftrightarrow x \subseteq A$

Se $A \in V_\alpha$, $A \subseteq V_\alpha$ per la transitività di V_α, quindi $\mathcal{P}(A) \subseteq \mathcal{P}(V_\alpha) = V_{s(\alpha)}$, quindi $\mathcal{P}(A) \in \mathcal{P}(V_{s(\alpha)}) = V_{\alpha+2}$.

(7) Infinito: $\exists X \in V_* \; \emptyset \in X \wedge \forall y \in V_* \; y \in X \to y \cup \{y\} \in X$

Basta prendere $X = \omega \in V_{s(\omega)}$.

(8) Rimpiazzamento: $F : V_* \to V_*$ funzione classe e $X \in V_* \to F[X] \in V_*$

Se $X \in V_\alpha$, per transitività, $a \in X \to a \in V_\alpha$. Quindi $F(a)$ è ben definito e $\in V_*$ per $a \in X$. Sia α_a minimo con $F(a) \in V_{\alpha_a}$. Sia $\beta = \sup \{\alpha_a \mid a \in X\}$. Allora $F[A] \subseteq V_\beta$, e $F[A] \in V_{s(\beta)}$.

(5) Scelta. $\forall X \in V_* \; (\forall y \in X \; y \neq \emptyset) \to \exists f \in V_* \; f$ di scelta su X.

Sia f una funzione di scelta su $X \in V_\alpha$, dimostriamo che $f \in V_*$. Osserviamo che $f \subseteq \mathcal{P}(\mathcal{P}(X)) \subseteq \mathcal{P}(\mathcal{P}(V_\alpha)) = V_{\alpha+2}$. Quindi $f \in V_{\alpha+3}$.

∎

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 $\alpha < \lambda$. Possiamo quindi dare la definizione seguente

Def Dato $x \in V_*$, detto α il minimo ordinale per cui $x \in V_\alpha$, il rango di x, $\mathrm{rank}(x)$, è definito da $\alpha = \mathrm{rank}(x) + 1$.

Ossia:

$$x \in V_\alpha \iff \mathrm{rank}(x) < \alpha$$

Lemma Se $x \in y \in V_*$ allora $\mathrm{rank}(x) < \mathrm{rank}(y)$.

Dim $y \in V_{s(\mathrm{rank}(y))} = \mathcal{P}(V_{\mathrm{rank}(y)})$, quindi $y \subseteq V_{\mathrm{rank}(y)}$, di conseguenza $x \in V_{\mathrm{rank}(y)}$, per cui $\mathrm{rank}(x) < \mathrm{rank}(y)$. ∎

Def Diciamo che una classe C è ben fondata se per ogni insieme S di elementi di C, S contiene un x minimale per appartenenza ($\in$-minimale), ossia tale che $x \cap S = \emptyset$.
"epsilon-minimale"

Prop 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

$$x_0 \ni x_1 \ni x_2 \ni \dots$$

Dim Se $\{x_i\}_{i \in \omega}$ è una catena infinita discendente, allora $\{x_i \mid i \in \omega\}$ non ha un elemento $\in$-minimale.

D'altro canto, 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 $\bar{x} \in S$

$$x_0 = \bar{x} \qquad x_{n+1} = f(\{y \in S \mid y \in x_n\})$$

dove l'insieme a cui è applicata f non è vuoto, altrimenti x_n sarebbe $\in$-minimale ∎

Una classe transitiva ben fondata non può, quindi, contenere mostri.

Prop La classe V_α è ben fondata

Dim Dato un insieme S di elementi di V_α, consideriamo $x \in S$ di rango minimo. Se esistesse $y \in S$ con $y \in x$ allora avremmo $\mathrm{rank}(y) < \mathrm{rank}(x)$ ↯ ∎

Teo Se gli assiomi della teoria degli insiemi sono coerenti, essi non dimostrano l'esistenza di una catena infinita discendente per appartenenza.

Dim Supponiamo di poter dimostrare che questa catena esiste. Allora, siccome gli assiomi valgono relativizzati a V_α, potremmo svolgere l'intera dimostrazione relativizzata, ed otterremmo che esiste una catena infinita discendente in V_α. D'altro canto abbiamo dimostrato che questa non può esistere. Avremmo quindi la dimostrazione di un assurdo. ∎

A questo punto siamo giustificati, se lo desideriamo, ad assumere che i mostri non esistano. Potremmo, per esempio, fare la cosa codarda ed assumere che la classe di tutti gli insiemi V coincida con V_*

$$V = V_*$$

I codardi, però, non fanno mai le cose troppo apertamente, quindi assumiamo quest'altro enunciato equivalente

(10) Assioma (buona fondazione)
"La classe di tutti gli insiemi è ben fondata."
$\forall S \neq \emptyset \; \exists x \in S \; x \cap S = \emptyset$

Per dimostrare $V = V_*$ usando la buona fondazione, è comodo fare leva sul principio di $\in$-induzione
"epsilon-induzione"

Teo (principio di $\in$-induzione) Se una classe C soddisfa

$$\forall S \; (\forall x \in S \; x \in C) \to S \in C$$

Allora $C = V$, ossia $\forall S \; S \in C$.

La dimostrazione di questo enunciato richiede (10). Prima, però, enunciamo una proposizione che non la richiede.

Prop (esistenza della chiusura transitiva)
Dato un insieme X esiste il più piccolo insieme transitivo $tc(X)$ tale che $X \subseteq tc(X)$.

Dim Costruiamo per ricorsione la successione $\{X_n\}_{n\omega}$

$$X_0 = X \qquad X_{n+1} = \bigcup X_n$$

Si verifica immediatamente che

$$tc(X) = \bigcup \{X_n \mid n\omega\}$$ ☙

Dim (principio di $\in$-induzione)

Prendiamo, 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, $\forall y \in x \; y \in tc(\{S\})$. E' quindi necessario che $\forall y \in x \; y \in C$. Ma allora $x \in C$ e $x \notin S'$ ↯ ☒

Prop $V = V_*$ —— Ossia $\forall x \; \exists \alpha \in Ord \; x \in V_\alpha$.

Dim Per $\in$-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 $S \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$. ☒

Cor Non esistono catene infinite discendenti per appartenenza.

I nostri sono stati sconfitti.

Fine della storia.

Esercizi

- Definiamo $\beth_0 = \aleph_0$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$, $\beth_\lambda = \sup\{\beth_\alpha \mid \alpha < \lambda\}$ con λ limite. Dimostrare che $\forall \alpha \in Ord \; |V_{\omega+\alpha}| = \beth_\alpha$
- Dimostrare che $rank(x) = \sup\{rank(y)+1 \mid y \in x\}$
- Dimostrare che V_ω soddisfa tutti gli assiomi <u>eccetto</u> l'assioma dell'infinito
- Dimostrare che $V_{\omega+\omega}$ soddisfa tutti gli assiomi <u>eccetto</u> l'assioma del rimpiazzamento
- Dimostrare che l'esistenza dell'ordinale $\omega+\omega$ non segue dagli assiomi della teoria degli insiemi <u>escluso</u> il rimpiazzamento, a patto che questi non si contraddicano.
- Dimostrare che, se κ è inaccessibile, allora tutti gli assiomi della teoria degli insiemi valgono in V_κ.
- Dimostrare che, se la teoria degli insiemi è coerente, allora non dimostra l'esistenza di un cardinale inaccessibile.